ISSN 0178-8930
HZ201930

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

4/2019 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, Der externe Datenschutzbeauftragte

HODIS-MAYER, Datenverarbeitung im Beschäftigungsverhältnis zur Aufdeckung von Straftaten

SPITTKA, Si tacuisses ... – nemo tenetur und die DS-GVO

WADA, Annahme des Angemessenheitsbeschlusses durch die EU für Japan

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (42): Weitere Aspekte zur Benennung von Datenschutzbeauftragten

GMEINER, Zur Vorlageberechtigung des (Interdiözesanen) Datenschutzgerichts an den EuGH

Rechtsprechung

Aus dem Inhalt

EUGH, Nationale Gesetzgeber müssen Arbeitgeber zur Arbeitszeiterfassung verpflichten

BVERFG, Zum Anspruch eines Strafgefangenen auf Nutzung eines Computers

BAG, Ordentliche Kündigung eines Chefarztes wegen der Religion

BAG, Unzulässiger Eingriff in das allgemeines Persönlichkeitsrecht der Arbeitnehmer per Betriebsvereinbarung

LSG BERLIN-BRANDENBURG, Anspruch auf Löschung der gespeicherten Kopien eines Personalausweises ohne Passbild

LG KÖLN, Zum Umfang des Auskunftsanspruchs nach § 15 DS-GVO

LG ROSTOCK, Schwärzung von Drittkonten in der Auskunft des Bundeszentralamts für Steuern durch den Gerichtsvollzieher

35. Jahrgang
August 2019
Seiten 155–216

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Prof. Golas neu konzipiertes Datenschutzbuch:

Unverzichtbar für alle, die mit Personaldaten arbeiten.

jetzt bestellen

PRAXISNAH

- **ausführliche Fallbeispiele und konkrete Lösungsansätze**

ETABLIERT

- **8. aktualisierte und erweiterte Neuauflage**

NÜTZLICH

- **ausgewertete Stellungnahmen der Aufsichtsbehörden**

Handbuch Beschäftigtendatenschutz
8. völlig neu bearbeitete Auflage 2019
726 Seiten / Hardcover / € 139,99 inkl. E-Book
ISBN 978-3-89577-801-8

Bestellen Sie direkt unter:
datakontext.com/handbuch

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

35. Jahrgang 2019
Heft 4
Seiten 155–216

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 155

Veranstaltungen 156

Aufsätze

Prof. Peter GOLA
Der externe Datenschutzbeauftragte 157

Radu HODIS-MAYER
Datenverarbeitung im Beschäftigungsverhältnis zur Aufdeckung von Straftaten 164

Jan SPITTKA
Si tacuisses … – nemo tenetur und die DS-GVO 167

Toshihiro WADA
Annahme des Angemessenheitsbeschlusses durch die EU für Japan 172

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (42): Weitere Aspekte zur Benennung von Datenschutzbeauftragten 176

Dipl.-Jur. Robert GMEINER
Zur Vorlageberechtigung des (Interdiözesanen) Datenschutzgerichts an den EuGH 180

Rechtsprechung

Nationale Gesetzgeber müssen Arbeitgeber zur Arbeitszeiterfassung verpflichten
(EuGH, Urteil vom 14.05.2019 – C-55/18 –) 184

Zum Anspruch eines Strafgefangenen auf Nutzung eines Computers
(BverfG, Beschluss vom 27.03.2019 – 2 BvR 2268/18 –) 190

Ordentliche Kündigung eines Chefarztes wegen der Religion
(BAG, Urteil vom 20.02.2019 – 2 AZR 746/14 –) 191

Unzulässiger Eingriff in das allgemeines Persönlichkeitsrecht der Arbeitnehmer per Betriebsvereinbarung
(BAG, Beschluss vom 11.12.2018 – 1 ABR 12/17 –) 204

Anspruch auf Löschung der gespeicherten Kopien eines Personalausweises ohne Passbild
(LSG Berlin-Brandenburg, Urteil vom 30.04.2019 –L 26 AS 2611/17 –) 205

Zum Umfang des Auskunftsanspruchs nach § 15 DS-GVO
(LG Köln, Teilurteil vom 18.03.2019 – 26 O 25/18 –) 207

Schwärzung von Drittkonten in der Auskunft des Bundeszentralamts für Steuern durch den Gerichtsvollzieher
(LG Rostock, Beschluss vom 07.05.2019 – 3 T 66/19 (3) –) 208

Zu den Grenzen des Akteneinsichtsrechts eines Ratsmitglieds (Ls)
(VerwG Düsseldorf, Urteil vom 03.05.2019, 1 K 3063/18 –) 209

Rechtsschutz gegen eine Beanstandung des Landesbeauftragten für Informationsfreiheit (Ls)
(VerwG Stuttgart, Urteil vom 21.02.2019 – 14 K 17293/17 –) 209

Datenschutzrechtliche Zulässigkeit eines Ortungssystems im Beschäftigungskontext (Ls)
(VerwG Lüneburg, Teilurteil vom 19.03.2019 – 4 A 12/19, –) 209

DS-GVO-Vorlagefragen an den EuGH (Ls)
(VerwG Wiesbaden, Beschluss v. 28.03.2019 – Az.: C-272/19 –) 210

Zimmer in einer Gemeinschaftsunterkunft als Wohnung; Durchsuchung; fehlende richterliche Anordnung; Gefahr im Verzug (Ls)
(VerwG Hamburg 9. Kammer, Urteil vom 15.02.2019, 9 K 1669/18 –) 210

Bekanntgabe der Benotung einer Pflicht-Modulprüfung eines Bachelorstudiengangs im online-Portal der Hochschule (Ls)
(VerwG Hamburg, Urteil vom 18.12.2018 – 2 K 1233/18 –) 210

Berichte, Informationen, Sonstiges

Bitkom: Mehrheit wünscht sich digitale Plattformen aus Deutschland 212

Neufassung der Orientierungshilfe „Selbstauskünfte für Mietinteressenten“ 212

Neufassung des „Code of Conduct“der Versicherungswirtschaft 213

Literaturhinweise

Buchbesprechungen

Fritz Schmidt/Harald Schweißguth/ Jan Heiner Hoffmann/David Hummel, Datenschutz in der Wohnungswirtschaft (REDAKTION) 213

Christian Weiß/Nico Reisener, Datenschutz in der Insolvenzkanzlei (REDAKTION) 213

Norbert Pohlmann, Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung (SCHRIFTLEITUNG) 214

Johannes Knaut, Die Bedeutung des Datenschutzrechts bei Beweisverboten in Zivil- und Arbeitsgerichtsbarkeit (REDAKTION) 214

Lutz Bergmann/Roland Möhrle/Armin Herb, Datenschutzrecht: Bundesdatenschutzgesetz – Europäische Datenschutz-Grundverordnung (REDAKTION) 214

Neuerscheinungen
Aufsätze 215

Nachgefasst 216

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

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 4/2019; DATAKONTEXT, Frechen; C.H. Beck

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	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Vertrieb:
Jürgen Weiß
Telefon: (02234) 989 49-71
weiss@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
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf
Telefon: (0221) 25 08-60 71
wolfgang.scharf@agentur-8020.de
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
35. Jahrgang 2019 Heft 4
Seiten 155 – 216

RDV
Recht der Datenverarbeitung

35. Jahrgang · August 2019 · Seiten 155 – 216

Editorial

Aus 10 mach 20 – zur Anhebung der Bestellpflicht von betrieblichen Datenschutzbeauftragten

Auf der Tagesordnung der bis in die Morgenstunden des 27. Juni verlaufenden Marathonsitzung des Bundestags stand u.a. die abschließende Beratung des Entwurfs eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU)2016/679 und zur Umsetzung der Richtlinie (EU)2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpU). Für die Aussprache waren 27 Minuten vorgesehen, die zum Teil für den – nicht angenommenen – Antrag noch verbliebener AfD-Abgeordneter auf Beendigung der Sitzung wegen Beschlussunfähigkeit des Parlaments verbraucht wurden. Die meisten der zur Aussprache angemeldeten Abgeordneten gaben ihre Reden zu Protokoll. Drei Abgeordnete äußerten sich kurz und zwar – trotz der mit dem 2. DSAnpU anstehenden 152 Gesetzesänderungen – im Wesentlichen zu der von der CDU-Fraktion eingebrachten Änderung in § 38 Abs. 1 Satz 1 BDSG das Wort „zehn" durch die Angabe „20" zu ersetzen. (27.06.2019 – BT-Plenarprotokoll 19/107, S. 13295D – 13296A <http://dipbt.bundestag.de:80/dip21/btp/19/19107.pdf#P.13295>). Der Abgeordnete Axel Müller (CDU) begründete dies als „Erleichterung" für „rund 90 Prozent der Handwerksbetriebe und die überwiegende Mehrzahl der Vereine". „Damit erfüllen wir eine Forderung, die nach Einführung der Datenschutz-Grundverordnung vielfach an uns herangetragen wurde. Das zeigt auch, dass dieser Gesetzgeber durchaus in der Lage ist, sich veränderten Bedingungen anzupassen und dafür Sorge zu tragen, dass Auswüchse abgestellt werden."

Anders bewertete der Abgeordnete Dr. Notz (Grüne) das „vermeintliche Geschenk an die Wirtschaft". Vielmehr schade es der Wirtschaft mehr, als es ihr nütze; denn die rechtlichen Pflichten blieben exakt dieselben. Es sei nur niemand mehr zuständig. Das Einzige, was steige, sei die Haftung.

Auch seitens der SPD war zuvor – obwohl sie koalitionstreu die Gesetzesänderung mittrug – zu bedenken gegeben worden, dass nur von einer scheinbaren Entbürokratisierung gesprochen werden könne, da auch unterhalb der Grenze der 20 Beschäftigten die Datenschutzpflichten unvermindert sind und fortgelten. Wichtig sei deshalb hervorzuheben, dass es künftig niemandem verwehrt sei, bereits unterhalb der neuen Schwelle einen betrieblichen Datenschutzbeauftragten zu bestellen. Seitens der FDP wurde eingewandt, das der eigentliche Punkt bei der Bestellung eines Datenschutzbeauftragten nicht getroffen werde. Relevant sei nicht die Frage der Anzahl der Mitarbeiter, sondern die Art der Datenverarbeitung sei entscheidend.

Wie man auch immer zu der Gesetzesänderung steht: Es darf – im Gegensatz zu dem Argument der FDP – nicht übersehen werden, dass die Bestellpflicht bereits nach der DS-GVO auch bei Kleinstbetrieben und Vereinen abhängig von den Zwecken der Verarbeitung und eben auch der Art der verarbeiteten Daten durchaus weiterhin besteht (Art. 37 Abs. 1 Nr. 2 und 3 DS-GVO). Und selbstverständlich bleibt – mit oder ohne DSB – die Durchführungsverantwortung sowieso bei dem Handwerker oder Vereinsvorstand. Es steht ihm aber nunmehr frei zu entscheiden, ob er dazu Hilfe benötigt.

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.

Termin	Thema	Ort	Kontakt
10.09.2019	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Stuttgart	GDD e.V. und DATAKONTEXT
09.-13.09.2019	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
16.09.2019	Planung und Umsetzung der Überwachungsaufgabe des DSB	Köln	GDD e.V. und DATAKONTEXT
16.09.2019	Datenschutz und Betriebsrat unter der DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
17.09.2019	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
19.09.2019	Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO	Düsseldorf	GDD e.V. und DATAKONTEXT
23.09.2019	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	Köln	GDD e.V. und DATAKONTEXT
24.09.2019	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG 2018	Köln	GDD e.V. und DATAKONTEXT
26.09.2019	Big Data-Analysen nach DS-GVO und BDSG 2018	Köln	GDD e.V. und DATAKONTEXT
30.09.2019	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT
08.10.2019	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
08.10.2019	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
07.-09.10.2019	Einführung in den technisch-organisatorischen Daten-schutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
08.-09.10.2019	Workshop zur DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
15.10.2019	Compliance Tests und Schwachstellenscannen	Köln	GDD e.V. und DATAKONTEXT
17.10.2019	DS-GVO-konforme Prüfung personenbezogener Daten mit SAP-Systemen	Berlin	GDD e.V. und DATAKONTEXT
21.10.2019	Teleworking unter Beachtung von Datenschutz und Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
22.10.2019	Die Aufgaben und der Tätigkeitsbericht des DSB praxisnah im Unternehmen	Berlin	GDD e.V. und DATAKONTEXT
22.10.2019	Datenschutz in medizinischen Einrichtungen	Köln	GDD e.V. und DATAKONTEXT
23.10.2019	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
28.10.2019	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Köln	GDD e.V. und DATAKONTEXT
28.-29.10.2019	Neues Datenschutzrecht kompakt	Frankfurt/M.	GDD e.V. und DATAKONTEXT
30.10.2019	Verzeichnis von Verarbeitungstätigkeiten	Berlin	GDD e.V. und DATAKONTEXT
04.11.2019	Basiswissen IT-Sicherheit	Berlin	GDD e.V. und DATAKONTEXT
04.-05.11.2019	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT

DATAKONTEXT GmbH, Telefon: 0 22 34/9 89 49 40

Aufsätze

Prof. Peter Gola

Der externe Datenschutzbeauftragte

Behörden und private Stellen können bei der Erfüllung ihrer Pflicht zur Benennung eines Datenschutzbeauftragten die Aufgabe einem ihrer Beschäftigten oder einem externen Dienstleister übertragen (Art. 37 Abs. 6 DS-GVO; für Bundesbehörden wiederholend und relevant für vom Geltungsbereich der JI-RL erfasste Behörden in § 5 Abs. 8 BDSG). Der Beitrag zeigt auf, welche Kriterien öffentliche oder private Verantwortliche bei der Benennung externer Beauftragter zu beachten haben und inwieweit Unterschiede zu internen Datenschutzbeauftragten bestehen.

Vorbemerkung

Die durch Art. 37 Abs. 6 DS-GVO weiterhin[1] eröffnete Möglichkeit der Benennung eines externen Datenschutzbeauftragten kann insbesondere bei kleineren Unternehmen und Behörden sinnvoll sein, wenn diese keine eigenen für die Übernahme der Funktion geeignete Mitarbeiter haben und bei denen u.a. auf Grund des Umfangs der anfallenden Tätigkeit nur eine Teilzeitaufgabe anfällt, für deren Wahrnehmung das Eingehen eines Arbeitsverhältnis u.a. aus Kostengründen[2] nicht sinnvoll erscheint. Zudem ist zwar auch der externe Beauftragte in seiner Rechtsposition durch den Abberufungsschutz aus Art. 38 Abs. 3 S. 2 DS-GVO geschützt, nicht aber durch den nur dem im Arbeitsverhältnis beschäftigten DSB zustehenden Kündigungsschutz (§ 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG), so dass eine Beendigung seiner Tätigkeit um einiges leichter ist als bei einem internen DSB. Für eine Entscheidung zugunsten eines externen Datenschutzbeauftragten spricht ferner, dass dessen Expertise und Erfahrungen sofort in Anspruch genommen werden können und der initiale Aufwand für die Ausbildung eines eigenen Mitarbeiters zum Datenschutzbeauftragten entfällt. Vorteile des internen Datenschutzbeauftragten sind demgegenüber die regelmäßig bessere Kenntnis der Prozesse und Spezifika der benennenden Stelle. Der Beauftragte kann seinen Aufgaben in der Regel nur dann umfassend nachkommen, wenn er sich möglichst nahe am Ort des Geschehens befindet und nicht nur nachträglich kontrolliert, sondern kontinuierlich berät und bereits bei der Planung und Vorbereitung von Datenverarbeitungsvorhaben dahingehend mitwirkt, dass dem Datenschutz frühzeitig Rechnung getragen wird. Die erforderliche Nähe zu dem Unternehmen oder der Behörde geht ggf. auch nicht verloren, wenn gleichen Tätigkeiten nachgehende Stellen einen gemeinsamen Datenschutzbeauftragten bestellen.

Als externer Datenschutzbeauftragter fungiert auch der Konzerndatenschutzbeauftragte (Art. 37 Abs. DS-GVO) und zwar bei all denjenigen Konzernunternehmen, für die er zwar benannt, bei denen er jedoch nicht beschäftigt ist. Gleiches gilt ggf. für einen für mehrere Behörden gemeinsam bestellten Beauftragten (Art. 37 Abs. DS-GVO). Für Behörden gilt seit dem 25.5.2018 zudem, dass diese nicht nur einem Bediensteten einer anderen öffentlichen Stelle, sondern auch einem privaten Dienstleister die DSB-Funktion übertragen können.

I. Der Dienstleitungsvertrag des externen Beauftragten

1. Ein Dienstleistungsvertrag als Basis der Benennung

Die Basis der Tätigkeit externer Datenschutzbeauftrage bildet ein, zwecks Erfüllung der diesbezüglichen Dokumentationspflicht, schriftlich zu schließender Dienstleistungs- bzw. Geschäftsbesorgungsvertrags,[3] mit oder neben dem ein an sich einseitig ergehender Bestellungsakt verbunden ist.[4] Mindestinhalt dieses Vertrages müssen neben den im Einzelnen hinsichtlich Zeitumfang und Häufigkeit aufzulistenden Leistungen Aussagen sein[5] zu der Abwicklung der Arbeit bzw. organisatorischen Eingliederung, dem Einsatz von Hilfspersonal, der Unabhängigkeit, der Vergütung und einem Aufwendungsersatz, der Haftung, der Schweigepflicht und der Laufzeit und Beendigung.

1 Vgl. zuvor zur Regelung des § 4 f Abs. 2 S. 4 BDSG a.F. bei Gola/Schomerus, BDSG, 12. Aufl. § 4 f Rn. 171.

2 Wie aus entsprechenden Offerten im Internet ersehbar, bieten externe DSB ihre Leistungen schon mit Monatshonoraren von 50 € an.

3 Drews, in: Simitis/Hornung/Spieker, Datenschutzrecht, 1. Aufl. DS-GVO Art. 37 Rn. 52; vgl. im Einzelnen auch bei Kremer/Sander, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl., S. 96 f.

4 Vgl. z.B. das Vertragsmuster der ER Secure GmbH: https://www.er-secure.de/v/sachsen.pdf.

5 Vgl. den Mustervertrag bei Kremer/Sander, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl., S. 91 ff.

2. Der externe DSB als „datenschutzrechtlicher" Teil der verantwortlichen Stelle

Nimmt der externe Datenschutzbeauftragte im Rahmen seiner Kontrollfunktion sein Recht auf Zugang zu den in der verantwortlichen Stelle gespeicherten personenbezogen Daten wahr (Art. 38 Abs. 2DS-GVO), handelt es sich nicht um eine – wenn auch erlaubte – Datenweitergabe an einen anderen Verantwortlichen oder einen Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO)[6]. Vielmehr wird auch der externe Beauftragte auf Grund der gesetzlichen geregelten Stellung als Teil der verantwortlichen Stelle tätig. Gleiches gilt, wenn sich Betroffene an den Beauftragten wenden (Art. 38 Abs. 4 DS-GVO) und der DSB den Vorgang speichert.[7] Diesem Tatbestand hat der mit ihm abzuschließende Vertrag Rechnung zu tragen.

3. Mitbestimmung

Die Entscheidung, die Funktion des Datenschutzbeauftragten mit einem Arbeitnehmer oder einem externen Dienstleister zu besetzen, liegt in der Organisationshoheit des Arbeitgebers. Entscheidet er ich für die externe Besetzung, scheidet ein Mitbestimmungsrecht aus. Auch wenn der externe Datenschutzbeauftragte datenschutzrechtlich Teil der ihn benennenden Stelle ist,[8] ist das arbeitsrechtlich nicht der Fall, d.h. mangels Arbeitnehmereigenschaft bestehen Mitbestimmungsrechte bei der Bestellung[9] regelmäßig nicht, es sei – so das LAG Frankfurt[10] – dass doch eine Eingliederung des DSB in das betriebliche Geschehen erfolgt, was dadurch zum Ausdruck kommen kann, dass das Unternehmen dem DSB einen Büroraum zur Verfügung stellt. In einigen Bundesländern ist dagegen Mitbestimmung klar geregelt,[11] indem ihre Personalvertretungsgesetze generell Mitbestimmung bei der Bestellung eines behördlichen DSB einräumen, d.h. also unabhängig davon, ob es sich um einen Bediensteten oder einen externen Beauftragten handelt.

II. Gemeinsame Datenschutzbeauftragte

1. Allgemeines

Die DS-GVO gestattet sowohl mehreren privaten als auch öffentlichen Stellen, einen für sie tätigen „gemeinsamen" Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 2 und 3 DS-GVO). Handelt es sich hierbei um einen bei einer der Stellen beschäftigten Bediensteten, ist dieser hier interner und bei den anderen Stellen externer Datenschutzbeauftragter.

2. Gemeinsamer Datenschutzbeauftragter bei Unternehmensgruppen

a) Der Bestellvorgang

Die DS-GVO gestattet Unternehmensgruppen (Art. 4 Nr. 10 DS-GVO) in Artikel 37 Abs. 2 die Benennung eines gemeinsamen Datenschutzbeauftragten, vorausgesetzt, dieser ist aus allen Niederlassungen leicht erreichbar. Eine Unternehmensgruppe ist in Art. 4 Ziffer 16 DS GVO dahingehend definiert, dass sie aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Diese Definition entspricht der des Konzerns in § 18 AktG. Die Bestellung wird dann – auch wenn Art. 35 Abs. 1 DS GVO den für die Verarbeitung Verantwortlichen als „Besteller" vorsieht – von dem herrschenden Unternehmen zu erfolgen haben. In Betracht kommt aber auch das Unternehmen, mit dem der Beauftragte einen Arbeits- oder Dienstvertrag hat. In jedem Falle kann ein Konzern nunmehr für alle konzernangehörigen Unternehmen verpflichtende oder freiwillige Benennungen in einem Akt vornehmen.[12] Die Benennung derselben Person für alle Konzerngesellschaften bietet vor allem den Vorteil, dass eine einheitliche Behandlung von Datenschutzfragen konzernweit gewährleistet ist.

b) Die leichte Erreichbarkeit

Die DS-GVO zieht mit der in Art. 7 Abs. 2 DS-GVO geforderten leichten Erreichbarkeit des DSB eine bisher nicht bekannte tatsächliche Grenze für die Benennung von Konzerndatenschutzbeauftragten.

Der Begriff der Erreichbarkeit bezieht sich dabei auf die Wahrnehmung der Aufgaben des Datenschutzbeauftragten als Ansprechpartner für Betroffene (Artikel 38 Abs. 4 DS-GVO) und die Aufsichtsbehörde (Art. 39 Abs. 1 lit. e DS-GVO), gilt aber auch für dessen Aufgaben als einrichtungsinterner Ansprechpartner (Art. 39 Abs.1 lit. a DS-GVO).[13]

Die leichte Erreichbarkeit erfordert zunächst, dass mit dem Datenschutzbeauftragten nicht nur per Telefon oder über andere gesicherte Kommunikationskanäle, sondern nötigenfalls auch persönlich Kontakt aufgenommen werden kann, indem er in der Niederlassung regelmäßig oder fallbezogen anwesend ist[14] oder er unter zumutbarem Aufwand von der Niederlassung aus aufgesucht werden kann.[15] Ob insoweit eine Tagesreise für Hin- und Rückfahrt noch akzeptabel ist, mag dahinstehen.[16]

6 Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 37 Rn. 42

7 vgl. aber auch Kremer/Sander, in: Koreng/Lachenmann, Formularbuch Datenschutzrecht, 2. Aufl., S. 98, die den externen DSB als Verantwortlichen einordnen.

8 Bergt, in: Kühling/Buchner, DSGVO/BDSG, 2. Aufl., DS-GVO Art. 37 Rn. 36, 51.

9 Zur Situation bei internen Datenschutzbeauftragten, vgl. Gola, in: Gola/Heckmann, BDSG § 5 Rn. 11.

10 LAG Frankfurt, Beschl. v. 28. 8. 1989.

11 Vgl. § 66 Nr. 6 BBgPersVG; § 71 Abs. 3 Nr. 1b BWLPVG; § 72 Abs. 4; Nr. 6 NWPVG; § 67 Abs. 1 Nr. 6 NPersV; § 80 Abs. 2 Nr. 8 RPLPVG.

12 Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., DS-GVO Art. 37 Rn. 27; Klug, in: Gola, DS-GVO, 2. Aufl., Art. 37 Rn. 17; Paal, in: Paal/Pauly, DS-GVO 2. Aufl., Art. 37 Rn. 10; Maier/Hosseini, in: Roßnagel, Europäische Datenschutz-Grundverordnung, S. 210; Gierschmann, ZD 2016, 51 (52); Marschall/Müller, ZD 2016, 415 (416); wohl auch Heberlein, in: Ehmann/Selmayr, GS-GVO, 2. Aufl. Art. 37 Rn. 29; Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 195.

13 Art.-29-Datenschutzgruppe WP 243 rev. 01, S. 12.

14 Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. DS-GVO Art. 37 Rn. 28.

15 Jaspers/Reif, in: Heidelberger Kommentar, DS-GVO Art. 37 Rn. 12.

16 So jedenfalls Jaspers/Reif, in: Heldelbeger Kommentar, DS-GVO Art. 37, Rn. 39; Paal, in: Paal/Pauly, GS-GVO, 2. Aufl., Art. 37 Rn. 10.

Leichte Erreichbarkeit setzt in internationalen Konzernen die – ggf. unter Einsatz von Hilfspersonal[17] – bestehende Möglichkeit der sprachlichen Verständigung voraus.[18] Der Verweis auf die Arbeitssprache des Konzerns ist nicht ausreichend; maßgebend ist die Landessprache.[19]

Die leichte Erreichbarkeit bedingt zudem die Kommunikation, auf welchem Wege der Datenschutzbeauftragte erreicht werden kann, die ggf. mehr umfassen muss, als die in Art. 37 Abs. 7 DS-GVO vorgeschriebene Mitteilung der Kontaktdaten und z.B. Sprechzeiten in den Niederlassungen oder die Veröffentlichung der Kontaktdaten des Hilfspersonals im Intranet beinhalten kann.[20]

3. Gemeinsame Datenschutzbeauftragte mehrerer Behörden

a) Die Erlaubnisnorm

Nach Art. 37 Abs. 3 DS-GVO und Art. 32 Abs. 3 JI-RL und den die JI-RL umsetzenden nationalstaatlichen Normen (vgl. § 5 Abs. 2 BDSG, § 5 Abs. 2 HDSIG, § 37 Abs. 2 RhPflDSG) kann von mehreren öffentlichen Einrichtungen und Stellen in Anbetracht ihrer Organisationsstruktur und Größe ein gemeinsamer DSB benannt werden. Das Verfahren wird durch die Verwaltungsorganisation bestimmt. So kann beispielsweise bei einer Ober- oder Mittelbehörde ein Datenschutzbeauftragter benannt werden, der gleichzeitig auch die DSB-Funktion für die nachgeordneten Behörden wahrnimmt.[21] Für kleinere Kommunen kann sich aufgrund ihrer personellen und organisatorischen Strukturen bei der Benennung eines eigenen Beschäftigten die Gefahr einer möglichen Interessenkollision mit den sonstigen Aufgaben (sog. „Linienaufgaben") dieser Person ergeben.[22] Daher mag insoweit angezeigt sein, dass mehrere kleinere Kommunen oder Schulen einen gemeinsamen (Vollzeit)-Datenschutzbeauftragten benennen. Das ULD Schleswig Holstein[23] weist dazu darauf hin, dass der Datenschutzbeauftragte bei allen Stellen, für die er benannt ist, die Aufgaben auch zeitlich wahrnehmen können muss. Dies sei nicht mehr der Fall, wenn die Zeitanteile für eine benennende Stelle so gering werden, dass eine ernsthafte Wahrnehmung der Aufgaben nicht mehr erwartet werden kann. So wären z.B. die Benennung eines gemeinsamen Datenschutzbeauftragten für einen Kreis und sämtliche kreisangehörigen Ämter nicht mehr von der Privilegierung nach Art. 37 Abs. 3 DSGVO erfasst. Ebenso könnte etwa die Benennung eines gemeinsamen Datenschutzbeauftragten für mehrere kreisfreie Städte oder Kreise nicht auf Art. 37 Abs. 3 DSG-VO gestützt werden, es sei denn, dass es nach den Gegebenheiten genügt, wenn ihm ein Team zur Unterstützung bereitgestellt wird.[24]

Im Gegensatz zu „gemeinsamen betrieblichen Beauftragten" (Art. 37 DS-GVO) fordert der Wortlaut des Art. 37 nicht eine leichte Erreichbarkeit des gemeinsamen behördlichen DSB, dies vielleicht deshalb, weil hier das Problem regelmäßig nicht auftreten wird. Gleichwohl ist sie aber unter dem Gesichtspunkt der Organisationsstruktur zu berücksichtigen.[25]

b) Durchführung der Benennung

Bei der Benennung eines gemeinsamen behördlichen Datenschutzbeauftragten stellen sich Fragen des Vollzugs dieses Vorgangs. Dabei geht es einmal darum, ob trotz der Zuständigkeit des Beauftragten für mehrere Behörden ein einseitiger Benennungsakt genügt, und zum anderen darum, dass dieser einseitige Akt arbeits- bzw. dienstrechtlich mit dem Beschäftigungsverhältnis kompatibel sein muss.

Dazu ist festzuhalten, dass die Benennung kein Beschäftigungsverhältnis begründet, sondern ein solches als Grundverhältnis voraussetzt,[26] sei es dass es bereits besteht oder dass es parallel mit der Benennung begründet oder abgeändert wird und der benannte Datenschutzbeauftragte auf Grund der Pflichten aus dem Arbeitsvertrag,[27] des beamtenrechtlich übertragenen Amts oder eines Dienstleistungsvertrag zur Übernahme der Tätigkeit verpflichtet ist.[28] Ansonsten müsste eine freiwillige Übernahme der Aufgabe, also die Zustimmung zur Ernennung vorliegen. Des Weiteren muss die Stelle, die die Benennung durchführt, gegenüber den Behörden, für die der Datenschutzbeauftragte tätig werden soll, organisationsbefugt sein. Voraussetzung dafür ist die Zu- bzw. eine Übereinstimmung zwischen den Stellen, für die der DSB zuständig sein soll, es sei denn, dass eine übergeordnete Stelle die Entscheidungsbefugnis hat oder an sich zieht.

Liegt also der Fall vor, dass eine Ober- oder Mittelbehörde im Rahmen ihrer Kompetenz einen auch für die nachgeordneten Behörden zuständigen Datenschutzbeauftragten benennt, so ist die Benennung wirksam, wenn der Benannte auch arbeits-/dienstrechtlich die Aufgabe übernehmen

17 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 196.

18 Heberlein, in: Ehmann/Sedlmayr, DS-GVO, 2. Aufl. Art. 37 Rn. 30; Paal, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. DS-GVO Art. 37 Rn. 10; Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. DS-GVO Art. 37 Rn. 29; Bittner, RDV 2014, 183 (184).

19 BayLDA, Hinweise zur Umsetzung der DS-GVO, Kurzpapier XIX, Stand: 02.05.2017; Datenschutzkonferenz Kurzpapier Nr. 12 (Stand: 16.1.2018), S. 2.

20 Jaspers/Reif, in: Heidelberger Kommentar, DS-GVO Art. 37 Rn 68; Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 196.

21 Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 37 Rn. 31.

22 NdsLSB, Benennung von gemeinsamen DSB im öffentlichen Bereich – https://lfd.niedersachsen.de/download/133910/Benennung_von_gemeinsa.

23 ULD Schleswig-Holstein, Praxisreihe: Datenschutzbestimmungen praktisch umsetzen; Band 2: Datenschutzbeauftragte, Ziff. 2.8; https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2 Abschnitt 2.2.

24 LfDI Baden-Württemberg, Praxisratgeber, Die/Der Beauftragte für den Datenschutz – Teil II: Persönliche Voraussetzungen, Durchführung der Benennung, Stellung und Aufgaben, Beendigung der Benennung, 2018, S. 17; https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/20.

25 Vgl. auch Jaksch/van Daake, DuD 2018, 758.

26 Heberlein, in: Ehmann/Selmayr, DS-GVO 2. Aufl., 2018, Art. 37 Rn. 14.

27 Nach dem ULD Schleswig-Holstein, https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2-datenschutzbeauftragte.pdf ist eine Einstufung unterhalb E 11/A 12 nicht angemessen.

28 BAG, Urt. v. 13.03.2007 – 9 AZR 612/05 sowie Urt. v. 29.09.2010 – 10 AZR 588/09; zur Wertigkeit der Funktion: https://www.lfd.niedersachsen.de/download/120512/Aufgaben_DSB.pdf.

muss. In Bayern ist eine entsprechende Kompetenzzuweisung in Art. 12 Abs. 3 BayDSG erfolgt, der staatlichen Behörden gestattet, die Bestellung des Datenschutzbeauftragten durch eine höhere Behörde vorzunehmen.

Soll ein gemeinsamer Datenschutzbeauftragter für mehrere Kommunen benannt werden, so ist der Arbeitgeber/Dienstherr der zu Benennenden zu einer diesbezüglichen einheitlichen Benennung nur berechtigt, wenn alle betroffenen Kommunen hiermit einverstanden sind und die Befugnis delegiert haben. Gleiches gilt – abhängig von der Schulorganisation des Landes – für Schulen, indem ggf. jeder betroffene Schulleiter der Beauftragung zustimmen muss.[29]

III. Juristische Person als externer Datenschutzbeauftragter?

Die DS-GVO lässt es offen, ob der Datenschutzbeauftragte nur eine natürliche Person sein kann oder ob einer juristischen Person als externer Dienstleister die Aufgabe übertragen werden kann.[30] Die Formulierungen der Art. 37 f. DS-GVO können jedoch dahingehend interpretiert werden, dass die Funktion des Datenschutzbeauftragten nur von einer natürlichen Person wahrgenommen werden kann.[31] Die Aufsichtsbehörden bejahten dies bereits im Hinblick auf die Regelungen des BDSG aF[32] und halten auch mehrheitlich an dieser Auffassung fest.[33] Diese Meinung wird in der Literatur wohl weitgehen geteilt,[34] wobei zumindest im Hinblick auf das drohende Bußgeldszenario geraten wird, dass „besser eine natürliche Person benannt werden" sollte.[35]

Die Aufsichtsbehörden dokumentieren ihre Auffassung mehrheitlich auch u.a. dadurch, dass sie nur die Meldung natürlicher Personen in ihrem Online-Meldeverfahren ermöglichen.[36] Andererseits sieht das Meldeformular des Hessischen Landesdatenschutzbeauftragten auch die Meldung juristischer Personen vor, wobei gleichzeitig die dortige „Kontaktperson" anzugeben ist.[37] Dies mag der Auffassung der BfDI entsprechen. Die BfDI[38] macht gegenüber der Meinung, dass auch eine juristische Person ein externer DSB sein kann, zutreffend geltend, dass es auch dann nach der DS-GVO einer (natürlichen) Person bedarf, die innerhalb dieser Organisation Funktionen des Datenschutzbeauftragten wahrnimmt und dabei sämtliche Voraussetzungen für die Benennung als Datenschutzbeauftragter erfüllt. Nur insoweit bestehen keine Bedenken, einen oder kumulativ mehrere qualifizierte Angehörige, einer juristischen Person namentlich und verantwortlich zum Datenschutzbeauftragten zu benennen, wobei der entsprechende Geschäftsbesorgungsvertrag mit dem Beratungsunternehmen etc. abgeschlossen wird, das den zu benennenden Mitarbeiter stellt. Wohl auch der europäische Datenschutzausschuss (EDSA)[39] geht in Auslegung von Art. 37 Abs. 6 DSGVO von diesem Konzept aus, so dass der Verantwortliche oder Auftragsverarbeiter mit einem Dritten (natürliche oder juristische Person) einen Dienstleistungsvertrag schließen kann, nach dem eine natürliche Person allein oder mehrere Personen als „Team", d.h. als kumulativ benannte Datenschutzbeauftragte die „Funktion des Datenschutzbeauftragten" übernehmen sollen.[40] Dabei muss die erforderliche Weisungsfreiheit des/der DSB aber auch gegenüber dem sie abstellenden Dienstleister gewährleistet sein.

Ansonsten ist die Benennung juristischer Personen als Datenschutzbeauftragte unzulässig,[41] da Wortlaut und Systematik der DS-GVO nur natürliche Personen als Datenschutzbeauftragte vorsehen. Dies macht u.a. Artikel 37 Absatz 5 DS-GVO deutlich, nach dem Datenschutzbeauftragte auf Grundlage ihrer beruflichen Qualifikation und ihres Fachwissens benannt werden. Nur natürliche Personen können die nötige „berufliche" Fachkunde und Zuverlässigkeit aufweisen, und nur zu diesen ist eine vertrauliche Beziehung der Beteiligten möglich.[42] Für diese einzelnen natürlichen Personen dürfen keine Interessenkonflikte bei der Wahrnehmung von Aufgaben für einen Verantwortlichen oder Auftragsverarbeiter bestehen. Weiterhin spricht auch die Zubilligung eines Zeugnisverweigerungsrechts gegenüber dem Datenschutzbeauftragten unter den Voraussetzungen des § 38 Abs. 2 BDSG n. F. i.V.m. § 6 Abs. 6 BDSG n. F. für diese Auffassung.

29 Https://www.landesschulbehoerde-niedersachsen.de/themen/schulorganisation.

30 Vgl. zur Problematik Bergt, in: Kühling/Buchner, DSGVO/BDSG, 2. Aufl., DS-GVO Art. 37 Rn. 36; Gola, RDV 2018, 257; wohl auch zutreffend ablehnend Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 37 Rn. 43; Stutz, in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, Teil B Rn. 34.

31 So z.B. Heberlein, Juris 1/2019, S. 19.

32 ULD Schleswig-Holstein, Praxisreihe: Datenschutzbestimmungen, Ziff. 2.8; https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2 Abschnitt 2.2.

33 LfDI NRW, Häufig gestellte Fragen zu Datenschutzbeauftragten (FAQ), Stand: 11/2018, S. 11 = https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte; LfDI Baden-Württemberg, Praxisratgeber Die/Der Beauftragte für den Datenschutz-Teil II: Persönliche Voraussetzungen, Durchführung der Benennung, Stellung und Aufgaben, Beendigung der Benennung, 1 Aufl. 2018, S. 5.

34 Heberlein, in: Ehmann/Sedlmayr, DSGVO/BDSG, 2. Aufl., DS-GVO Art. 37 Rn. 43; Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 197.

35 Bergt, in: Kühling/Buchner, DSGVO/BDSG, 2. Aufl., DS-GVO Art.37 Rn. 36.

36 Berlin: https://www.datenschutz-Berlin.de/meldeformular/; Brandenburg: https://www.Ida.brandenburg.de/cms/detail.php/bb1.c.233960.de/bbo_contact; Saarland: https://datenschutz.saarland.de/online-services/meldeformular-datenschutzbeauftragter/; Sachsen-Anhalt: https://datenschutz.sachsen-anhalt.de/service/online-formulare-des-landesbeauftragten/datenschutzbeauftragten-melden/?no_cache=1.

37 Https://datenschutz.hessen.de/datenschutz/datenschutzbeauftragte/me.

38 26. TB (2015/2016), Ziff. 1.6.

39 EDSA WP 243 rev. 01. S. 27; vgl. bei Baumgartner/Hansch, ZD 2019, 99 (102).

40 So auch ULD Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2-datenschutzbeauftragte.pdf.

41 LfDI NRW, Häufig gestellte Fragen zu Datenschutzbeauftragten (FAQ); https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte.; a.A. Baumgartner/Hansch, ZD 2019, 99 (102), die der juristischen Person die Fachkunde des Mitarbeiters zurechnen wollen, ebenso Sörup/Batmann, ZD 2018, 553.

42 So auch BayLDSB, Orientierungshilfe Ziff. II 3 ahttps://www.datenschutz-bayern.de/technik/orient/behDSB.htm.

IV. Inkompatibilitäten bei Benennung externer Datenschutzbeauftragter

1. Allgemeines

Art. 37 Abs. 6 DS-GVO gestattet dem Datenschutzbeauftragten, auch andere Aufgaben und Pflichten wahrzunehmen, wobei die den DSB benennende Stelle sicherstellen muss, dass sich hieraus nicht Interessenkonflikte ergeben. Diese Regelung gilt auch für externe Datenschutzbeauftragte,[43] bedarf jedoch sinngemäßer Interpretation. Sie bedeutet zunächst, dass der externe DSB diese Aufgabe bei mehreren Verantwortlichen wahrnehmen kann und dass der ihn beauftragende Verantwortlichen ihm auch andere Funktionen übertragen kann. Im letztgenannten Fall liegt es dann eindeutig in der Hand des Verantwortlichen, hierbei möglicherweise entstehende Interessenkonflikte auszuschließen. Im erstgenannten Fall hat die benennende Stelle keine „Sicherstellungsmöglichkeiten" außer dem Verlangen einer diesbezüglichen vertraglichen Verpflichtung.[44] Die Regelung des Art. 37 Abs. 6 2. Hs DS-GVO enthält damit nicht nur eine Organisationspflicht, sondern auch eine Benennungsvoraussetzung eines externen Datenschutzbeauftragten.[45] Dies allein schon deswegen, weil es bei der Benennung externer Datenschutzbeauftragter eben auch um Interessenkonflikte geht, die nicht die benennende Stelle, sondern nur der externe Dienstleister lösen kann. Ist er hierzu nicht in der Lage, muss seine Benennung unterbleiben, bzw. es bedarf zwingend der Abberufung und der Kündigung oder bei entsprechender diesbezüglicher Täuschung der Anfechtung des Dienstleistungsvertrags. Bestehende Interessenkonflikte führen nämlich nicht zur Unwirksamkeit der Bestellung, sondern zur Pflicht des Verantwortlichen, diese zu beseitigen. Die Aufsichtsbehörde kann von dem Verantwortlichen, der Privatwirtschaft die Abberufung eines Datenschutzbeauftragten bei Vorliegen eines Interessenkonflikts verlangen (§ 40 Abs. 6 S. 2 BDSG), wobei generell ein „hinweisartiges" Einschreiten bei Behörden auch schon nach Art. 58 lit. DS-GVO angezeigt ist.

2. Beispiele

Auch bei dem externen Datenschutzbeauftragten gilt. dass er in Erfüllung seiner Aufgaben nach Art. 39 DS-GVO nicht die Ergebnisse seiner in anderer Funktion ausgeübten Arbeit kontrollieren kann.[46]

Einem externen Dienstleister kann z.B. nicht die Aufgabe des DSB übertragen werden, wenn er bereits für den Verantwortlichen als Wirtschaftsprüfer oder Steuerberater tätig ist,[47] da er insoweit zur Wahrnehmung von Mandanteninteressen verpflichtet ist.[48] Gleiches gilt, wenn er bereits als externer Dienstleister das IT-Sicherheitskonzept des Unternehmens entwickelt hat und betreut.[49]

Konflikte können auch auftreten, wenn der Beauftragte auch Datenschutzbeauftragter bei Auftragsverarbeitern der benennenden Stelle ist. Der DSB kann sich vor die Frage gestellt sehen, ob er bei dem Auftragnehmer festgestellte Unregelmäßigkeiten dem Auftraggeber mitzuteilen darf bzw. muss. Um hier nicht gegen die Treuepflicht gegenüber dem einen oder anderen „Besteller" zu verstoßen, sollte die Problematik in dem Bestellschreiben geklärt werden.

Das gilt auch für gemeinsam benannte Beauftragte eines Konzerns (Art. 37 Abs. 2 DS-GVO). Auch wenn theoretisch in der Praxis in Konzernunternehmen die Interessen gleichlaufen sollten, können ggf. gleichwohl Interessenkonflikte auftreten.

Auch Verwandtschaftsbeziehungen mit dem Inhaber oder dem Geschäftsführer des Unternehmens bzw. dem Leiter der Behörde sind kritisch zu prüfen.[50]

3. Wahrnehmung der DSB-Funktion durch Rechtsanwälte

a) Die Doppelte Problematik

Die Frage, ob ein Rechtsanwalt als Datenschutzbeauftragter tätig werden kann, stellt sich unter zwei Aspekten. Und zwar zum einen, ob ein Arbeitnehmer parallel zur Tätigkeit als interner oder auch externer DSB oder auch Syndikus Anwalt seines Arbeitgebers sein kann und zum anderen, ob er als selbstständiger Rechtsanwalt neben der Tätigkeit als externer DSB für seinen Auftraggeber generell oder nur in Sachen Datenschutz nicht als Anwalt tätig werden darf.[51] Keine berufs- oder datenschutzrechtlichen Bedenken bestehen jedoch, wenn ein Anwalt zugleich den Beruf des Datenschutzbeauftragten ausübt und für seine Mandanten nur entweder in der einen oder der anderen Funktion tätig wird.[52] Dabei stellt sich dann die weitere Frage, ob die Tätigkeit als Datenschutzbeauftragte eine Anwaltstätigkeit oder eine der Gewerbesteuer unterliegende Tätigkeit ist.

43 Heberlein, in: Ehmann/Selmayr, DSGVO, 2. Aufl. Art. 37 Rn. 42 und 25; Gola/Schomerus, BDSG, 12. Aufl. § 4f Rn. 24, Simitis, in Simitis: BDSG § 4f Rn. 47 mit Nachw.

44 Bergt, in: Kühling/Buchner, DSGVO/BDSG, 2. Aufl. DS-GVO Art. 37 Rn. 39, Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. Art. 37 Rn. 25.

45 Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., DS-GVO Art. 38 Rn. 39.

46 Baumgartner/Hansch, Der betriebliche Datenschutzbeauftragte, ZD 2019, 99 (102).

47 Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 38 Rn. 25; Art. 29-Gruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 recv. 01, S. 19; a.A. Haag, in: Forgo/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., Kap. 3, S. 229 unter Hinweis auf die nach dem Standesrecht bestehende Pflicht zur objektiven Beratung.

48 Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 38 Rn. 25.

49 Baumgartner/Hansch, ZD 2019, 101 (102); LfDI Baden-Württemberg, Brink/Stoor, Praxisratgeber: Die/der Beauftragte für den Datenschutz-Teil II 1. Aufl. 2018, S. 6; https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/20.

50 LDI NRW, Häufig gestellte Fragen zu Datenschutzbeauftragten (FAQ), https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte; HessDSB, 41. TB 2012, Ziff. 4.6; LfDI Baden-Württemberg, Brink/Stoor, Praxisratgeber, Die/Der Beauftragte für den Datenschutz – Teil II: Persönliche Voraussetzungen, Durchführung der Benennung, Stellung und Aufgaben, Beendigung der Benennung, 2018, S. 17; https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/20.

51 Baumgartner/Hansch, DuD 2019, 86 (87).

52 Vgl. bei Härtung, Anwaltsblatt 2018, 76 ff.

b) Der Rechtsanwalt als DSB und Vertreter in (gleichgelagerten) Rechtssachen

Der Fall, dass der als DSB bestellte Rechtsanwalt seinen Auftraggeber zugleich als Rechtsanwalt in Datenschutzfragen vor Gericht vertritt, wird in der Regel zu einer Interessenkollision führen. Dies kann nicht deshalb grundsätzlich verneint werden, weil Rechtsanwälte „als Organe der ‚Rechtspflege zur objektiven Beratung geeignet und verpflichtet sind."[53] Vielmehr ist unter dem Gesichtspunkt des Datenschutzes zu bedenken, dass der Anwalt nur die Interessen seines Mandanten zu vertreten hat, während der Datenschutzbeauftragte die Interessen der betroffenen Personen zu wahren und mit der Aufsichtsbehörde zusammenzuarbeiten hat (Art. 39 DS-GVO). Keine Bedenken bestehen wohl zu Recht, wenn die Beratung oder gerichtliche Vertretung in anderen Rechtsfragen erfolgt.[54]

Dieses sich im Rahmen der Beurteilung des nach Art. 38 Abs. 6 DS-GVO zu vermeidenden Interessenkonflikts ergebende Ergebnis folgt auch aus dem anwaltlichen Berufsrecht. Gemäß § 45 Abs. 1 Nr. 4 BRAO darf ein Rechtsanwalt nicht tätig werden „wenn er in derselben Angelegenheit außerhalb seiner Anwaltstätigkeit … bereits beruflich tätig war; dies gilt nicht, wenn die berufliche Tätigkeit beendet ist."

Wer in seinem Zweitberuf als DSB arbeitet, darf die benennende Stelle in dieser Angelegenheit nicht mehr anwaltlich beraten und vertreten. Hat ein Unternehmen einen Anwalt zum betrieblichen Datenschutzbeauftragten bestellt, führt dies somit auch zu einem berufsrechtlichen Verbot, in datenschutzrechtlichen Angelegenheiten für das Unternehmen anwaltlich tätig zu werden. Dieses Tätigkeitsverbot beschränkt sich nicht auf die Person des Anwalts, sondern bezieht sich nach § 45 Abs. 3 BRAO auf „die mit dem Rechtsanwalt in Sozietät oder in sonstiger Weise zur gemeinschaftlichen Berufsausübung verbundenen oder verbunden gewesenen Rechtsanwälte".

c) Der Syndikusanwalt und der DSB als externer DSB in Personalunion

Wer als Angestellter für Kunden seines Arbeitgebers als externer Datenschutzbeauftragter tätig ist, kann nach Auffassung des BGH nicht als Syndikusrechtsanwalt zugelassen werden.[55] Der Mitarbeiter werde nicht in Rechtsangelegenheiten des Arbeitgebers tätig, wenn er die Kunden seines Arbeitgebers berate, nehme er nicht Rechtsangelegenheiten des Arbeitgebers wahr, was tatbestandliche Voraussetzung für die Zulassung als Syndikusrechtsanwalt sei.

d) Der Syndikusanwalt und der der interne DSB in Personalunion

Ob die Funktionen von Syndikusanwalt und internem betrieblichen oder behördlichen[56] Datenschutzbeauftragten in der Hand einer Person liegen können, ist ebenfalls einmal eine Frage des anwaltlichen Berufsrechts und zum anderen der datenschutzrechtlich verbotenen Interessenkollision. Berufsrechtlich ist die Tätigkeit als Datenschutzbeauftragter ein „Zweitberuf" des Anwalts. Ein Zweitberuf ist dem Anwalt erlaubt, wenn der Beruf mit dem Anwaltsberuf „vereinbar" ist. Datenschutzrechtlich ist die Übertragung der Funktion des DSB an einen angestellten Rechtsanwalt jedenfalls nicht per se ausgeschlossen.[57]

V. Haftung im Verhältnis zur benennenden Stelle

Werden die sich aus dem mit dem externen Datenschutzbeauftragten bestehenden Dienstleistungs- bzw. Geschäftsbesorgungsvertrag (§ 675 BGB) ergebenden Pflichten von dem DSB schuldhaft verletzt, kann die verantwortliche Stelle nach § 280 Abs. 1 BGB Ersatz des ihr hieraus entstandenen Schadens verlangen, der auch in einem Bußgeld oder darin bestehen kann, dass die Datenverarbeitung unter finanziellem Aufwand an die Vorgaben der Aufsichtsbehörde angepasst werden muss.

Vom Fall der aktiven Falschberatung zu unterscheiden ist der Fall, dass der Datenschutzbeauftragte seinem Überwachungsauftrag (Art. 39 Abs.1 lit. b DS-GVO) nicht ordnungsgemäß nachgekommen ist mit der Folge, dass eine datenschutzwidrige Maßnahme mit für den Arbeitgeber negativen vermögensrechtlich Folgen durchgeführt wurde. Sofern die Haftung darauf gestützt wird, dass der Datenschutzbeauftragte den Verstoß gegenüber dem Verantwortlichen bzw. Auftragsverarbeiter nicht moniert hat, stellt sich die Frage nach der haftungsbegründenden Kausalität. Selbst wenn der Datenschutzbeauftragte gebotene Kontrollmaßnahmen unterlassen und nicht auf bestehende Rechtsverstöße hingewiesen hat, so bedeutet dies nicht zwingend, dass die Unternehmens- bzw. Behördenleitung entsprechende Hinweise andernfalls auch umgesetzt hätte und damit die Rechtsverletzung unterblieben wäre.[58]

Liegt der Vorwurf gegenüber dem Datenschutzbeauftragten in einem Unterlassen, ist im Übrigen stets zu prüfen, ob der Datenschutzbeauftragte über die betreffende Datenverarbeitung überhaupt rechtzeitig informiert war.

Hinsichtlich dieser Haftungsvoraussetzungen bestehen keine Unterschiede zwischen internen und externen Datenschutzbeauftragten. Anderes gilt jedoch hinsichtlich der Frage des Verschuldens. Da dem externen DSB nicht die im Arbeitsverhältnis geltenden Haftungserleichterungen[59] zu-

53 So Baumgartner/Hansch, DuD 2018, 86 (87).

54 Haag, in: Forgo/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., Teil II, Kap. 3, betrieblicher Datenschutzbeauftragter, Rn. 63.

55 BGH, Urt. v. 02.07.2018 – AnwZ (Brfg) 49/17.

56 BGH, Urt. v. 15.10.2018 – AnwZ (Brfg) 20/18. „a) Die Zulassung als Syndikusrechtsanwalt nach §§ 46 f. BRAO ist grundsätzlich auch für ein Arbeitsverhältnis im öffentlichen Dienst möglich".

57 Für Beschäftigte der Rechtsabteilung als Datenschutzbeauftragte auch BayLDA, 5. TB (2011/2012), S. 16 f.; differenzierend Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., DS-GVO Art. 38 Rn. 42; auch eine Benennung des Leiters der Rechtsabteilung ist denkbar nach Auffassung von Heberlein, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. Art. 38 Rn. 23; ähnlich Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 201, nach denen der konkrete Aufgabenzuschnitt des Leiters entscheidend ist.

58 Schlemann, Recht des betrieblichen Datenschutzbeauftragten, 2. Aufl., S. 286 f.

59 Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. DS-GVO Art. 37 Rn. 53.

gutekommen, haftet er für jedes Verschulden. Somit empfiehlt sich hier der Abschluss einer entsprechenden Vermögensschadenhaftpflichtversicherung[60]. Zudem kann eine Haftungseinschränkung vertraglich vereinbart werden. Möglich ist ein pauschaler Haftungsausschluss für leicht fahrlässig verursachte Schäden,[61] wie er dem internen Datenschutzbeauftragten von der Rechtsprechung im Rahmen des innerbetrieblichen Schadensausgleichs[62] zugestanden wird. Ebenfalls möglich ist eine summenmäßige Beschränkung, wenn die Haftung für vertragstypische, vorhersehbare und vorsätzlich herbeigeführte Schäden abgedeckt bleibt.[63] Die Haftungssumme sollte dann mit der Deckungssumme der Berufshaftpflichtversicherung identisch sein.

Hingewiesen werden muss aber auch darauf, dass eine Haftung des DSB bei falscher oder unterlassener Beratung in Zweifel gezogen wird,[64] da die gesetzliche Beratungspflicht und damit auch die – regelmäßig identische – vertragliche Verpflichtung nicht existiere, um die benennende Stelle vor Schäden zu bewahren. Der Beratungsauftrag diene dem Schutz betroffener Personen und schütze die benennende Stelle lediglich im Rahmen einer Reflexwirkung.

VI. Fazit

Nachdem der Gesetzgeber die Benennung von betrieblichen Datenschutzbeauftragten erst bei der Zahl von 20 einschlägig[65] Beschäftigten verpflichtend machen will[66], werden mit Minimal"-Summen per Standard-Fernberatung abgewickelte Betreuungen dem gesetzlichen Auftrag des DSB nicht mehr gerecht werden. Die Verantwortlichen müssen sachbezogen entscheiden, ob ein externer oder ein interner DSB den betrieblichen Belangen besser nachkommen kann, wobei Kostengesichtspunkte erst nachrangig eine Rolle spielen dürfen.

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

60 Breyer/Duensing, DuD 2018, 86.

61 Vgl. bei Kremer/Sander, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, S. 105 ff.

62 BAG, Beschl. v. 27.09.1994 – GS1/89.

63 BGH, Urt. v. 11.11.1993 – VIII ZR 238/91.

64 Reif, Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG – Arbeitshilfe für die betriebliche Praxis, 2. Aufl., 2019 Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V.

65 VGl. Gola, RDV 2019, S. 131 und in diesem Heft, S. 176.

66 BT-Beschluss vom 27.6.2019.

Das neue Zeitalter im kommunalen Datenschutz

Datenschutz in der Kommunalverwaltung
Recht – Technik – Organisation

Herausgegeben von
Dr. Martin Zilkens und **Dr. Lutz Gollan**
5., völlig neu bearbeitete und wesentlich erweiterte Auflage 2019, XLVII, 788 Seiten, fester Einband, € (D) 108,–, ISBN 978-3-503-18758-4

Direkter Zugang zu allen Detailfragen: Die **5. Auflage des Zilkens/Gollan (Hrsg.), Datenschutz in der Kommunalverwaltung**, berücksichtigt alles, was sich mit der DSGVO geändert hat, und ist in Umfang und Tiefe seiner Erläuterungen einzigartig geblieben! Für Problemlösungen, die haargenau zur Kommunalpraxis passen. Mit **außerordentlich differenziertem Kapitel zum bereichsspezifischen Datenschutz**, das noch einmal **erweitert und inhaltlich überarbeitet** wurde.

Online informieren und bestellen:
www.ESV.info/18758

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G · 10785 Berlin · Tel. (030) 25 00 85-265
Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info

Radu Hodis-Mayer

Datenverarbeitung im Beschäftigungsverhältnis zur Aufdeckung von Straftaten

Die Mitgliedstaaten haben über die Eröffnungsklausel in Art. 88 DS-GVO die Möglichkeit, durch „Rechtsvorschriften oder durch Kollektivvereinbarungen" die Datenverarbeitung im Beschäftigungskontext näher zu regeln.[1] Hiervon hat der deutsche Gesetzgeber mit § 26 BDSG Gebrauch gemacht. Die Rechtsprechung hat sich in der Vergangenheit mit der Zulässigkeit der Datenverarbeitung im Beschäftigungsverhältnis nach Maßgabe des § 32 BDSG a.F. auseinandergesetzt. Auch wenn in der Literatur die Übertragung der von der Rechtsprechung zu einer verdeckten Videoüberwachung entwickelten Grundsätze auf § 26 BDSG teilweise abgelehnt wird, sind die Regelungen des § 32 BDSG a.F. letztendlich „weitgehend wortgleich in § 26 überführt worden".[2] Es besteht jedenfalls die Möglichkeit, dass diese Grundsätze auch künftig, wenn nur auch teilweise, in der Rechtsprechung Beachtung finden. Vor diesem Hintergrund untersucht dieser Aufsatz, anhand einer Entscheidung des BAG zu BDSG a.F., diese Grundsätze.

I. Sachverhalt

In seinem Urteil vom 20.10.2016 – 2 AZR 395/15 – hat sich das BAG mit der Frage befasst, inwiefern personenbezogene Daten im Beschäftigungsverhältnis, zur Aufdeckung von Straftaten erhoben, verarbeitet oder benutzt und unter welchen Bedingungen die sich daraus ergebenden Erkenntnisse in einem Kündigungsschutzverfahren verwendet werden können.

In einem Ersatzteillager der Beklagten, einem Kfz-Vertragshändler, wurden Inventurdifferenzen festgestellt. Bis zu diesem Zeitpunkt durften die Mitarbeiter eigenhändig Teile aus dem Lager entnehmen und falls diese doch nicht benötigt wurden, zurückbringen.

Mit Hilfe eines Aushangs wurden diese Differenzen im Betrieb bekannt gemacht. Die bisherige Handhabe wurde dahingehend geändert, als den Mitarbeitern, bis auf zwei Lageristen, den Zutritt zum Lager und die eigenständige Entnahme von Ersatzteilen untersagt wurde. Mit den Lagermitarbeitern wurden auch Gespräche geführt. Eine Aufklärung der Fehlbestände war jedoch nicht möglich.

Aus diesem Grund ließ die Beklagte den Lagerraum mit Hilfe einer Videokamera überwachen. Kenntnis hiervon hatten nur die Lageristen und der Betriebsleiter. Der Betriebsrat wurde nicht beteiligt.

Auf den sodann erstellten Aufzeichnungen konnte beobachtet werden, wie ein Mitarbeiter (der spätere Kläger) Ersatzteile aus einem Regal entnimmt und mit diesen den Lagerraum verlässt. Aufgrund dieser Erkenntnisse wurden sodann eine außerordentliche sowie eine ordentliche Kündigung ausgesprochen. Hiergegen richtete sich die Kündigungsschutzklage des Klägers.

Die Vorinstanzen haben der Klage stattgegeben. Der Sachvortrag der Beklagten, der auf diesen Aufzeichnungen gestützt war, durfte nach Ansicht des LAG, aufgrund eines Eingriffs in das allgemeine Persönlichkeitsrecht des Klägers, nicht verwertet werden.

II. Rechtsgrundlage eines Verwertungsverbotes

Zunächst eruiert das BAG die mögliche Rechtsgrundlage für ein Sachvortrags- oder Beweisverwertungsverbot.

Ein solches Verbot ist nach BAG weder der ZPO noch dem Arbeitsgerichtsgesetz zu entnehmen. Denn in der Regel ist im Rahmen eines Gerichtsverfahrens der komplette Sachvortrag zu verwerten. Dies gebieten der Anspruch auf rechtliches Gehör gemäß Art. 103 Abs. 1 GG sowie § 286 ZPO, wonach das Gericht den gesamten Inhalt „der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme" bei seiner Entscheidung berücksichtigen muss.[3]

Das BDSG wiederum enthält zwar Vorschriften über die Zulässigkeit der Verarbeitung von personenbezogenen Daten, jedoch keine dahingehende Sanktion, wonach Erkenntnisse, die unter Verstoß gegen das BDSG gewonnen wurden, einem Sachvortrags- oder Beweisverwertungsverbot im Prozess unterliegen. Zu der alten Fassung des BDSG hat das BAG entschieden, dass dessen Vorschriften zwar eine Konkretisierung des Schutzes „des Rechts auf informationelle Selbstbestimmung und am eigenen Bild", jedoch keine Anordnung enthalten, „dass unter ihrer Missachtung gewonnene Erkenntnisse oder Beweismittel bei der Feststellung des Tatbestands im arbeitsgerichtlichen Verfahren vom Gericht nicht berücksichtigt werden dürften"[4].

Als Legitimation für die Annahme eines Beweis- oder Sachverwertungsverbotes bleibt nach BAG nur der zwingend gebotene Schutz des allgemeinen Persönlichkeitsrechts mit

1 Vgl. Art. 88 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).

2 Kühling/Buchner, DS-GVO, BDSG Kommentar, 2. Aufl., § 26 BDSG, Rn. 3.

3 Vgl. § 286 ZPO.

4 Vgl. u.a. BAG, Urteil vom 29.06.2017 – 2 AZR 597/16, NJW 2017, 2853, beck-online, Rn. 22.

seinen besonderen Ausprägungen.[5] Denn bei der Urteilsfindung sind die Gerichte an die Grundrechte gebunden, so dass Erkenntnisse, die durch einen Eingriff in das allgemeine Persönlichkeitsrecht eines Betroffenen gewonnen worden sind, möglicherweise gegen diesen nicht verwendet werden dürfen. Hierbei kommt nach Auffassung des BAG nicht nur ein Beweis-, sondern sogar ein Sachvortragsverwertungsverbot (Nichtbeachtung unstreitigen Sachvortrags) in Betracht.[6]

Das allgemeine Persönlichkeitsrecht umfasst nicht allein die Privat- und Intimsphäre, sondern auch das Recht am eigenen Bild und das Recht auf informationelle Selbstbestimmung.[7] Danach kann jeder Mensch selbst über die Preisgabe und Verwendung persönlicher Daten entscheiden.

Ob ein Eingriff in das allgemeine Persönlichkeitsrecht stattgefunden hatte, prüft sodann das BAG anhand des Regelungswerks des § 32 BDSG a.F.

III. Zulässigkeit der Datenverarbeitung nach BDSG

Die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis setzte nach § 32 Abs. 1 S. 2 BDSG a.F. voraus, dass Anhaltspunkte für eine Straftat im Beschäftigungsverhältnis gegeben waren, die Maßnahme erforderlich war und das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss dieser Maßnahme nicht überwog, insbesondere die Maßnahme nicht unverhältnismäßig war.[8]

1. Verdacht einer Straftat

Nach dem Wortlaut des § 32 Abs. 1 S. 1 BDSG a.F. bedurfte es zunächst für die Datenverarbeitung des Verdachtes einer Straftat im Beschäftigungsverhältnis. BAG sieht einen Eingriff in das Recht am eigenen Bild aber auch dann als gerechtfertigt, wenn „nur" der konkrete Verdacht einer „anderen schweren Verfehlung zulasten des Arbeitgebers"[9] gegeben ist. Nach BAG entfaltete § 32 Abs. 1 S. 2 BDSG a.F. keine „Sperrwirkung" gegenüber der Erlaubnisnorm des Satzes 1, mit der Folge, dass eine verdeckte Videoüberwachung auch beim Verdacht einer schweren Pflichtverletzung eingesetzt werden kann, wenn die Verhältnismäßigkeit der Maßnahme gewährleistet ist.[10]

Der Wortlaut der Vorschrift – „den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat" – würde, für sich genommen, den Einsatz einer verdeckten Videoüberwachung erst dann erlauben, wenn sich der Verdacht auf den durch die Maßnahme Betroffenen beziehen würde. Das BAG entscheidet sich für eine großzügigere Auslegung. Der Verdacht müsse sich nicht „gegen einen einzelnen, bestimmten Arbeitnehmer richten", sondern es reiche vielmehr aus, dass dieser „einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern" umfasst.[11] Das BAG sieht sich an diesem Auslegungsergebnis trotz des Wortlautes der Vorschrift nicht gehindert. Dabei verweist es auf die Gesetzesbegründung, wonach das Regelwerk des § 32 BDSG a.F. die bisherigen Rechtsprechungsgrundsätze nicht ändern soll.[12] Es muss aus Sicht des BAG nur sichergestellt werden, dass der Kreis der Verdächtigen nicht durch weniger einschneidende Maßnahmen eingeschränkt werden kann.

Des Weiteren stellte sich die Frage, wie sicher es sein muss, dass eine Straftat begangen worden ist, bevor eine versteckte Videoüberwachung eingesetzt wird. Ein „dringender Verdacht" ist nach Auffassung des BAG nicht erforderlich. Ein „einfacher Verdacht" sei vielmehr ausreichend. Es müsse, mit anderen Worten, nicht mit großer Wahrscheinlichkeit feststehen, dass eine Straftat begangen worden ist. Es reiche vielmehr ein „gewisses Maß an Konkretisierung und Verdichtung", so dass die Begehung einer Straftat „nach der Lebenserfahrung" als möglich erscheint.[13]

Dieser Verdacht könnte vorliegend nach Auffassung des BAG gegeben sein, auch wenn andere Ursachen für die vorgetragenen Inventurdifferenzen nicht ausgeschlossen werden können. Nach BAG hat das LAG den Vortrag der Beklagten – die Differenzen seien in kurzen zeitlichen Abständen aufgetreten, es seien leicht zu entfernende Teile betroffen, die anderen Maßnahmen hätten nicht geholfen – nicht ausreichend gewürdigt. Denn diese Angaben könnten einen hier ausreichenden „Anfangsverdacht" begründen.

2. Erforderlichkeit der Videoüberwachung

Nach Auffassung des BAG waren, unter Zugrundelegung des Vortrags der Beklagten, keine weniger einschneidenden, jedoch gleichermaßen erfolgversprechenden Maßnahmen ersichtlich. Der angestrebte Zweck der Aufklärung hätte man insbesondere nicht mit einer offenen Videoüberwachung erreichen können. In einem ähnlichen Fall hat das BAG ausgeführt: „Derart auf Heimlichkeit angelegtes Verhalten kann

5 Vgl. Art. 1 Abs. 3 und Art. 2 Abs. 1 GG.

6 Vgl. LAG Hessen, Urteil vom 21.09.2018 – 10 Sa 601/18, wonach ein Verstoß gegen § 32 Abs. 1 S. 1 a.F. dazu führt, dass sogar der unbestrittene Inhalt einer E-Mail nicht verwertet werden kann.

7 Vgl. BVerfG, Urteil vom 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07 (NJW 2008, 1505, beck-online, Rn. 61).

8 Der Wortlaut des § 32 Abs. 1 S. 2 BDSG a.F wurde größtenteils in § 26 BDSG übernommen.

9 BAG, Urteil vom 20.10.2016 – 2 AZR 395/15, Rn. 22.

10 BAG, Urteil vom 29.06.2017 – 2 AZR 597/16 NJW 2017, 2853, beck-online, Rn. 28 ff.

11 BAG, Urteil vom 20.10.2016 – 2 AZR 395/15, Rn. 22.

12 BT-Drs. 16/13657, S. 20 lautet auszugsweise: „§ 32 enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll". Eine abweichende Auffassung ist auch nicht der Gesetzesbegründung zu dem BDSG n.F. zu entnehmen, vgl. BT-Drs. 18/11325. In der Literatur ist diese Auffassung teilweise auf Kritik gestoßen, vgl. Kühling/Buchner, § 26 BDSG, Rn. 59 mit Verweis auf Brink, in: NK-ArbR § 32, Rn. 160.

13 BGH Beschl. v. 11.08.2016 – StB 12/16, BeckRS 2016, 15673, beck-online, Rn. 9.

seiner Natur nach nicht durch offen angekündigte Beobachtung entdeckt werden."[14]

3. Angemessenheit

Die Maßnahme ist nach Auffassung des BAG allgemein nicht unangemessen. Räumlich betreffe diese nur das Lager und somit genau den Ort, an welchem die vermissten Gegenstände aufbewahrt worden sind. Durch das Zutrittsverbot sei außerdem der Kreis der möglicherweise betroffenen Personen eingeschränkt worden. Wer trotzdem unbefugt diesen Bereich betrete, müsse den Eingriff hinnehmen.

4. Sonstige Gründe für ein Verwertungsverbot

Nach Ansicht des BAG kann sich der Kläger auch nicht darauf berufen, dass die Videoüberwachung möglicherweise das allgemeine Persönlichkeitsrecht anderer Personen verletzt habe. Sinn und Zweck des § 32 BDSG a.F. bestehe nicht in einer Generalprävention.[15]

Auch ein Verstoß gegen die nach § 32 Abs. 1 S. 2 BDSG a.F. erforderliche Dokumentationspflicht[16] führt für BAG nicht zu einer Unverwertbarkeit des Sachvortrags. Sinn und Zweck dieser Dokumentationspflicht bestehe darin, die Rechtmäßigkeitskontrolle zu gewährleisten. Dieser Zweck könne aber auch dadurch erreicht werden, dass der Arbeitgeber in dem späteren Prozess die konkreten Anhaltspunkte für den Verdacht vorträgt.[17] Dies würde dann die bezweckte Rechtmäßigkeitskontrolle erlauben.

Ebenso wenig ergäbe sich ein Verwertungsverbot aus der fehlenden Zustimmung des Betriebsrates. Die Verletzung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG sei jedenfalls dann unbeachtlich, wenn die Datenverarbeitung nach „allgemeinen Grundsätzen" zulässig sei. Denn in diesem Fall sei der auch mit dieser Vorschrift bezweckte Schutz des allgemeinen Persönlichkeitsrechts erreicht, falls die Maßnahme etwa nach Maßnahme des BDSG zulässig sei.[18]

Die Entscheidung des Berufungsgerichtes wurde sodann aufgehoben. Nach Zurückverweisung der Sache an die Vorinstanz, ist die Angelegenheit derzeit beim LAG Köln – 4 Sa 1198/14 anhängig.

IV. Fazit

Mit dieser Entscheidung präzisiert das BAG die an einem Verdacht im Sinne des § 32 Abs. 1 S. 2 BDSG a.F. zu stellenden Anforderungen. Nach BAG ist der Einsatz einer heimlichen Videoüberwachung nicht nur beim Verdacht einer „Straftat", sondern auch beim Verdacht einer „schweren Verfehlung" im Arbeitsverhältnis zulässig. Dies erlaube der Grunderlaubnistatbestand des § 32 Abs. 1 S. 1 BDSG a.F., denn § 32 Abs. 1 S. 2 BDSG a.F. entfalte insoweit keine Sperrwirkung. Dies erscheint konsequent. Eine schwere Pflichtverletzung kann für die Entscheidung bezüglich der Beendigung des Arbeitsverhältnisses von gleicher Bedeutung sein wie eine Straftat.

Die Grundsätze bezüglich des erforderlichen Verdachtsgrades stellen einerseits sicher, dass kein uferloser Einsatz von heimlichen Überwachungsmethoden zulässig ist. Andererseits eröffnen diese dem Arbeitgeber einen gewissen Beurteilungsspielraum, da dieser mit solchen Maßnahmen nicht so lange warten muss, bis eine an Sicherheit grenzende Wahrscheinlichkeit gegeben ist.

Hilfreich sind auch die Ausführungen bezüglich der Substantiierbarkeit des Sachvortrags des der Überwachungsmaßnahme einsetzenden Arbeitgebers. Dieser muss insbesondere das Gericht überzeugen, dass mildere und vergleichbar geeignete Mittel ausgeschöpft worden sind. Wenn eine weitere Einschränkung der Betroffenen durch mildere Mittel nicht möglich ist, darf die verdeckte Überwachungsmaßnahme eingesetzt werden.

Des Weiteren wird klargestellt, dass nicht jeglicher Verstoß gegen die Vorschriften des BDSG a.F. eine Unverwertbarkeit der sich aus der Überwachungsmaßnahme ergebenden Erkenntnisse nach sich zieht. Eine Unverwertbarkeit kommt erst dann in Betracht, wenn damit eine Perpetuierung eines Eingriffs in grundrechtlich geschützte Positionen stattfinden würde.

Man darf letztendlich mit Spannung abwarten, ob die Rechtsprechung diese Grundsätze auch nach Inkrafttreten der DS-GVO anwenden wird. In der Literatur wird die Auffassung vertreten, dass § 26 BDSG eine verdeckte Videoüberwachung nicht mehr erlauben würde.[19] Denn das in Art. 88 Abs. 2 DS-GVO verankerte Transparenzgebot könne nach Maßgabe des Art. 23 Abs. 1 DS-GVO nur durch eine gesetzliche Regelung eingeschränkt, und eine solche könne nicht in Art. 26 BDSG hineingelesen werden.

Radu Hodis-Mayer
ist seit 2013 als Rechtsanwalt in der Kanzlei Raab & Kollegen in Fürth tätig. Er studierte Rechtswissenschaften an der Friedrich-Alexander Universität in Erlangen. Das 2. Staatsexamen absolvierte er im Jahre 2012. Zu seinen Tätigkeitsbereichen gehört unter anderem auch der Datenschutz. Im Rahmen der 3. Rumänisch-Deutschen Konferenz zum Europäischen Informationsrecht, Cluj-Napoca, Rumänien, referierte er zum Thema "Beschäftigtendatenschutz in Deutschland".

14 BAG, Urteil vom 27.03.2003 – 2 AZR 51/02, NJW 2003, 3436, beck-online.

15 Zur Bestätigung dieses Grundsatzes vgl. auch LAG Baden-Württemberg Urt. v. 06.06.2018 – 21 Sa 48/17, BeckRS 2018, 30862, beck-online, Rn. 109: „ist für die Zulässigkeit der Verwertung von Zufallsfunden eine datenschutzkonforme und daher rechtmäßige Erhebung von Daten auf Grund einer anderen Motivation heraus nicht notwendig".

16 Dies gilt auch für § 26 Abs. 1 S. 2 BDSG. Nach der Rechtsprechung sind „Schaden, Kreis der Verdächtigen und die Indizien" zu dokumentieren, Kühling/Buchner, § 26 BDSG, Rn. 60.

17 So auch LAG Rheinland-Pfalz, Urteil vom 11.04.2019 – 5 Sa 371/18 und LAG Hamm Urt. v. 20.12.2017 – 2 Sa 192/17.

18 So auch BAG Urt. v. 31.01.2019 – 2 AZR 426/18.

19 So Kühling/Buchner, § 26 BDSG, Rn. 22.

Jan Spittka

Si tacuisses … – nemo tenetur und die DS-GVO*

Die DS-GVO enthält für Verantwortliche und Auftragsverarbeiter diverse Informations-, Kooperations- und Meldepflichten. Würde man diese Pflichten unmodifiziert anwenden, müssten sich die Verpflichteten häufig selbst belasten. Dieser Beitrag gibt einen Überblick über die Anwendung des nemo tenetur-Grundsatzes auf deutscher und europäischer Ebene und zur Europarechtskonformität des Auskunftsverweigerungsrechts und des Verwendungsverbots im deutschen Datenschutzrecht.

I. Überblick

Si tacuisses, philosophus mansisses – wenn du geschwiegen hättest, so wärest du ein Philosoph geblieben. Die Datenschutz-Grundverordnung (DS-GVO) sieht jedoch diverse Konstellationen vor, in denen datenschutzrechtlich Verantwortliche und Auftragsverarbeiter nicht schweigen dürfen, sondern zur aktiven Kommunikation verpflichtet sind. So besteht für Verantwortliche und Auftragsverarbeiter und gegebenenfalls deren Vertreter[1] die Pflicht, auf Anfrage mit der zuständigen Datenschutzbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Die Behörden haben gegenüber den Verantwortlichen und Auftragsverarbeitern umfassende Informationsrechte. Kommt es zu einer „Verletzung des Schutzes personenbezogener Daten", kann die Pflicht entstehen, diese an die zuständige Datenschutzbehörde und gegebenenfalls die betroffenen Personen zu melden. Verstöße gegen diese Pflichten können sanktioniert werden. Es stellt sich daher die Frage nach dem Verhältnis dieser Pflichten zur Selbstbelastungsfreiheit im Straf- und Ordnungswidrigkeitenverfahren (nemo tenetur se ipsum accusare).

II. Auskunfts- und Meldepflichten unter der DS-GVO

1. Auskunftspflichten

Gemäß Art. 58 Abs. 1 lit. a) DS-GVO kann die Datenschutzbehörde den Verantwortlichen oder Auftragsverarbeiter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Behörde erforderlich sind. Die Bereitstellung kann – je nach Information – durch Übermittlung von Kopien, Daten bzw. Datenträgern oder eigens für die Informationsübermittlung erstellte Zusammenfassungen oder Vermerke erfolgen.[2] Ein Verstoß gegen eine Aufforderung der Behörde ist nicht direkt bußgeldbewehrt. Allerdings kann ein Verstoß gegen die Kooperationspflicht nach Art. 31 DS-GVO vorliegen,[3] der gemäß Art. 83 Abs. 4 lit. a) DS-GVO mit einer Geldbuße sanktioniert werden kann. Zudem besteht in Deutschland die Möglichkeit, die Befolgung einer Auskunftsanordnung mit den Mitteln der Verwaltungsvollstreckung, also Zwangsgeld, durchzusetzen. Kommt der Verantwortliche oder Auftragsverarbeiter seinen Auskunftspflichten ordnungsgemäß nach, besteht für ihn die Gefahr, dass er der Datenschutzbehörde Informationen offenlegt, die Datenschutzverstöße belegen und im Anschluss für ein Bußgeldverfahren verwendet werden.

2. Meldepflichten

Neben den Auskunftspflichten auf Anfrage enthält die DS-GVO im Fall einer „Verletzung des Schutzes personenbezogener Daten" (Art. 4 Nr. 12 DS-GVO) die Pflicht zur unaufgeforderten Meldung an die Behörde (Art. 33 DS-GVO) und zur Benachrichtigung der betroffenen Personen (Art. 34 DS-GVO).[4] Verstöße gegen die Melde- bzw. Benachrichtigungspflicht können gemäß Art. 58 Abs. 2 lit i) DS-GVO i.V.m. Art. 83 Abs. 4 lit. a) DS-GVO mit einer Geldbuße geahndet werden. Für den Auftragsverarbeiter besteht gemäß Art. 33 Abs. 2 DS-GVO eine eigene Meldepflicht gegenüber dem Verantwortlichen.

Gemäß Art. 33 Abs. 3 lit. a) DS-GVO muss die Meldung an die Datenschutzbehörde u.a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und, soweit möglich, eine Angabe der betroffenen Datenkategorien enthalten. Es kann also sein, dass der Datenschutzbehörde im Rahmen der Meldung Informationen offengelegt werden, die Verstöße gegen die DS-GVO belegen, z.B. unzureichende technische und organisatorische Maßnahmen i. S. d. Art. 32 DS-GVO. Als Beispiel kann hier auf das Bußgeldverfahren des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg gegen den Social-Media-Anbieter „Knuddels" verwiesen werden.[5] Es kann zudem sein, dass im Rahmen der Meldung herauskommt, dass personenbezogene Daten betroffen sind, die nicht (mehr) hätten verarbeitet werden dürfen. Diese Informationen kann die Datenschutzbehörde gegebenenfalls auch aus den Benachrichtigungen der betroffenen Personen entnehmen. Auch im Rahmen der Pflichten nach Art. 33, 34 DS-GVO kann der Verantwortliche also in die Zwickmühle geraten, sich selbst belasten zu müssen oder aber gegen bußgeldbewehrte Pflichten aus der DS-GVO zu verstoßen.

* Dieser Aufsatz ist Grundlage für einen Vortrag auf der diesjährigen DSRI-Herbstakademie „Die Macht der Daten und der Algorithmen". Eine Langfassung wird im Tagungsband erscheinen.

1 Auf die Pflichten der Vertreter i. S. d. Art. 27 DS-GVO wird im Folgenden nicht mehr gesondert eingegangen.

2 Grittmann, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 58 DSGVO, Rn. 12.

3 Grittmann, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 58 DSGVO, Rn. 12.

4 Siehe Spittka, DSRITB 2017, 387, 389 ff. zu den konkreten Voraussetzungen der Meldepflicht.

5 LfDI Baden-Württemberg, Pressemitteilung v. 22.11.2018, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/.

III. Der nemo tenetur-Grundsatz im deutschen und europäischen Recht

Der Grundsatz „nemo tenetur se ipsum accusare" besagt, dass niemand gezwungen werden darf, sich selbst in einem Straf- oder Ordnungswidrigkeitenverfahren zu belasten. Der Grundsatz der Selbstbelastungsfreiheit ist, mit unterschiedlicher Begründung, sowohl im deutschen Verfassungsrecht als auch auf Ebene des Gemeinschaftsrechts dem Grunde nach anerkannt. Fraglich ist jedoch der konkrete Umfang und, inwieweit der Grundsatz auch für Unternehmen gilt.

1. Rechtsprechung des BVerfG

Das Bundesverfassungsgericht (BVerfG) leitet den nemo tenetur-Grundsatz zunächst aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), ab.[6] Ein Zwang zur Selbstbezichtigung berühre zugleich die Würde des Menschen, dessen Aussage als Mittel gegen ihn selbst verwendet wird.[7] Klang dies bereits in früheren Entscheidungen an,[8] stützt das BVerfG die Selbstbelastungsfreiheit in neueren Entscheidungen ausdrücklich auf das Rechtsstaatsprinzip, Art. 20 Abs. 3 GG.[9] Im Rahmen des Strafverfahrens dürfe niemand gezwungen werden, sich durch seine eigene Aussage einer Straftat zu bezichtigen oder zu seiner Überführung aktiv beizutragen.[10] Das BVerfG wendet den nemo tenetur-Grundsatz nicht nur im Straf-, sondern auch im Ordnungswidrigkeitsverfahren an.[11] Die Anwendung des nemo tenetur-Grundsatzes auf juristische Personen hat das BVerfG bislang ausdrücklich abgelehnt.[12] Der Bezug der Selbstbelastungsfreiheit zur Menschenwürde sei i. R. d. Art. 19 Abs. 3 GG dem Wesen nach nicht auf juristische Personen anwendbar.[13] Zudem begehe ein Organwalter unter Verletzung von Pflichten der juristischen Person die Tat. Die Festsetzung einer Geldbuße gegen die juristische Person gemäß § 30 Gesetz über Ordnungswidrigkeiten (OWiG) enthalte weder einen Schuldvorwurf noch eine ethische Missbilligung, sondern solle lediglich einen Ausgleich für die aus der Tat gezogenen Vorteile schaffen.[14]

Inwieweit diese Wertung des BVerfG zukünftig Bestand haben wird, ist mehr als fraglich. Das alleinige Abstellen auf die Menschenwürde widerspricht der Verankerung der Selbstbelastungsfreiheit im Rechtsstaatsprinzip.[15] Das Rechtsstaatsprinzip steht als justizielles Grundrecht auch juristischen Personen zu.[16] Warum ein Bußgeld, das gegen eine juristische Person verhängt wird, einen anderen Charakter haben soll als ein Bußgeld gegen eine natürliche Person, ist dogmatisch nicht wirklich nachvollziehbar.[17] Bei Ordnungswidrigkeitenverfahren aufgrund mutmaßlicher Verstöße gegen die DS-GVO muss zudem berücksichtigt werden, dass das als Verantwortlicher oder Auftragsverarbeiter handelnde Unternehmen originärer Adressat der Geldbuße ist, ohne dass eine Zurechnung über § 30 OWiG erforderlich wäre.[18] Schließlich gesteht das BVerfG das Grundrecht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG,[19] in jüngeren Entscheidungen auch juristischen Personen zu.[20] Auch insoweit dürfte eine pauschale Ablehnung der Selbstbelastungsfreiheit für Unternehmen nicht mehr haltbar sein.

2. Rechtsprechung des EGMR und des EuGH

a) EGMR

Der EGMR leitet den nemo tenetur-Grundsatz in ständiger Rechtsprechung aus dem Recht auf ein faires Verfahren nach Art. 6 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) ab.[21] Das Recht zu schweigen und das Recht, nicht zu seiner eigenen Beschuldigung beizutragen, sind nach Auffassung des Gerichts international allgemein anerkannte Grundsätze, die ein Kernstück des von Art. 6 Abs. 1 EMRK garantierten fairen Verfahrens darstellen.[22] Die Selbstbelastungsfreiheit umfasst zunächst das Recht zu schweigen, nicht aber ein allgemeines Verbot, unabhängig vom Willen des Beschuldigten existierende Beweismittel mittels Zwang zu erlangen, wie etwa aufgrund eines Durchsuchungsbeschlusses erlangte Dokumente oder Atemalkoholkontrollen oder Blut-, Urin- oder Gewebeproben zwecks DNA-Analyse.[23] Die Grenze zwischen einer aktiven Beweismittelherausgabepflicht und einer unzulässigen Selbstbelastung ist jedoch dort überschritten, wo der Beschuldigte aufgefordert wird, Dokumente zusammenzustellen und zu übergeben.[24] Zur Geltung des nemo tenetur-Grundsatzes für Unternehmen hat sich der EGMR noch nicht ausdrücklich geäußert.[25] Die in Art. 6 Abs. 1 EMRK verankerten prozessualen Verteidigungsrechte werden aber auch juristischen Personen zuerkannt.[26]

6 BVerfGE 38, 105, 113; BVerfGE 55, 144, 150; BVerfGE, 56, 37, 43.
7 BVerfGE, 56, 37, 42.
8 BVerfGE 38, 105, 113; BVerfGE 55, 144, 150.
9 BVerfG, NJW 2014, 3506, 3506 f.
10 BVerfG, NJW 2014, 3506, 3507.
11 BVerfGE 55, 144, 150.
12 BVerfG, NJW 1997, 1841, 1843 f.
13 BVerfG, NJW 1997, 1841, 1843.
14 BVerfG, NJW 1997, 1841, 1844.
15 Dannecker, ZStW 2015, 370, 375 f.
16 Dannecker, ZStW 2015, 370, 379.
17 Dannecker, ZStW 2015, 370, 376; Gräfin von Galen/Maass, in: Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 2017, § 30 OWiG, Rn. 78.
18 Datenschutzkonferenz (DSK), Entschließung v. 03.04.2019, Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!, abrufbar unter https://www.datenschutzkonferenz-online.de/media/e.
19 BVerfG, NJW 1984, 419, 421 f.
20 BVerfG, NJW 2018, 2385, 2386.
21 EGMR, NJW 2002, 499, 501 m.w.N. – J. B./Schweiz.
22 EGMR, NJW 2002, 499, 501 – J. B./Schweiz.
23 EGMR, Urt. v. 17.12.1996, 43/1994/490/672, Rn. 69 – Saunders/Vereinigtes Königreich.
24 EGMR, NJW 2002, 499, 501 m.w.N. – J. B./Schweiz; Dannecker, ZStW 2015, 991, 1004.
25 Dannecker, ZStW 2015, 370, 371.
26 Dannecker, ZStW 2015, 370, 371 f., 405 f.; EMGR, Urt. v. 27.09.2011, 43509/08, Rn. 45 – Menarini Diagnostics S.R.L./Italien.

Was die Anwendung des Art. 6 Abs. 1 EMRK auf die Bußgeldbestimmungen der DS-GVO betrifft, so ist zwar die EU selbst der EMRK nicht beigetreten, die EU-Mitgliedsstaaten, und damit die Träger der Datenschutzbehörden, haben die EMRK jedoch ratifiziert. Das Recht auf ein faires Verfahren wird zudem auch durch Art. 47 Abs. 2 S. 1 der Charta der Grundrechte der Europäischen Union (GRCh) gewährt. Über Art. 52 Abs. 3 GRCh ist die Auslegung des Art. 6 Abs. 1 EMRK bei der Auslegung des Art. 47 Abs. 2 S. 1 GRCh heranzuziehen. Über Art. 6 Abs. 1 EUV wird die GRCh zudem allgemein in das Gemeinschaftsrecht inkorporiert. Art. 6 Abs. 1 EMRK ist daher von den nationalen Datenschutzbehörden bei der Anwendung der Bußgeldvorschriften der DS-GVO zu berücksichtigen.[27]

b) EuGH

Der EuGH hat sich bislang im Zusammenhang mit kartellrechtlichen Sanktionen durch die Europäische Kommission gegenüber Unternehmen mit der Frage der Selbstbelastungsfreiheit auseinandergesetzt.[28] Das Gericht geht hierbei von einem äußerst begrenzten „Geständnisverweigerungsrecht" aus.[29] Nach den im Fall Orkem aufgestellten und später fortgeführten Grundsätzen gesteht der EuGH Unternehmen grundsätzlich den Schutz durch Art. 6 EMRK zu, und zwar auch in Verwaltungsverfahren, sofern diese zu Sanktionen führen können.[30] Das Gericht sieht die Grenze zur unzulässigen Selbstbelastung jedoch dann überschritten, wenn die Kommission durch eine Entscheidung, mit der Auskünfte angefordert werden, die Verteidigungsrechte des Unternehmens beeinträchtigt.[31] Dies soll erst dann der Fall sein, wenn dem Unternehmen die Verpflichtung auferlegt wird, Antworten zu erteilen, durch die es das Vorliegen einer Zuwiderhandlung eingestehen müsste, für die die Kommission den Beweis zu erbringen hat.[32] Demgegenüber soll es zulässig sein, das Unternehmen zu verpflichten, der Kommission alle erforderlichen Auskünfte über ihm eventuell bekannte Tatsachen zu erteilen und der Kommission erforderlichenfalls die in seinem Besitz befindlichen Schriftstücke, die sich hierauf beziehen, zu übermitteln, selbst wenn sie dazu verwendet werden können, den Beweis für ein wettbewerbswidriges Verhalten des betreffenden oder eines anderen Unternehmens zu erbringen.[33] Dieser Ansatz bleibt hinter dem Schutzniveau des Art. 6 Abs. 1 EMRK in der Auslegung des EGMR zurück.[34]

IV. Regelungen zur Lösung des Konflikts im deutschen Recht

1. Auskunftsverweigerungsrecht

Gemäß § 40 Abs. 4 S. 2 BDSG hat der gegenüber der Datenschutzbehörde Auskunftspflichtige, also der Verantwortliche oder Auftragsverarbeiter, das Recht, die Auskunft auf solche Fragen zu verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1-3 Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem OWiG aussetzen würde. Der Verweis auf die nahestehenden Personen ist erforderlich, da neben juristischen Person auch natürliche Personen Verantwortliche oder Auftragsverarbeiter sein können. Für diese hat es durchaus Sinn, nahestehende Personen einzubeziehen, ohne dass aber Unternehmen ausgenommen werden würden. Gemäß § 40 Abs. 4 S. 3 BDSG muss die Behörde den Auskunftspflichtigen auf das Auskunftsverweigerungsrecht hinweisen – ansonsten greift ein Beweisverwertungsverbot.[35] Das Auskunftsverweigerungsrecht umfasst nicht die Verweigerung von Auskünften zwecks Zugang zu Datenverarbeitungsanlagen und -geräten, z.B. durch Herausgabe des Passworts. Dies ist in § 40 Abs. 5 S. 1 BDSG gesondert geregelt.

Eine Einschränkung des Schutzes von Unternehmen resultiert nicht daraus, dass gemäß § 40 Abs. 4 S. 1 BDSG nicht nur die der Aufsicht unterliegenden Stellen, also der Verantwortliche und der Auftragsverarbeiter, einer Auskunftspflicht unterworfen werden, sondern auch die mit deren Leitung beauftragten Personen. Es wird vertreten, dass die Auskunftspflicht der mit der Leitung der jeweiligen Stelle beauftragten Personen mit den Regelungen der DS-GVO nicht vereinbar ist, da das Auskunfts- und Kooperationsrecht nach Art. 58 Abs. 1 lit. a) DS-GVO i.V.m. Art. 31 DS-GVO gegen den Verantwortlichen/Auftragsverarbeiter den Komplex bereits abschließend regelt.[36] Dem ist zuzustimmen, da Unternehmen nur durch ihre Leitungspersonen handeln können und sich diese daher auch für das Unternehmen auf das Auskunftsverweigerungsrecht berufen können müssen. Selbst wenn die mit der Leitung beauftragten Personen keinem Sanktionsrisiko ausgesetzt wären,[37] müssten sie das Auskunftsverweigerungsrecht zugunsten des Unternehmens ausüben können.[38] Da Unternehmen immer nur

27 Siehe zur Bindung der deutschen Datenschutzbehörden an die GRCh Spittka, Der Unternehmensbegriff der DSGVO in: Taeger, Rechtsfragen digitaler Transformationen, S. 117 (127 f.).

28 EuGH, Slg. 1989, 3283 – Orkem/Kommission; EuGH, EuR 2001, 427 – Mannesmannröhren-Werke/Kommission; EuGH, Slg. I 2006, 5943 – Kommission/SGL Carbon.

29 Schwarze/Bechtold/Bosch, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, 2008, S. 31; Dannecker, ZStW 2015, 370, 371.

30 EuGH, Slg. 1989, 3283, Rn. 31, 33 – Orkem/Kommission.

31 EuGH, Slg. 1989, 3283, Rn. 34 – Orkem/Kommission.

32 EuGH, Slg. 1989, 3283, Rn. 35 – Orkem/Kommission.

33 EuGH, Slg. 1989, 3283, Rn. 34 – Orkem/Kommission.

34 So auch Schwarze/Bechtold/Bosch, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, 2008, S. 32 ff.; Dannecker, ZStW 2015, 991, 1016.

35 Gola, in: Gola/Heckmann, BDSG, 13. Aufl. 2019, § 40, Rn. 28.

36 Die in § 40 Abs. 4 S. 1 enthaltene Auskunftspflicht der mit der Leitung der jeweiligen Stelle beauftragten Personen ist mit den Regelungen der DSGVO nicht vereinbar und kann damit vernachlässigt werden, Piltz, BDSG, § 40 Rn. 68 f.; a. A. Dix, in: Kühling/Buchner, DS-GVO BDSG, § 40 BDSG Rn. 12.

37 Für Sanktionierung Moos/Schefzig, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 83 DSGVO, Rn. 93; ablehnend Martini/Wagner/Wenzel, VerwArch 2018, 296 ff; wohl auch DSK, Entschließung v. 3.4.2019, Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! Es muss zudem auch § 42 Abs. 1 oder Abs. 2 BDSG berücksichtigt werden.

38 A. A. Dix, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 40 BDSG, Rn. 12.

über natürliche Personen handeln können, würde das Recht ansonsten leer laufen.

2. Verwendungsverbot

Laut § 43 Abs. 4 BDSG darf eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach Art. 34 Abs. 1 DS-GVO im Ordungswidrikeitenverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Abs. 1 Strafprozessordnung (StPO) bezeichneten Angehörigen[39] nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden. § 42 Abs. 4 BDSG enthält eine entsprechende Regelung für das Strafverfahren. Die bußgeldbewehrte Melde- bzw. Benachrichtigungspflicht des Verantwortlichen sowie die Meldepflicht des Auftragsverarbeiters werden durch ein Verwendungs- und damit auch Verwertungsverbot kompensiert, um das Spannungsverhältnis zu einer Selbstbelastung zu lösen.[40] Die Datenschutzbehörde darf die Informationen, welche sie direkt vom meldepflichtigen Verantwortlichen oder über eine Benachrichtigung der betroffenen Personen erhält daher grundsätzlich nicht für die Verhängung einer Geldbuße nach Art. 58 Abs. 2 lit. i) DS-GVO i.V.m. Art. 83 DS-GVO verwenden. Sofern Meldungen des Auftragsverarbeiters an den Verantwortlichen gemäß Art. 33 Abs. 2 DS-GVO an die Behörde gelangen, dürfen diese ebenfalls nicht für die Bebußung des Auftragsverarbeiters verwendet werden. Die Staatsanwaltschaft ist im Strafverfahren im selben Umfang an das Verwendungsverbot gebunden. Ein Verstoß resultiert in einem Beweisverwertungsverbot.

V. Vereinbarkeit der deutschen Regelungen mit der DS-GVO

1. Kritik an der Europarechtskonformität

Teilweise wird von Seiten der Datenschutzbehörden[41] und in der Literatur[42] vertreten, das Verwendungsverbot in § 43 Abs. 4 BDSG sei europarechtswidrig. Begründet wird dies damit, dass das Verwendungsverbot über diejenigen Verfahrensgarantien hinausgehe, die europarechtlich geboten seien.[43] Die grundsätzlich engere Auslegung des nemo tenetur-Grundsatzes auf europäischer Ebene impliziere eine Europarechtswidrigkeit.[44] Das Grundgesetz sei im Übrigen kein Prüfungsmaßstab.[45] Keine Bedenken werden gegen das strafprozessuale Verwendungsverbot nach § 42 Abs. 4 BDSG erhoben, da insoweit keine bindenden Vorgaben durch die DS-GVO bestünden.[46]

Eine vermittelnde Auffassung respektiert das Verwendungsverbot des § 43 Abs. 4 BDSG zwar grundsätzlich, will aber eine Ahndung von Datenschutzverstößen insoweit zulassen, als die Inhalte der Meldung im Rahmen des Aufsichtsverfahrens oder eines Bußgeldverfahrens von der Aufsichtsbehörde selber hätten ermittelt werden können. Hier solle die Rechtsprechung zu § 97 Insolvenzordnung (InsO) gelten.[47]

2. Stellungnahme

Die Kritik an § 43 Abs. 4 BDSG (und damit auch implizit an § 40 Abs. 4 S. 2 BDSG) hält einer näheren Betrachtung nicht stand. Zunächst ist die Annahme nicht zutreffend, dass nur Art. 6 Abs. 1 EMRK und Art. 47 Abs. 2 S. 1 GRCh, nicht aber das GG, Prüfungsmaßstab seien. Die deutschen Datenschutzbehörden sind auch an das GG gebunden, da die konkrete Anwendung auf Grundlage eines Anpassungs- und Umsetzungsgesetzes erfolgt.[48] Es ist zudem gerade nicht eindeutig, dass die Verwendungsverbote in §§ 40 Abs. 4 S. 2, 43 Abs. 4 BDSG über den Umfang des nemo tenetur-Grundsatzes i. S. d. Art. 6 Abs. 1 EMRK hinausgehen. Es dürfte zwar zutreffend sein, dass jedenfalls das Verwendungsverbot nach § 40 Abs. 4 S. 2 BDSG bei Auskunftspflichten über das enge Verständnis des EuGHs hinausgeht. Allerdings musste sich der EuGH bislang noch nicht mit einer bußgeldbewehrten aktiven Selbstanzeigepflicht auseinandersetzen. Die Pflichten nach Art. 33, 34 DS-GVO gehen deutlich über die, oft kritisierte,[49] Kronzeugenregelung im EU-Kartellrecht hinaus. Es ist also nicht absehbar, ob der EuGH den Zwang bei der Breach Notification noch für mit Art. 6 Abs. 1 EMRK vereinbar halten wird. Zudem muss auch die Auslegung des EGMR berücksichtigt werden. Gerade die Entscheidung J. B./Schweiz enthält zahlreiche Anhaltspunkte dafür, dass das umfassende Informationsrecht nach Art. 58 Abs. 1 lit. a) DS-GVO und erst recht die aktive Melde- und Benachrichtigungspflicht über die Grenzen einer zulässigen Einschränkung der Selbstbelastungsfreiheit hinausgehen. Zudem muss berücksichtigt werden, dass es sich bei der Auslegung des Art. 6 Abs. 1 EMRK durch den EGMR um eine case law-orientierte Entscheidungspraxis mit wenig dogmatischen Konturen handelt.[50] Solange der EGMR sich also nicht explizit zu den Pflichten unter der DS-GVO geäußert hat, ist es schlicht nicht absehbar, welche Bewertung das Gericht vornehmen wird.

Zudem stellt nicht jedes Verwendungsverbot nach mitgliedstaatlichem Recht einen Verstoß gegen die DS-GVO dar. Die Art. 58 Abs. 4, 83 Abs. 8 DS-GVO enthalten Öffnungsklauseln, damit die Ausübung der Befugnisse der Datenschutzbehörden vorbehaltlich geeigneter Garantien einschließlich ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des jeweiligen Mitgliedsstaates erfolgt. Vor dem Hintergrund, dass (i) es keine eindeutige Entscheidung des EGMR gegen die Gewährung umfassender

39 Auch dies ist nicht als Einschränkung auf natürliche Personen zu verstehen.

40 Der Gesetzgeber stellt ausdrücklich auf das Verbot einer Selbstbezichtigung ab, BT-Drs. 18/11325, S. 109.

41 LfDI Baden-Württemberg, 34. TB (2018), v. 04.02.2019, S. 17; a. A. LfDI Hamburg, 27. TB (2018), v. 21.02.2019, S. 52.

42 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 43 BDSG, Rn. 13.

43 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 43 BDSG, Rn. 13.

44 LfDI Baden-Württemberg, 34. TB (2018), v. 04.02.2019, S. 17.

45 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 43 BDSG, Rn. 10.

46 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 42 BDSG Rn. 60.

47 LfDI Hessen, 47. TB (2018), v. 31.12.2018, S. 172.

48 Spittka, DSRITB 2018, 117, 128 m.w.N.

49 Schwarze/Bechtold/Bosch, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, 2008, S. 33.

50 Dannecker, ZStW 2015, 991, 998.

Verwendungsverbote gibt, (ii) die Rechtsprechung des EuGH zur Selbstbelastungsfreiheit im Unionskartellrecht massiv kritisiert wird,[51] (iii) sich eine Änderung der Rechtsprechung des BVerfG zur Anwendung der Selbstbelastungsfreiheit für juristische Personen abzeichnet und (iv) in den letzten Jahren verstärkt ein Verständnis des nemo tenetur-Grundsatzes als prozessuale Gewährleistung gefordert wird,[52] muss den Mitgliedsstaaten hier Ermessensspielraum zugestanden werden. Der deutsche Gesetzgeber hat eine gut vertretbare Interpretation des sich entwickelnden Begriffs der Selbstbelastungsfreiheit vorgenommen. Es liegt gerade keine willkürliche Beschränkung der Rechte der Datenschutzbehörden – und damit mittelbar der betroffenen Personen – vor, die ja weiterhin verwaltungs- bzw. zivilrechtlich gegen Verantwortliche und Auftragsverarbeiter vorgehen können, da der nemo tenetur-Grundsatz unstreitig weder im Verwaltungsverfahren noch im Zivilprozess gilt.[53]

Eine Einschränkung des Verwendungsverbots unter Verweis auf § 97 InsO ist mit § 43 Abs. 4 BDSG nicht vereinbar. Das Verwendungsverbot in § 97 Abs. 1 S. 3 InsO schließt sogar etwaige Fernwirkungen mit ein,[54] sodass die Auskünfte nicht einmal als Grundlage für den Beginn gezielter Ermittlungen nach anderen selbstständigen Beweismitteln verwendet werden dürfen.[55] Die vom LfDI Hessen vorgenommene hypothetische ex post-Betrachtung soll gerade verhindert werden.

VI. Fazit

Das Auskunftsverweigerungsrecht in § 40 Abs. 4 S. 2 BDSG und das Verwendungsverbot in § 43 Abs. 4 BDSG sind mit dem Unionsrecht vereinbar und schaffen im Hinblick auf das Erfordernis eines fairen Verfahrens einen angemessenen Ausgleich zwischen den umfassenden Informations-, Kooperations- und Meldepflichten der DS-GVO und einem modernen Verständnis des nemo tenetur-Grundsatzes. Unternehmen müssen bei Auskunftsanfragen der Datenschutzbehörden und Bußgeldverfahren im Nachgang zu einem Data Breach eine dem Einzelfall angemessene und sinnvolle Verteidigungsstrategie wählen und dann konsequent durchhalten. Manchmal kann auch Kooperation der zielführende Weg sein.

Jan Spittka
Rechtsanwalt / Counsel, DLA Piper UK LLP, Köln.

51 Schwarze/Bechtold/Bosch, Rechtsstaatliche Defizite im Kartellrecht der Europäischen Gemeinschaft, 2008, S. 30 ff. m.w.N.

52 Dannecker, ZStW 2015, 370, 389 ff.; Dannecker, ZStW 2015, 991, 1011 ff.

53 Spittka, DSRITB 2016, 387, 397 f. m.w.N.

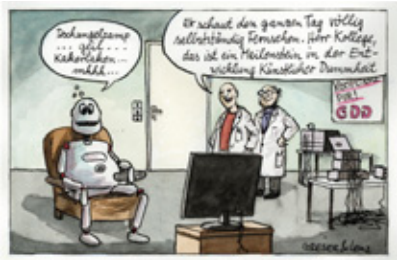
54 OLG Düsseldorf, BeckRS 2016, 127246; BT-Drs. 12/2443, 142.

55 BGH, BeckRS 2017, 127539; Werner, in: Fridgen/Geiwitz/Göpfert, BeckOK InsO, 14. Edition, Stand: 25.04.2019, § 97, Rn. 17.

BESUCHEN SIE DIE FACHTAGUNG ZUM THEMA DATENSCHUTZ!

43. DAFTA
21.–22. NOVEMBER 2019

MIT DEM 38. RDV-FORUM AM 20. NOVEMBER 2019



VON DER UNTERNEHMENSPRAXIS BIS ZUR KÜNSTLICHEN INTELLIGENZ (KI)

- Rund 350 Teilnehmer informieren sich auf neun verschiedenen Parallelforen rund um die Themen Datenschutz und Datensicherheit
- Top-Referenten führen durch Fachvorträge und spannende Diskussionsrunden
- Aussteller präsentieren ihre Lösungen und Tools für die Datenschutzpraxis
- Veranstaltung mit Tradition: Die DAFTA ist eine der größten Fachtagungen zum Thema Datenschutz in Europa
- In zehn Vortragsmodulen informieren Sie unsere Experten über Aktuelles im Umfeld von Datenschutz und Informationssicherheit. Seien auch Sie dabei!

Jetzt informieren und anmelden unter **dafta.de**
DATAKONTEXT GmbH · Postfach 41 28 · 50217 Frechen · Tel.: +49 22 34/989 49-40 · Fax: +49 22 34/989 49-44
Internet: datakontext.com · E-Mail: tagungen@datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Toshihiro Wada, LL.M.

Annahme des Angemessenheitsbeschlusses durch die EU für Japan

Der 23. Januar 2019 war ein wichtiger Tag für Datenschutzrechtler und -interessenten. Die Europäische Kommission (i. F. EU-Kommission) nahm den Angemessenheitsbeschluss bezüglich des japanischen Datenschutzniveaus gemäß Art. 45 Abs. 3 DS-GVO an.[1] Zugleich statuierte die japanische Datenschutzbehörde, die Personal Information Protection Commission (i. F. PPC), dass das Datenschutzniveau der EU mit dem japanischen vergleichbar sei.[2] Als Folge dieser Ereignisse wurde eine wechselseitige und freie Datenübermittlung zwischen dem Europäischen Wirtschaftsraum (i. F. EWR) und Japan unter Einhaltung eines hohen Datenschutzniveaus möglich. Vor der eingehenden Thematisierung einer sich abzeichnenden Globalisierung des Datenschutzes beschäftigt sich dieser Beitrag mit der Frage, was die Annahme des Angemessenheitsbeschlusses durch die EU für Japan bedeutet und wie die Datenübermittlung zwischen der EU und Japan stattfindet.

I. Bedeutung der gegenseitigen Anerkennung eines gleichwertigen Datenschutzniveaus zwischen der EU und Japan

1. Vorbild für zukünftige Angemessenheitsbeschlüsse

Der Prozess der bilateralen Anerkennung eines gleichwertigen Datenschutzniveaus zwischen der EU und Japan kann als ein erfolgreiches Beispiel für zukünftige Angemessenheitsbeschlüsse für Drittländer gesehen werden. Die EU-Kommission erkannte zum ersten Mal seit Entstehen der Norm das Datenschutzniveau eines Drittlandes als in den Grundzügen gleichwertig zu den Maßgaben der DS-GVO an. Die EU-Kommission und Japan führten nach der Mitteilung der EU-Kommission am 10. Januar 2017 im Rahmen eines Meinungsaustauschs mehrfach tiefgehende Gespräche.[3] Darüber hinaus besuchten die Kommissarin, der Kommissar, sowie Mitarbeiter und Mitarbeiterinnen der PPC die Datenschutzbehörden in den 16 EU-Mitgliedstaaten, während die Delegation des Europäischen Parlaments (i. F. EU-Parlament) im Ausgleich nach Tokio kam.[4] Die EU und Japan bemühen sich um das gegenseitige Verständnis im Hinblick auf das jeweilige Datenschutzrecht. An diesem Vorgehen könnten sich auch andere Länder orientieren, um dem Ziel eines Angemessenheitsbeschlusses näher zu kommen.

2. Ein Schritt zum internationalen Datenschutzstandard der DS-GVO

Die DS-GVO wird mittels des Angemessenheitsbeschlusses ein mittelbar geltender internationaler Datenschutzstandard. Die gegenseitige Anerkennung des gleichwertigen Datenschutzniveaus zwischen der EU und Japan fungierte folglich als ein Schritt in Richtung der globalen Verbreitung des europäischen Datenschutzstandards.

Das Drittland hat zur Datenübermittlung auf der Grundlage eines Angemessenheitsabschlusses ein angemessenes Schutzniveau i. S. d. Art. 45 Abs. 1 S. 1 DS-GVO zu schaffen. Dazu muss es keine mit den EU-Regelungen identischen Datenschutzvorschriften vorsehen, sondern ein der Sache nach gleichwertiges Schutzniveau gewährleisten, um angemessene Schutzstandards zu garantieren.[5] Art. 45 Abs. 2 Buchst. a bis c DS-GVO benennt die konkreten Prüfungspunkte, die bei der Entscheidung über die Gewährung eines Angemessenheitsbeschlusses relevant werden. Aufgrund dieser Vorgaben sind Drittländer wie Japan an den strengen Maßstab des europäischen Datenschutzrechts gebunden.

Der im September 2015 reformierte Act on the Protection of Personal Information (i. F. APPI) ist seit dem 30.05.2017 in Kraft.[6] Er wurde modernisiert und zielt auf die internationale datenschutzrechtliche Harmonisierung ab. Im Zuge dessen kann z.B. auch biometrisches oder genetisches Material als personenbezogene Information i. S. d. Art. 2 Abs. 1 APPI eingeordnet werden (Art. 2 Abs. 2 Nr. 1 APPI).[7] Konkretisiert werden die Anforderungen an die Verarbeitung

1 Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen, Stand: 19.03.2019, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019D0419&from=EN, zuletzt abgerufen am 16.04.2019.

2 PPC, The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force, Stand: 23.01.2019, https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/, zuletzt abgerufen am 07.05.2019.

3 EU-Kommission, Mitteilung der Kommission an das Europäische Parlament und der Rat, Austausch und Schutz personenbezogener Daten in einer globalisierten Welt, COM(2017) 7 final, Stand: 10.01.2017, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0007&from=DE, zuletzt abgerufen am 16.04.2019.

4 PPC, Ōshū kakkoku to no taiwa jisseki [Gespräch mit den europäischen Ländern], https://www.ppc.go.jp/enforcement/cooperation/cooperation/dialogues-Europe/, zuletzt abgerufen am 16.04.2019; Albrecht, Jan Philipp, Datenschutz und Freihandel mit Japan?, Stand: 31.10.2017, https://www.janalbrecht.eu/2017/10/2017-10-31-datenschutz-und-freihandel-mit-japan/, zuletzt abgerufen am 16.04.2019.

5 EuGH, Urteil vom 06.10.2015 – C-362/14, Schrems, Rn. 73-74.

6 Gesetz über den Schutz personenbezogener Informationen (Gesetz Nr. 57, 2003). Die Übersetzung in englischer Sprache (Stand: Dezember 2016) ist abrufbar unter https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf, zuletzt abgerufen am 23.04.2019. Die Terminologie des APPI in der übersetzten, deutschen Fassung entstammt dem Angemessenheitsbeschluss (Fn. 1).

7 Zum Begriff „personenbezogene Information", ErwgGr 18 im Angemessenheitsbeschluss (Fn. 1).

sensibler Daten (personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen) i. S. d. Art. 2 Abs. 3 APPI (z.B. Art. 17 Abs. 2 APPI) und anonymisierter Daten (anonym verarbeitete personenbezogene Informationen) i. S. d. Art. 2 Abs. 9 APPI (Art. 36 ff. APPI).[8] Zudem wurde – entsprechend der Vorgaben aus Art. 45 Abs. 2 DS-GVO – die Datenübermittlung an Dritte im Ausland normiert (Art. 24 S. 1 APPI) und die unabhängige Datenschutzbehörde PPC eingerichtet (Art. 40 ff. und Art. 59 ff. APPI).

Obwohl der modernisierte APPI bereits einige Ähnlichkeiten mit der DS-GVO aufweist, lassen sich immer noch erhebliche Unterschiede zwischen den beiden Regelwerken ausmachen. Die PPC schuf infolgedessen ergänzende Vorschriften, die als zusätzliche Garantie eines Anpassungsbestrebens wirken sollen und vor allem auf die Verarbeitung von personenbezogenen Daten, die aus dem EWR nach Japan übermittelt werden, Anwendung finden.[9] Der japanische Datenverarbeitende (personenbezogene Information handhabender Unternehmer) i. S. d. Art. 2 Abs. 5 APPI ist bei der Verarbeitung personenbezogener Daten aus dem EWR zur Einhaltung dieser ergänzenden Vorschriften verpflichtet.[10]

3. Wirtschaftlicher Aspekt

Man muss die Datenübermittlung zwischen dem EWR und Japan im Zusammenhang mit dem Wirtschaftspartnerschaftsabkommen betrachten, welches seit dem 1. Februar 2019 in Kraft ist. Die EU-Kommission erklärte schon 2015 in ihrem Vorschlag zum „Handel für alle", dass das Freihandelsabkommen und das Abkommen über den Handel mit Dienstleistungen (TiSA) durch Regeln für den elektronischen Geschäftsverkehr und den grenzüberschreitenden Datenverkehr ergänzt werden soll und die EU gegen neue Formen des digitalen Protektionismus vorgehen wird. Davon bleiben die bestehenden Datenschutzregelungen unberührt.[11]

Die datenschutzrelevante Zusammenarbeit zwischen der EU und Japan findet in verschiedenen Bereichen statt. So stellt beispielsweise Art. 8.63 des Wirtschaftspartnerschaftsabkommens auf den Datentransfer und den Schutz personenbezogener Daten im Finanzdienstleistungssektor ab.[12] Im Lichte des Verbraucherschutzes beschäftigen sich die EU und Japan mit dem Schutz personenbezogener Daten von Nutzern des elektronischen Geschäftsverkehrs gemäß Art. 8.78 Abs. 3 des Wirtschaftspartnerschaftsabkommens.

4. Wege zur Datenübermittlung aus dem EWR nach China

In Anbetracht der vorangegangenen Darstellungen stellt sich im Umkehrschluss die Frage, warum die EU bislang noch in keine konkreten Verhandlungen mit China über den gemeinsamen Datenschutz getreten ist.[13] China spielt für die EU als Handelspartner eine sehr große Rolle.[14] In der Zukunft wird der Datenschutz im Handelsverkehr mit China für die europäischen Bürgerinnen und Bürger daher sicherlich relevant.

In den letzten Jahren konnte man die Entwicklung eines chinesischen Datenschutzrechts beobachten.[15] Von Bedeutung ist hier insbesondere der sog. Nationalstandard „Information security technology – Personal information security specification" (i. F. Nationalstandard), der seit dem 1. Mai 2018 Geltung besitzt.[16] Er besteht aus einer Präambel, einem Vorwort, 54 Artikeln, vier Anhängen sowie einem von fremden Datenschutzregelungen geprägtem Literaturverzeichnis. Er hat keine rechtliche Verbindlichkeit, sondern wird als orientierungsstiftende Richtlinie angesehen.[17] Er zielt auf die sichere und angemessene Behandlung der personal information i. S. d. Art. 3.1 Nationalstandard sowie einer durch Datenschutz erreichten Verbesserung des gesellschaftlichen Wohlergehens (general welfare) ab[18] und findet gemäß Art. 1 S. 2 Nationalstandard sowohl im öffentlichen Sektor als auch Privatsektor Anwendung.[19]

8 Zum Begriff „personenbezogene Informationen, die einer besonderen Sorgfalt bedürfen", ErwgGr 65-69 im Angemessenheitsbeschluss (Fn. 1). Zum Begriff „anonym verarbeitete personenbezogene Informationen", ErwgGr 27-31 im Angemessenheitsbeschluss (Fn. 1). Zur Verarbeitung anonymisierter Daten im APPI, Geminn/Laubach/Fujiwara, ZD 2018, 413, 417-419.

9 Anhang I „Ergänzende Vorschriften nach dem Gesetz über den Schutz personenbezogener Informationen für die Handhabung von auf der Grundlage eines Angemessenheitsbeschlusses aus der EU übermittelten personenbezogenen Daten" im Angemessenheitsbeschluss für Japan (Fn. 1).

10 ErwgGr 15 im Angemessenheitsbeschluss für Japan (Fn. 1). Zum Begriff „personenbezogene Information handhabender Unternehmer" ErwgGr 32 bis 34 im Angemessenheitsbeschluss für Japan (Fn. 1).

11 EU-Kommission, Handel für alle, Stand: 2015, S. 14, http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153880.PDF, zuletzt abgerufen am 16.04.2019.

12 EU-Kommission, Vorschlag für einen Beschluss des Rates über den Abschluss des Wirtschaftspartnerschaftsabkommens zwischen der Europäischen Union und Japan, COM(2018) 192 final, 2018/0091 (NLE), Stand: 18.04.2018, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52018PC0192#document2, zuletzt abgerufen am 16.04.2019.

13 Krempl, Stefan, Microsoft-Präsident: Europa muss die Welt beim Datenschutz führen, Stand: 15.02.2019, https://www.heise.de/newsticker/meldung/Microsoft-Praesident-Europa-muss-die-Welt-beim-Datenschutz-fuehren-4310022.html, zuletzt abgerufen am 16.04.2019.

14 EU-Kommission, Countries and regions, China, Stand: 07.05.2019, http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/, zuletzt abgerufen am 07.05.2019.

15 Luo, Yan/Lu, Raymond/Yu, Zhijing, China Privacy Developments in 2018, Stand: 04.01.2019, https://wp.nyu.edu/compliance_enforcement/2019/01/04/china-privacy-developments-in-2018/, zuletzt abgerufen am 16.04.2019.

16 GB/T 35273–2017. Der Originaltext ist abrufbar unter https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf, zuletzt abgerufen am 16.04.2019. Die nicht offizielle Übersetzung in englischer Sprache ist abrufbar unter https://www.chinalawtranslate.com/en/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E8%A7%84%E8%8C%83/, Stand: 30.01.2018, zuletzt abgerufen am 16.04.2019. Siehe auch Luo, Yan, China Releases Draft Amendments to the Personal Information Protection Standard, Stand: 11.02.2019, https://www.insideprivacy.com/international/china/china-releases-draft-amendments-to-the-personal-information-protection-standard/, zuletzt abgerufen am 09.05.2019.

17 Delval, Galaad, Old rules, new specification for data protection in mainland China, Stand: 03.05.2018, https://iapp.org/news/a/old-rules-new-specification-for-data-protection-in-mainland-china/, zuletzt abgerufen am 16.04.2019.

18 Siehe hierzu Vorwort im Nationalstandard (Fn. 16).

19 Luo, Yan/Bradley-Schmieg, Philippe, China Issues New Personal Information Protection Standard, Stand: 25.01.2018, https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/, zuletzt abgerufen am 23.04.2019.

Der Nationalstandard verwendet dem EU-Recht vergleichbare Begriffe für personenbezogene (Art. 3.1 Nationalstandard) und sensible Daten (Art. 3.2 Nationalstandard).[20] Art. 4 Buchst. a bis g Nationalstandard regelt Grundsätze für die Sicherheit der personal information. Sie sind mit den Grundsätzen aus den basic principles of national application im Guidelines governing the protection of privacy and transborder flows of personal data von OECD vergleichbar.[21] Gemäß Art. 5.3 Buchst. a und Art. 4 Buchst. c Nationalstandard muss der personal data controller i. S. d. Art. 3.4 Nationalstandard i. d. R. eine Einwilligung vom personal data subject i. S. d. Art. 3.3 Nationalstandard einholen, bevor er die personal information erhebt bzw. verwendet.[22] Aufgrund der mehrfachen Zitation von Dokumenten der EU, den USA, dem OECD und APEC im Nationalstandard kann man annehmen, dass China scheinbar ein grundsätzliches Interesse an einer datenschutzrechtlichen Harmonisierung besitzt.[23]

Allerdings erschwert der Unterschied der Rechtskulturen die potentielle Ausstellung eines Angemessenheitsbeschlusses für China. Hervorzuheben ist vor allem, dass die in Art. 45 Abs. 2 a DS-GVO geforderte Achtung und Gewährleistung der Menschenrechte und der Grundfreiheiten hinter dem europäischen Standard zurückbleiben.[24] Darüber hinaus bedroht die staatliche Zensur Chinas die freie Nutzung des Internets durch die Bürgerinnen und Bürger. Diese Punkte widersprechen den Grundprinzipien des europäischen Datenschutzrechts.

Das EU-Parlament besitzt dennoch keine grundsätzlich ablehnende Einstellung in Bezug auf die Datenübermittlung aus dem EWR nach China. Eine Untersagung von Datenübertragungen zwischen der EU und China sei nicht praktikabel.[25] Die Entwicklung des Cloud-Computing und die daraus entstehende Datenübermittlung wirkten als überzeugende technische Argumente und stützten damit diese Ansicht.[26] Vor diesem Hintergrund versucht die EU, die sichere Datenübermittlung über ein bilaterales Abkommen zwischen der EU und China sowie über ein sog. Privacy Shield mit den USA zu ermöglichen. Das EU-Parlament entsendete daher bereits eine Delegation aus dem Ausschuss „Bürgerliche Freiheiten, Justiz und Inneres (LIBE)“ nach China.[27] Im Umkehrschluss wurde dem EU-Parlament eine Anfrage hinsichtlich der Übermittlung personenbezogener Daten vom EWR nach China vorgelegt.[28] Aktuell finden zudem entsprechende Verhandlungen zwischen der EU und China statt.

II. Datenübermittlung von Japan in den EWR

1. Begriff der Übermittlung

In Japan liegt eine Übermittlung i. S. d. Art. 23 Abs. 1 APPI dann vor, wenn der Datenverarbeitende nicht nur sich selbst, sondern auch dem anderen Datenverarbeitenden personenbezogene Daten i. S. d. Art. 2 Abs. 6 APPI oder gespeicherte personenbezogene Daten i. S. d. Art. 2 Abs. 7 APPI zur Verfügung stellt.[29] Es muss keine körperliche Übermittlung stattfinden, eine Distribution personenbezogener Daten über ein digitales Netzwerk reicht aus.[30] Ein Datenaustausch zwischen den unterschiedlichen Abteilungen derselben juristischen Person wird jedoch nicht als Datenübermittlung i. S. d. Art. 23 Abs. 1 APPI angesehen.

2. Einwilligung

Wegen des Angemessenheitsbeschlusses werden die Voraussetzungen an die Einholung einer Einwilligung von der betroffenen Person abgemildert. Der Datenverarbeitende muss gemäß Art. 24 S. 1 APPI eine Einwilligung bezüglich der Datenübermittlung an den Dritten im Ausland einholen. Da die PPC das Datenschutzniveau der EU anerkannte, reicht schon die Einwilligung in die Datenübermittlung an den Dritten ebenso wie die inländische Datenübermittlung gemäß Art. 23 Abs. 1 APPI.

3. Entfallen einer Einholung der Einwilligung von der betroffenen Person

Art. 23 Abs. 1 Nr. 1 bis 4 APPI regelt das Entfallen einer Einwilligung von Seiten der betroffenen Person. So können bestimmte grenzüberschreitende Datenübermittlungen ausnahmsweise ohne Einwilligung erfolgen. Dies ist z.B. dann der Fall, wenn eine gesetzliche Gestattung angeordnet ist oder die Einholung einer Einwilligung mit erheblichen Schwierigkeiten, etwa bei Bestehen von Lebensgefahr, verbunden ist oder aufgrund des vorrangigen Schutzes von Körpers und Vermögens unzumutbar und somit entbehrlich wird.

4. Empfänger als Nichtdritter

Falls die Tochtergesellschaft in Japan und die Muttergesellschaft in Deutschland personenbezogene Daten i. S. d. Art. 2 Abs. 6 APPI, wie Kunden- oder Arbeitnehmerdaten, nur unter dem bei der Erhebung festgelegten Verwendungszweck zusammen nutzen wollen, ist die Muttergesellschaft als Empfängerin gemäß Art. 23 Abs. 5 Nr. 3 APPI nicht als Dritte einzuordnen.[31] Infolgedessen kann die Datenübermittlung von Japan in den EWR ohne Einwilligung stattfin-

20 Siehe auch Anhang A Tabelle A. 1 und Anhang B Tabelle B. 1 im Nationalstandard (Fn. 16).

21 OECD, the OECD privacy framework, Stand: 2013, S. 14-15, http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, zuletzt abgerufen am 11.04.2019.

22 Siehe zum Entfallen der Einwilligung Art. 5.4 Buchst. a bis k Nationalstandard. Zur Einwilligung Sacks, Samm, China's Emerging Data Privacy System and GDPR, Stand: 09.03.2018, https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr, zuletzt abgerufen am 16.04.2019.

23 Siehe hierzu Literaturverzeichnis im Nationalstandard (Fn. 16), S. 29.

24 EU-Parlament, The data protection regime in China, Stand: Oktober 2015, S. 7, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf, zuletzt abgerufen am 16.04.2019.

25 Monteleone, Shara, Personal data transfers to China, Stand: am 20.06.2016, http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/583836/EPRS_ATA(2016)583836_EN.pdf, zuletzt angerufen am 28.03.2019.

26 Monteleone (Fn. 25).

27 Monteleone (Fn. 25).

28 EU-Parlament, Parlamentarische Anfragen, Stand: 01.03.2016, http://www.europarl.europa.eu/doceo/document/O-8-2016-000036_DE.html, zuletzt abgerufen am 23.04.2019.

29 Zum Begriff „personenbezogene Daten“, ErwgGr 19 bis 22 im Angemessenheitsbeschluss für Japan (Fn. 1). Zum Begriff „gespeicherte personenbezogene Daten“, ErwgGr 23-26 im Angemessenheitsbeschluss (Fn. 1).

30 PPC, Kojin jōhō no hogo ni kansuru hōritsu ni tsuite no gaidorain (tsūsoku hen), [Richtlinien über APPI (Allgemeiner Teil)], Stand: Januar 2019, S. 25, abrufbar unter https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf, zuletzt abgerufen am 16.04.2019.

31 PPC, (Fn. 30), S. 52-54.

den. In diesem Fall muss die Tochtergesellschaft in Japan der betroffenen Person jedoch ankündigen oder zuvor bekanntmachen,

- dass Kunden- oder Arbeitnehmerdaten gemeinschaftlich genutzt werden,
- welche spezifischen Kategorien von Daten betroffen sind,
- mit wem und zu welchem Zweck diese gemeinschaftlich genutzt werden und
- wer für die gemeinschaftliche Nutzung verantwortlich ist.

Eine Datenübermittlung zwischen der Mutter- und der Tochtergesellschaft wird i. d. R. der Datenübermittlung an den Dritten gemäß Art. 23 Abs. 1 APPI zugeordnet. Die oben genannte Ausnahme ist in der Praxis praktikabel und relevant.

5. Aufzeichnungspflicht bei der Datenübermittlung

Der Datenverarbeitende als Veräußerer muss gemäß Art. 25 Abs. 1 S. 1 APPI i.V.m. den Durchsetzungsvorschriften zum Gesetz über den Schutz personenbezogener Informationen (i. F. PPC-Vorschriften) aufzeichnen, wann und an wen er personenbezogene Daten i. S. d. Art. 2 Abs. 6 APPI übermittelte, es sei denn die Übermittlung fällt unter eine der in Art. 25 Abs. 1 S. 2 i.V.m. Art. 23 Abs. 1 Nr. 1 bis 4 oder Abs. 5 Nr. 1 bis 3 APPI genannten Ausnahmen.[32] Der Datenverarbeitende hat gemäß Art. 25 Abs. 1 S. 1 APPI i.V.m. Art. 12 Abs. 1 PPC-Vorschriften die Wahl zwischen einer schriftlichen, elektronischen oder einer Aufzeichnung in der Gestalt eines Mikrofilms. Gemäß Art. 25 Abs. 2 APPI i.V.m. Art. 14 Nr. 1 bis 3 PPC-Vorschriften ist der Datenverarbeitende zur Verwahrung der Aufzeichnung verpflichtet.

III. Verarbeitung personenbezogener Daten vom EWR in Japan nach den ergänzenden Vorschriften

1. Sensible Daten

Anders als in Art. 9 Abs. 1 DS-GVO zählen nicht zu den sensiblen Daten i. S. d. Art. 2 Abs. 3 APPI: personenbezogene Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht, sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die erste ergänzende Vorschrift stuft diese Informationen jedoch in die Kategorie sensibler Daten i. S. d. Art. 2 Abs. 3 APPI ein.[33] Deshalb muss der Datenverarbeitende in Japan diese dennoch wie sensible Daten behandeln. Der Datenverarbeitende hat eine Einwilligung von der betroffenen Person einzuholen, es sei denn, eine der Ausnahmen aus Art. 17 Abs. 2 Nr. 1 bis 6 APPI ist einschlägig, etwa, wenn eine gesetzliche Gestattung oder Schwierigkeiten bei der Einholung der Einwilligung von der betroffenen Person im Hinblick auf den Schutz des Lebens, des Körpers oder des Vermögens vorliegen.

2. Gespeicherte personenbezogene Daten

Zu personenbezogenen Daten i. S. d. Art. 2 Abs. 6 APPI gehören gespeicherte personenbezogene Daten i. S. d. Art. 2 Abs. 7 APPI, die nach Art. 5 Kabinettsverordnung zur Durchsetzung des Gesetzes über den Schutz personenbezogener Informationen (i. F. Kabinettsverordnung) über einen Zeitraum von mehr als sechs Monaten gespeichert werden.[34] Im Kontext von gespeicherten personenbezogenen Daten geht es um Rechte Einzelner (Art. 28 bis 30 APPI), die den Rechten der betroffenen Person im Kapitel 3 der DS-GVO ähnlich sind. Nach der zweiten ergänzenden Vorschrift werden die aus dem EWR nach Japan übermittelten personenbezogenen Daten unabhängig von der sechsmonatigen Zeitdauer zwischen dem Anfang ihrer Speicherung und ihrer Löschung als gespeicherte personenbezogene Daten angesehen.[35] EU-Bürgerinnen und EU-Bürger können deshalb ihre Rechte als betroffene Person auch in Japan ausüben.

3. Verwendungszweck personenbezogener Daten

Der Grundsatz der Datenminimierung findet auch in Japan Geltung. Der Datenverarbeitende als Empfänger muss gemäß Art. 26 Abs. 1 S. 1 Nr. 2 APPI im Zeitpunkt der Datenerhebung prüfen und wissen, wie der Vorgänger als Übermittelnder im EWR personenbezogene Daten erhoben hat und welcher Verwendungszweck festgelegt wurde, es sei denn, es liegt eine Ausnahme gemäß Art. 26 Abs. 1 S. 2 i.V.m. Art. 23 Abs. 1 Nr. 1 bis 4 oder Abs. 5 Nr. 1 bis 3 APPI vor. Diese Informationen muss der Datenverarbeitende bei Empfang der personenbezogenen Daten gemäß Art. 26 Abs. 1 S. 1 und Abs. 3 APPI festhalten.[36] Der Datenverarbeitende hat gemäß Art. 15 Abs. 1 APPI den Verwendungszweck zu bestimmen. Der Nutzungsumfang der personenbezogenen Daten ist gem. Art. 16 Abs. 1 APPI auf das für den zuvor festgelegten Verwendungszweck begrenzte, notwendige Maß zu beschränken, sofern der Datenverarbeitende noch keine Einwilligung in die über den Verwendungszweck hinausgehende Verarbeitung von der betroffenen Person eingeholt hat.

4. Weitergabe vom EWR übermittelter personenbezogener Daten aus Japan ins Ausland außerhalb des EWR

Auch bei einer Weitergabe gemäß Art. 45 DS-GVO der aus dem EWR übermittelten personenbezogenen Daten aus Japan ins Ausland außerhalb des EWR kommt Art. 24 APPI zur Anwendung.[37] Mithin bedarf es gemäß Art. 24 S. 1 APPI i. d. R. einer Einwilligung von der betroffenen Person in die Datenübermittlung an den Datenverarbeitenden im Ausland.

32 Zu den von der PPC verkündeten Durchsetzungsvorschriften zum Gesetz über den Schutz personenbezogener Informationen (Vorschriften der Kommission für den Schutz personenbezogener Informationen Nr. 3, 2016), ErwgGr 12 im Angemessenheitsbeschluss (Fn. 1). Die Übersetzung in englischer Sprache (Stand: Dezember 2016) ist abrufbar unter https://www.ppc.go.jp/files/pdf/PPC_rules.pdf, zuletzt abgerufen am 18.04.2019.

33 Ergänzende Vorschriften (1) (Fn. 9).

34 Kabinettsverordnung zur Durchsetzung des Gesetzes über den Schutz personenbezogener Informationen (Kabinettsverordnung Nr. 507, 2003). Die Übersetzung in englischer Sprache (Stand: Dezember 2016) ist abrufbar unter https://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf, zuletzt abgerufen am 18.04.2019.

35 Ergänzende Vorschriften (2) (Fn. 9).

36 Ergänzende Vorschriften (3) (Fn. 9).

37 Ergänzende Vorschriften (4) (Fn. 9).

5. Anonymisierte Daten

Der Anonymisierungsprozess wird bei personenbezogenen Daten aus dem EWR verschärft.[38] Falls der Datenverarbeitende personenbezogene Daten aus dem EWR anonymisieren will, bedarf es unmittelbar nach der Anonymisierung der Vernichtung der Informationen darüber, welche Beschreibung von den aus dem EWR nach Japan übermittelten personenbezogenen Daten ausgenommen wurde und welche technische Schritte im Anonymisierungsprozess verwendet wurden. Erst wenn die betroffene Person nach dem Löschvorgang nicht mehr identifiziert werden kann, kann von anonymisierten Daten i. S. d. Art. 2 Abs. 9 APPI gesprochen werden.

IV. Ausblick

Die japanische Digitalpolitik befindet sich in der nächsten Phase. Japan hat das Ziel, geeignete Rahmenbedingungen für die internationale Datenübermittlung zu schaffen. Der japanische Premierminister Shinzō Abe präsentierte diese Zielsetzung des „Data Free Flow with Trust (i. F. D.F.F.T.)" im Weltwirtschaftsforum in Davos.[39] Er betonte den immensen Nutzen und Wert von Daten. Während personenbezogene Daten geschützt werden müssten, sollten anonymisierte Daten mit Relevanz für die Bereiche Medizin, Industrie oder Straßenverkehr grenzüberschreitend und frei übermittelt werden können.[40] Der Gedanke und Vorschlag des D.F.F.T. zählte neben dem Klimawandel zu den besonders wichtigen Diskussionsthemen im Rahmen des G20-Gipfels in Osaka am 28. und 29. Juni 2019.[41]

Toshihiro Wada LL.M.
Der Verfasser ist wissenschaftliche Hilfskraft der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Westfälischen Wilhelms-Universität Münster.

38 Ergänzende Vorschriften (5) (Fn. 9).

39 World Economic Forum, 'Defeatism about Japan is now defeated': Read Abe's Davos speech in full, Stand: 23.01.2019, https://www.weforum.org/agenda/2019/01/abe-speech-transcript/, zuletzt abgerufen am 16.04.2019.

40 World Economic Forum (Fn. 39).

41 World Economic Forum (Fn. 39).

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (42): Weitere Aspekte zur Benennung von Datenschutzbeauftragten

Zusammengestellt und erläutert von Prof. Peter Gola*

Auch die im April/Mai 2019 erschienenen Tätigkeitsberichte des LfD Bayern, des ULD Schleswig-Holstein, des LfDI Mecklenburg-Vorpommern und des ULD des Saarlands befassen sich mit aktuellen Fragen der Benennung von Datenschutzbeauftragten.

I. Voraussetzungen der Bestellpflicht bei privaten Datenverarbeitern

1. Die umfangreiche Verarbeitung

Das Unabhängige Datenschutzzentrum Saarland erörtert die Auslegung zweier die Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter festlegender unbestimmter Rechtsbegriffe (27. TB, 2017/2018, Abschn. 9). Dabei geht es einmal um den Begriff „umfangreich" gemäß Art. 37 DS-GVO. Art. 37 Abs. 1 DS-GVO verlangt auf jeden Fall die Benennung eines Datenschutzbeauftragten, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische

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

Überwachung von betroffenen Personen erforderlich machen, oder wenn sie in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht. Wann eine umfangreiche Datenverarbeitung vorliegt, wird zwar nicht in dem Verordnungstext, aber in dem gleichwohl vagen Erwägungsgrund 91 der DS-GVO zumindest angedeutet. Gemeint sind u.a. solche Verarbeitungen, die eine große Menge personenbezogener Daten oder eine große Zahl von Personen betreffen und die wahrscheinlich – beispielsweise aufgrund ihrer Sensibilität – ein hohes Risiko mit sich bringen, sowie Verarbeitungsvorgänge, bei denen in großem Umfang neue Technologien eingesetzt werden, oder solche, denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen immanent ist.

Bezüglich einer Datenverarbeitung durch Ärzte, Apotheker und sonstige Angehörige eines Gesundheitsberufes hat die DSK, vorbehaltlich einer anderslautenden Regelung durch den Europäischen Datenschutzausschuss (EDSA), im Beschluss vom 26. April 2018 versucht eine eindeutige Lösung zu finden, indem dann von einer umfangreichen Datenverarbeitung auszugehen ist, wenn mindestens zehn Beschäftigte mit der personenbezogenen Datenverarbeitung betraut sind, was dann aber auch bis dato nicht mehr die Verarbeitung von Gesundheitsdaten bedingt, falls die Verarbeitung „ständig" erfolgt (§ 38 Abs. 1 BDSG). Zu beachten ist, dass nach Auffassung der DSK der Arzt bei der Personenzahl mit zu berücksichtigen ist. Gestützt wird diese Auffassung auf Erwägungsgrund 91 zur DS-GVO, in dem es heißt: „Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt." Dem folgend soll sowohl bei Einzelpraxen als auch bei Gemeinschaftspraxen in der Regel nicht von einer umfangreichen Datenverarbeitung im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen sein.

2. Die ständige Verarbeitung

Obwohl das die Bestellpflicht nach § 38 Abs. 1 S. 1 BDSG mitbestimmende Tatbestandsmerkmal der „ständigen" Beschäftigung bei der Datenverarbeitung aus den Vorschriften des BDSG a.F. übernommen wurde, wird es auch jetzt noch unterschiedlich ausgelegt (vgl. Gola, Bericht Aufsichtsbehörden, RdV 2019, 131) Das Unabhängige Datenschutzzentrum des Saarlands hält an seiner Rechtsauslegung des Begriffs vor Wirksamwerden der DS-GVO fest, indem eine Person ständig mit der Datenverarbeitung beschäftigt ist, wenn sie auf unbestimmte Zeit mit der Verarbeitung personenbezogener Daten betraut ist. Dabei spielen weder die Arbeitszeit noch der Zeitpunkt der Aufgabenübertragung eine Rolle. Sowohl der gerade erst eingestellte Arbeitnehmer bzw. derjenige, der gerade erst mit der Datenverarbeitung beauftragt ist, als auch der Teilzeitbeschäftigte sind mit zu berücksichtigen, sofern nur das Beschäftigtsein mit der Datenverarbeitung auf unbestimmte Zeit gerichtet ist (vgl. bereits Linnenkohl, Der betriebliche Beauftragte für den Datenschutz, NJW 1979, S. 1190 ff.; Gola/Schomerus, BDSG, 12. Aufl. (2015), § 4f Rn. 11).

3. Umfangreiche Überwachung als „Kerntätigkeit" in Kindertagesstätten

Bei Kindertagesstätten in privater Trägerschaft sieht das ULD Schleswig-Holstein (37. TB, 2017/2018, Abschn. 5.4.3) eine DSB-Bestellpflicht bereits nach Art. 37 Abs. 1 lit.b DS-GVO gegeben, weil die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen. Zur Kerntätigkeit eines Verantwortlichen gehören alle Vorgänge, die einen festen Bestandteil seiner Haupttätigkeit darstellen. Dieser Tatbestand sei in Kindertagesstätten durch das systematische Beobachten und Dokumentieren der kindlichen Entwicklung als Bestandteil der Arbeit der Erzieherinnen und Erzieher erfüllt. Kontinuierliche Beobachtung und eine darauf aufbauende Bildungsdokumentation seien notwendig, um Kinder und ihre Lernprozesse zu verstehen und um sie als Grundlage von Gesprächen mit dem Team, den Eltern und der Grundschule nutzen zu können, wobei es keine Rolle spiele, ob diese Dokumentation in elektronischer oder konventioneller Form geführt werde.

Eine weitere Voraussetzung für die Benennungspflicht ist, dass die Beobachtungs- und Entwicklungsdokumentation als „umfangreiche regelmäßige und systematische Beobachtung" im Sinne von Art. 37 Abs. 1 lit.b DS-GVO zu qualifizieren ist. Dies treffe zu, da mit der Dokumentation die Entwicklungsfortschritte, Verhaltensänderungen und das Sozialverhalten und damit der Verlauf der Entwicklungsschritte der Kinder festgehalten werden um die geistige, sprachliche und motorische Entwicklung, die Vorlieben, Interessen und das Verhalten der Kinder zu analysieren. Daneben könnte aber auch – abhängig von dem Personalbestand der Kindertagesstätte – die 10-Personen-Regelung" des § 38 Abs. 1 S. 1 BDSG greifen.

4. Die „Zehn Personen"-Regelung

a) Allgemeines

Dazu, wie die nach § 38 Abs. 1 S. 1 BDSG maßgebende 10- bzw. zukünftig 20-Personen-Grenze zu ziehen ist, gibt das ULD Schleswig-Holstein (37. TB, 2017/2018, Abschn. 5.4.2) beispielhafte Hinweise. Nach Auffassung des ULD hatte der Gesetzgeber bereits bei der Vorgängervorschrift im alten Bundesdatenschutzgesetz die Intention, eine „Beschäftigung" von Personen nicht nur für Arbeitnehmer, sondern etwa auch für Auszubildende oder freie Mitarbeiter anzunehmen. Diese Intention habe sich mit der Geltung der Neuregelung seit dem 25.05.2018 nicht geändert, zumal der Gesetzgeber auch vom Wortlaut her gesehen die Altregelung übernommen hat. Jegliche Personen, welche Zugriff auf Kundendatenbanken nehmen, etwa vertragliche Unterlagen einsehen können, Personaldaten verwalten oder in automa-

tisierter Form personenbezogene Daten verarbeiten, müssen bei der Frage der Verpflichtung zur Benennung eines Datenschutzbeauftragten mitgezählt werden.

b) Kassenpersonal

Mitarbeiterinnen und Mitarbeiter an Kassen, die lediglich eine EC-oder Kundenkarte einlesen, jedoch nicht auf eine Kundendatenbank mit Daten zugreifen oder gegebenenfalls nur manuell die Kontodaten auf der Karte in Augenschein nehmen, jedoch nicht in automatisierter Form zur Kenntnis nehmen können, insbesondere nicht nach Abschluss des Bezahlvorgangs, sind dagegen nicht mitzuzählen.

c) Monteure im Handwerk

Bei der Anwendung der 10-Personen-Regel im Zusammenhang mit der Beauftragung von Monteuren in Handwerksbetrieben ist nach Auffassung des ULD zu differenzieren. Erhalten die Monteure lediglich die Kontaktdaten der Kunden sowie Angaben zur Ausführung eines Auftrags, der vor Ort erledigt werden soll, so sind diese Personen nicht mitzuzählen. Diese Einschätzung beruht auf der Annahme, dass in diesen Fällen nur sehr wenige personenbezogene Daten flüchtig zur Kenntnis genommen werden, dies oft nicht in automatisierter Form erfolgt und entsprechende Angaben nicht im dauerhaften Zugriff der Monteure verbleiben. Anders wäre der Sachverhalt zu beurteilen, wenn die Monteure einen Zugriff auf eine Kundendatenbank erhalten und etwa dauerhaft Auftragshistorien abrufen können. Im letzteren Fall wären die Monteure im Rahmen der 10-Personen-Regel mitzuzählen.

d) Betreuer in Sportvereinen

Bei Sportvereinen stellt sich die Frage, ob bei den 10 automatisiert personenbezogenen Daten verarbeitenden Personen Betreuer mitgezählt werden müssen, die z.B. auf Datenbanken mit Angaben zu Mitgliedern und Sportlerinnen und Sportlern bestimmungsgemäß Zugriff nehmen. Verarbeiten Trainer Spielerdaten wie etwa Trainings-und Wettkampfergebnisse, Kontaktdaten der Spieler, Angaben zum Gesundheitszustand, zum Muskelaufbau und zur Ernährung, so sind auch diese hinzuzuzählen. Sportvereine müssen dabei den Überblick darüber haben, welche Mitglieder welche personenbezogenen Daten der Sportlerinnen und Sportler „ständig“ verarbeiten und zu Datenzugriffen autorisiert sind, um die Verpflichtung zur Benennung eines Datenschutzbeauftragten nachzukommen.

II. Bestellpflicht bei Behörden

1. Allgemeines

In seinem 37. Tätigkeitbericht geht das ULD Schleswig-Holstein auch grundlegend auf die geänderte Regelungen zur Benennung – d.h. unter dem von dem deutschen Datenschutzrecht vor Geltung der DS-GVO verwendeten deckungsgleichen Begriff der „Bestellung“ – behördlicher Datenschutzbeauftragter ein, die seit dem 25.5.2018 für alle als Verantwortliche und Auftragsverarbeiter agierende Behörden oder öffentliche Stellen gilt. Ausgenommen sind nur Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln. Die Benennungspflicht trifft alle öffentlichen Stellen, unabhängig von der Größe, namentlich die Landesbehörden und Kommunen und die von den letzteren gegründeten Zweckverbände und gemeinsamen Kommunalunternehmen. Erfasst sind z.B. aber auch kleine, ehrenamtlich arbeitende Wasser-und Bodenverbände, denn diese sind nach § 1 Wasserverbandsgesetz Körperschaften des öffentlichen Rechts. Eigenbetriebe zählen als Teil der Kommune. Daher geht das ULD davon aus, dass ein von der Kommune bestellter DSB auch für den Eigenbetrieb zuständig ist, soweit nicht der Eigenbetrieb einen eigenen DSB bestellt hat.

2. Kommunale Kindertagesstätten

Entsprechendes gilt für kommunale Kindertagesstätten (Kitas). Eine kommunale Kitas unterliegt Art. 37 Abs. 1 lit.a DS-GVO, da sie zwar regelorganisatorisch verselbstständigt, andererseits aber rechtlich ein Teil der Kommune und damit Teil einer öffentlichen Stelle sei. Nach Art. 37 Abs. 3 DS-GVO kann für mehrere öffentliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden. Daher kann z.B. der Datenschutzbeauftragte der Kommune auch Datenschutzbeauftragter der kommunalen Kita sein. Wenn für die Kita kein gesonderter Datenschutzbeauftragter benannt wurde, geht das ULD davon aus, dass der kommunale DSB auch für die kommunalen Kitas zuständig ist (ULD Schleswig Holstein, 37 TB, 2017/2018, Ziff. 5.4.3).

3. Bestellpflicht bei beliehenen Handwerksbetrieben

a) Allgemeines

Dazu, wann z.B. beliehene Handwerksbetriebe, also Berufsgruppen, welche zwar privatrechtlich organisiert sind und am freien Markt handwerklich-gewerbliche Dienstleistungen anbieten und zugleich als Beliehene im Rahmen ihrer Berufsausübung auch staatliche hoheitliche Aufgaben wahrnehmen, einen Datenschutzbeauftragten zu bestellen haben, und insbesondere dazu, ob sie insoweit auf Grund ihrer „Doppelstellung“ als Behörden zu behandeln sind, bezieht auch das Unabhängige Datenschutzzentrum des Saarlands Stellung (27. TB, 2017/2018, Abschn. 9.3). Betroffen sind das Schornsteinfegerwesen sowie Kfz-Werkstätten, die Kfz-Betriebstauglichkeitsuntersuchungen erbringen.

b) Schornsteinfeger

Nach der von dem Unabhängigen Datenschutzzentrum vertretenen Rechtsansicht ist das Schornsteinfegerwesen durch das Schornsteinfeger-Handwerksgesetz (Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk v. 26.11.2008 (BGBl. I S. 2242), zuletzt geändert d. Gesetz v. 17.7.2017 (BGBl. I S. 2495), nicht vollständig liberalisiert, indem bestimmte Tätigkeiten nach wie vor den bevollmächtigten Bezirksschornsteinfegern vorbehalten sind (Bsp. Feuerstättenschau), welche hierbei als Beliehene hoheitliche Tätigkeiten wahrnehmen (§ 8 i.V.m. §§ 14 ff. SchfHwG). Im Rahmen dieser Tätigkeit sind bevollmächtigte Bezirksschornsteinfeger Verantwortliche i. S. d.Art. 4 Nr. 7 DS-GVO,

§ 2 Abs. 1 S. 3 SaarlDSG und unterliegen der Pflicht, einen behördlichen Datenschutzbeauftragten nach Art. 37 Abs. 1 lit. a DS-GVO zu benennen.

c) AU-Kfz-Werkstätten

Gleiches gilt für Autowerkstätten, welche als gemäß Nr. 1.1 Anlage VIII c Straßenverkehrs-Zulassungs-Ordnung (StVZO) (Straßenverkehrs-Zulassungs-Ordnung vom 26.4.2012 (BGBl. I S. 679), zuletzt geändert d. Verordnung v. 20.10.2017 (BGBl. I S. 3723)) als anerkannte „AU-Werkstätten" neben den „üblichen" Werkleistungen spezielle Abgasuntersuchungen anbieten,die gemäß Nr. 3.1.1.1 Anlage VIII StVZO einen eigenständigen Bestandteil der andernfalls durch einen anerkannten Prüfingenieur (z.B. TÜV, Dekra, KÜS, GTÜ) durchgeführten Hauptuntersuchung (HU) bilden. Soweit derartige Leistungen erbracht werden, handeln die Kfz-Werkstätten im Rahmen hoheitlicher Aufgaben und sind öffentliche Stellen i. S. d. § 2 Abs. 4 S. 2 BDSG, § 2 Abs. 1 S. 3 SDSG, was eine Bestellungspflicht nach Art. 37 Abs.1 lit. a DS-GVO nach sich zieht.

Obgleich von Gesetzes wegen in beiden vorgenannten Konstellationen demnach kein Weg an der Benennung einer sich speziell mit dem Datenschutz befassenden Person vorbeiführt, wird seitens des saarländischen ULD nicht verkannt, dass gerade die Durchführung von Abgasuntersuchungen als Teiluntersuchung zur Hauptuntersuchung nur einen Bruchteil der übrigen Werkstattarbeiten ausmachen dürfte und gerade kleinere Betriebe von der Pflicht zur Bestellung eines eigenen Datenschutzbeauftragten oftmals strukturell wie finanziell überfordert sein dürften. Gleiches gilt für die meisten Schornsteinfegerbetriebe, denen hierzu oftmals nicht die personellen Ressourcen zur Verfügung stehen dürften. In der Bestellung gemeinsamer Datenschutzbeauftragter nach Art. 37 Abs. 3 DS-GVO, etwa durch die jeweiligen Berufsinnungen, wird ein praktikabler Weg zur Erfüllung der gesetzlichen Verpflichtungen gesehen.

4. Am Wettbewerb teilnehmende öffentliche Stellen

Der BayLfD außert sich in seinem 28. Tätigkeitsbericht (2017/2018, Abschn. 2.5) zur Benennung von Datenschutzbeauftragte durch am Wettbewerb teilnehmenden bayerischen öffentlichen Stellen. Er macht dabei klar, die für privatwirtschaftliche Verantwortlich geltende 10-Personen-Regelung des § 38 Abs. 1 S. 1 BDSG nicht anwendbar ist. Dazu wird ausgeführt: „Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten zwar nach Art. 1 Abs. 3 Satz 1 BayDSG für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht öffentliche Stellen. Zu diesen Vorschriften gehört auch § 38 Abs. 1 Satz 1 BDSG. Die Datenschutz-Grundverordnung bestimmt allerdings in Art. 37 Abs. 1 Buchst. a DS-GVO: „Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird [...]." § 38 Abs. 1 Satz 1 BDSG ergänzt ausdrücklich die in Art. 37 Abs. 1 Buchst. b und c DS-GVO geregelten Benennungstatbestände, die an die Qualität sowie die Quantität der Verarbeitungen bei dem betreffenden Verantwortlichen anknüpfen. § 38 Abs. 1 Satz 1 BDSG ist jedoch nicht zugleich als Einschränkung von Art. 37 Abs. 1 Buchst. a DS-GVO konzipiert. Mit der Formulierung „Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679" hat der Bundesgesetzgeber gerade auf den Anwendungsvorrang des Unionsrechts reagiert."

III. Die Arbeitsbedingungen behördlicher Datenschutzbeauftragter

1. Der aufgabengerechte Zeitanteil behördlicher Datenschutzbeauftragter

Der der Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (14. TB, 2018, Ziff. 3-1) stellte fest, dass insbesondere den Datenschutzbeauftragten größerer Verwaltungskörperschaften nicht der nötige Zeitanteil zur Wahrnehmung ihrer Aufgaben zu Verfügung steht, und fordert für behördliche Datenschutzbeauftragte größerer Verwaltungen Vollzeitstellen, zumal die Datenschutzbeauftragten oft nicht nur für den Bereich ihrer Kernverwaltung, sondern auch für nachgeordnete Bereiche, wie zum Beispiel Schulen oder kommunale Eigenbetriebe mitverantwortlich seien. Im Zuge der Umsetzungen der mit der Europäischen Datenschutz-Grundverordnung verbundenen Maßnahmen gewinne diese Forderung neue Aktualität. Exemplarisch nennt er hierfür die Umsetzung der notwendigen Dokumentations- und Informationspflichten oder auch die Mitwirkung an e-Government-Projekten, wie zum Beispiel der Einführung der e-Akte und deren Umsetzung (vor allem bezogen auf technische und organisatorische Maßnahmen). Um den Aufgaben und der damit verbundenen verstärkten Rolle der Datenschutzbeauftragten innerhalb der Verwaltung gerecht werden zu können, wurde gegenüber den Landkreisen, kreisfreien und großen kreisangehörigen Städten die Empfehlung ausgesprochen, die Zeitanteile der behördlichen Datenschutzbeauftragten jeweils auf eine Vollzeitstelle anzuheben.

In gleiche Richtung argumentiert das ULD Schleswig-Holstein (37. TB, 2017/2018, Absch. 4.1.2) Es geht derzeit davon aus, dass bei Kommunen eine Obergrenze von 1.000 Beschäftigten pro Vollzeitstelle eines DSB gilt. Diese sei auch bei der Benennung von gemeinsamen DSB zu beachten. Hat ein Kreis z.B. etwa 700 Beschäftigte, so dürfen die von einem gemeinsam bestellten DSB betreuten Kommunen oder Zweckverbände zusammen nicht mehr als 300 Beschäftigte haben. Wird diese Anzahl überschritten, ist in der Regel die Schaffung einer weiteren (ggf. anteilsmäßigen) Stelle erforderlich.

Die vormalige BfDI hat nach Geltung der DS-GVO den Schlüssel für eine Stelle mit 500 Beschäftige festgesetzt (uldsh.de/DS-GVO-bundesverwaltung, S.29f. der PDF-Datei).

2. Die angemessene Dotierung behördlicher Datenschutzbeauftragter

Bei der Benennung eigener Beschäftigter als DSB ist nach dem ULD Schleswig-Holstein zu beachten, dass die Stelle an-

gemessen dotiert ist. Eine Vergütung unterhalb E11/A12 sei nicht angemessen, da die Aufgabe der behördlichen DSB von einer erheblichen Komplexität ist. Diese ergebe sich z.B. aus einem Urteil des Finanzgerichts München vom 25. Juli 2017 (das allerdings noch auf die alte Rechtslage und den Privatbereich abstellt) (uldsh.de/fg-muenchen-dsb).

IV. Keine Benennung einer juristischen Person zum Datenschutzbeauftragten

U.a. neben anderen Aufsichtsbehörden (LfDI NRW, Häufig gestellte Fragen zu Datenschutzbeauftragten (FAQ), Stand: 11/2018, S. 11= https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte; LfDI Baden-Württemberg, Praxisratgeber Die/der Beauftragte für den Datenschutz, Teil II: Persönliche Voraussetzungen, Durchführung der Benennung, Stellung und Aufgaben, Beendigung der Benennung, 1 Aufl. 2018, S. 5). empfiehlt auch das Unabhängige Datenschutzzentrum des Saarlands mangels hierzu gesicherter Rechtsansicht jedenfalls zur Zeit nur eine natürlichen Person zum Datenschutzbeauftragten zu benennen (27. TB, 2017/2018, Abschn. 9.2). Es weist darauf hin, dass die DS-GVO in ihrer englischen Fassung im Zusammenhang mit dem Datenschutzbeauftragten nur von „he or she" spricht, was als Indiz dafür gewertet werden, dass das Rechtsregime der DS-GVO bei dem Datenschutzbeauftragten von einer natürlichen Person ausgeht und eine juristische Person bis zu einer gegenteiligen Aussage des EDSA nicht in Betracht kommt. Das ULD Schleswig-Holstein (37. TB, 2017/2018, Ziff. 5.4.1) vertritt die gleiche Auffassung, wobei es damit argumentiert, dass Datenschutzbeauftragte auf der Grundlage ihrer beruflichen Qualifikation und insbesondere des Fachwissens benannt werden, was den Schluss nahelege, dass die erforderliche Befähigung im Rahmen einer Berufsausbildung bzw. eines Studiums erworben wurde, was nur durch natürliche Personen erfolgen kann. Es weist aber auch darauf hin, dass z.B. eine GmbH die Dienste ihrer Mitarbeiter als Datenschutzbeauftragte anbieten könne, die dann von anderen Unternehmen entsprechend benannt werden. Der zugrunde liegende Dienstleistungsvertrag dürfe aber nicht ohne weiteres von einem Verantwortlichen oder Auftragsverarbeiter gekündigt werden können und den natürlichen Personen, die auf Basis des Vertrags als Datenschutzbeauftragte eingesetzt werden, sei eine Art arbeitsrechtlicher Kündigungsschutz zu gewähren, der sie vor ungerechtfertigten Entlassungen durch deren Arbeitgeber schützt (vgl. die Hinweise der europäischen Datenschutzaufsichtsbehörden zur Benennung von Datenschutzbeauftragten (WP 243: www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pd).

Auch nach dem BayLfd (28. TB, 2017/2018, Abschn. 3.1.4) ist die Benennung einer juristischen Person als Datenschutzbeauftragte nicht möglich. Wird der Dienstleistungsvertrag mit einer juristischen Person geschlossen, ist daher ein Beschäftigter dieser juristischen Person konkret als Datenschutzbeauftragter für die öffentliche Stelle zu benennen. Bei der Benennung eines externen Datenschutzbeauftragten muss der Dienstleistungsvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben insbesondere durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird.

Zur Vorlageberechtigung des (Interdiözesanen) Datenschutzgerichts an den EuGH

Dipl.-Jur. Robert Gmeiner*

I. Einleitung

Durch § 1 Abs. 1, 2 KDGO[1] wurden das Interdiözesane Datenschutzgericht sowie das Datenschutzgericht errichtet.[2] Ziel ihrer Errichtung ist – ausweislich der Präambel – die „Herstellung und Gewährleistung eines wirksamen gerichtlichen Rechtsschutzes auf dem Gebiet des Datenschutzes". Das Datenschutzrecht, das einen effektiven Datenrechtsschutz erfordert,[3] ist seit dem 25. Mai 2018 durch die Datenschutzgrundverordnung[4] (DSGVO) europarechtlich vollharmonisiert.[5] Daher stellt sich die Frage, ob das Datenschutzgericht als Kirchengericht nach Art. 267 AEUV berechtigt ist, dem EuGH datenschutzrechtliche Fragen zur Vorabentscheidung vorzulegen.

* Der Autor ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Finanz- und Steuerrecht (Prof. Dr. Hellermann) an der Universität Bielefeld sowie am Lehrstuhl für Bürgerliches Recht, Wirtschaftsrecht, Arbeitsrecht und Rechtstheorie (Prof. Dr. Klocke) an der EBS Law School in Wiesbaden.

1 Kirchliche Datenschutzgerichtsordnung (KABl. [Diözese Rottenburg-Stuttgart] 2018, 192).

2 Nachfolgend umfasst der Begriff „Datenschutzgericht" sowohl das Interdiözesane Datenschutzgericht erster Instanz (§ 1 Abs. 1 S. 1 KDGO) als auch das Datenschutzgericht zweiter Instanz (§ 1 Abs. 2 S. 1 KDGO).

3 Albrecht, CR 2016, 88 (95).

4 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 (ABl. EU 2016 Nr. L 119/1).

5 Schantz, in: BeckOK-Datenschutzrecht, Stand: 26. Ed. 2017, DSGVO Art. 1 Rn. 8.

II. Kirchenrechtliche Verpflichtung

1. Der gesetzliche Richter

Der EuGH ist als gesetzlicher Richter i.S.v. Art. 101 Abs. 1 S. 2 GG anerkannt.[6] Unterlässt das Gericht eine Vorlage an den EuGH, obwohl es nach Art. 267 Abs. 3 AEUV hierzu verpflichtet wäre, liegt – unter hier nicht zu interessierenden genaueren Umständen – ein Entzug des gesetzlichen Richters und damit eine Verletzung des Art. 101 Abs. 1 S. 2 GG vor.

Öffentlich-rechtliche Religionsgemeinschaften und damit auch ihre Organe[7] sind für innerkirchliche Maßnahme grundsätzlich nicht an grundgesetzliche Grundrechte gebunden.[8] Nur wenn sie ausnahmsweise vom Staat abgeleitete Hoheitsaufgaben wahrnehmen, unterliegen sie der Grundrechtsbindung nach Art. 1 Abs. 3 GG.[9] Es kann vorliegend dahinstehen, ob der (kirchliche) Datenschutz eine staatliche Aufgabe darstellt oder nicht. Der kirchliche Arbeitsgerichtshof (KAGH) hat für das kirchliche Arbeitsgerichtsverfahren entschieden, dass der grundgesetzliche Anspruch auf den gesetzlichen Richter die kirchlichen (Arbeits-)Gerichte ebenfalls unmittelbar bindet. Der Anspruch auf den gesetzlichen Richter gelte „für das kirchliche Gerichtsverfahren gleichermaßen."[10] Demnach hat das Kirchengericht nicht nur in einer vorher abstrakt-generell bestimmten Besetzung über das Verfahren zu befinden, sondern es hat das Verfahren notfalls nach anderen Vorschriften auszusetzen und die Entscheidungen anderer Gerichte einzuholen.

2. Aussetzungspflicht

Aufgabe des Datenschutzgerichts ist nach § 2 Abs. 1 KDGO ist die Überprüfung von Entscheidungen der Datenschutzaufsichten der katholischen Kirche in Deutschland sowie für gerichtliche Rechtsbehelfe der betroffenen Person gegen den Verantwortlichen oder den kirchlichen Auftragsverarbeiter.

Das Datenschutzgericht ist aber nicht nur an das Kirchliche Datenschutzrecht gebunden, sondern auch an das staatliche Recht, § 3 Abs. 3 S. 1 KDGO. Der Begriff des staatlichen Rechts darf dabei aber nicht eng nationalstaatlich verstanden werden. Der Datenschutz soll nach der Präambel der KDGO „im Einklang mit der europäischen Datenschutz-Grundverordnung" erfolgen, sodass der Datenschutzrichter zur Auslegung und Anwendung des Kirchlichen Datenschutzgesetzes (KDG[11]) die europäische Datenschutzgrundverordnung heranzuziehen hat. Gestützt wird dies durch die Präambel des KDG, die ausdrücklich auf Art. 91 DS-GVO Bezug nimmt. Datenschutzrechtliche Regelungen der Religionsgemeinschaften können nach Art. 91 Abs. 1 DS-GVO allerdings nur insoweit angewendet werden, wie sie im Einklang der DSGVO stehen. Aus Sicht des Unionsrechts muss somit sichergestellt sein, dass nicht nur die abstrakten Regelungen des kirchlichen Datenschutzrechts, sondern auch ihre konkrete Anwendung im Einzelfall den unionsrechtlichen Vorgaben entspricht. Die Anwendung des kirchlichen Datenschutzrechts ist daher von der Rechtsprechung des EuGH abhängig. Da die staatlichen Gerichte das kirchliche Recht nicht mittelbar anwenden dürfen,[12] kann eine unionsrechtskonforme Anwendung des kirchlichen Datenschutzrechts nur durch eine Vorlage des Datenschutzgerichts an den EuGH gewährleitstet werden.

III. Europarechtliche Berechtigung

Ergeben sich im Rahmen eines Rechtsstreits vor einem Gericht Fragen zur Auslegung des Unionsrechts, so kann[13] das Gericht das Verfahren aussetzen und sie zur Entscheidung dem EuGH vorlegen, Art. 267 AEUV.

1. Der Begriff des „Gerichts"

Kirchenrechtliche Regelungen können nur dann die Zuständigkeit der staatlichen Gerichte begründen, wenn diese ausdrücklich von den allgemeinen Prozessordnungen hierzu ermächtigt wurden.[14] Allein die kirchenrechtliche Vorlagepflicht (II.2) kann daher nicht die Vorlageberechtigung zum EuGH begründen. Daher ist zu fragen, ob das Datenschutzgericht dem Begriff des „Gerichts" in Art. 267 AEUV unterfällt, der unionsrechtlich autonom auszulegen ist.[15] Zur Einordnung einer Institution als Gericht stellt der EuGH auf verschiedene Gesichtspunkte „wie gesetzliche Grundlage der Einrichtung, ständiger Charakter, obligatorische Gerichtsbarkeit, streitiges Verfahren, Anwendung von Rechtsnormen durch diese Einrichtung sowie deren Unabhängigkeit"[16] ab. Fraglich beim Datenschutzgericht ist allein das Merkmal der gesetzlichen Grundlage der Errichtung. Sie beruht auf § 1 Abs. 1 S. 1 KDGO bzw. § 1 Abs. 2 S. 1 KDGO, also auf kirchlichem Recht.

Als Voraussetzung für die Anerkennung als vorlageberechtigtes Gericht fordert der EuGH eine hinreichende Einbindung in die öffentliche Gewalt des Mitgliedsstaates, sodass der Mitgliedsstaat die Möglichkeit zur Durchsetzung der Vorlagepflicht hat.[17]

6 BVerfGE 73, 339 (366 ff.); 135, 155 (230); BVerfGK 8, 401 (404); 13, 303 (307); 17, 533 (543); Paraschas, DRiZ 2018, 348 (349).

7 Vgl. Klingbeil, AcP 217 (2017), 848 (864).

8 BVerfGE 18, 385 (387); Kahl, in: Bonner Kommentar zum Grundgesetz, Stand: 169. Lfg. 2014, Art. 1 Abs. 3 Rn. 263; Herdegen, in: Maunz/Dürig, Grundgesetz, Stand: 44. Lfg. 2005, Art. 1 Abs. 3 Rn. 103; Hillgruber, in: Beck'scher Onlinekommentar zum Grundgesetz, Stand: 39. Ed. 2018, Art. 1 Rn. 69.

9 BVerfGE 18, 385 (387); 19, 226 (236 f.); 30, 415 (422); Kahl (Fn. 8), Art. 1 Abs. 3 Rn. 262; Herdegen (Fn. 8), Art. 1 Abs. 3 Rn. 103; Hillgruber (Fn. 8), Art. 1 Rn. 69.

10 KAGH, Urt. v. 07.07.2017 – M 01/2016, Rn. 18 = BeckRS 2017, 118710.

11 Gesetz über den Kirchlichen Datenschutz (KDG) i.d.F. des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20.11.2017 (KABl. [Diözese Rottenburg-Stuttgart] 2018, 69).

12 Gmeiner, ZIS 2016, 19 (21 f.).

13 Letztinstanzliche Gerichte (hier: das Datenschutzgericht zweiter Instanz [§ 1 Abs. 2 KDGO]) sind zur Vorlage verpflichtet, Art. 267 Abs. 2 AEUV.

14 BFHE 137, 385 (388).

15 EuGH, Urt. v. 30.03.1993 – Rs. C-24/92, Corbiau, Slg. 1993, I-1300 (1304, Rn. 14).

16 EuGH, Urt. v. 30.05.2002 – Rs. C-516/99, Schmidt, Slg. 2002, I-4593 (4606, Rn. 34).

17 EuGH, Urt. v. 23.03.1982 – Rs. 102/81, Nordsee/Reederei Mond, Slg. 1982, 1096 (1110, Rn. 13).

2. Prozessrecht

Nicht erforderlich ist hierfür, dass das Gericht in den Staatsaufbau organisatorisch eingegliedert ist.[18] So hat der EuGH auch Schiedsgerichte als vorlageberechtigte Gerichte anerkannt, sofern die Zuständigkeit und Entscheidungsbefugnis nicht vom Willen der gegnerischen Partei abhängt.[19]

Für die Diözese Rottenburg-Stuttgart findet das Kirchliche Datenschutzgesetz nach Art. 1 Abs. 2 des Dekrets zu seiner Inkraftsetzung[20] für die Diözese selbst, für alle Rechtspersonen sowie für nichtrechtsfähige Vereinigungen, Stiftungen, Eigenbetriebe und andere Einrichtungen, die der Aufsicht des Bischofs der Diözese unterliegen, Anwendung. Das Recht auf eine gerichtliche Entscheidung nach § 49 Abs. 1 KDG und § 49 Abs. 2 KDG gegenüber der Datenschutzaufsicht ist somit nicht von ihrer Einwilligung in das datenschutzgerichtliche Verfahren abhängig. Dies gilt auch für das Inkraftsetzungs-Dekret, welches ebenfalls unabhängig von einer Unterwerfungserklärung der Datenschutzaufsicht unter die Jurisdiktionsgewalt der Datenschutzgerichte Rechtswirkungen erzeugt.[21] Die Zuständigkeit des Datenschutzgerichts hängt somit nicht vom Willen der beklagten Datenschutzaufsicht ab.[22]

3. Haftungsrecht

Eine weitere Möglichkeit zur Einflussnahme zur Erfüllung der Vorlagepflicht kann man in einem Staatshaftungsanspruch gegen den Gerichtsträger bei einer unterbliebenen Vorlage erblicken.[23] Ob der Schadensersatz nach § 50 KDG, insb. dessen Abs. 4, dem genügt, kann dahinstehen. In Betracht zu ziehen ist jedoch ein Anspruch aus § 839 BGB[24] i.V.m. Art. 34 S. 1 GG. Der Beamtenbegriff in § 839 BGB ist dabei weit zu verstehen. Beamter in diesem Sinne ist jeder, der in einem öffentlich- oder privatrechtlichen Dienstverhältnis zu einer juristischen Person des öffentlichen Rechts steht.[25] Die Richter werden nach § 6 Abs. 1 S. 1 KDGO vom Vorsitzenden der Bischofskonferenz für das Gericht berufen, sodass sie in einem Dienstverhältnis zu einer juristischen Person des öffentlichen Rechts stehen.

Weitere Voraussetzung ist das Handeln in Ausübung eines öffentlichen Amtes. Bei Kirchen ist zwischen dem inneren, geistlichen Bereich und Verwaltungshandeln zu unterscheiden.[26] Auch wenn die Kirchen keine staatliche Gewalt ausüben, so handelt es sich bei ihnen dennoch um öffentlich-rechtliche Körperschaften, die öffentliche Gewalt ausüben.[27] Die Rechtsprechung in Datenschutzangelegenheiten ist keine geistliche Maßnahme, sondern ein Verwaltungshandeln, wie es auch vor staatlichen Stellen stattfindet. Jedes Verwaltungshandeln, ob kirchlich oder weltlich, unterliegt denselben Grundsätzen und Rechtfertigungen,[28] sodass für das Verwaltungshandeln im Gegensatz zum geistlichen Bereich aus Art. 140 GG i.V.m. Art. 137 Abs. 3 S. 1 WRV kein verfassungsrechtliches Bedürfnis für einen Haftungsausschluss besteht.[29] In der Rechtsprechung und Literatur ist daher weitestgehend anerkannt, dass die Kirchen für Verwaltungshandeln aus § 839 BGB i.V.m. Art. 34 S. 1 GG durch eine Haftungsverlagerung[30] auf Schadensersatz für das Verhalten ihrer Beamten haften.[31] Legt ein Kirchengericht daher trotz der Vorlagepflicht nach Art. 267 Abs. 3 AEUV nicht an den EuGH vor, kommt eine Haftung der Kirchen nach § 839 i.V.m. Art. 34 S. 1 GG in Betracht.

4. Zwischenergebnis

Die Kirchen sind nicht nur nach dem Kirchenrecht zur Vorlage an den EuGH verpflichtet, sondern nach dem Unionsrecht hierzu auch berechtigt.

Bestätigt wird dies durch den effet-utile-Grundsatzes des Art. 4 Abs. 3 EUV. Der EuGH geht davon aus, dass er auch bei der Frage, ob ein Gericht i.S.v. Art. 267 Abs. 3 AEUV vorliegt zum Tragen kommt.[32] Zur Wahrung ihrer Rechtssetzungshoheit[33] lässt Art. 91 Abs. 1 DS-GVO die Datenschutzvorschriften der Religionsgemeinschaften neben der DS-GVO bestehen,[34] soweit die sie inhaltsgleich mit der Verordnung sind. Dies setzt aber wiederum voraus, dass der EuGH die Möglichkeit haben muss zu kontrollieren, ob dem tatsächlich so ist.

IV. Fazit

Das Datenschutzgericht ist ein Gericht im Sinne von Art. 267 AEUV und daher an den EuGH vorlageberechtigt. Aus kirchenrechtlicher Sicht ist es zur Vorlage verpflichtet, wenn die Voraussetzungen hierfür vorliegen. Verfahrensrechtlich abgesichert[35] ist sie im Kirchenrecht über Art. 101 Abs. 1 S. 2 GG.

18 EuGH, Urt. v. 04.11.1997 – Rs. 337/95, Dior, Slg. 1997, I-6034 (6043, Rn. 21).

19 EuGH, Urt. v. 17.10.1989 – Rs. 109/88, Handels- og Kontorfunktionærernes, Slg. 1989, 3220 (3224, Rn. 7); Urt. v. 27.01.2005 – Rs. C-125/04, Denuit, Slg. 2005, I-925 (932, Rn. 13).

20 Dekret zur Inkraftsetzung des Gesetzes über den kirchlichen Datenschutz (KDG) für die Diözese Rottenburg-Stuttgart v. 07.02.2018 (KABl. [Diözese Rottenburg-Stuttgart] 2018, 69).

21 Hierzu Gmeiner, Nomok@non Kurzaufsatz Nr. 9, Rn. 4 ff.

22 Dies gilt nach § 5 Abs. 3 KDGO auch für die Richter, die vorab durch einen abstrakt-generellen Geschäftsverteilungsplan zu bestimmen sind.

23 Schima, Das Vorabentscheidungsverfahren vor dem EuGH, 3. Aufl. 2015, S. 36.

24 Keiner Entscheidung bedarf vorliegend, ob das Kirchengericht unter § 839 Abs. 1 S. 1 BGB oder § 839 Abs. 2 S. 1 BGB fällt.

25 Baldus/Grzeszick/Wienhues, Staatshaftungsrecht, 5. Aufl. 2018, Rn. 102.

26 Der Begriff ist – entsprechend dem Beamtenbegriff – weit zu verstehen.

27 BVerfGE 18, 385 (387).

28 BGHZ 22, 383 (390).

29 BGHZ 22, 383 (390).

30 Vgl. BVerfG (K), VersR 2016, 170 (173).

31 BGHZ 22, 383 (388); 154, 54 (57 f.); OLG Stuttgart, Beschl. v. 25.11.2014 – 4 W 83/14, Rn. 13 ff. (juris); Vinke, in: Soergel, BGB, 13. Aufl. 2005, § 839 Rn. 81; Papier/Shirvani, in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 839 Rn. 142; Eicholt, NJOZ 2010, 1859 (1862); a.A. OLG Düsseldorf, NVwZ 2001, 1449 (1450) mit Verweis auf die Entscheidung BGHSt 37, 191 (192 f.), die sich allerdings mit dem Begriff des Amtsträgers i.S.v. § 11 Abs. 1 Nr. 2 StGB und nicht mit dem Beamtenbegriff nach § 839 Abs. 1 S. 1 BGB befasst.

32 EuGH, Urt. v. 06.10.1981 – Rs. 246/81, Broekmeulen, Slg. 1981, 2312 (2328, Rn. 16).

33 Mundil, in: BeckOK-Datenschutzrecht, Stand: 26. Ed. 2017, Art. 91 Rn. 20.

34 Pauly, in: Paal/Pauly, Datenschutzgrundsverordnung, 2. Aufl. 2018, Art. 91 Rn. 1.

35 Ein unionsrechtliches Vorlageerzwingungsverfahren gibt es nicht: Paraschas, DRiZ 2018, 348 (349). Eine Verfassungsbeschwerde wegen der Verletzung von Art. 101 Abs. 1 S. 2 GG kommt allerdings nicht in Betracht, da die Kirchengerichte keine öffentliche Gewalt i.S.v. § 90 Abs. 1 BVerfGG darstellen; vgl. BVerfGE 18, 385 (387).

beck-online
DIE DATENBANK

Datenschutz- und Informationsfreiheitsrecht PLUS | PREMIUM

Datenschutz- und Informationsfreiheitsrecht PLUS

Das Basispaket zum Datenschutz beinhaltet u.a. die **ZD – Zeitschrift für Datenschutz, Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht** und den BeckOK Datenschutzrecht, Hrsg. Wolff/Brink, mit Kommentierung zur DS-GVO und zum neuen BDSG, sowie Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht (Nomos) und **Koreng/Lachenmann, Formularhandbuch Datenschutzrecht.** Dazu gibt es zahlreiche Arbeitshilfen: Rechtsprechung in Hülle und Fülle, sorgfältig aktualisierte Gesetzestexte und konkrete Lösungen für die Unternehmenspraxis.

Infos: beck-shop.de/11249239

▸ schon ab **€ 57,–/Monat***

Datenschutz- und Informationsfreiheitsrecht PREMIUM

Das nächste Level im Datenschutz- und Informationsfreiheitsrecht erreichen Sie mit dem Aufbaumodul PREMIUM. Denn hier stehen Ihnen zusätzliche renommierte Werke wie etwa **Gola, Datenschutz-Grundverordnung, Ehmann/Selmayr, Datenschutz-Grundverordnung, Kühling/Buchner, DS-GVO/BDSG** oder **Brink/Polenz/Blatt, Informationsfreiheitsgesetz** zur Verfügung. Ein Muss für Spezialisten und eine große Hilfe für jeden Praktiker.

Infos: beck-shop.de/20833162

▸ schon ab **€ 89,–/Monat***

* (zzgl. MwSt., 6-Monats-Abo)

JETZT
4 Wochen
kostenlos
testen
beck-online.de

facebook.com/verlagchbeck | twitter.com/beckonlinede

C.H.BECK

Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München | 167552

Rechtsprechung

Nationale Gesetzgeber müssen Arbeitgeber zur Arbeitszeiterfassung verpflichten

(**Europäischer Gerichtshof**, Urteil vom 14. Mai 2019 – C-55/18 –)

Die Art. 3, 5 und 6 der Richtlinie 2003/88/EG des Europäischen Parlaments und des Rates vom 4. November 2003 über bestimmte Aspekte der Arbeitszeitgestaltung sind im Licht von Art. 31 Abs. 2 der Charta der Grundrechte der Europäischen Union sowie von Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391/EWG des Rates vom 12. Juni 1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit dahin auszulegen, dass sie der Regelung eines Mitgliedstaats entgegenstehen, die nach ihrer Auslegung durch die nationalen Gerichte die Arbeitgeber nicht verpflichtet, ein System einzurichten, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann.

Sachverhalt:

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 31 Abs. 2 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta), der Art. 3, 5, 6, 16 und 22 der Richtlinie 2003/88/EG des Europäischen Parlaments und des Rates vom 4. November 2003 über bestimmte Aspekte der Arbeitszeitgestaltung (ABl. 2003, L 299, S. 9) sowie von Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391/EWG des Rates vom 12. Juni 1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit (ABl. 1989, L 183, S. 1).

Es ergeht in einem Rechtsstreit zwischen der Federación de Servicios de Comisiones Obreras (CCOO) und der Deutsche Bank SAE über das Fehlen eines betriebsinternen Systems zur Erfassung der von den Arbeitnehmern dieses Unternehmens geleisteten täglichen Arbeitszeit.

Rechtlicher Rahmen
Unionsrecht

Richtlinie 89/391

Art. 4 Abs. 1 der Richtlinie 89/391 bestimmt:

„Die Mitgliedstaaten treffen die erforderlichen Vorkehrungen, um zu gewährleisten, dass die Arbeitgeber, die Arbeitnehmer und die Arbeitnehmervertreter den für die Anwendung dieser Richtlinie erforderlichen Rechtsvorschriften unterliegen."

Art. 6 Abs. 1 dieser Richtlinie sieht vor:

„Im Rahmen seiner Verpflichtungen trifft der Arbeitgeber die für die Sicherheit und den Gesundheitsschutz der Arbeitnehmer erforderlichen Maßnahmen, einschließlich der Maßnahmen zur Verhütung berufsbedingter Gefahren, zur Information und zur Unterweisung sowie der Bereitstellung einer geeigneten Organisation und der erforderlichen Mittel.
…"

Art. 11 Abs. 3 der Richtlinie bestimmt:

„Die Arbeitnehmervertreter mit einer besonderen Funktion bei der Sicherheit und beim Gesundheitsschutz der Arbeitnehmer haben das Recht, den Arbeitgeber um geeignete Maßnahmen zu ersuchen und ihm diesbezüglich Vorschläge zu unterbreiten, um so jeder Gefahr für die Arbeitnehmer vorzubeugen und/oder die Gefahrenquellen auszuschalten."

Art. 16 Abs. 3 der Richtlinie lautet:

„Die Bestimmungen dieser Richtlinie gelten uneingeschränkt für alle Bereiche, die unter die Einzelrichtlinien fallen; gegebenenfalls bestehende strengere bzw. spezifische Bestimmungen in diesen Einzelrichtlinien bleiben unberührt."

Richtlinie 2003/88

Im dritten und vierten Erwägungsgrund der Richtlinie 2003/88 heißt es:

„(3) Die Bestimmungen der Richtlinie [89/391] bleiben auf die durch die vorliegende Richtlinie geregelte Materie – unbeschadet der darin enthaltenen strengeren und/oder spezifischen Vorschriften – in vollem Umfang anwendbar.

(4) Die Verbesserung von Sicherheit, Arbeitshygiene und Gesundheitsschutz der Arbeitnehmer bei der Arbeit stellen Zielsetzungen dar, die keinen rein wirtschaftlichen Überlegungen untergeordnet werden dürfen."

Art. 1
(„Gegenstand und Anwendungsbereich")
der Richtlinie 2003/88 bestimmt:

„…
(2) Gegenstand dieser Richtlinie sind
a) die täglichen und wöchentlichen Mindestruhezeiten, der Mindestjahresurlaub, die Ruhepausen und die wöchentliche Höchstarbeitszeit sowie

b) bestimmte Aspekte der Nacht- und der Schichtarbeit sowie des Arbeitsrhythmus.

…
(4) Die Bestimmungen der Richtlinie [89/391] finden unbeschadet strengerer und/oder spezifischer Vorschriften in der vorliegenden Richtlinie auf die in Abs. 2 genannten Bereiche voll Anwendung."

Art. 3
(„Tägliche Ruhezeit") der Richtlinie 2003/88 lautet:

„Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, damit jedem Arbeitnehmer pro 24-Stunden-Zeitraum eine Mindestruhezeit von elf zusammenhängenden Stunden gewährt wird."

Art. 5
(„Wöchentliche Ruhezeit") dieser Richtlinie sieht vor:

„Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, damit jedem Arbeitnehmer pro Siebentageszeitraum eine kontinuierliche Mindestruhezeit von 24 Stunden zuzüglich der täglichen Ruhezeit von elf Stunden gemäß Art. 3 gewährt wird.

Wenn objektive, technische oder arbeitsorganisatorische Umstände dies rechtfertigen, kann eine Mindestruhezeit von 24 Stunden gewählt werden."

Art. 6
(„Wöchentliche Höchstarbeitszeit“)
der Richtlinie bestimmt:

„Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, damit nach Maßgabe der Erfordernisse der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer:

a) die wöchentliche Arbeitszeit durch innerstaatliche Rechts- und Verwaltungsvorschriften oder in Tarifverträgen oder Vereinbarungen zwischen den Sozialpartnern festgelegt wird;

b) die durchschnittliche Arbeitszeit pro Siebentageszeitraum 48 Stunden einschließlich der Überstunden nicht überschreitet.“

Art. 16 der Richtlinie 2003/88 legt die Höchstbezugszeiträume für die Anwendung ihrer Art. 5 und 6 fest.

Art. 17
(„Abweichungen“) dieser Richtlinie sieht in Abs. 1 vor:

„Unter Beachtung der allgemeinen Grundsätze des Schutzes der Sicherheit und der Gesundheit der Arbeitnehmer können die Mitgliedstaaten von den Artikeln 3 bis 6, 8 und 16 abweichen, wenn die Arbeitszeit wegen der besonderen Merkmale der ausgeübten Tätigkeit nicht gemessen und/oder nicht im Voraus festgelegt wird oder von den Arbeitnehmern selbst festgelegt werden kann, und zwar insbesondere in Bezug auf nachstehende Arbeitnehmer:

a) leitende Angestellte oder sonstige Personen mit selbstständiger Entscheidungsbefugnis;

b) Arbeitskräfte, die Familienangehörige sind;

c) Arbeitnehmer, die im liturgischen Bereich von Kirchen oder Religionsgemeinschaften beschäftigt sind.“

Art. 19 der Richtlinie betrifft die Grenzen der von dieser Richtlinie vorgesehenen Abweichungen von Bezugszeiträumen.

Art. 22 Abs. 1 der Richtlinie bestimmt:

„(1) Es ist einem Mitgliedstaat freigestellt, Art. 6 nicht anzuwenden, wenn er die allgemeinen Grundsätze der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer einhält und mit den erforderlichen Maßnahmen dafür sorgt, dass

a) kein Arbeitgeber von einem Arbeitnehmer verlangt, im Durchschnitt des in Art. 16 Buchstabe b) genannten Bezugszeitraums mehr als 48 Stunden innerhalb eines Siebentagezeitraums zu arbeiten, es sei denn der Arbeitnehmer hat sich hierzu bereit erklärt;

…

c) der Arbeitgeber aktuelle Listen über alle Arbeitnehmer führt, die eine solche Arbeit leisten;

d) die Listen den zuständigen Behörden zur Verfügung gestellt werden, die aus Gründen der Sicherheit und/oder des Schutzes der Gesundheit der Arbeitnehmer die Möglichkeit zur Überschreitung der wöchentlichen Höchstarbeitszeit unterbinden oder einschränken können;

…“

Spanisches Recht

Das Estatuto de los Trabajadores (Arbeitnehmerstatut) in der Fassung des Real decreto legislativo 2/2015, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (Königliches Gesetzesdekret 2/2015 zur Billigung der Neufassung des Arbeitnehmerstatuts) vom 23. Oktober 2015 (BOE Nr. 255 vom 24. Oktober 2015, S. 100224 (im Folgenden: Arbeitnehmerstatut) sieht in Art. 34 („Arbeitszeit“) vor:

„1. Die Arbeitszeit wird durch Tarifvertrag oder Arbeitsvertrag festgelegt.

Die Höchstarbeitszeit beträgt im Jahresdurchschnitt 40 Wochenstunden.

…

3. Zwischen dem Ende eines Arbeitszeitraums und dem Beginn des folgenden liegen mindestens zwölf Stunden.

Die Anzahl der tatsächlich geleisteten gewöhnlichen Arbeitsstunden darf neun Stunden täglich nicht überschreiten, sofern nicht in einem Tarifvertrag oder in Ermangelung dessen in einer Vereinbarung zwischen dem Unternehmen und den Arbeitnehmervertretern eine andere Verteilung der täglichen Arbeitszeit vereinbart wird, wobei in jedem Fall die täglichen Ruhezeiten zu beachten sind.

…“

Art. 35 („Überstunden“) des
Arbeitnehmerstatuts bestimmt:

„1. Arbeitsstunden, die über die im Einklang mit dem vorstehenden Artikel festgelegte Höchstdauer der Regelarbeitszeit hinaus geleistet werden, stellen Überstunden dar. …

2. Die Zahl der Überstunden darf 80 Stunden jährlich nicht überschreiten. …

…

4. Die Leistung von Überstunden ist freiwillig, soweit sie nicht in einem Tarifvertrag oder in einem Individualarbeitsvertrag innerhalb der Grenzen von Abs. 2 festgelegt ist.

5. Für die Berechnung der Überstunden wird die Arbeitszeit jedes Arbeitnehmers täglich aufgezeichnet und zum für die Zahlung der Vergütung festgelegten Zeitpunkt zusammengezählt, wobei dem Arbeitnehmer eine Kopie der Aufstellung im Beleg zur entsprechenden Zahlung übermittelt wird.“

Das Real Decreto 1561/1995, sobre jornadas especiales de trabajo (Königliches Dekret 1561/1995 über Sonderarbeitszeiten) vom 21. September 1995 (BOE Nr. 230 vom 26. September 1995, S. 28606) sieht in seiner dritten Zusatzbestimmung („Zuständigkeiten der Arbeitnehmervertreter im Bereich der Arbeitszeit“) vor:

„Unbeschadet der den Arbeitnehmervertretern im Bereich der Arbeitszeit im Arbeitnehmerstatut und im vorliegenden Real Decreto zuerkannten Befugnisse haben diese Vertreter das Recht: …

…

b) jeden Monat vom Arbeitgeber über die von den Arbeitnehmern geleisteten Überstunden unterrichtet zu werden, unabhängig von der gewählten Form des Ausgleichs; sie erhalten zu diesem Zweck eine Kopie der Aufstellung nach Art. 35 Abs. 5 des Arbeitnehmerstatuts.“

Ausgangsverfahren und Vorlagefragen

Am 26. Juli 2017 erhob die CCOO, eine Arbeitnehmervereinigung, die Teil einer bedeutenden Gewerkschaft auf nationaler Ebene in Spanien ist, gegen die Deutsche Bank vor der Audiencia Nacional (Nationaler Gerichtshof, Spanien) eine Verbandsklage; mit dieser Klage begehrte sie die Feststellung, dass die Deutsche Bank nach Art. 35 Abs. 5 des Arbeitnehmerstatuts und der dritten Zusatzbestimmung des Königlichen Gesetzesdekrets 1561/1995 verpflichtet sei, ein System zur Erfassung der von ihren Mitarbeitern geleisteten täglichen Arbeitszeit einzurichten, mit dem die Einhaltung zum einen der vorgesehenen Arbeitszeit und zum anderen der Verpflichtung, die Gewerkschaftsvertreter über die monatlich geleisteten Überstunden zu unterrichten, überprüft werden könne.

Nach Auffassung der CCOO ergibt sich die Verpflichtung zur Einrichtung eines solchen Erfassungssystems aus den Art. 34 und 35 des Arbeitnehmerstatuts in ihrer Auslegung im Licht von Art. 31 Abs. 2 der Charta, der Art. 3, 5, 6 und 22 der Richtlinie 2003/88 sowie der von der Internationalen Arbeitsorganisation am 28. November 1919 in Washington bzw. am 28. Juni 1930 in Genf ange-

nommenen Übereinkommen Nr. 1 über die Arbeitszeit (Gewerbe) und Nr. 30 über die Arbeitszeit (Handel und Büros).

Die Deutsche Bank macht dagegen geltend, den Urteilen Nr. 246/2017 vom 23. März 2017 (Rec. 81/2016) und Nr. 338/2017 vom 20. April 2017 (Rec. 116/2016) des Tribunal Supremo (Oberstes Gericht, Spanien) lasse sich entnehmen, dass das spanische Recht keine solche allgemeingültige Verpflichtung vorsehe.

Die Audiencia Nacional (Nationaler Gerichtshof) stellt fest, dass die Deutsche Bank trotz zahlreicher Regeln über die Arbeitszeit, die aus einer Vielzahl von auf sie anwendbaren nationalen Branchentarifverträgen und Betriebsvereinbarungen hervorgegangen seien, kein betriebsinternes System zur Erfassung der von ihren Mitarbeitern geleisteten Arbeitszeit eingerichtet habe, mit dem die Einhaltung der vereinbarten Arbeitszeiten überprüft und die möglicherweise geleisteten Überstunden berechnet werden könnten. Insbesondere verwende die Deutsche Bank eine Software (Absences Calendar), mit der nur die ganztägigen Fehlzeiten wie Urlaub oder sonstige freie Tage – ohne jedoch die von einem jeden Arbeitnehmer geleistete Arbeitszeit und die Zahl der geleisteten Überstunden zu messen – erfasst werden könnten.

Die Audiencia Nacional (Nationaler Gerichtshof) weist auch darauf hin, dass die Deutsche Bank dem Begehren der Inspección de Trabajo y Seguridad Social de las provincias de Madrid y Navarra (Inspektion für Arbeit und soziale Sicherheit der Provinzen Madrid und Navarra, Spanien, im Folgenden: Arbeitsinspektion) nicht nachgekommen sei, ein System zur Erfassung der täglich geleisteten Arbeitszeit einzurichten, und dass diese daher das Vorliegen eines Verstoßes festgestellt und die Auferlegung einer Sanktion vorgeschlagen habe. Dieser Sanktionsvorschlag sei jedoch anschließend durch das in Rn. 21 des vorliegenden Urteils genannte Urteil des Tribunal Supremo (Oberstes Gericht) vom 23. März 2017 verworfen worden.

Die Audiencia Nacional (Nationaler Gerichtshof) führt aus, dass sich aus der in dieser Rn. 21 angeführten Rechtsprechung des Tribunal Supremo (Oberstes Gericht) ergebe, dass Art. 35 Abs. 5 des Arbeitnehmerstatuts – vorbehaltlich einer anderslautenden Vereinbarung – nur die Führung einer Aufstellung der von den Arbeitnehmern geleisteten Überstunden sowie die Übermittlung der Zahl dieser Überstunden am jeweiligen Monatsende an die Arbeitnehmer und ihre Vertreter auferlege.

Nach Auffassung der Audiencia Nacional (Nationaler Gerichtshof) liegen dieser Rechtsprechung folgende Erwägungen zugrunde. Erstens sei die Verpflichtung zur Führung einer Aufstellung in Art. 35 des Arbeitnehmerstatuts über die Überstunden, und nicht in Art. 34 dieses Statuts über die „gewöhnliche" Arbeitszeit, welche als die Arbeitszeit definiert werde, die die Höchstarbeitszeit nicht überschreite, vorgesehen. Zweitens habe der spanische Gesetzgeber in allen Fällen, in denen er eine verpflichtende Erfassung der geleisteten Arbeitszeit habe vorsehen wollen, diese für einen speziellen Fall vorgesehen, wie den Fall der Teilzeitbeschäftigten und der mobilen Arbeitnehmer, der Arbeitnehmer in der Handelsmarine und der Arbeitnehmer bei der Eisenbahn. Drittens erlege Art. 22 der Richtlinie 2003/88 ebenso wie das spanische Recht die Pflicht auf, eine Liste der in besonderen Fällen geleisteten Arbeitszeit zu führen, nicht aber eine Liste der „gewöhnlichen" Arbeitszeit. Viertens habe die Schaffung einer Liste über die von einem jeden Arbeitnehmer geleistete Arbeitszeit zu einer Verarbeitung personenbezogener Daten mit der Gefahr eines ungerechtfertigten Eingriffs des Unternehmens in das Privatleben der Arbeitnehmer zur Folge. Fünftes werde das Versäumnis, eine solche Liste zu führen, in den nationalen Vorschriften über die Zuwiderhandlungen und Sanktionen im sozialen Bereich nicht als eindeutiger und offensichtlicher Verstoß eingestuft. Sechstens beeinträchtige die Rechtsprechung des Tribunal Supremo (Oberstes Gericht) nicht die Arbeitnehmerrechte, da nach Art. 217 Abs. 6 der Ley de Enjuiciamiento Civil 1/2000 (Zivilprozessordnung 1/2000) vom 7. Januar 2000 (BOE Nr. 7 vom 8. Januar 2000, S. 575) ohne eine Erfassung der „gewöhnlichen" Arbeitszeit zwar nicht unterstellt werden dürfe, dass Überstunden geleistet würden, es aber gleichwohl zulasten des Arbeitgebers, der keine solche Erfassung eingeführt habe, gehe, wenn der Arbeitnehmer durch andere Mittel beweise, dass er Überstunden in diesem Sinne geleistet habe.

Die Audiencia Nacional (Nationaler Gerichtshof) hegt Zweifel an der Vereinbarkeit der durch das Tribunal Supremo (Oberstes Gericht) vorgenommenen Auslegung von Art. 35 Abs. 5 des Arbeitnehmerstatuts mit dem Unionsrecht. Das vorlegende Gericht weist zunächst darauf hin, dass eine Umfrage unter der erwerbstätigen Bevölkerung in Spanien im Jahr 2016 ergeben habe, dass 53,7 % der geleisteten Überstunden nicht erfasst worden seien. Ferner ergebe sich aus zwei Berichten der Dirección General de Empleo del ministerio de Empleo y Seguridad Social (Generaldirektion Beschäftigung des Ministeriums für Beschäftigung und soziale Sicherheit, Spanien) vom 31. Juli 2014 und vom 1. März 2016, dass es zur Ermittlung, ob Überstunden geleistet worden seien, erforderlich sei, die Zahl der gewöhnlich geleisteten Arbeitsstunden genau zu kennen. Daraus erkläre sich, warum die Arbeitsinspektion die Deutsche Bank aufgefordert habe, ein System zur Erfassung der von einem jeden Arbeitnehmer geleisteten Arbeitszeit einzurichten, da ein solches System als das einzige Mittel angesehen werde, um mögliche Überschreitungen der Höchstgrenzen im Bezugszeitraum zu überprüfen. Mit der Auslegung des spanischen Rechts durch das Tribunal Supremo (Oberstes Gericht) verlören zum einen die Arbeitnehmer praktisch ein wesentliches Beweismittel, mit dem sie dartun könnten, dass ihre Arbeitszeit die Höchstarbeitszeiten überschritten habe, und zum anderen ihre Vertreter die erforderlichen Mittel für die Überprüfung der Achtung der in dem Bereich geltenden Regeln, so dass die Kontrolle der Einhaltung der Arbeitszeit und der Ruhezeiten vom guten Willen des Arbeitgebers abhänge.

Nach Auffassung des vorlegenden Gerichts könne unter solchen Umständen das innerstaatliche spanische Recht nicht die tatsächliche Beachtung der von der Richtlinie 2003/88 vorgesehenen Verpflichtungen hinsichtlich der Mindestruhezeiten und der wöchentlichen Höchstarbeitszeit sowie die sich aus der Richtlinie 89/391 ergebenden Verpflichtungen in Bezug auf die Rechte der Arbeitnehmervertreter gewährleisten.

Unter diesen Umständen hat die Audiencia Nacional (Nationaler Gerichtshof) beschlossen, das Verfahren auszusetzen und dem Gerichtshof die folgenden Fragen zur Vorabentscheidung vorzulegen:

1. Ist davon auszugehen, dass das Königreich Spanien durch die Art. 34 und 35 des Arbeitnehmerstatuts nach ihrer Auslegung in der Rechtsprechung die erforderlichen Maßnahmen erlassen hat, um die Wirksamkeit der Grenzen für die Dauer der täglichen Arbeitszeit sowie der wöchentlichen und täglichen Ruhezeiten, die in den Art. 3, 5 und 6 der Richtlinie 2003/88 vorgesehen sind, für Vollzeitarbeitnehmer zu gewährleisten, die sich nicht ausdrücklich individuell oder kollektiv zur Ableistung von Überstunden verpflichtet haben und die keine mobilen Arbeitnehmer, Arbeitnehmer in der Handelsmarine oder Arbeitnehmer im Eisenbahnsektor sind?

2. Sind Art. 31 Abs. 2 der Charta sowie die Art. 3, 5, 6, 16 und 22 der Richtlinie 2003/88 in Verbindung mit Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391 dahin auszulegen, dass sie innerstaatlichen Rechtsvorschriften wie den Art. 34 und 35 des Arbeitnehmerstatuts entgegenstehen, aus denen nach gefestigter Rechtsprechung nicht abzuleiten ist, dass von den Unternehmen verlangt werden kann, ein System zur Erfassung der täglichen effektiven Arbeitszeit für Vollzeitarbeitnehmer einzuführen, die sich nicht ausdrücklich individuell oder kollektiv zur Ableistung von

Überstunden verpflichtet haben und die keine mobilen Arbeitnehmer, Arbeitnehmer in der Handelsmarine oder Arbeitnehmer im Eisenbahnsektor sind?

3. Ist davon auszugehen, dass der den Mitgliedstaaten durch Art. 31 Abs. 2 der Charta sowie die Art. 3, 5, 6, 16 und 22 der Richtlinie 2003/88 in Verbindung mit Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391 auferlegten Verpflichtung, die Dauer der Arbeitszeit aller Arbeitnehmer allgemein zu begrenzen, für gewöhnliche Arbeitnehmer durch die innerstaatlichen Rechtsvorschriften in den Art. 34 und 35 des Arbeitnehmerstatuts Genüge getan wird, aus denen nach gefestigter Rechtsprechung nicht abzuleiten ist, dass von den Unternehmen verlangt werden kann, ein System zur Erfassung der täglichen effektiven Arbeitszeit für Vollzeitarbeitnehmer einzuführen, die sich nicht ausdrücklich individuell oder kollektiv zur Ableistung von Überstunden verpflichtet haben, im Unterschied zu mobilen Arbeitnehmern, Arbeitnehmern in der Handelsmarine und Arbeitnehmern im Eisenbahnsektor?

Zu den Vorlagefragen

Mit seinen Fragen, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob die Art. 3, 5, 6, 16 und 22 der Richtlinie 2003/88 in Verbindung mit Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391 sowie Art. 31 Abs. 2 der Charta dahin auszulegen sind, dass sie der Regelung eines Mitgliedstaats entgegenstehen, die nach ihrer Auslegung durch die nationalen Gerichte die Arbeitgeber nicht verpflichtet, ein System einzurichten, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann.

Einleitend ist darauf hinzuweisen, dass das Recht eines jeden Arbeitnehmers auf eine Begrenzung der Höchstarbeitszeit und auf tägliche und wöchentliche Ruhezeiten nicht nur eine Regel des Sozialrechts der Union ist, die besondere Bedeutung hat, sondern auch in Art. 31 Abs. 2 der Charta, der nach Art. 6 Abs. 1 EUV der gleiche rechtliche Rang wie den Verträgen zukommt, ausdrücklich verbürgt ist (vgl. in diesem Sinne Urteile vom 5. Oktober 2004, Pfeiffer u.a., C 397/01 bis C 403/01, EU:C:2004:584, Rn. 100, sowie vom 6. November 2018, Max-Planck-Gesellschaft zur Förderung der Wissenschaften, C 684/16, EU:C:2018:874, Rn. 20).

Die Bestimmungen der Richtlinie 2003/88, insbesondere ihre Art. 3, 5 und 6, konkretisieren dieses Grundrecht und sind daher in dessen Licht auszulegen (vgl. in diesem Sinne Urteile vom 11. September 2014, A, C 112/13, EU:C:2014:2195, Rn. 51 und die dort angeführte Rechtsprechung, sowie vom 6. November 2018, Bauer und Willmeroth, C 569/16 und C 570/16, EU:C:2018:871, Rn. 85).

Um sicherzustellen, dass dieses Grundrecht beachtet wird, dürfen die Bestimmungen der Richtlinie 2003/88 insbesondere nicht auf Kosten der Rechte, die dem Arbeitnehmer nach dieser Richtlinie zustehen, restriktiv ausgelegt werden (vgl. entsprechend Urteil vom 6. November 2018, Bauer und Willmeroth, C 569/16 und C 570/16, EU:C:2018:871, Rn. 38 sowie die dort angeführte Rechtsprechung).

Unter diesen Umständen ist zur Beantwortung der vorgelegten Fragen diese Richtlinie unter Beachtung der Bedeutung des Grundrechts eines jeden Arbeitnehmers auf eine Begrenzung der Höchstarbeitszeit und auf tägliche und wöchentliche Ruhezeiten auszulegen.

Insoweit ist zunächst darauf hinzuweisen, dass die zweite und die dritte Frage des vorlegenden Gerichts u.a. Art. 22 der Richtlinie 2003/88 betreffen, nach dessen Abs. 1 die Mitgliedstaaten, wenn sie von der Möglichkeit Gebrauch machen, Art. 6 dieser Richtlinie über die wöchentliche Höchstarbeitszeit nicht anzuwenden, mit den erforderlichen Maßnahmen dafür sorgen müssen, dass der Arbeitgeber aktuelle Listen über alle betroffenen Arbeitnehmer führt und dass diese Listen den zuständigen Behörden zur Verfügung gestellt werden.

Das Königreich Spanien hat jedoch, wie sich aus den Erörterungen in der mündlichen Verhandlung vor dem Gerichtshof ergibt, von dieser Möglichkeit keinen Gebrauch gemacht. Daher ist Art. 22 der Richtlinie 2003/88 in der Rechtssache des Ausgangsverfahrens nicht anzuwenden und im vorliegenden Fall folglich nicht auszulegen.

Nach dieser Klarstellung ist darauf hinzuweisen, dass durch die Richtlinie 2003/88 Mindestvorschriften festgelegt werden sollen, die dazu bestimmt sind, die Lebens- und Arbeitsbedingungen der Arbeitnehmer durch eine Angleichung namentlich der innerstaatlichen Arbeitszeitvorschriften zu verbessern (vgl. u.a. Urteile vom 26. Juni 2001, BECTU, C 173/99, EU:C:2001:356, Rn. 37, vom 10. September 2015, Federación de Servicios Privados del sindicato Comisiones obreras, C 266/14, EU:C:2015:578, Rn. 23, sowie vom 20. November 2018, Sindicatul Familia Constan a u.a., C 147/17, EU:C:2018:926, Rn. 39).

Diese Harmonisierung der Arbeitszeitgestaltung auf der Ebene der Europäischen Union bezweckt, einen besseren Schutz der Sicherheit und der Gesundheit der Arbeitnehmer durch die Gewährung von – u.a. täglichen und wöchentlichen – Mindestruhezeiten und angemessenen Ruhepausen zu gewährleisten sowie eine Obergrenze für die wöchentliche Arbeitszeit vorzusehen (vgl. u.a. Urteile vom 5. Oktober 2004, Pfeiffer u.a., C 397/01 bis C 403/01, EU:C:2004:584, Rn. 76, vom 25. November 2010, Fuß, C 429/09, EU:C:2010:717, Rn. 43, sowie vom 10. September 2015, Federación de Servicios Privados del sindicato Comisiones obreras, C 266/14, EU:C:2015:578, Rn. 23).

Daher müssen die Mitgliedstaaten nach den Art. 3 und 5 der Richtlinie 2003/88 die erforderlichen Maßnahmen treffen, damit jedem Arbeitnehmer pro 24-Stunden-Zeitraum eine Mindestruhezeit von elf zusammenhängenden Stunden und pro Siebentageszeitraum eine kontinuierliche Mindestruhezeit von 24 Stunden zuzüglich der täglichen Ruhezeit von elf Stunden gemäß Art. 3 gewährt wird (Urteil vom 7. September 2006, Kommission/Vereinigtes Königreich, C 484/04, EU:C:2006:526, Rn. 37).

Darüber hinaus verpflichtet Art. 6 Buchst. b der Richtlinie 2003/88 die Mitgliedstaaten, für die durchschnittliche wöchentliche Arbeitszeit eine Obergrenze von 48 Stunden vorzusehen, wobei ausdrücklich klargestellt ist, dass diese Obergrenze die Überstunden einschließt; von dieser Regel kann, abgesehen von dem vorliegend nicht einschlägigen Fall von Art. 22 Abs. 1 dieser Richtlinie, selbst bei Einverständnis des betroffenen Arbeitnehmers in keinem Fall abgewichen werden (vgl. in diesem Sinne Urteil vom 25. November 2010, Fuß, C 429/09, EU:C:2010:717, Rn. 33 und die dort angeführte Rechtsprechung).

Die Mitgliedstaaten müssen daher zur Gewährleistung der vollen Wirksamkeit der Richtlinie 2003/88 die Beachtung dieser Mindestruhezeiten gewährleisten und jede Überschreitung der wöchentlichen Höchstarbeitszeit verhindern (Urteil vom 14. Oktober 2010, Fuß, C 243/09, EU:C:2010:609, Rn. 51 und die dort angeführte Rechtsprechung).

Die Art. 3 und 5 sowie Art. 6 Buchst. b der Richtlinie 2003/88 legen zwar nicht die konkreten Maßnahmen fest, mit denen die Mitgliedstaaten die Umsetzung der in ihnen vorgesehenen Rechte sicherstellen müssen. Wie sich bereits aus ihrem Wortlaut ergibt, überlassen diese Bestimmungen es den Mitgliedstaaten, diese Maßnahmen zu ergreifen, indem sie die insoweit „erforderlichen Maßnahmen" treffen (vgl. in diesem Sinne Urteil vom 26. Juni 2001, BECTU, C 173/99, EU:C:2001:356, Rn. 55).

Auch wenn die Mitgliedstaaten daher zu diesem Zweck über einen gewissen Spielraum verfügen, müssen sie angesichts des von der Richtlinie 2003/88 verfolgten wesentlichen Ziels, einen wirksamen Schutz der Lebens- und Arbeitsbedingungen der Arbeitnehmer sowie einen besseren Schutz der Sicherheit und der Gesundheit der Arbeitnehmer zu gewährleisten, sicherstellen, dass die praktische

Wirksamkeit dieser Rechte in vollem Umfang gewährleistet wird, indem ihnen tatsächlich die täglichen und wöchentlichen Mindestruhezeiten und die Obergrenze für die durchschnittliche wöchentliche Höchstarbeitszeit, die in dieser Richtlinie festgesetzt sind, zugutekommen (vgl. in diesem Sinne Urteile vom 1. Dezember 2005, Dellas u.a., C 14/04, EU:C:2005:728, Rn. 53, vom 7. September 2006, Kommission/Vereinigtes Königreich, C 484/04, EU:C:2006:526, Rn. 39 und 40, sowie vom 14. Oktober 2010, Fuß, C 243/09, EU:C:2010:609, Rn. 64).

Daraus folgt, dass die von den Mitgliedstaaten festgelegten Modalitäten zur Sicherstellung der Umsetzung der Bestimmungen der Richtlinie 2003/88 nicht zu einer Aushöhlung der in Art. 31 Abs. 2 der Charta und den Art. 3 und 5 sowie Art. 6 Buchst. b dieser Richtlinie verankerten Rechte führen dürfen (vgl. in diesem Sinne Urteil vom 7. September 2006, Kommission/Vereinigtes Königreich, C 484/04, EU:C:2006:526, Rn. 44).

Insoweit ist darauf hinzuweisen, dass der Arbeitnehmer als die schwächere Partei des Arbeitsvertrags anzusehen ist, so dass verhindert werden muss, dass der Arbeitgeber ihm eine Beschränkung seiner Rechte auferlegen kann (Urteile vom 5. Oktober 2004, Pfeiffer u.a., C 397/01 bis C 403/01, EU:C:2004:584, Rn. 82, vom 25. November 2010, Fuß, C 429/09, EU:C:2010:717, Rn. 80, und vom 6. November 2018, Max-Planck-Gesellschaft zur Förderung der Wissenschaften, C 684/16, EU:C:2018:874, Rn. 41).

Ebenso ist festzustellen, dass ein Arbeitnehmer aufgrund dieser schwächeren Position davon abgeschreckt werden kann, seine Rechte gegenüber seinem Arbeitgeber ausdrücklich geltend zu machen, da insbesondere die Einforderung dieser Rechte ihn Maßnahmen des Arbeitgebers aussetzen könnte, die sich zu seinem Nachteil auf das Arbeitsverhältnis auswirken können (vgl. in diesem Sinne Urteile vom 25. November 2010, Fuß, C 429/09, EU:C:2010:717, Rn. 81, und vom 6. November 2018, Max-Planck-Gesellschaft zur Förderung der Wissenschaften, C 684/16, EU:C:2018:874, Rn. 41).

Im Licht dieser allgemeinen Erwägungen ist zu prüfen, ob und inwieweit die Einrichtung eines Systems, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, erforderlich ist, um die tatsächliche Einhaltung der wöchentlichen Höchstarbeitszeit sowie der täglichen und wöchentlichen Mindestruhezeiten sicherzustellen.

Insoweit ist im Einklang mit den Ausführungen des Generalanwalts in den Nrn. 57 und 58 seiner Schlussanträge festzustellen, dass ohne ein solches System weder die Zahl der vom Arbeitnehmer tatsächlich geleisteten Arbeitsstunden sowie ihre zeitliche Lage noch die über die gewöhnliche Arbeitszeit hinausgehende, als Überstunden geleistete Arbeitszeit objektiv und verlässlich ermittelt werden kann.

Unter diesen Umständen erscheint es für die Arbeitnehmer äußerst schwierig oder gar praktisch unmöglich, die ihnen durch Art. 31 Abs. 2 der Charta und die Richtlinie 2003/88 verliehenen Rechte durchzusetzen, um tatsächlich in den Genuss der Begrenzung der wöchentlichen Arbeitszeit sowie der in dieser Richtlinie vorgesehenen täglichen und wöchentlichen Mindestruhezeiten zu kommen.

Die objektive und verlässliche Feststellung der Zahl der täglichen und wöchentlichen Arbeitsstunden ist nämlich für die Beurteilung grundlegend, ob zum einen die wöchentliche Höchstarbeitszeit, die in Art. 6 der Richtlinie 2003/88 festgelegt wird und die nach dieser Bestimmung die Überstunden einschließt, in dem in Art. 16 Buchst. b oder Art. 19 dieser Richtlinie vorgesehen Bezugszeitraum beachtet wurde, und ob zum anderen die in den Art. 3 und 5 dieser Richtlinie festgelegten täglichen oder wöchentlichen Mindestruhezeiten, was die tägliche Ruhezeit betrifft, in jedem 24-Stunden-Zeitraum oder, was die wöchentliche Ruhezeit betrifft, im Bezugszeitraum nach Art. 16 Buchst. a dieser Richtlinie eingehalten wurden.

Da die Mitgliedstaaten, wie sich aus der in den Rn. 40 und 41 des vorliegenden Urteils genannten Rechtsprechung ergibt, zur Gewährleistung der vollen Wirksamkeit der Richtlinie 2003/88 alle erforderlichen Maßnahmen treffen müssen, um die Beachtung der Mindestruhezeiten zu gewährleisten und jede Überschreitung der wöchentlichen Arbeitszeit zu verhindern, ist eine nationale Regelung, die keine Verpflichtung vorsieht, von einem Instrument Gebrauch zu machen, mit dem die Zahl der täglichen und wöchentlichen Arbeitsstunden objektiv und verlässlich festgestellt werden kann, nach der in Rn. 42 des vorliegenden Urteils genannten Rechtsprechung nicht geeignet, die praktische Wirksamkeit der von Art. 31 Abs. 2 der Charta und von dieser Richtlinie verliehenen Rechte sicherzustellen, da weder die Arbeitgeber noch die Arbeitnehmer überprüfen können, ob diese Rechte beachtet werden, wodurch sie das Ziel dieser Richtlinie, das darin besteht, einen besseren Schutz der Sicherheit und der Gesundheit der Arbeitnehmer sicherzustellen, gefährden kann.

Es ist insoweit unerheblich, dass die im vorliegenden Fall nach spanischem Recht geltende wöchentliche Höchstarbeitszeit, wie die spanische Regierung vorträgt, für den Arbeitnehmer günstiger ist als die in Art. 6 Buchst. b der Richtlinie 2003/88 vorgesehene. Dies ändert nämlich, wie diese Regierung weiter ausführt, nichts daran, dass die in diesem Bereich erlassenen innerstaatlichen Bestimmungen Teil der Umsetzung dieser Richtlinie in das innerstaatliche Recht sind, deren Einhaltung die Mitgliedstaaten mit der Festlegung der zu diesem Zweck erforderlichen Modalitäten sicherstellen müssen. Im Übrigen ist es ohne ein System, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, für einen Arbeitnehmer ebenso schwierig oder gar praktisch unmöglich, die tatsächliche Einhaltung der wöchentlichen Höchstarbeitszeit – unabhängig von deren Dauer – sicherzustellen.

Diese Schwierigkeit wird nicht dadurch behoben, dass die Arbeitgeber in Spanien nach Art. 35 des Arbeitnehmerstatuts ein System zur Erfassung der Überstunden einrichten müssen, die von Arbeitnehmern geleistet werden, die sich dazu bereit erklärt haben. Die Einstufung als „Überstunden" setzt nämlich voraus, dass die Dauer der von dem jeweiligen Arbeitnehmer geleisteten Arbeitszeit bekannt ist und somit zuvor gemessen wurde. Die Verpflichtung, nur die geleisteten Überstunden zu erfassen, bietet den Arbeitnehmern daher kein wirksames Mittel, mit dem zum einen gewährleistet werden kann, dass die von der Richtlinie 2003/88 festgelegte wöchentliche Höchstarbeitszeit, die die Überstunden einschließt, nicht überschritten wird, und zum anderen, dass die in dieser Richtlinie vorgesehenen täglichen und wöchentlichen Mindestruhezeiten in jedem Fall eingehalten werden. In jedem Fall kann mit dieser Verpflichtung nicht das Fehlen eines Systems kompensiert werden, das für die Arbeitnehmer, die der Leistung von Überstunden nicht zugestimmt haben, die tatsächliche Beachtung der Regeln u.a. über die wöchentliche Höchstarbeitszeit gewährleisten könnte.

Im vorliegenden Fall ergibt sich zwar, wie die Deutsche Bank und die spanische Regierung geltend machen, aus den dem Gerichtshof vorgelegten Unterlagen, dass ein Arbeitnehmer, wenn es an einem System, mit dem die Arbeitszeit gemessen werden kann, fehlt, nach den spanischen Verfahrensvorschriften von anderen Beweismitteln, wie u.a. Zeugenaussagen, der Vorlage von E Mails oder der Untersuchung von Mobiltelefonen oder Computern, Gebrauch machen kann, um Anhaltspunkte für eine Verletzung dieser Rechte beizubringen und so eine Beweislastumkehr zu bewirken.

Anders als durch ein System, mit dem die täglich geleistete Arbeitszeit gemessen wird, kann mit solchen Beweismitteln jedoch nicht objektiv und verlässlich die Zahl der von dem Arbeitnehmer täglich oder wöchentlich geleisteten Arbeitszeit festgestellt werden.

Insbesondere ist darauf hinzuweisen, dass aufgrund der schwächeren Position des Arbeitnehmers in einem Arbeitsverhältnis der

Zeugenbeweis allein nicht als wirksames Beweismittel angesehen werden kann, mit dem eine tatsächliche Beachtung der in Rede stehenden Rechte gewährleistet werden kann, da die Arbeitnehmer möglicherweise zögern, gegen ihren Arbeitgeber auszusagen, weil sie befürchten, dass dieser Maßnahmen ergreift, durch die das Arbeitsverhältnis zu ihren Ungunsten beeinflusst werden könnte.

Dagegen bietet ein System, mit dem die von den Arbeitnehmern geleistete tägliche Arbeitszeit gemessen werden kann, diesen ein besonders wirksames Mittel, einfach zu objektiven und verlässlichen Daten über die von ihnen geleistete tatsächliche Arbeitszeit zu gelangen, und kann diesen Arbeitnehmern dadurch sowohl den Nachweis einer Verkennung der ihnen durch die Art. 3 und 5 sowie von Art. 6 Buchst. b der Richtlinie 2003/88 verliehenen Rechte, die das in Art. 31 Abs. 2 der Charta verankerte Grundrecht präzisieren, als auch den zuständigen Behörden und nationalen Gerichten die Kontrolle der tatsächlichen Beachtung dieser Rechte erleichtern.

Es kann auch nicht angenommen werden, dass die Schwierigkeiten aufgrund des Umstands, dass ein System, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, fehlt, durch die Ermittlungs- und Sanktionsbefugnisse, die den Kontrollorganen wie der Arbeitsinspektion nach innerstaatlichem Recht verliehen werden, abgemildert werden können. Ohne ein solches System haben diese Behörden nämlich kein wirksames Mittel, sich den Zugang zu objektiven und verlässlichen Daten über die von den Arbeitnehmern in den einzelnen Unternehmen geleistete Arbeitszeit zu verschaffen, der sich für die Ausübung ihres Kontrollauftrags und gegebenenfalls zur Verhängung einer Strafe als erforderlich erweisen kann (vgl. in diesem Sinne Urteil vom 30. Mai 2013, Worten, C 342/12, EU:C:2013:355, Rn. 37 und die dort angeführte Rechtsprechung).

Daraus folgt, dass es, wie darüber hinaus aus den in Rn. 26 des vorliegenden Urteils genannten, vom vorlegenden Gericht vorgelegten Unterlagen hervorgeht, ohne ein System, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, keine Garantie dafür gibt, dass die tatsächliche Beachtung des von der Richtlinie 2003/88 verliehenen Rechts auf eine Begrenzung der Höchstarbeitszeit sowie auf Mindestruhezeiten den Arbeitnehmern vollständig gewährleistet wird, da sie dem Arbeitgeber einen Spielraum lässt.

Auch wenn die Verantwortlichkeit des Arbeitgebers für die Beachtung der durch die Richtlinie 2003/88 verliehenen Rechte nicht unbeschränkt sein kann, kann die Regelung eines Mitgliedstaats, die nach ihrer Auslegung durch die nationalen Gerichte keine Pflicht des Arbeitgebers zur Messung der geleisteten Arbeitszeit begründet, die in den Art. 3 und 5 sowie in Art. 6 Buchst. b dieser Richtlinie verankerten Rechte aushöhlen, indem sie den Arbeitnehmern nicht die tatsächliche Beachtung des Rechts auf eine Begrenzung der Höchstarbeitszeit und auf Mindestruhezeiten gewährleistet und daher nicht mit dem Ziel dieser Richtlinie vereinbar ist, die diese Mindestvorschriften als unerlässlich für den Schutz der Sicherheit und der Gesundheit der Arbeitnehmer betrachtet (vgl. entsprechend Urteil vom 7. September 2006, Kommission/Vereinigtes Königreich, C 484/04, EU:C:2006:526, Rn. 43 und 44).

Um die praktische Wirksamkeit der von der Richtlinie 2003/88 vorgesehenen Rechte und des in Art. 31 Abs. 2 der Charta verankerten Grundrechts zu gewährleisten, müssen die Mitgliedstaaten die Arbeitgeber daher verpflichten, ein objektives, verlässliches und zugängliches System einzuführen, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann.

Dieses Ergebnis wird durch die Bestimmungen der Richtlinie 89/391 bestätigt. Wie sich aus Art. 1 Abs. 2 und 4 der Richtlinie 2003/88 und ihrem dritten Erwägungsgrund sowie aus Art. 16 Abs. 3 der Richtlinie 89/391 ergibt, findet diese Richtlinie auf die täglichen und wöchentlichen Mindestruhezeiten und die wöchentliche Höchstarbeitszeit unbeschadet strengerer und/oder spezifischerer Vorschriften in der Richtlinie 2003/88 uneingeschränkt Anwendung.

Insoweit ergibt sich die Einrichtung eines objektiven, verlässlichen und zugänglichen Systems, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, aus der allgemeinen Verpflichtung der Mitgliedstaaten und der Arbeitgeber nach Art. 4 Abs. 1 und Art. 6 Abs. 1 der Richtlinie 89/391, eine Organisation und die erforderlichen Mittel zum Schutz der Sicherheit und der Gesundheit der Arbeitnehmer bereitzustellen. Darüber hinaus ist ein solches System erforderlich, damit die Arbeitnehmervertreter, die bei der Sicherheit und dem Gesundheitsschutz der Arbeitnehmer eine besondere Funktion haben, ihr in Art. 11 Abs. 3 dieser Richtlinie vorgesehenes Recht ausüben können, den Arbeitgeber um geeignete Maßnahmen zu ersuchen und ihm Vorschläge zu unterbreiten.

Doch obliegt es nach der in Rn. 41 des vorliegenden Urteils genannten Rechtsprechung, wie der Generalanwalt in den Nrn. 85 bis 88 seiner Schlussanträge ausgeführt hat, den Mitgliedstaaten, im Rahmen des ihnen insoweit eröffneten Spielraums, die konkreten Modalitäten zur Umsetzung eines solchen Systems, insbesondere dessen Form, festzulegen, und zwar gegebenenfalls unter Berücksichtigung der Besonderheiten des jeweiligen Tätigkeitsbereichs, sogar der Eigenheiten bestimmter Unternehmen, namentlich ihrer Größe; dies gilt unbeschadet von Art. 17 Abs. 1 der Richtlinie 2003/88, nach dem die Mitgliedstaaten unter Beachtung der allgemeinen Grundsätze des Schutzes der Sicherheit und der Gesundheit der Arbeitnehmer Ausnahmen u.a. von den Art. 3 bis 6 dieser Richtlinie vornehmen dürfen, wenn die Dauer der Arbeitszeit wegen besonderer Merkmale der ausgeübten Tätigkeit nicht bemessen und/oder vorherbestimmt ist oder von den Arbeitnehmern selbst bestimmt werden kann.

Die vorangehenden Erwägungen können nicht dadurch entkräftet werden, dass bestimmte Sondervorschriften des Unionsrechts im Transportbereich, wie u.a. Art. 9 Buchst. b der Richtlinie 2002/15/EG des Europäischen Parlaments und des Rates vom 11. März 2002 zur Regelung der Arbeitszeit von Personen, die Fahrtätigkeiten im Bereich des Straßentransports ausüben (ABl. 2002, L 80, S. 35) und von Paragraf 12 des Anhangs der Richtlinie 2014/112/EU des Rates vom 19. Dezember 2014 zur Durchführung der von der Europäischen Binnenschifffahrts Union (EBU), der Europäischen Schifferorganisation (ESO) und der Europäischen Transportarbeiter-Föderation (ETF) geschlossenen Europäischen Vereinbarung über die Regelung bestimmter Aspekte der Arbeitszeitgestaltung in der Binnenschifffahrt (ABl. 2014, L 367, S. 86), ausdrücklich die Verpflichtung zur Erfassung der Arbeitszeit der diesen Vorschriften unterliegenden Arbeitnehmer vorsehen.

Auch wenn das Bestehen eines Bedürfnisses nach besonderem Schutz den Unionsgesetzgeber veranlassen konnte, eine solche Verpflichtung bezüglich bestimmter Arbeitnehmergruppen vorzusehen, ist nämlich eine ähnliche Verpflichtung, die in der Einrichtung eines objektiven, verlässlichen und zugänglichen Systems besteht, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, allgemeiner für alle Arbeitnehmer erforderlich, um die praktische Wirksamkeit der Richtlinie 2003/88 zu gewährleisten und der Bedeutung des in Art. 31 Abs. 2 der Charta verankerten Grundrechts, auf die in Rn. 30 des vorliegenden Urteils verwiesen wird, Rechnung zu tragen.

Was im Übrigen die von der spanischen Regierung und der Regierung des Vereinigten Königreichs angesprochenen Kosten betrifft, die mit einem solchen System für die Arbeitgeber verbunden sein könnten, ist darauf hinzuweisen, dass, wie sich aus dem vierten Erwägungsgrund der Richtlinie 2003/88 ergibt, der wirksame Schutz der Sicherheit und der Arbeitnehmergesundheit nicht rein wirtschaftlichen Überlegungen untergeordnet werden darf (vgl. in

diesem Sinne Urteile vom 26. Juni 2001, BECTU, C 173/99, EU:C:2001:356, Rn. 59, sowie vom 9. September 2003, Jaeger, C 151/02, EU:C:2003:437, Rn. 66 und 67).

Im Übrigen haben, wie der Generalanwalt in Nr. 84 seiner Schlussanträge ausgeführt hat, weder die Deutsche Bank noch die spanische Regierung genau und konkret angegeben, worin die praktischen Hindernisse für die Einrichtung eines Systems, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann, im vorliegenden Fall bestünden.

Schließlich ist darauf hinzuweisen, dass nach ständiger Rechtsprechung die sich aus einer Richtlinie ergebende Verpflichtung der Mitgliedstaaten, das in der Richtlinie vorgesehene Ziel zu erreichen, und ihre Pflicht nach Art. 4 Abs. 3 EUV, alle zur Erfüllung dieser Verpflichtung geeigneten Maßnahmen allgemeiner oder besonderer Art zu treffen, allen Trägern öffentlicher Gewalt der Mitgliedstaaten und damit im Rahmen ihrer Zuständigkeiten auch den Gerichten obliegen (vgl. u.a. Urteile vom 19. April 2016, DI, C 441/14, EU:C:2016:278, Rn. 30, und vom 13. Dezember 2018, Hein, C 385/17, EU:C:2018:1018, Rn. 49).

Folglich müssen die mit der Auslegung des nationalen Rechts betrauten nationalen Gerichte bei dessen Anwendung sämtliche nationalen Rechtsnormen berücksichtigen und die im nationalen Recht anerkannten Auslegungsmethoden anwenden, um seine Auslegung so weit wie möglich am Wortlaut und Zweck der fraglichen Richtlinie auszurichten, damit das von ihr festgelegte Ergebnis erreicht und so Art. 288 Abs. 3 AEUV nachgekommen wird (Urteil vom 19. April 2016, DI, C 441/14, EU:C:2016:278, Rn. 31 und die dort angeführte Rechtsprechung).

Das Erfordernis einer unionsrechtskonformen Auslegung umfasst die Verpflichtung der nationalen Gerichte, eine gefestigte Rechtsprechung gegebenenfalls abzuändern, wenn sie auf einer Auslegung des nationalen Rechts beruht, die mit den Zielen einer Richtlinie unvereinbar ist (Urteile vom 19. April 2016, DI, C 441/14, EU:C:2016:278, Rn. 33, vom 17. April 2018, Egenberger, C 414/16, EU:C:2018:257, Rn. 72, und vom 11. September 2018, IR, C 68/17, EU:C:2018:696, Rn. 64).

Nach alledem ist auf die Vorlagefragen zu antworten, dass die Art. 3, 5 und 6 der Richtlinie 2003/88 im Licht von Art. 31 Abs. 2 der Charta sowie von Art. 4 Abs. 1, Art. 11 Abs. 3 und Art. 16 Abs. 3 der Richtlinie 89/391 dahin auszulegen sind, dass sie der Regelung eines Mitgliedstaats entgegenstehen, die nach ihrer Auslegung durch die nationalen Gerichte die Arbeitgeber nicht verpflichtet, ein System einzurichten, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann.

Zum Anspruch eines Strafgefangenen auf Nutzung eines Computers

(**Bundesverfassungsgericht,** Beschluss vom 27. März 2019 – 2 BvR 2268/18 –)

1. **Das Recht eines Gefangenen im bayerischen Strafvollzug, in angemessenem Umfang Bücher und andere Gegenstände zur Fortbildung oder zur Freizeitbeschäftigung zu besitzen, kann aufgrund der grundsätzlich gegebenen Eignung eines Gegenstandes für sicherheits- oder ordnungsgefährdende Verwendungen eingeschränkt werden, sofern derartige Verwendungen nur mit einem von der Anstalt nicht erwartbaren Kontrollaufwand ausgeschlossen werden können.**

2. **Verschaffen besondere Gründe in der Person des Gefangenen seinem Interesse am Besitz eines bestimmten Gegenstandes ein erhöhtes Gewicht, ist dieses nach dem Grundsatz der Verhältnismäßigkeit etwa bei der Bestimmung des für die Anstalt zumutbaren Kontrollaufwands zu berücksichtigen.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Verfassungsbeschwerde betrifft die Frage des Anspruchs eines Strafgefangenen auf den Besitz eines Computers (Laptop) beziehungsweise auf die Nutzung der in der Justizvollzugsanstalt Straubing vorhandenen Computer zum Verfassen von Schriftsätzen, insbesondere für gerichtliche Verfahren.

Aus den Gründen:

1. Die Kammer nimmt die Verfassungsbeschwerde nicht zur Entscheidung an, weil die Annahmevoraussetzungen des § 93a Abs. 2 BVerfGG nicht vorliegen. Der Verfassungsbeschwerde kommt keine grundsätzliche Bedeutung zu. Ihre Annahme ist auch nicht zur Durchsetzung von Grundrechten oder grundrechtsgleichen Rechten des Beschwerdeführers angezeigt, denn sie hat keine hinreichende Aussicht auf Erfolg (vgl. BVerfGE 90, 22 <25 f.>; 96, 245 <250>; BVerfGK 12, 189 <196>).

Die angegriffenen Entscheidungen, die einen Anspruch des Beschwerdeführers auf Besitz eines Laptops nebst Druckers beziehungsweise hilfsweise auf Nutzung von Computern der Justizvollzugsanstalt zum Verfassen von Schriftsätzen im Ergebnis verneint haben, sind nach den geltenden Maßstäben für die Überprüfung fachgerichtlicher Entscheidungen (vgl. BVerfGE 18, 85 <92 f.>) verfassungsrechtlich nicht zu beanstanden.

2. Das Recht eines Gefangenen im bayerischen Strafvollzug, in angemessenem Umfang Bücher und andere Gegenstände zur Fortbildung oder zur Freizeitbeschäftigung zu besitzen, unterliegt gesetzlichen Einschränkungen. Nach Art. 72 Abs. 2 Nr. 2 BayStVollzG besteht dieses Recht unter anderem dann nicht, wenn der Besitz, die Überlassung oder die Benutzung des Gegenstands die Sicherheit oder Ordnung der Anstalt gefährden würde. Das Vorliegen einer solchen Gefährdung kann ohne Verfassungsverstoß allein aufgrund der grundsätzlich gegebenen Eignung eines Gegenstandes für sicherheits- oder ordnungsgefährdende Verwendungen bejaht werden, sofern derartige Verwendungen nur mit einem von der Anstalt nicht erwartbaren Kontrollaufwand ausgeschlossen werden können (vgl. BVerfG, Beschlüsse der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 4 und vom 12. Juni 2002 – 2 BvR 697/02 –, juris, Rn. 2, jeweils m.w.N.). Auf die Frage, ob ein Laptop als elektronisches Unterhaltungsmedium im Sinne von Art. 72 Abs. 2 Nr. 2 Halbsatz 2 BayStVollzG anzusehen ist, kommt es dabei nicht an. Lässt sich der erforderliche Kontrollaufwand durch technische Vorkehrungen, wie zum Beispiel eine Verplombung, auf ein leistbares Maß reduzieren, so dass dem Gefangenen der Besitz des betreffenden Gegenstandes ohne Gefahr für Sicherheit oder Ordnung der Anstalt ermöglicht werden kann, gebietet es der Grundsatz der Verhältnismäßigkeit, diese Möglichkeit zu nutzen. Darüber hinaus können besondere Gründe in der Person des Gefangenen seinem Interesse am Besitz eines bestimmten Gegenstandes ein erhöhtes Gewicht verschaffen, das nach dem Grundsatz der Verhältnismäßigkeit etwa bei der Bestimmung des für die Anstalt zumutba-

ren Kontrollaufwands zu berücksichtigen ist (vgl. BVerfG, Beschlüsse der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 4 und vom 12. Juni 2002 – 2 BvR 697/02 –, juris, Rn. 2, jeweils m.w.N.).

3. Es bestehen keine Anhaltspunkte dafür, dass diese verfassungsrechtlichen Maßstäbe im vorliegenden Fall verfehlt worden wären.

a) Das Landgericht hat sich mit der Frage der Eignung des begehrten Laptops, aber auch einer privaten Nutzung von Computern der Justizvollzugsanstalt für sicherheits- oder ordnungsgefährdende Verwendungen unter Einbeziehung der oben genannten verfassungsrechtlichen Maßstäbe konkret auseinandergesetzt und diese im Ergebnis bejaht, weil in den Datenspeicher des Computers Textinhalte (z.B. Erkenntnisse über Fluchtwege, verbotene Außenkontakte, Aufstellungen über die Abgabe von Betäubungsmitteln an Mitgefangene und andere verbotene Beziehungen zwischen den Gefangenen) eingegeben und – im Falle der privaten Nutzung von Anstaltscomputern wie auch bei der Gewährung eines privaten Laptops – unerlaubt und unkontrolliert ausgetauscht werden können. Diese generelle Eignungsbeurteilung lässt Anhaltspunkte für Willkür nicht erkennen (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 5).

Der vom Beschwerdeführer erhobene Einwand, die Speicherkapazität eines Laptops müsse außer Betracht bleiben, weil er Sachverhalte der Kenntnis der Justizvollzugsanstalt auch dadurch entziehen könne, dass er sich diese schlicht merke, verfängt nicht. Das Landgericht hat nicht auf die Speicherkapazität von Computern als solche, sondern auf die erweiterten Möglichkeiten der Informationsspeicherung, die mit der Verfügung über einen Computer verbunden sind, abgestellt. Diese begründen zusätzliche Möglichkeiten eines sicherheitsgefährdenden Missbrauchs (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 6).

Hinsichtlich der Frage, ob den festgestellten, durch Verplombung oder Einhausung nicht ausschließbaren, erheblichen Sicherheitsgefahren mit Kontrollen seitens der Justizvollzugsanstalt ausreichend begegnet werden kann, ist das Landgericht zu der Einschätzung gelangt, dass eine Entkräftung der Sicherheitsbedenken durch Kontrollen wegen des damit verbundenen erheblichen zusätzlichen zeitlichen Aufwandes ausscheide. Dass das Gericht dabei auf eine generalisierende Betrachtungsweise abgestellt hat, ist verfassungsrechtlich nicht zu beanstanden (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 10). Ebenso begegnet es keinen Bedenken, dass das Landgericht, der Versagungsentscheidung der Justizvollzugsanstalt folgend, darauf abgestellt hat, dass Maßnahmen, mit denen eine ausreichende Kontrollierbarkeit sichergestellt werden kann, auch bei gleicher Handhabung vergleichbarer anderer Fälle umsetzbar sein müssen (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 31. März 2003 – 2 BvR 1848/02 –, juris, Rn. 11). Dass das Gericht diese Frage der Sache nach verneint hat, ist nachvollziehbar.

Das vom Beschwerdeführer geltend gemachte Interesse, einen Laptop zwecks Anfertigung und Speicherung von Schriftsätzen an Behörden und Gerichte zu nutzen, um ihn in die Lage zu versetzen, eine Vielzahl auch komplexer Verfahren zur Wahrung seiner Rechte zu führen, hat zwar grundsätzlich Gewicht. Es ist aber kein seinem Gewicht nach so außergewöhnliches Interesse, dass allein auf die isolierte Möglichkeit gefahrenabwehrender Kontrollen in seinem konkreten Fall abgestellt werden müsste. Zudem ist weder dargetan noch ersichtlich, dass dem Beschwerdeführer ohne den Besitz des Laptops der Zugang zu Gerichten unzumutbar erschwert wäre. Die einschränkenden Faktoren, die der Beschwerdeführer benennt, etwa die Notwendigkeit, um 20 Uhr mit dem Anfertigen von Schriftsätzen aufzuhören, weil seine Schreibmaschine andere Gefangene störe, erscheinen vielmehr zumutbar. Hinsichtlich weiterer geltend gemachter Beschränkungen, etwa der vorgetragenen Notwendigkeit, angegriffene Entscheidungen stets händisch auf der mechanischen Schreibmaschine abzutippen oder Mehrfachfertigungen von Schriftsätzen zu erstellen, ist nicht ersichtlich, warum der Beschwerdeführer die Möglichkeit der Anfertigung von Kopien, auf die die Justizvollzugsanstalt in ihrer Stellungnahme vom 3. Januar 2018 explizit hingewiesen hat, nicht als gangbare Lösung ansieht. Ebenso hat er nicht nachvollziehbar dargetan, warum er die von der Justizvollzugsanstalt in Aussicht gestellte Möglichkeit, den Besitz einer elektrischen Schreibmaschine zu gewähren, mit der wenigstens eine gewisse Erleichterung einträte, ablehnt.

Schließlich folgt aus dem in der Verfassungsbeschwerde und im fachgerichtlichen Verfahren geltend gemachten Grundsatz der Waffengleichheit in gerichtlichen Verfahren nicht das Recht auf eine gleichwertige technische Ausstattung oder auf den Zugang zu einem Computer (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 12. Juni 2002 – 2 BvR 697/02 –, juris, Rn. 6).

b) Der generelle Vortrag des Beschwerdeführers, dass angesichts des prägenden Charakters, den die elektronische Datenverarbeitung im modernen gesellschaftlichen Leben hat, aus dem Angleichungsgrundsatz, aber auch aus Resozialisierungsgesichtspunkten ein erhebliches (und stetig steigendes) Interesse an einem Zugang von Strafgefangenen zu Computern besteht, ist zwar bedenkenswert. Diese Gesichtspunkte sind aber für sich genommen nicht geeignet, unter Ausklammerung legitimer Sicherheitsbedenken einen verfassungsrechtlichen Anspruch auf den Zugang zu neuen Medien im Strafvollzug zu vermitteln.

Etwas anderes folgt auch nicht aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR). Zwar hat dieser in Fällen, die den Internetzugang für Strafgefangene betrafen, die gesteigerte Bedeutung der neuen Medien im heutigen Alltag betont (siehe EGMR, Kalda v. Estonia, Urteil vom 19. Januar 2016, Nr. 17429/10, § 52, und Jankovskis v. Lithuania, Urteil vom 17. Januar 2017, Nr. 21575/08, § 54 und § 62). Eine grundsätzliche Verpflichtung der Vertragsstaaten, einen Zugang zu diesen zu ermöglichen, hat er der – im vorliegenden Fall ohnehin nicht einschlägigen – Informationsfreiheit nach Art. 10 Abs. 1 Satz 2 EMRK indes nicht entnommen (vgl. EGMR, Kalda v. Estonia, Urteil vom 19. Januar 2016, Nr. 17429/10, § 45, und Jankovskis v. Lithuania, Urteil vom 17. Januar 2017, Nr. 21575/08, § 55).

Ordentliche Kündigung eines Chefarztes wegen der Religion

(**Bundesarbeitsgericht**, Urteil vom 20. Februar 2019 – 2 AZR 746/14 –)

§ 9 Abs. 2 AGG ist aufgrund von unionsrechtlichen Vorgaben dahin auszulegen, dass eine der Kirche zugeordnete Einrichtung nicht das Recht hat, bei einem Verlangen an das loyale und aufrichtige Verhalten im Sinne

ihres jeweiligen Selbstverständnisses Beschäftigte in leitender Stellung je nach deren Konfession oder Konfessionslosigkeit unterschiedlich zu behandeln, wenn nicht die Religion oder die Weltanschauung im Hinblick auf die Art der betreffenden beruflichen Tätigkeiten oder die Umstände ihrer Ausübung eine berufliche Anforderung ist, die angesichts des Ethos der in Rede stehenden Einrichtung wesentlich, rechtmäßig und gerechtfertigt ist und dem Grundsatz der Verhältnismäßigkeit entspricht.

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer ordentlichen Kündigung.

Die Beklagte betreibt ua. Krankenhäuser. Dabei verfolgt sie vorrangig eine religiöse Zielsetzung in Form der Verwirklichung von Aufgaben der Caritas als Lebens- und Wesensäußerung der römisch-katholischen Kirche. Die Beklagte unterliegt der Aufsicht des Erzbischofs von Köln. Der Kläger ist katholisch und war bei ihr seit dem Jahre 2000 auf der Grundlage eines Dienstvertrags vom 12. Oktober 1999 als Abteilungsarzt mit der Dienstbezeichnung „Chefarzt" beschäftigt.

Die Parteien schlossen den Dienstvertrag unter Zugrundelegung der vom Erzbischof von Köln erlassenen Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse vom 22. September 1993 (Amtsblatt des Erzbistums Köln S. 222; GrO 1993) und der Grundordnung für katholische Krankenhäuser in Nordrhein-Westfalen vom 5. November 1996 (Amtsblatt des Erzbistums Köln S. 321; GrOK-NRW). Nach Art. 3 Abs. 2 GrO 1993 konnten kirchliche Dienstgeber pastorale, katechetische sowie in der Regel erzieherische und leitende Aufgaben nur einer Person übertragen, die der katholischen Kirche angehört. Zu den in diesem Sinne leitend tätigen Mitarbeitern gehörten Abteilungsärzte (Abschnitt A. 5. Satz 2 GrOK-NRW). Art. 4 Abs. 1 GrO 1993 forderte von den katholischen Mitarbeitern, dass sie die Grundsätze der katholischen Glaubens- und Sittenlehre anerkennen und beachten. Nach Art. 5 Abs. 2 GrO 1993 handelte es sich beim Abschluss einer nach dem Glaubensverständnis und der Rechtsordnung der Kirche ungültigen Ehe um einen schwerwiegenden Loyalitätsverstoß, der eine Kündigung rechtfertigen konnte. Die Weiterbeschäftigung war grundsätzlich ausgeschlossen, wenn der Loyalitätsverstoß von einem leitenden Mitarbeiter begangen wurde (Art. 5 Abs. 3 GrO 1993). In § 10 Abs. 4 Nr. 2 des Dienstvertrags der Parteien ist das Leben in kirchlich ungültiger Ehe oder eheähnlicher Gemeinschaft als wichtiger Grund zur außerordentlichen Kündigung genannt.

Eine ungültige Ehe schließt nach katholischem Rechtsverständnis (vgl. Canon [Can.] 1085 § 1 Codex Iuris Canonici [CIC]), wer durch das Band einer früheren Ehe gebunden ist. Eine neue Eheschließung ist auch dann nicht erlaubt, wenn eine frühere Ehe nichtig oder aufgelöst worden ist, die Nichtigkeit bzw. die Auflösung der früheren Ehe aber noch nicht rechtmäßig und sicher feststeht (Can. 1085 § 2 CIC).

Der Kläger war mit seiner ersten Ehefrau nach katholischem Ritus verheiratet. Diese trennte sich von ihm im August 2005. Die Ehe wurde im März 2008 geschieden. Aus ihr waren zwei Töchter hervorgegangen. Mit seiner späteren zweiten Ehefrau lebte der Kläger von 2006 bis 2008 unverheiratet zusammen. Im August 2008 heiratete er ein zweites Mal standesamtlich, ohne dass seine erste Ehe kirchenrechtlich für nichtig erklärt worden war. Die Beklagte erfuhr von der erneuten Eheschließung spätestens im November 2008. Nach Anhörung der bei ihr bestehenden Mitarbeitervertretung kündigte die Beklagte das Arbeitsverhältnis der Parteien mit Schreiben vom 30. März 2009 fristgerecht zum 30. September 2009.

Dagegen hat der Kläger rechtzeitig Kündigungsschutzklage erhoben und die Auffassung vertreten, die Kündigung sei sozial ungerechtfertigt. Die erneute Heirat stelle keinen Kündigungsgrund dar. Er habe sich nicht kirchenfeindlich verhalten. Die Kündigung verstoße gegen den Gleichbehandlungsgrundsatz. Nach der GrO 1993 habe die Wiederheirat eines evangelischen oder konfessionslosen Abteilungsarztes keine Folgen für dessen Arbeitsverhältnis mit der Beklagten gehabt.

Die Beklagte hat beantragt, die Klage abzuweisen. Sie hat die Auffassung vertreten, die Kündigung sei sozial gerechtfertigt. Der Kläger sei eine ungültige Ehe im Sinne des katholischen Kirchenrechts eingegangen und habe dadurch in erheblicher Weise gegen seine Verpflichtungen aus dem Arbeitsverhältnis verstoßen. Soweit sie anderen wiederverheirateten Chefärzten nicht gekündigt habe, handele es sich – abgesehen von aus anderen Gründen mit dem Streitfall ihres Erachtens nicht vergleichbaren Fällen – nicht um katholische Arbeitnehmer, von denen nicht in derselben Weise wie von katholischen Mitarbeitern die Befolgung der katholischen Glaubens- und Sittenlehre verlangt werden könne.

Das Arbeitsgericht hat der Klage stattgegeben. Das Landesarbeitsgericht hat die Berufung der Beklagten zurückgewiesen. Mit ihrer Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter. Das ihr Rechtsmittel zurückweisende Senatsurteil vom 8. September 2011 (– 2 AZR 543/10 – BAGE 139, 144) hat das Bundesverfassungsgericht mit Beschluss vom 22. Oktober 2014 (- 2 BvR 661/12 – BVerfGE 137, 273) aufgehoben und die Sache an das Bundesarbeitsgericht zurückverwiesen. Der Senat hat mit Beschluss vom 28. Juli 2016 (– 2 AZR 746/14 [A] – BAGE 156, 23) den Gerichtshof der Europäischen Union nach Art. 267 AEUV um die Beantwortung von Fragen zur Auslegung von Unionsrecht und vorrangig von Art. 4 Abs. 2 UnterAbs. 2 der Richtlinie 2000/78/EG (RL 2000/78/EG) ersucht. Hierüber hat der Gerichtshof mit Urteil vom 11. September 2018 (– C-68/17 –) entschieden.

Aus den Gründen:

Die Revision ist unbegründet. Das Landesarbeitsgericht hat im Ergebnis zutreffend erkannt, dass die Kündigung der Beklagten vom 30. März 2009 sozial ungerechtfertigt iSd. § 1 Abs. 2 KSchG ist.

I. Der Erste Abschnitt des Kündigungsschutzgesetzes fand nach § 1 Abs. 1, § 23 Abs. 1 KSchG im Kündigungszeitpunkt auf das Arbeitsverhältnis der Parteien Anwendung.

II. Die Kündigung der Beklagten ist weder durch Gründe im Verhalten noch in der Person des Klägers iSv. § 1 Abs. 2 KSchG bedingt. Es fehlt an einem kündigungsrelevanten Verstoß des Klägers gegen eine vertragliche Loyalitätspflicht. Die Loyalitätserwartung, den heiligen und unauflöslichen Charakter der kirchlichen Eheschließung zu achten, stellt auch keine berechtigte Anforderung der Beklagten an die persönliche Eignung des Klägers dar. Die Vereinbarung im Dienstvertrag der Parteien, mit der Art. 4 Abs. 1 sowie Art. 5 Abs. 2 und Abs. 3 GrO 1993 in Bezug genommen wurden, war jedenfalls im Zeitpunkt der streitbefangenen Kündigung gem. § 7 Abs. 2 AGG unwirksam, soweit danach – iVm. Abschnitt A. 5. Satz 2 GrOK-NRW – bei Abteilungsärzten der Abschluss einer nach dem Glaubensverständnis und der Rechtsordnung der katholischen Kirche ungültigen Ehe einen Loyalitätsverstoß darstellt, der grundsätzlich eine Kündigung des Arbeitsverhältnisses rechtfertigt. Ebenso gem. § 7 Abs. 2 AGG unwirksam ist § 10 Abs. 4 Nr. 2 des Dienstvertrags, soweit danach das Leben in kirchlich ungültiger Ehe einen wichtigen Grund zur außerordentlichen Kündigung darstellt. Es handelt sich um Beschäftigungs- und Entlassungsbe-

dingungen iSd. § 2 Abs. 1 Nr. 2 AGG, die den Kläger gem. § 7 Abs. 1 iVm. § 3 Abs. 1 Satz 1 AGG unmittelbar wegen eines in § 1 AGG genannten Grundes benachteiligen, ohne dass dies nach § 9 Abs. 2 AGG gerechtfertigt ist. Nichts anderes würde gelten, soweit die Beklagte diese Loyalitätserwartungen nicht aus dem schriftlichen Dienstvertrag der Parteien, sondern aus ungeschriebenen nebenvertraglichen Pflichten (§ 241 Abs. 2 BGB) herleiten wollte.

1. Gemäß § 7 Abs. 1 AGG dürfen Beschäftigte nicht wegen eines in § 1 AGG genannten Grundes benachteiligt werden. Bestimmungen in Vereinbarungen, die gegen das Benachteiligungsverbot verstoßen, sind nach § 7 Abs. 2 AGG unwirksam. Sie sind auch dann an dieser Bestimmung zu messen, wenn sie zwar – wie hier – vor Inkrafttreten des AGG am 18. August 2006 abgeschlossen wurden, aber noch danach eine benachteiligende Wirkung entfalten (BAG 25. März 2015 – 5 AZR 458/13 – Rn. 24; 20. Juni 2013 – 2 AZR 295/12 – Rn. 37, BAGE 145, 296). § 33 AGG enthält insoweit keine entgegenstehende Übergangsregelung. Die benachteiligende Wirkung der Beschäftigungsbedingung, das Eingehen einer nach dem Glaubensverständnis und der Rechtsordnung der katholischen Kirche ungültigen Ehe stelle einen Loyalitätsverstoß dar, dauerte über den Zeitpunkt des Inkrafttretens des AGG an. Sie sollte fortdauernd eine entsprechende arbeitsvertragliche Pflicht des Klägers begründen, gegen die er durch die erneute Eheschließung im August 2008 verstieß. Die benachteiligende Wirkung der Entlassungsbedingungen, wonach ein entsprechender Loyalitätsverstoß die Kündigung des Arbeitsverhältnisses rechtfertigen konnte, trat mit der darauf gestützten Kündigung der Beklagten vom 30. März 2009 ein.

2. Der Kläger wurde durch die fraglichen Beschäftigungs- und Entlassungsbedingungen wegen seiner Religion iSd. § 1 AGG, nämlich der Zugehörigkeit zur katholischen Kirche, gegenüber nicht der katholischen Kirche angehörenden Abteilungsärzten unmittelbar benachteiligt (§ 3 Abs. 1 Satz 1 AGG). Das Leben in einer kirchlich ungültigen Ehe war gem. Art. 4 Abs. 1 iVm. Art. 5 Abs. 2 und Abs. 3 Satz 1 der mit dem Dienstvertrag in Bezug genommenen GrO 1993 nur bei katholischen leitenden Arbeitnehmern, zu denen auch Abteilungsärzte gehörten, ein die Weiterbeschäftigung in der Regel nicht zulassender Verstoß gegen die Loyalitätsanforderungen, der eine Kündigung des Arbeitsverhältnisses rechtfertigen konnte. Hingegen hatte die Wiederheirat eines evangelischen oder konfessionslosen Abteilungsarztes nach den Regelungen der GrO 1993 keine Folgen für dessen Arbeitsverhältnis mit der Beklagten.

3. Diese Benachteiligung war nicht gem. § 9 Abs. 2 AGG gerechtfertigt.

a) Nach § 9 Abs. 2 AGG berührt das Verbot unterschiedlicher Behandlung wegen der Religion oder der Weltanschauung nicht das Recht der in Abs. 1 der Bestimmung genannten Religionsgemeinschaften, der ihnen zugeordneten Einrichtungen ohne Rücksicht auf ihre Rechtsform oder der Vereinigungen, die sich die gemeinschaftliche Pflege einer Religion oder Weltanschauung zur Aufgabe machen, von ihren Beschäftigten ein loyales und aufrichtiges Verhalten im Sinne ihres jeweiligen Selbstverständnisses zu verlangen. § 9 AGG dient der Umsetzung von Art. 4 Abs. 2 RL 2000/78/EG (BT-Drs. 16/1780 S. 35). Die Zulässigkeit einer unterschiedlichen Behandlung wegen der Religion oder der Weltanschauung bei den Loyalitätsanforderungen gem. § 9 Abs. 2 AGG ist daher, soweit die im nationalen Recht anerkannten Auslegungsmethoden es zulassen, unter Beachtung der Richtlinie und der zu ihrer Auslegung ergangenen Rechtsprechung des Gerichtshofs der Europäischen Union zu prüfen.

b) § 9 Abs. 2 AGG ist aufgrund der unionsrechtlichen Vorgaben, insbesondere von Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG, für eine der Kirche zugeordnete Einrichtung – nur über diese hat der Senat vorliegend zu befinden – dahin auszulegen, dass die Einrichtung nicht das Recht hat, bei einem Verlangen an das loyale und aufrichtige Verhalten im Sinne ihres jeweiligen Selbstverständnisses Beschäftigte in leitender Stellung je nach deren Konfession oder Konfessionslosigkeit unterschiedlich zu behandeln, wenn nicht die Religion oder die Weltanschauung im Hinblick auf die Art der betreffenden beruflichen Tätigkeiten oder die Umstände ihrer Ausübung eine berufliche Anforderung ist, die angesichts des Ethos der in Rede stehenden Einrichtung wesentlich, rechtmäßig und gerechtfertigt ist und dem Grundsatz der Verhältnismäßigkeit entspricht. Die Frage, ob diese Kriterien erfüllt sind, unterliegt einer wirksamen gerichtlichen Kontrolle.

aa) Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG bestimmt, dass die Kirchen und andere öffentliche oder private Organisationen, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht, im Einklang mit den einzelstaatlichen verfassungsrechtlichen Bestimmungen und Rechtsvorschriften von den für sie arbeitenden Personen verlangen können, dass sie sich loyal und aufrichtig im Sinne des Ethos der Organisation verhalten, sofern die Bestimmungen der Richtlinie im Übrigen eingehalten werden.

bb) Der Gerichtshof der Europäischen Union hat entschieden, dass eine Ungleichbehandlung bei der Anforderung eines loyalen und aufrichtigen Verhaltens im Sinne des Ethos des Arbeitgebers gem. Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG, die sich ausschließlich auf die Konfession der Beschäftigten stützt, ua. die in Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG genannten Kriterien einzuhalten hat (EuGH 11. September 2018 – C-68/17 – Rn. 49), was angesichts des sich aus Art. 47 der Charta der Grundrechte der Europäischen Union (GRC) ergebenden Rechts auf wirksamen gerichtlichen Schutz der sich für die jeweilige Person aus dem Unionsrecht ergebenden Rechte gegebenenfalls einer wirksamen gerichtlichen Kontrolle unterliegen muss (EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 59). Eine Kirche oder eine andere öffentliche oder private Organisation, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht, darf daher bei der Anforderung, sich loyal und aufrichtig im Sinne dieses Ethos zu verhalten, ihre Beschäftigten in leitender Stellung nur dann je nach deren Zugehörigkeit zur Religion bzw. deren Bekenntnis zur Weltanschauung dieser Kirche oder dieser anderen Organisation unterschiedlich behandeln, wenn die Religion oder die Weltanschauung im Hinblick auf die Art der betreffenden beruflichen Tätigkeiten oder die Umstände ihrer Ausübung eine wesentliche, rechtmäßige und gerechtfertigte berufliche Anforderung angesichts dieses Ethos ist (EuGH 11. September 2018 – C-68/17 – Rn. 55). Maßgeblich ist danach, ob die fragliche Loyalitätspflicht als Teil der betreffenden Religion im Hinblick auf die Art der Tätigkeit oder die Umstände ihrer Ausübung eine wesentliche, rechtmäßige und gerechtfertigte berufliche Anforderung angesichts dieses Ethos ist (vgl. EuGH 11. September 2018 – C-68/17 – Rn. 49 f.). Dies zu beurteilen, ist Sache des nationalen Gerichts (EuGH 11. September 2018 – C-68/17 – Rn. 56).

(1) „Wesentlich“ ist eine berufliche Anforderung iSv. Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG, sofern die Zugehörigkeit zu der Religion bzw. das Bekenntnis zu der Weltanschauung, auf der

das Ethos der betreffenden Kirche oder Organisation beruht, aufgrund der Bedeutung der betreffenden beruflichen Tätigkeit für die Bekundung dieses Ethos oder die Ausübung des in Art. 17 AEUV und in Art. 10 GRC anerkannten Rechts dieser Kirche oder Organisation auf Autonomie notwendig erscheinen muss (EuGH 11. September 2018 – C-68/17 – Rn. 51; vgl. in diesem Sinne auch EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 50, 65).

(2) Die Anforderung ist „rechtmäßig" iSv. Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG, wenn sie nicht zur Verfolgung eines sachfremden Ziels ohne Bezug zum Ethos oder zur Ausübung des Rechts der Kirche oder Organisation auf Autonomie dient (EuGH 11. September 2018 – C-68/17 – Rn. 52; 17. April 2018 – C-414/16 – [Egenberger] Rn. 66).

(3) Das Erfordernis, die Anforderung müsse „gerechtfertigt" iSv. Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG sein, impliziert nicht nur, dass die Einhaltung der in Art. 4 Abs. 2 RL 2000/78/EG genannten Kriterien durch ein innerstaatliches Gericht überprüfbar sein muss, sondern auch, dass es der Kirche oder Organisation, die eine berufliche Anforderung aufgestellt hat, obliegt, im Licht der tatsächlichen Umstände des Einzelfalls darzutun, dass die geltend gemachte Gefahr einer Beeinträchtigung ihres Ethos oder ihres Rechts auf Autonomie wahrscheinlich und erheblich ist, so dass sich eine solche Anforderung als notwendig erweist (EuGH 11. September 2018 – C-68/17 – Rn. 53; vgl. in diesem Sinne auch EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 67).

(4) Schließlich muss die Anforderung mit dem Grundsatz der Verhältnismäßigkeit im Einklang stehen, was bedeutet, dass die nationalen Gerichte prüfen müssen, ob die Anforderung angemessen ist und nicht über das zur Erreichung des angestrebten Ziels Erforderliche hinausgeht (EuGH 11. September 2018 – C-68/17 – Rn. 54; 17. April 2018 – C-414/16 – [Egenberger] Rn. 68).

cc) Nach der Rechtsprechung des Gerichtshofs der Europäischen Union obliegt es den nationalen Gerichten, unter Berücksichtigung sämtlicher nationaler Rechtsnormen und der im nationalen Recht anerkannten Auslegungsmethoden zu entscheiden, ob und inwieweit eine nationale Rechtsvorschrift wie § 9 Abs. 2 AGG im Einklang mit der RL 2000/78/EG ausgelegt werden kann, ohne dass dies zu einer Auslegung contra legem führt (EuGH 11. September 2018 – C-68/17 – Rn. 63; vgl. in diesem Sinne auch EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 71 und die dort angeführte Rechtsprechung; zum Rahmenbeschluss über den Europäischen Haftbefehl vgl. BVerfG 15. Dezember 2015 – 2 BvR 2735/14 – Rn. 77, BVerfGE 140, 317). Die sich aus einer Richtlinie ergebende Verpflichtung der Mitgliedstaaten, das in der Richtlinie vorgesehene Ziel zu erreichen, und ihre Pflicht, alle zur Erfüllung dieser Verpflichtung geeigneten Maßnahmen allgemeiner oder besonderer Art zu treffen, obliegt allen Trägern öffentlicher Gewalt der Mitgliedstaaten und damit im Rahmen ihrer Zuständigkeiten auch den Gerichten (EuGH 19. April 2016 – C-441/14 – [Dansk Industri] Rn. 30). Die mit der Auslegung des nationalen Rechts betrauten nationalen Gerichte müssen bei dessen Anwendung sämtliche nationalen Rechtsnormen berücksichtigen und die im nationalen Recht anerkannten Auslegungsmethoden anwenden, um seine Auslegung so weit wie möglich am Wortlaut und Zweck der fraglichen Richtlinie auszurichten, damit das von ihr festgelegte Ergebnis erreicht und so Art. 288 Abs. 3 AEUV nachgekommen wird (EuGH 19. April 2016 – C-441/14 – [Dansk Industri] Rn. 31; in diesem Sinne bereits EuGH 5. Oktober 2004 – C-397/01 bis C-403/01 – [Pfeiffer ua.] Rn. 113 f. sowie 19. Januar 2010 – C-555/07 – [Kücükdeveci] Rn. 48).

dd) Die Verpflichtung des nationalen Richters, bei der Auslegung und Anwendung der einschlägigen Vorschriften des innerstaatlichen Rechts das Unionsrecht heranzuziehen, findet zwar ihre Grenzen in den allgemeinen Rechtsgrundsätzen und darf nicht als Grundlage für eine Auslegung contra legem des nationalen Rechts dienen (EuGH 19. April 2016 – C-441/14 – [Dansk Industri] Rn. 32; vgl. auch EuGH 15. April 2008 – C-268/06 – [Impact] Rn. 100; 24. Januar 2012 – C-282/10 – [Dominguez] Rn. 25; 15. Januar 2014 – C-176/12 – [Association de médiation sociale] Rn. 39). Das Erfordernis einer unionsrechtskonformen Auslegung umfasst jedoch die Verpflichtung der nationalen Gerichte, eine gefestigte Rechtsprechung gegebenenfalls abzuändern, wenn sie auf einer Auslegung des nationalen Rechts beruht, die mit den Zielen einer Richtlinie unvereinbar ist (EuGH 11. September 2018 – C-68/17 – Rn. 64; 17. April 2018 – C-414/16 – [Egenberger] Rn. 72; dem folgend BAG 5. Dezember 2012 – 7 AZR 698/11 – Rn. 37, BAGE 144, 85; BGH 28. Oktober 2015 – VIII ZR 158/11 – Rn. 37, BGHZ 207, 209; 26. November 2008 – VIII ZR 200/05 – Rn. 21 mwN, BGHZ 179, 27). Eine solche Rechtsfortbildung kann in Betracht kommen, wenn der Gesetzgeber mit der von ihm geschaffenen Regelung eine Richtlinie umsetzen wollte, hierbei aber deren Inhalt missverstanden hat (BGH 28. Oktober 2015 – VIII ZR 158/11 – aaO; 21. Dezember 2011 – VIII ZR 70/08 – Rn. 32 f., BGHZ 192, 148). Ein nationales Gericht darf nicht davon ausgehen, dass es eine nationale Vorschrift nicht im Einklang mit dem Unionsrecht auslegen könne, nur weil sie in ständiger Rechtsprechung in einem nicht mit dem Unionsrecht zu vereinbarenden Sinne ausgelegt worden ist (EuGH 11. September 2018 – C-68/17 – Rn. 65; 17. April 2018 – C-414/16 – [Egenberger] Rn. 73 und die dort angeführte Rechtsprechung).

ee) Unter Anwendung dieser Grundsätze ist § 9 Abs. 2 AGG im Einklang mit dem Unionsrecht und insbesondere Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG dahin auszulegen, dass Anforderungen an ein loyales und aufrichtiges Verhalten im Sinne des jeweiligen Selbstverständnisses der Religionsgemeinschaft, die zu einer Ungleichbehandlung von Beschäftigten in leitender Stellung je nach deren Konfession oder Konfessionslosigkeit führen, die in Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG genannten Kriterien einhalten müssen, wobei die Frage, ob die danach geforderten Voraussetzungen gegeben sind, einer wirksamen gerichtlichen Kontrolle unterliegt.

(1) Wortlaut und Gesetzessystematik geben für die Möglichkeit einer unionsrechtskonformen Auslegung von § 9 Abs. 2 AGG kein eindeutiges Ergebnis vor. Die Vorschrift spricht zwar – anders als Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG – nicht von einem „(K)önnen …", „(s)ofern die Bestimmungen dieser Richtlinie im übrigen eingehalten werden", sondern davon, das Verbot unterschiedlicher Behandlung wegen der Religion oder der Weltanschauung berühre nicht das „Recht" der Religionsgemeinschaften und der ihnen zugeordneten Einrichtungen, von ihren Beschäftigten ein loyales und aufrichtiges Verhalten im Sinne ihres jeweiligen Selbstverständnisses zu verlangen. Die Regelung nimmt damit – anders als Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG – zumindest explizit nicht Bezug auf andere, dieses Recht näher definierende Bestimmungen. Der normative Begriff des „Rechts" lässt aber auch ausreichend sprachlichen Raum für eine richtlinienkonforme Lesart, nach der es sich um ein im Einklang mit dem umzusetzenden Unionsrecht stehendes Recht handeln muss.

(2) Ein solchermaßen unionsrechtskonformes Verständnis von § 9 Abs. 2 AGG erlauben auch die Entstehungsgeschichte der Vorschrift und der darin zum Ausdruck kommende Wille des deutschen Gesetzgebers, Art. 4 Abs. 2 RL 2000/78/EG in nationales Recht umzusetzen. Der Gesetzgeber meinte zwar, der Erwägungsgrund 24 der RL 2000/78/EG lasse es zu, dass die Mitgliedstaaten spezifische Bestimmungen entsprechend dem deutschen Verfassungsverständnis auch hinsichtlich von Verhaltensanforderungen beibehalten oder vorsehen, die eine Religions- oder Weltanschauungsgemeinschaft an ihre Mitarbeiter stelle, und dass es dabei den Kirchen und Weltanschauungsgemeinschaften selbst obliege, dementsprechend verbindliche innere Regelungen zu schaffen (BT-Drs. 16/1780 S. 35 f.). Damit hat er aber, wie aufgrund der Entscheidung des Gerichtshofs der Europäischen Union vom 11. September 2018 (- C-68/17 -) nunmehr feststeht, den Inhalt der RL 2000/78/EG missverstanden, die – anders als das deutsche Verfassungsverständnis – eine tätigkeitsbezogene Rechtfertigung von Ungleichbehandlungen bei den Loyalitätserwartungen allein aufgrund der Religion verlangt, die überdies einer wirksamen Kontrolle durch die staatlichen Gerichte unterliegen muss. Das ändert indes nichts an der ausdrücklich verlautbarten gesetzgeberischen Grundentscheidung, die Vorgaben der RL 2000/78/EG umzusetzen. Ein unionsrechtskonformes Verständnis von § 9 Abs. 2 AGG respektiert diese und setzt sich damit nicht etwa über einen eindeutig erkennbaren entgegenstehenden Willen des Gesetzgebers hinweg (zu dieser Schranke vgl. BVerfG 6. Juni 2018 – 1 BvL 7/14, 1 BvR 1375/14 – Rn. 73).

c) Die demnach in unionsrechtskonformer Auslegung von § 9 Abs. 2 AGG zu stellenden Anforderungen an die Zulässigkeit einer Ungleichbehandlung des Klägers gegenüber den nicht der katholischen Konfession angehörenden Abteilungsärzten der Beklagten in Bezug auf die ihm auferlegte Loyalitätserwartung, den heiligen und unauflöslichen Charakter der kirchlichen Eheschließung zu achten, sind im Streitfall nicht erfüllt.

aa) Dies folgt allerdings nicht schon aus den Hinweisen, die der Gerichtshof der Europäischen Union in seine Entscheidung über das Vorabentscheidungsersuchen aufgenommen hat. Nach diesen erscheint dem Gerichtshof die Akzeptanz des Eheverständnisses der katholischen Kirche unter Berücksichtigung der vom Kläger ausgeübten beruflichen Tätigkeiten für die Bekundung des Ethos der Beklagten nicht notwendig und keine wesentliche Voraussetzung der beruflichen Tätigkeit iSv. Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG zu sein (EuGH 11. September 2018 – C-68/17 – Rn. 58). Die vorgenannten Ausführungen des Gerichtshofs entfalten weder nach Unionsrecht noch nach nationalem Recht für den Senat Bindungswirkung. Sie betreffen nicht die abstrakte Auslegung von Unionsrecht, sondern sind einzelfallbezogen und beschränken sich auf die Anwendung von Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG auf einen Sachverhalt, für dessen Feststellung dem Gerichtshof die Befugnis fehlt. Sie enthalten lediglich Hinweise, mit denen dieser dem Senat „auf der Grundlage der Akten des Ausgangsverfahrens" und der vor dem Gerichtshof abgegebenen schriftlichen und mündlichen Erklärungen eine Entscheidung über den Rechtsstreit ermöglichen möchte (EuGH 11. September 2018 – C-68/17 – Rn. 56).

bb) Zugunsten der Beklagten kann davon ausgegangen werden, dass es sich bei ihr um eine private Organisation handelt, deren Ethos iSv. Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG auf religiösen Grundsätzen beruht (vgl. dazu EuGH 11. September 2018 – C-68/17 – Rn. 41). Allerdings hat der Senat in seinem Vorabentscheidungsersuchen die Frage aufgeworfen, ob privatrechtlich verfasste Einrichtungen, die sich in marktüblicher Weise im Gesundheitswesen betätigen, vom Anwendungsbereich des Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG erfasst werden. Der Gerichtshof der Europäischen Union hat diese Fragestellung nur dahingehend beantwortet, dass insoweit Erwägungen zur Rechtsnatur und zur Rechtsform der betreffenden Körperschaft ohne Bedeutung sind und die Bezugnahme auf private Organisationen auch nach Privatrecht gegründete Einrichtungen umfasst (EuGH 11. September 2018 – C-68/17 – Rn. 40). Zur „Marktüblichkeit" der Betätigung hat sich der Gerichtshof hingegen nicht verhalten. Einer darauf gestützten Nachfrage des Senats bedarf es indes nicht. Die Revision der Beklagten unterliegt auch dann der Zurückweisung, wenn die beruflichen Tätigkeiten der Arbeitnehmer innerhalb ihrer Einrichtungen von § 9 Abs. 2 AGG in unionsrechtskonformer Auslegung erfasst werden.

cc) Eine Ungleichbehandlung bei der Anforderung eines loyalen und aufrichtigen Verhaltens im Sinne des Ethos des Arbeitgebers, die sich – wie hier – ausschließlich auf die Konfession der Beschäftigten stützt, hat aufgrund der unionsrechtskonformen Auslegung von § 9 Abs. 2 AGG ua. die in Art. 4 Abs. 2 UnterAbs. 1 RL 2000/78/EG genannten Kriterien (vgl. Rn. 19) einzuhalten (EuGH 11. September 2018 – C-68/17 – Rn. 49). Danach hängt es von der Art der fraglichen Tätigkeiten oder den Umständen ihrer Ausübung ab, ob die Religion oder Weltanschauung eine wesentliche, rechtmäßige und gerechtfertigte berufliche Anforderung angesichts des Ethos der betreffenden Kirche oder Organisation im Sinne dieser Vorschrift darstellen kann. Dies setzt einen – objektiv bestehenden – direkten Zusammenhang zwischen der vom Arbeitgeber aufgestellten beruflichen Anforderung und der fraglichen Tätigkeit voraus. Ein solcher Zusammenhang kann sich entweder aus der Art dieser Tätigkeit ergeben – zB wenn sie mit der Mitwirkung an der Bestimmung des Ethos der betreffenden Kirche oder Organisation oder einem Beitrag zu deren Verkündigungsauftrag verbunden ist – oder aus den Umständen ihrer Ausübung, zB der Notwendigkeit, für eine glaubwürdige Vertretung der Kirche oder Organisation nach außen zu sorgen (EuGH 11. September 2018 – C-68/17 – Rn. 50; vgl. in diesem Sinne auch EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 62 f.).

dd) Unter Anwendung dieser Grundsätze liegen die in unionsrechtskonformer Auslegung von § 9 Abs. 2 AGG zu fordernden Voraussetzungen für eine Ungleichbehandlung des Klägers gegenüber den nicht der katholischen Konfession angehörenden Abteilungsärzten in Bezug auf die Loyalitätsanforderung, den heiligen und unauflöslichen Charakter der kirchlichen Eheschließung zu achten, nicht vor. Die Achtung des Gebots, keine nach kanonischem Recht ungültige Ehe einzugehen, war für die Bekundung des Ethos der Beklagten keine im Hinblick auf die Art der beruflichen Tätigkeiten des Klägers oder die Umstände ihrer Ausübung wesentliche, rechtmäßige und gerechtfertigte berufliche Anforderung. In Bezug auf diesen Teil ihres Ethos war die Ungleichbehandlung des Klägers gegenüber den nicht der katholischen Kirche angehörigen Abteilungsärzten nicht durch § 9 Abs. 2 AGG gerechtfertigt.

(1) Dies gilt zunächst mit Blick auf die Art der vom Kläger ausgeübten Tätigkeiten.

(a) Soweit diese die Beratung und medizinische Pflege in einem Krankenhaus sowie die Leitung der medizinischen Abteilung „Innere Medizin" als Chefarzt zum Gegenstand haben,

wirkte der Kläger dadurch weder an der Bestimmung des Ethos der Beklagten mit noch leistete er einen Beitrag zu deren Verkündigungsauftrag.

(b) Der von der Beklagten zur Rechtfertigung der Ungleichbehandlung angeführte Umstand, die vom Kläger ausgeübte Tätigkeit lasse sich nicht auf die Ausübung des Heilberufs „Arzt" im rein praktischen Sinne reduzieren, sondern sei untrennbar mit ihrem karitativen Wirken insgesamt und dessen religiöser Dimension verbunden, vermag eine tätigkeitsbezogene Differenzierung ebenfalls nicht zu begründen. Alle Abteilungsärzte sind in diesem Sinne in das karitative Wirken der Beklagten einbezogen.

(c) Ihre Behauptung, der Kläger sei ua. im Bereich der internistischen Onkologie tätig gewesen, was ein besonders hohes Maß an Vertrauen zwischen dem behandelnden Arzt und dem Patienten voraussetze, lässt keinen Zusammenhang mit der Wesentlichkeit, also Notwendigkeit einer beruflichen Anforderung erkennen, im Privatleben den heiligen und unauflöslichen Charakter der kirchlichen Eheschließung zu achten. Die Beklagte macht vielmehr auch mit Blick auf die konkrete Tätigkeit des Klägers letztlich allein geltend, diese sei als karitative Tätigkeit Teil des Sendungsauftrags der römisch-katholischen Kirche. Das trifft indes nach ihrem eigenen Vorbringen auf alle im karitativen Dienst der Beklagten am Mitmenschen zu erfüllenden Tätigkeiten zu.

(d) Die Auffassung der Beklagten, die ihres Erachtens gegebene Notwendigkeit, vom Kläger die Beachtung der Gebote der katholischen Glaubens- und Sittenlehre zu fordern, werde nicht dadurch infrage gestellt, dass sie vereinzelt gem. Art. 3 Abs. 2 GrO 1993 auch Personen nicht katholischer Konfession auf Stellen mit medizinischer Verantwortung und Leitungsaufgaben beschäftige, übersieht, dass die Abstufung von Loyalitätsanforderungen je nach Konfessionszugehörigkeit der Beschäftigten zwar nach deutschem Verfassungsrecht zulässig sein mag (so ausdrücklich BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 159 ff., BVerfGE 137, 273), unionsrechtlich aber tätigkeitsbezogen gerechtfertigt sein muss. Soweit die Beklagte geltend macht, die fraglichen Stellen „ähnelten" sich bloß, lässt dies, wie ausgeführt, keinen relevanten Unterschied in Bezug auf die Forderung nach der Beachtung des kanonischen Eheverständnisses durch die Abteilungsärzte erkennen. Es ist auch unerheblich, ob die Beschäftigung von nicht-katholischen Abteilungsärzten eine bloße Reaktion auf die gesellschaftliche Entwicklung der religiösen Pluralisierung und „Entkirchlichung" darstellt, wie die Beklagte geltend macht. Sie führt zwar weiter aus, es habe für die Integrität der Dienstgemeinschaft und die Vertrauensbasis der Mitarbeiterschaft, der Patienten und ihrer Angehörigen ein signifikant anderes Gewicht, ob in Ausnahmefällen in leitenden Funktionen auch Personen beschäftigt würden, die aus kirchenrechtlichen Gründen von Beginn an nur verminderten Loyalitätspflichten unterliegen, oder ob katholische Mitarbeiter – wie der Kläger – die ihnen obliegenden Verpflichtungen bewusst brächen. Nach den unionsrechtlichen Anforderungen ist aber die „Integrität der Dienstgemeinschaft" für sich genommen kein eine Ungleichbehandlung bei den Loyalitätsanforderungen allein aufgrund der Konfession der Beschäftigten rechtfertigender Grund. Auch der Verweis der Beklagten auf die – vom Bundesverfassungsgericht aufgehobene – Senatsentscheidung vom 8. September 2011 (– 2 AZR 543/10 – Rn. 37, BAGE 139, 144) greift insofern zu kurz. Der Senat hatte sich dort nicht mit der Frage befasst, ob nach Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG Loyalitätsanforderungen auch innerhalb derselben (Leitungs-)Funktion allein nach der Konfessionszugehörigkeit der Beschäftigten abgestuft werden dürfen.

(2) Etwas anderes ergibt sich nicht aus den Umständen der Ausübung der beruflichen Tätigkeiten des Klägers.

(a) Soweit die Beklagte geltend macht, der Kläger nehme als leitender Mitarbeiter iSd. GrO Repräsentationsfunktionen wahr, die eine besondere Bedeutung für den Bestand und die Entwicklung der Einrichtung sowie die Glaubwürdigkeit der Kirche auch in der außerkirchlichen Öffentlichkeit hätten, vermag dies nicht die Ungleichbehandlung bei den Loyalitätsanforderungen trotz gleich gelagerter (Leitungs-)Tätigkeit allein aufgrund der Konfessionszugehörigkeit zu rechtfertigen.

(b) Die von der Beklagten angeführte Vorbild- und Führungsfunktion des Klägers nach innen hinsichtlich der Erfüllung der an ihn selbst sowie die weiteren Mitarbeiter der Beklagten gestellten Loyalitätsanforderungen kann die unterschiedlichen Loyalitätsanforderungen allein aufgrund der Konfessionszugehörigkeit der Beschäftigten ebenfalls nicht begründen. Die Beklagte unternimmt insoweit den Versuch, die Ungleichbehandlung mit der Ungleichbehandlung – den unterschiedlichen Loyalitätsanforderungen je nach Konfessionszugehörigkeit – und nicht nach der Art der Tätigkeit oder den Umständen ihrer Ausübung zu rechtfertigen. Dies verkennt erneut die unionsrechtlichen Anforderungen an eine solche Ungleichbehandlung allein aufgrund der Konfessionszugehörigkeit.

(c) Auch die Behauptung, das Verhalten des Klägers werde von den Mitarbeitern, den Patienten und ihren Angehörigen ihr zugerechnet, stützt die Beklagte allein darauf, dass ihre ethische Glaubwürdigkeit gerade durch ihr Führungspersonal vermittelt werde. Zum Führungspersonal gehören indes ebenso die von ihr beschäftigten nicht-katholischen Abteilungsärzte. Die Argumentation der Beklagten läuft auch insofern darauf hinaus, die Ungleichbehandlung rechtfertige sich allein aus der unterschiedlichen Konfessionszugehörigkeit der Beschäftigten, was indes nach der maßgeblichen Auslegung des Unionsrechts durch den Gerichtshof der Europäischen Union einer Rechtfertigung nach der Art der ausgeübten Tätigkeit oder den Umständen ihrer Ausübung bedarf.

(d) Mit dem Hinweis darauf, ihre Mitarbeiter dürften sich berechtigterweise die Frage stellen, warum sie selbst den jeweiligen Loyalitätsanforderungen Folge leisten sollten, wenn ihnen nicht einmal der Kläger als leitender Mitarbeiter Folge leisten müsse, setzt die Beklagte wiederum die Zulässigkeit unterschiedlicher Loyalitätsanforderungen allein aufgrund der Konfessionszugehörigkeit der Mitarbeiter voraus, anstatt sie nach der Art ihrer Tätigkeiten oder den Umständen ihrer Ausübung zu begründen.

4. Kein anderes Ergebnis in Bezug auf die Unwirksamkeit der Kündigung vom 30. März 2009 ergäbe sich, wenn eine unionsrechtskonforme Auslegung von § 9 Abs. 2 AGG deshalb unzulässig wäre, weil ihr der gesetzgeberische Wille entgegenstünde (vgl. Rn. 28). In diesem Fall hätte die Vorschrift wegen des zu ihr im Widerspruch stehenden Unionsrechts als Grundlage für die Rechtfertigung einer Ungleichbehandlung in Bezug auf die Loyalitätsanforderungen aufgrund der Religion gänzlich unangewendet zu bleiben (EuGH 11. September 2018 – C-68/17 – Rn. 71).

III. Nationales Verfassungsrecht steht weder der unionsrechtskonformen Auslegung von § 9 Abs. 2 AGG noch einer Unanwendbarkeit der Norm entgegen.

1. Allerdings sind nach der Rechtsprechung des Bundesverfassungsgerichts unterschiedlich abgestufte Anforderungen der

Loyalitätsobliegenheiten nach der Konfession des kirchlichen Arbeitnehmers mit ihrer grundlegenden Kategorisierung nach Katholiken (Art. 4 Abs. 1 GrO 1993), Nichtkatholiken (Art. 4 Abs. 2 GrO 1993) und Nichtchristen (Art. 4 Abs. 3 GrO 1993) verfassungsrechtlich ebenso gerechtfertigt wie die arbeitsrechtliche Sanktionierung von Verstößen aufgrund der Konfession einerseits und der leitenden Stellung andererseits (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 159 ff., BVerfGE 137, 273). Es gehört zum von Art. 4 Abs. 1 und Abs. 2 iVm. Art. 140 GG und Art. 137 Abs. 3 Satz 1 WRV garantierten kirchlichen Selbstbestimmungsrecht, dass die Religionsgemeinschaften autonom eine Abstufung der an die Beschäftigten gerichteten Loyalitätsanforderungen vorsehen und insofern auch bei gleich gelagerter Tätigkeit nach der Religion der Mitarbeiter unterscheiden dürfen (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 145, 151, 159 ff., aaO; 4. Juni 1985 – 2 BvR 1703/83, 2 BvR 1718/83, 2 BvR 856/84 – zu B II 1 d der Gründe, BVerfGE 70, 138).

2. Im Anwendungsbereich des Unionsrechts geht dieses entgegenstehendem nationalen Recht jedoch vor (grundlegend EuGH 15. Juli 1964 – C-6/64 – [Flaminio Costa/E.N.E.L.]). Dies gilt auch im Verhältnis zu nationalem Verfassungsrecht (EuGH 9. März 1978 – C-106/77 – [Simmenthal] Rn. 17 f.; im Grundsatz ebenso BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 115, BVerfGE 142, 123; 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I 1 b der Gründe, BVerfGE 126, 286). Diesen Anwendungsvorrang erfordert die wirksame Entfaltung des Rechts der Europäischen Union. Er entspricht der Ermächtigung des Art. 23 Abs. 1 GG, der insoweit ein Wirksamkeits- und Durchsetzungsversprechen enthält (vgl. BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] aaO). Hoheitsakte der Europäischen Union und – soweit sie durch das Unionsrecht determiniert werden – auch Akte der deutschen öffentlichen Gewalt sind daher mit Blick auf den Anwendungsvorrang des Unionsrechts grundsätzlich nicht am Maßstab der im Grundgesetz verankerten Grundrechte zu messen (BVerfG 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] Rn. 36, BVerfGE 140, 317; 4. Oktober 2011 – 1 BvL 3/08 – [Investitionszulagengesetz] zu B I 1 a der Gründe, BVerfGE 129, 186). Dies gilt auf der Grundlage von Art. 23 Abs. 1 GG nicht nur für Verordnungen, sondern auch für Richtlinien nach Art. 288 Abs. 3 AEUV und an die Bundesrepublik Deutschland gerichtete Beschlüsse der Kommission nach Art. 288 Abs. 4 AEUV (früher: Entscheidungen der Kommission nach Art. 249 Abs. 4 EGV; BVerfG 4. Oktober 2011 – 1 BvL 3/08 – [Investitionszulagengesetz] aaO). Auch eine innerstaatliche Rechtsvorschrift, die eine Richtlinie oder einen Beschluss in deutsches Recht umsetzt, wird nicht an den Grundrechten des Grundgesetzes gemessen, soweit das Unionsrecht keinen Umsetzungsspielraum lässt, sondern – wie hier – zwingende Vorgaben macht (BVerfG 4. Oktober 2011 – 1 BvL 3/08 – [Investitionszulagengesetz] aaO; vgl. auch BVerfG 13. März 2007 – 1 BvF 1/05 – [Emissionshandel] zu C I 1 d der Gründe, BVerfGE 118, 79; 2. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – [Vorratsdatenspeicherung] zu B II der Gründe, BVerfGE 125, 260). Dies gilt jedenfalls solange, wie die Europäische Union einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Union generell gewährleistet, der dem vom Grundgesetz jeweils als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt (BVerfG 4. Oktober 2011 – 1 BvL 3/08 – [Investitionszulagengesetz] aaO; vgl. auch BVerfG 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] Rn. 43, aaO und 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] BVerfGE 73, 339; 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] BVerfGE 102, 147; 13. März 2007 – 1 BvF 1/05 – [Emissionshandel] aaO). Das Bundesverfassungsgericht hat insofern seine ursprünglich angenommene generelle Zuständigkeit, den Vollzug von Gemeinschaftsrecht (jetzt: Unionsrecht) in Deutschland am Maßstab der Grundrechte der deutschen Verfassung zu prüfen (vgl. BVerfG 29. Mai 1974 – 2 BvL 52/71 – [Solange I] BVerfGE 37, 271), im Vertrauen auf die entsprechende Aufgabenwahrnehmung durch den Gerichtshof der Europäischen Gemeinschaften (jetzt: Union) zurückgestellt (BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C II 1 b aa (4) (a) der Gründe, BVerfGE 123, 267; vgl. BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] zu B II 1 f der Gründe, aaO; bestätigt in BVerfG 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] zu B II 2 a der Gründe, aaO).

3. Das hier maßgebliche Unionsrecht in der Auslegung des Gerichtshofs der Europäischen Union ist nicht seinerseits in Deutschland unanwendbar. Es beruht weder auf einem Akt ultra vires noch berührt es die Verfassungsidentität der Bundesrepublik Deutschland im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Ob diese ihrerseits mit dem Verständnis des Gerichtshofs vom Vorrang des Unionsrechts (dazu zuletzt etwa EuGH 11. Dezember 2018 – C-493/17 – Rn. 19) im Einklang steht, bedarf daher ebenso wenig einer Entscheidung wie die Frage, wie ein Konflikt zwischen dem Gerichtshof und dem Bundesverfassungsgericht bei unterschiedlichen Auffassungen in Bezug auf die Gültigkeit von Unionsrecht gegebenenfalls aufzulösen wäre.

a) Maßnahmen von Organen, Einrichtungen und sonstigen Stellen der Europäischen Union, die ultra vires ergehen, verletzen nach der Rechtsprechung des Bundesverfassungsgerichts das im Zustimmungsgesetz gem. Art. 23 Abs. 1 Satz 2 GG niedergelegte Integrationsprogramm (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 143 und 152, BVerfGE 142, 123). Das Unionsrecht bleibt demnach – auch soweit es als autonome (Teilrechts-)Ordnung verstanden wird – von der vertraglichen Ermächtigung abhängig (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 144, aaO). Nur insoweit kann es am Anwendungsvorrang teilhaben (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 146, aaO). Eine entsprechende Prüfung setzt eine hinreichend qualifizierte Kompetenzüberschreitung voraus. Diese muss offensichtlich und für die Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten von struktureller Bedeutung sein (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 147, aaO; 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I 1 c cc (1) der Gründe, BVerfGE 126, 286). Da hinreichend qualifizierte Kompetenzüberschreitungen zugleich die Identität der Verfassung berühren, stellt die Ultra-vires-Kontrolle einen besonderen, an das Zustimmungsgesetz gem. Art. 23 Abs. 1 Satz 2 GG anknüpfenden Anwendungsfall des allgemeinen Schutzes der Verfassungsidentität durch das Bundesverfassungsgericht dar (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 153, aaO).

aa) Ein Akt liegt offensichtlich außerhalb der übertragenen Kompetenzen, wenn sich die Kompetenz – bei Anwendung allgemeiner methodischer Standards – unter keinem rechtlichen Gesichtspunkt begründen lässt (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 149, BVerfGE 142, 123; vgl. auch BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I

1 c cc (2) und (3) der Gründe, BVerfGE 126, 286). Dieses Verständnis von Offensichtlichkeit folgt aus dem Gebot, die Ultra-vires-Kontrolle zurückhaltend auszuüben (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO unter Verweis auf Rn. 154 ff.). Bezogen auf den Gerichtshof der Europäischen Union folgt es zudem aus der Unterschiedlichkeit der Aufgaben und Maßstäbe, die das Bundesverfassungsgericht einerseits und der Gerichtshof andererseits zu erfüllen oder anzuwenden haben (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO). Dabei ist auch zu berücksichtigen, dass der Gerichtshof Anspruch auf Fehlertoleranz hat (BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I 1 c cc (3) der Gründe, aaO). Eine Grenze findet dieser mit der Aufgabenzuweisung des Art. 19 Abs. 1 Satz 2 EUV notwendig verbundene Spielraum erst bei einer offensichtlich schlechterdings nicht mehr nachvollziehbaren und daher objektiv willkürlichen Auslegung der Verträge. Erst wenn der Gerichtshof diese Grenze überschreitet, soll auch sein Handeln nicht mehr durch Art. 19 Abs. 1 Satz 2 EUV gedeckt sein und seiner Entscheidung für Deutschland das gem. Art. 23 Abs. 1 Satz 2 iVm. Art. 20 Abs. 1 und Abs. 2 und Art. 79 Abs. 3 GG erforderliche Mindestmaß an demokratischer Legitimation fehlen (so BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO). Die Annahme einer offensichtlichen Kompetenzüberschreitung setzt allerdings nicht voraus, dass keine unterschiedlichen Rechtsauffassungen zu dieser Frage vertreten werden (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 150, aaO). Dass Stimmen im Schrifttum, in der Politik oder den Medien einer Maßnahme Unbedenklichkeit attestieren, hindert die Feststellung einer offensichtlichen Kompetenzüberschreitung grundsätzlich nicht. „Offensichtlich" kann die Kompetenzüberschreitung auch dann sein, wenn sie das Ergebnis einer sorgfältigen und detailliert begründeten Auslegung ist. Insoweit gelten im Rahmen der Ultra-vires-Kontrolle die allgemeinen Grundsätze (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO).

bb) Eine strukturell bedeutsame Verschiebung zulasten mitgliedstaatlicher Kompetenzen kann nur vorliegen, wenn die Kompetenzüberschreitung ein für das Demokratieprinzip und die Volkssouveränität erhebliches Gewicht besitzt (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 151, BVerfGE 142, 123). Das ist etwa der Fall, wenn sie geeignet ist, die kompetenziellen Grundlagen der Europäischen Union zu verschieben und so das Prinzip der begrenzten Einzelermächtigung zu unterlaufen. Davon ist auszugehen, wenn die Inanspruchnahme der Kompetenz durch das Organ, die Einrichtung oder sonstige Stelle der Europäischen Union eine Vertragsänderung nach Art. 48 EUV oder die Inanspruchnahme einer Evolutivklausel erforderte (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO; vgl. EuGH Gutachten 2/94 vom 28. März 1996 [EMRK-Beitritt] Rn. 30), für Deutschland also ein Tätigwerden des Gesetzgebers, sei es nach Art. 23 Abs. 1 Satz 2 GG, sei es nach Maßgabe des Integrationsverantwortungsgesetzes (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO).

b) Im Rahmen der sog. Identitätskontrolle prüft das Bundesverfassungsgericht überdies, ob die durch Art. 79 Abs. 3 GG für unantastbar erklärten Grundsätze bei der Übertragung von Hoheitsrechten durch den deutschen Gesetzgeber oder durch eine Maßnahme von Organen, Einrichtungen und sonstigen Stellen der Europäischen Union berührt werden (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 138, BVerfGE 142, 123; 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] Rn. 36, 43, BVerfGE 140, 317; 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C I 2 e bb der Gründe, BVerfGE 123, 267).

aa) Das betrifft die Wahrung des Menschenwürdekerns der Grundrechte (Art. 1 GG; BVerfG 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] Rn. 48, BVerfGE 140, 317) ebenso wie die Grundsätze, die das Demokratie-, Rechts-, Sozial- und Bundesstaatsprinzip iSd. Art. 20 GG prägen (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 138, BVerfGE 142, 123).

bb) Mit Blick auf das Demokratieprinzip ist ua. sicherzustellen, dass dem Deutschen Bundestag bei einer Übertragung von Hoheitsrechten nach Art. 23 Abs. 1 GG eigene Aufgaben und Befugnisse von substanziellem politischem Gewicht verbleiben (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 138, BVerfGE 142, 123; vgl. auch BVerfG 12. Oktober 1993 – 2 BvR 2134/92, 2 BvR 2159/92 – [Maastricht] zu C I der Gründe, BVerfGE 89, 155; 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu B I 3 a aa und C I 3 der Gründe, BVerfGE 123, 267) und dass er in der Lage bleibt, seine haushaltspolitische Gesamtverantwortung wahrzunehmen (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] aaO mwN). Die europäische Vereinigung auf der Grundlage einer Vertragsunion souveräner Staaten darf nicht so verwirklicht werden, dass in den Mitgliedstaaten kein ausreichender Raum zur politischen Gestaltung der wirtschaftlichen, kulturellen und sozialen Lebensverhältnisse mehr bleibt (BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C I 3 a cc der Gründe, aaO). Dies gilt ua. für solche politischen Entscheidungen, die in besonderer Weise auf kulturelle, historische und sprachliche Vorverständnisse angewiesen sind und die sich im parteipolitisch und parlamentarisch organisierten Raum einer politischen Öffentlichkeit diskursiv entfalten. Zu solchen wesentlichen Bereichen demokratischer Gestaltung gehören auch Fragen des Umgangs mit dem religiösen oder weltanschaulichen Bekenntnis sowie Entscheidungen zum Status von Kirchen, Religions- und Weltanschauungsgemeinschaften und der Einbeziehung des Transzendenten in das öffentliche Leben, die als besonders sensibel für die demokratische Selbstgestaltungsfähigkeit eines Verfassungsstaates gelten (BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C I 3 a cc und dd der Gründe, aaO). Für die Beurteilung, ob eine verfassungswidrige Entleerung der Aufgaben des Deutschen Bundestags vorliegt, kommt es nicht auf quantitative Relationen, sondern darauf an, dass der Bundesrepublik Deutschland für zentrale Regelungs- und Lebensbereiche substanzielle innerstaatliche Gestaltungsmöglichkeiten verbleiben (BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C II 1 c der Gründe, aaO).

cc) Soweit Maßnahmen von Organen, Einrichtungen oder sonstigen Stellen der Europäischen Union Auswirkungen zeitigen, die die in den Art. 1 und Art. 20 GG niedergelegte Verfassungsidentität berühren, gehen sie über die grundgesetzlichen Grenzen offener Staatlichkeit hinaus (vgl. BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 137, BVerfGE 142, 123). Auf einer primärrechtlichen Ermächtigung kann eine derartige Maßnahme nicht beruhen, weil auch der mit der Mehrheit des Art. 23 Abs. 1 Satz 3 iVm. Art. 79 Abs. 2 GG entscheidende Integrationsgesetzgeber der Europäischen Union keine Hoheitsrechte übertragen kann, mit deren Inanspruchnahme eine Berührung der von Art. 79 Abs. 3 GG geschützten Verfassungsidentität einherginge. Die Identitätskontrolle verhindert nicht nur, dass der Europäischen Union Hoheitsrechte jenseits des für eine Übertragung offenstehenden Bereichs eingeräumt werden, sondern auch, dass Maßnahmen von Organen, Einrichtungen und sonstigen Stellen der Europäischen Union umgesetzt werden, die eine entsprechende Wirkung entfalten und jedenfalls

faktisch einer mit dem Grundgesetz unvereinbaren Kompetenzübertragung gleichkämen (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 139 mwN, aaO). Anders als die Ultra-vires-Kontrolle betrifft die Identitätskontrolle nicht die Einhaltung der Reichweite der übertragenen Zuständigkeit. Vielmehr wird die in Rede stehende Maßnahme der Europäischen Union in materieller Hinsicht an der „absoluten Grenze" der Grundsätze der Art. 1 und Art. 20 GG gemessen (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 153 mwN, aaO).

4. Die Prüfung, ob Ultra-vires- oder Identitätskontrolle nach den vom Bundesverfassungsgericht entwickelten Maßstäben vorliegend einen Ausschluss des Anwendungsvorrangs des Unionsrechts gebieten, obliegt dem erkennenden Senat insofern, als er – bejahendenfalls – erwägen muss, eine Entscheidung des Bundesverfassungsgerichts herbeizuführen (vgl. BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 162, BVerfGE 142, 123; 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] Rn. 43, BVerfGE 140, 317; 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C I 2 e bb der Gründe, BVerfGE 123, 267). Die Feststellung der Unanwendbarkeit von Unionsrecht in der Bundesrepublik Deutschland hat sich das Bundesverfassungsgericht vorbehalten (BVerfG 21. Juni 2016 – 2 BvE 13/13 ua. – [OMT-Programm] Rn. 155, aaO; 15. Dezember 2015 – 2 BvR 2735/14 – [Europäischer Haftbefehl] aaO; 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] aaO). Ein von diesem für denkbar gehaltenes, speziell auf die Ultra-vires- und Identitätskontrolle zugeschnittenes verfassungsgerichtliches Verfahren zur Absicherung der Verpflichtung deutscher Organe, kompetenzüberschreitende oder identitätsverletzende Unionsrechtsakte im Einzelfall in Deutschland unangewendet zu lassen (vgl. dazu BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] aaO), ist bislang allerdings weder vom deutschen Gesetzgeber geschaffen worden, noch hat das Bundesverfassungsgericht ausgesprochen, dass und gegebenenfalls unter welchen Voraussetzungen die Durchführung eines solchen – nicht normativ ausgestalteten – (Zwischen-)Verfahrens verfassungsrechtlich geboten ist.

5. Unter Anwendung der vorstehenden Grundsätze gebieten es weder die Ultra-vires- noch die Identitätskontrolle, das hier maßgebliche Unionsrecht in der Auslegung des Gerichtshofs der Europäischen Union bei der Auslegung oder Anwendung von § 9 Abs. 2 AGG unberücksichtigt zu lassen.

a) Der Europäische Rat hat mit dem Erlass der RL 2000/78/EG nicht offensichtlich außerhalb der ihm übertragenen Kompetenzen und damit ultra vires gehandelt. Insbesondere ist das Prinzip der begrenzten Einzelermächtigung nicht verletzt. Ermächtigungsgrundlage für die Richtlinie ist Art. 19 Abs. 1 AEUV (Ex-Art. 13 EGV aF; EUArbR/Mohr 2. Aufl. RL 2000/78/EG Art. 1 Rn. 2; für das Verbot der Altersdiskriminierung BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I 2 b cc der Gründe, BVerfGE 126, 286).

b) Der Gerichtshof der Europäischen Union hat bei der Auslegung von Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG seine Kompetenz nicht offensichtlich überschritten. Es kann daher dahinstehen, ob diese Überschreitung anderenfalls eine hinreichend weitreichende Kompetenzverschiebung im Verhältnis zwischen der Europäischen Union und den Mitgliedstaaten bewirkt hätte.

aa) Der Gerichtshof sichert die Wahrung des Rechts bei der Auslegung und Anwendung der Verträge (Art. 19 Abs. 1 Satz 2 EUV). Er entscheidet nach Maßgabe der Verträge im Wege der Vorabentscheidung auf Antrag der einzelstaatlichen Gerichte über die Auslegung des Unionsrechts oder über die Gültigkeit der Handlungen der Organe (Art. 19 Abs. 3 Buchst. b EUV). Dies umfasst – nach Auffassung des Bundesverfassungsgerichts – die Anwendung der spezifisch unionsrechtlich geprägten Methoden der Rechtsfindung, an die sich der Gerichtshof gebunden sieht und die der „Eigenart" der Verträge und den ihnen eigenen Zielen Rechnung tragen (BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] zu C I 1 c cc (3) der Gründe, BVerfGE 126, 286).

bb) Die hier in Rede stehende, auf das Vorabentscheidungsersuchen des Senats erfolgte Auslegung von Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG durch den Gerichtshof der Europäischen Union beruht nicht auf einer objektiv willkürlichen Auslegung der Verträge.

(1) Der Begriff des „Status" der Kirchen in Art. 17 AEUV bzw. in der durch den Erwägungsgrund 24 der Richtlinie in Bezug genommenen Erklärung Nr. 11 zum Status der Kirchen und weltanschaulichen Gemeinschaften zur Schlussakte des Vertrags von Amsterdam (Amsterdamer Kirchenerklärung) lässt nicht offensichtlich allein ein Verständnis entsprechend der teilweise in Deutschland vertretenen Auffassung zu, die nationalen Grundsätze zum Kirchenarbeitsrecht müssten bei der Ausgestaltung von Unionsrecht vollständig gewahrt bleiben (so etwa KR/Fischermeier 12. Aufl. Kirchl. ArbN Rn. 8; ders. ZMV-Sonderheft Tagung 2009 S. 7, 10 f.; Richardi ZfA 2008, 31, 49; Mohr/von Fürstenberg BB 2008, 2122, 2124 f.; Schliemann FS Richardi 2007 S. 959 ff.; ders., in: Reichold, Loyalitätsobliegenheiten im Umbruch S. 73 ff.; Schoenauer KuR 2012, 30, 35; Steinmeyer FS Wank 2014 S. 587, 591; Joussen NZA 2008, 675, 677 ff.; Thüsing, in: Essener Gespräche zum Thema Staat und Kirche Bd. 46, 129, 148; Thüsing/Fink-Jamann/von Hoff ZfA 2009, 153, 178 ff.; offengelassen BAG 25. April 2013 – 2 AZR 579/12 – Rn. 46, BAGE 145, 90; zu möglichen unionsrechtlichen Auslegungsvarianten vgl. auch Reichegger, Die Auswirkungen der Richtlinie 2000/78/EG auf das kirchliche Arbeitsrecht unter Berücksichtigung von Gemeinschaftsgrundrechten als Auslegungsmaxime, S. 219 ff.). Das demgegenüber vertretene Verständnis des Gerichtshofs, Art. 17 AEUV bringe zwar die Neutralität der Union demgegenüber zum Ausdruck, wie die Mitgliedstaaten ihre Beziehungen zu den Kirchen und religiösen Vereinigungen oder Gemeinschaften gestalten, könne jedoch nicht bewirken, dass die Einhaltung der in Art. 4 Abs. 2 RL 2000/78/EG genannten Kriterien einer wirksamen gerichtlichen Kontrolle entzogen würde (EuGH 11. September 2018 – C-68/17 – Rn. 48; 17. April 2018 – C-414/16 – [Egenberger] Rn. 56 bis 58), ist als Ergebnis einer spezifisch unionsrechtlichen Auslegung nachvollziehbar (dem EuGH zustimmend auch Reichold/Beer NZA 2018, 681, 682). Der Gerichtshof hat insbesondere den Umstand gewürdigt, dass der Wortlaut des Art. 17 AEUV im Kern der Amsterdamer Kirchenerklärung entspricht, auf die jedoch im Erwägungsgrund 24 der RL 2000/78/EG bereits Bezug genommen ist, was deutlich mache, dass der Unionsgesetzgeber sie beim Erlass der Richtlinie berücksichtigt haben müsse. Dieses Verständnis hält sich im Rahmen der Gesamtsystematik des europäischen Rechts (Joussen EuZA 2018, 421, 435; Junker NJW 2018, 1850, 1851 f.; Sagan EuZW 2018, 386; kritisch Greiner NZA 2018, 1289, 1291; Klumpp Anm. AP Richtlinie 2000/78/EG Nr. 42; kritisch hinsichtlich der Begründung des EuGH, dem Ergebnis aber zustimmend Classen EuR 2018, 752, 761). Nach dem Erwägungsgrund 24 ist die Rechtsetzung der Mitgliedstaaten in Bezug auf Ungleichbehandlungen wegen der Religion inhaltlichen Beschränkungen unterworfen („spezifische Bestimmungen über die wesentlichen, rechtmäßigen und gerechtfertigten beruflichen Anforderungen ..., die Voraussetzung für die Ausübung einer diesbezüglichen beruflichen Tätigkeit sein können"). Jedenfalls ist die Grenze der objektiven

Willkür nicht erreicht (zweifelnd auch Fremuth EuZW 2018, 723, 730). Dass ein anderes Verständnis von Art. 17 AEUV bzw. der Amsterdamer Kirchenerklärung vertretbar erscheinen mag (vgl. etwa Greiner jM 2018, 233, 235; Schuhmann ZAT 2018, 110, 112 f.; Thüsing/Mathy BB 2018, 2805, 2807), genügt ebenso wenig zur Annahme eines Aktes ultra vires wie der Umstand, dass der Gerichtshof seine Entscheidung nicht ausführlicher begründet hat (so auch Heuschmid/Höller AuR 2018, 587, 588; Jacobs RdA 2018, 263, 267; Klocke/Wolters BB 2018, 1460, 1464; Sagan EuZW 2018, 386, 387; zweifelnd Greiner aaO; Schuhmann ZAT 2018, 110, 115; Thüsing/Mathy RIW 2018, 559, 561).

(2) Entgegen der Auffassung von Krimphove (ArbRAktuell 2018, 511, 512) ist es – abgesehen davon, ob dies hinreichend offensichtlich wäre – nicht methodisch verfehlt, wenn der Gerichtshof mangels eines einschlägigen Freiheitsrechts auf ein Gleichheitsrecht „zurückgreift". Der Schutz vor Diskriminierung ist, worauf der Gerichtshof explizit hinweist (EuGH 11. September 2018 – C-68/17 – Rn. 69; 17. April 2018 – C-414/16 – [Egenberger] Rn. 76), mittlerweile auch durch Art. 21 Abs. 1 GRC gewährleistet (nicht durch Art. 17 AEUV, wie Krimphove an anderer Stelle annimmt: ArbRAktuell 2019, 27, 29) und steht insofern gleichrangig neben dem Schutz etwa der Religionsfreiheit gem. Art. 10 Abs. 1 GRC. Vor dem Inkrafttreten des Vertrags von Lissabon, nach dem die Charta den gleichen Rang wie die Verträge hat, ergab sich der Grundsatz des Verbots einer Diskriminierung wegen der Religion aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten (EuGH 11. September 2018 – C-68/17 – Rn. 69).

(3) Eine objektiv willkürliche Verletzung der Verträge resultiert auch nicht aus der Annahme des Gerichtshofs, Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG entgegenstehendes nationales Recht habe gegebenenfalls unangewendet zu bleiben, selbst wenn es um einen Sachverhalt vor Inkrafttreten des Vertrags von Lissabon gehe (EuGH 11. September 2018 – C-68/17 – Rn. 68 ff.). Die Argumentation des Gerichtshofs, vor dem Inkrafttreten des Vertrags von Lissabon folge der Grundsatz des Verbots einer Diskriminierung wegen der Religion aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten, habe auch als solcher allgemeiner Grundsatz des Unionsrechts zwingenden Charakter und verleihe dem Einzelnen ein Recht, das er in einem Rechtsstreit, der einen vom Unionsrecht erfassten Bereich betrifft, als solches geltend machen könne, so dass die nationalen Gerichte auch in Rechtsstreitigkeiten zwischen Privatpersonen verpflichtet seien, von der Anwendung mit diesem Verbot nicht im Einklang stehender nationaler Vorschriften abzusehen (EuGH 11. September 2018 – C-68/17 – Rn. 67 bis 69), hält sich ebenfalls im Rahmen der ihm übertragenen Kompetenz (einen Akt ultra vires nehmen insoweit auch Thüsing/Mathy BB 2018, 2805, 2808 nicht an; kritisch Greiner NZA 2018, 1289, 1291 bzgl. der „gemeinsamen Verfassungstraditionen" vor Inkrafttreten des Vertrags von Lissabon in Bezug auf eine konfessionsanknüpfende Ungleichbehandlung bei den Loyalitätsobliegenheiten; dagegen wiederum, dem EuGH zustimmend, Stein ZESAR 2018, 277, 281: für die gemeinsamen Verfassungstraditionen sei nicht der „kleinste gemeinsame Nenner" entscheidend). Sie entspricht der Rechtsprechung des Gerichtshofs zum Verbot der Diskriminierung wegen des Alters (vgl. EuGH 19. April 2016 – C-441/14 – [Dansk Industri] Rn. 36 mwN; 19. Januar 2010 – C-555/07 – [Kücükdeveci] Rn. 51; 22. November 2005 – C-144/04 – [Mangold] Rn. 77; Greiner NZA 2018, 1289, 1290; Thüsing/Mathy aaO; Klocke/Wolters BB 2018, 1460, 1464), die ihrerseits nicht ultra vires ergangen ist (BVerfG 6. Juli 2010 – 2 BvR 2661/06 – [Honeywell] Rn. 77 bis 79, BVerfGE 126, 286). Bereits in der Rechtssache Mangold hat der Gerichtshof darauf hingewiesen, das grundsätzliche Verbot aller nach der Richtlinie verbotenen Formen der Diskriminierung habe, wie sich aus der ersten und der vierten Begründungserwägung der Richtlinie ergebe, seinen Ursprung in verschiedenen völkerrechtlichen Verträgen und den gemeinsamen Verfassungstraditionen der Mitgliedstaaten (EuGH 22. November 2005 – C-144/04 – [Mangold] Rn. 74). Dies hat zwischenzeitlich eine Bestätigung in Art. 21 Abs. 1 der von allen Mitgliedstaaten beschlossenen Charta der Grundrechte der Europäischen Union gefunden.

(4) Es liegt – ungeachtet der Frage, ob dies einen Ausschluss des Anwendungsvorrangs des Unionsrechts zu begründen vermöchte – auch kein Eingriff in die völkerrechtliche Souveränität des Heiligen Stuhls vor, weil der Gerichtshof der Europäischen Union die nationalen Gerichte aufforderte, dem Unionsrecht entgegenstehendes kirchliches Recht nicht mehr anzuwenden (so aber Krimphove ArbRAktuell 2018, 511, 513; anders Krimphove ArbRAktuell 2019, 27, 29). Unangewendet zu bleiben hat gegebenenfalls allein dem Unionsrecht entgegenstehendes nationales, also staatliches (Verfassungs-)Recht (EuGH 11. September 2018 – C-68/17 – Rn. 71). Die GrO 1993 findet in Rechtsverhältnissen, die staatlichem Arbeitsrecht unterliegen, nicht autonom als Kirchenrecht Anwendung. Sie ist auch nicht Gegenstand eines Konkordats mit dem Heiligen Stuhl. Sie wurde vielmehr von den deutschen (Erz-)Bischöfen verabschiedet, um in Ausübung des kirchlichen Selbstbestimmungsrechts die in Deutschland verfassungsgerichtlich anerkannten Freiräume durch eine eigene kirchenrechtliche Regelung auszufüllen (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 10, BVerfGE 137, 273; vgl. Dütz NJW 1994, 1369; zum in der Bundesrepublik fortgeltenden Reichskonkordat vom 20. Juli 1933, Reichsgesetzblatt vom 18. September 1933 II S. 679, vgl. BVerfG 26. März 1957 – 2 BvG 1/55 – [Reichskonkordat] BVerfGE 6, 309).

c) Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG in der Auslegung des Gerichtshofs der Europäischen Union berührt nicht die in den Art. 1 und Art. 20 GG niedergelegte Verfassungsidentität der Bundesrepublik Deutschland.

aa) Der Menschenwürdekern der Grundrechte, insbesondere der Religionsfreiheit gem. Art. 4 Abs. 1 und Abs. 2 GG, ist nicht betroffen. Zwar ist das von Art. 4 Abs. 1 und Abs. 2 iVm. Art. 140 GG und Art. 137 Abs. 3 WRV geschützte Selbstbestimmungsrecht der Religionsgesellschaften berührt, an dem auch die Beklagte teilhat (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 146, BVerfGE 137, 273). Dem korporativen Gewährleistungsinhalt der Religionsfreiheit kommt indes kein Menschenwürdekern zu (dies außer Acht lassend Thüsing/Mathy BB 2018, 2805, 2808 f.; sowie dies. RIW 2018, 559, 562; zutreffend dagegen Classen EuR 2018, 752, 765; Fremuth EuZW 2018, 723, 730; auch Klocke/Wolters BB 2018, 1460, 1464). Kapitalgesellschaften, Vereine, Personengesellschaften etc. können die „Menschenwürde" ihrem Wesen nach nicht für sich in Anspruch nehmen (Art. 19 Abs. 3 GG; vgl. zuletzt BVerfG 13. Juli 2018 – 1 BvR 1474/12, 1 BvR 670/13, 1 BvR 57/14 – Rn. 92). Menschenwürde kommt nur natürlichen Personen zu. Auch der Menschenwürdekern der Religions- und Weltanschauungsfreiheit gem. Art. 4 Abs. 1 GG betrifft allein den Menschen als sittliche Person, der nur mit der Freiheit bestehen kann, sich eine religiöse oder weltanschauliche Überzeugung zu bilden, sie zu haben oder nicht zu haben (BeckOK GG/Germann Stand 15. November 2018 Art. 4 Rn. 1). Sind juristische Personen betroffen, kann lediglich die Menschenwürde der hinter ihnen stehenden Individuen tangiert sein (BeckOK GG/Hillgruber Stand 15. November 2018 Art. 1 Rn. 6; vgl. Jarass, in: Jarass/Pieroth GG 14.

Aufl. Art. 1 Rn. 7; Höfling, in: Sachs GG 8. Aufl. Art. 1 Rn. 66; Hofmann, in: Schmidt-Bleibtreu/Hofmann/Hennecke GG 14. Aufl. Art. 1 Rn. 10; Robbers, in: Umbach/Clemens GG Art. 1 Rn. 21; Herdegen, in: Maunz/Dürig GG Stand November 2018 Art. 1 Abs. 1 Rn. 72). Diese bleibt von der Entscheidung des Gerichtshofs unberührt (ebenso Fremuth EuZW 2018, 723, 730).

bb) Das Demokratieprinzip gem. Art. 20 Abs. 1 GG ist ebenfalls nicht berührt.

(1) Das Bundesverfassungsgericht hat zum Stand der Integration nach dem Vertrag von Lissabon entschieden, dass das Legitimationsniveau der Europäischen Union im Hinblick auf den Umfang der übertragenen Zuständigkeiten und den erreichten Grad von Verselbstständigung der Entscheidungsverfahren noch den deutschen verfassungsrechtlichen Anforderungen entspricht. Mit dem Vertrag von Lissabon ist weder die für die Verfassungsorgane unverfügbare verfassungsgebende Gewalt übertragen noch die staatliche Souveränität der Bundesrepublik Deutschland aufgegeben worden. Dem Deutschen Bundestag sind vielmehr eigene Aufgaben und Zuständigkeiten von hinreichendem Gewicht verblieben (BVerfG 30. Juni 2009 – 2 BvE 2/08 ua. – [Lissabon-Vertrag] zu C II 1 der Gründe, BVerfGE 123, 267).

(2) Daran ändert die Auslegung von Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG durch den Gerichtshof der Europäischen Union nicht in einer solchen Weise etwas, dass der Bundesrepublik Deutschland in Fragen des Umgangs mit dem religiösen oder weltanschaulichen Bekenntnis bzw. mit religiösen Gemeinschaften kein ausreichender Raum zur politischen Gestaltung dieses Lebensbereichs mehr verbliebe (vgl. zu Überlegungen in diese Richtung Fremuth EuZW 2018, 723, 730 f.; Schuhmann ZAT 2018, 110, 115). Die Entscheidung des Gerichtshofs wirkt sich zwar auf das Verhältnis der Kirchen und der ihnen zugeordneten Einrichtungen zu den dort beschäftigten Arbeitnehmern aus. Sie knüpft die Rechtfertigung einer Ungleichbehandlung wegen der Religion an tätigkeitsbezogene Voraussetzungen. Nach deutschem Verfassungsverständnis gehört es dagegen zum garantierten kirchlichen Selbstbestimmungsrecht, den Religionsgemeinschaften auch insoweit ein der Kontrolle durch staatliche Gerichte weitgehend entzogenes Recht zuzugestehen, verbindlich selbst unterschiedliche Loyalitätsanforderungen abhängig allein von der Konfessionszugehörigkeit der Beschäftigten zu stellen. Bei den inhaltlichen Anforderungen an Loyalitätspflichten für Arbeitnehmer, die in einer der Kirchen oder der ihnen zugeordneten Einrichtungen beschäftigt werden, und dem dafür geltenden gerichtlichen Prüfungsmaßstab, handelt es sich aber nicht um einen unverzichtbaren Teil der deutschen Verfassungsidentität (ähnlich Heuschmid/Höller AuR 2018, 587, 588; aA wohl Thüsing/Mathy BB 2018, 2805, 2809 sowie dies. RIW 2018, 559, 562), der einer Ausgestaltung durch Unionsrecht vollständig entzogen wäre. Auch nach Art. 140 GG iVm. Art. 137 Abs. 3 WRV ist das kirchliche Selbstbestimmungsrecht vielmehr nur innerhalb der Schranken des für alle geltenden Gesetzes garantiert (vgl. auch Roßbruch PflR 2018, 715, 717). Art. 137 Abs. 3 WRV geht als speziellere Norm insoweit Art. 4 Abs. 1 und Abs. 2 GG vor (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 85, BVerfGE 137, 273; sog. Schrankenspezialität). Zwar ist nach deutschem Verfassungsrecht dem Umstand Rechnung zu tragen, dass Art. 4 Abs. 1 und Abs. 2 GG die korporative Religionsfreiheit vorbehaltlos gewährleistet und insofern dem Selbstbestimmungsrecht sowie dem Selbstverständnis der Religionsgesellschaften bei dem Ausgleich der gegenläufigen Interessen besonderes Gewicht zuzumessen ist (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – aaO). Der Bundesrepublik Deutschland verbleibt aber nicht etwa allein deshalb kein ausreichender Raum zur politischen Gestaltung ihrer Beziehungen zu den Religionsgemeinschaften mehr, weil im Falle eines Konflikts mit dem Recht der Arbeitnehmer auf Schutz vor Diskriminierungen unionsrechtlich eine das Selbstbestimmungsrecht der Kirchen nicht mehr absolut setzende gerichtliche Kontrolle gefordert ist. Die nach deutschem Verfassungsverständnis tragenden Grundsätze des kirchlichen Arbeitsrechts bleiben vielmehr auch unionsrechtlich unangetastet (ebenso Schneedorf NJW 2019, 177, 179) und sind einer Gestaltung durch den deutschen Gesetzgeber damit nicht entzogen. Auch das Unionsrecht erkennt das Recht auf Autonomie der Kirchen und der anderen Organisationen an, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht (EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 50 f.). Die Vorgaben des Gerichtshofs in der Entscheidung vom 11. September 2018 (– C-68/17 –) sind zudem nur dann von Relevanz, wenn eine Kirche oder eine ihr zugeordnete Einrichtung unterschiedliche Loyalitätsanforderungen an Arbeitnehmer mit vergleichbaren (Leitungs-)Tätigkeiten allein aufgrund ihrer Konfession stellt. Die Bundesrepublik Deutschland verfügt in Fragen des Umgangs mit dem religiösen oder weltanschaulichen Bekenntnis bzw. mit religiösen Gemeinschaften weiterhin über ausreichenden Raum zur politischen Gestaltung dieses Lebensbereichs, weil die Kirchen bzw. die ihnen zugeordneten Einrichtungen auch nach Art. 4 Abs. 2 RL 2000/78/EG im Hinblick auf Ungleichbehandlungen wegen der Religion gegenüber anderen privaten oder öffentlichen Arbeitgebern privilegiert sind. Jenseits des Bereichs konfligierenden Diskriminierungsschutzes verbleibt den Religionsgemeinschaften auch unionsrechtlich uneingeschränkt das Recht auf Selbstbestimmung und auf Achtung des Status, den sie in den Mitgliedstaaten nach deren Rechtsvorschriften genießen (der „Status der Kirchen als solcher" ist nicht betroffen: Sagan EuZW 2018, 386, 387).

6. Die Auslegung von Art. 4 Abs. 2 UnterAbs. 2 RL 2000/78/EG durch den Gerichtshof der Europäischen Union erfordert keine Abkehr von der „Solange II"-Rechtsprechung des Bundesverfassungsgerichts bei der verfassungsrechtlichen Kontrolle von Unionsrecht.

a) Dies setzte voraus, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des Gerichtshofs der Europäischen Union nach Ergehen der „Solange II"-Entscheidung (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – BVerfGE 73, 339) unter den erforderlichen Grundrechtsstandard abgesunken wäre (zum Erfordernis, dies für eine zulässige Vorlage entsprechend Art. 100 Abs. 1 GG darzulegen, vgl. BVerfG 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] zu B I und II 2 d der Gründe, BVerfGE 102, 147). Das Bundesverfassungsgericht wird erst und nur dann im Rahmen seiner Gerichtsbarkeit wieder tätig, wenn der Gerichtshof den Grundrechtsstandard verlassen sollte, den es in der „Solange II"-Entscheidung festgestellt hat (BVerfG 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] zu B II 2 b der Gründe, aaO). Ein deckungsgleicher Schutz in den einzelnen Grundrechtsbereichen des Grundgesetzes durch das europäische Gemeinschaftsrecht – heute: Unionsrecht – und die darauf fußende Rechtsprechung des Gerichtshofs ist nicht gefordert (BVerfG 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] zu B II 2 c der Gründe, aaO). Den verfassungsrechtlichen Erfordernissen ist entsprechend den in der „Solange II"-Entscheidung genannten Voraussetzungen genügt, wenn die Rechtsprechung des Gerichtshofs einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften (Union) generell gewährleistet, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen

gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt. Dies ist bereits im Hoheitsbereich der Europäischen Gemeinschaften der Fall gewesen. Es ist ein Maß an Grundrechtsschutz erwachsen, das nach Konzeption, Inhalt und Wirkungsweise dem Grundrechtsstandard des Grundgesetzes im Wesentlichen gleich zu achten ist (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] zu B II 1 d der Gründe, aaO). Dieser Grundrechtsstandard ist insbesondere auch durch die Rechtsprechung des Gerichtshofs der (damals noch) Europäischen Gemeinschaften inhaltlich ausgestaltet worden, gefestigt und zureichend gewährleistet (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] zu B II 1 d aa der Gründe, aaO). Dies betrifft auch das Grundrecht der Religionsfreiheit (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] aaO). Dass sich auf der gemeinschaftsrechtlichen – heute: unionsrechtlichen – Ebene unter Umständen andersartige Fragen bei der Regelung von Grundrechten oder der Konkretisierung ihres Schutzbereichs stellen, vermag der Angemessenheit des gemeinschaftsrechtlichen Grundrechtsschutzes aus der Sicht des Grundgesetzes keinen generellen Abbruch zu tun (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] zu B II 1 e der Gründe, aaO). Von Grundgesetzes wegen sind auch Regelungen auf der Ebene der Gemeinschaft ermöglicht, die die Grundrechte im Einklang mit den Zielen und besonderen Strukturen der Gemeinschaft wahren; der Wesensgehalt der Grundrechte und zumal der Menschenrechte andererseits ist unabdingbar und muss auch gegenüber der Hoheitsgewalt der Gemeinschaft Bestand haben (BVerfG 22. Oktober 1986 – 2 BvR 197/83 – [Solange II] aaO).

b) Die europäische Rechtsentwicklung ist aufgrund der Auslegung von Art. 4 Abs. 2 RL 2000/78/EG durch den Gerichtshof der Europäischen Union nicht unter den demnach erforderlichen Grundrechtsstandard gesunken.

aa) Die RL 2000/78/EG trägt in der Auslegung des Gerichtshofs sowohl dem Schutz des Grundrechts der Arbeitnehmer, nicht wegen ihrer Religion oder Weltanschauung diskriminiert zu werden, als auch – durch Art. 4 Abs. 2 – dem in Art. 17 AEUV und in Art. 10 GRC – der Art. 9 der EMRK entspricht – anerkannten Recht auf Autonomie der Kirchen und der anderen öffentlichen oder privaten Organisationen Rechnung, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht (EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 50). Art. 4 Abs. 2 RL 2000/78/EG bezweckt die Herstellung eines angemessenen Ausgleichs zwischen einerseits dem Recht auf Autonomie der Kirchen und der anderen Organisationen, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht, und andererseits dem Recht der Arbeitnehmer, nicht wegen ihrer Religion oder Weltanschauung diskriminiert zu werden, falls diese Rechte im Widerstreit stehen sollten (EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 51).

bb) Der Umstand, dass dem Recht der Arbeitnehmer, nicht wegen ihrer Religion oder Weltanschauung diskriminiert zu werden – anders als nach deutschem Verständnis, das auch insoweit ein der gerichtlichen Überprüfung weitgehend entzogenes kirchliches Proprium anerkennt (Fremuth EuZW 2018, 723, 728; Menges ZMV 2018, 292) – ein gerichtlich nachprüfbares Gewicht beigemessen wird, führt nicht dazu, dass der Standard eines wirksamen Schutzes der Grundrechte gegenüber der Hoheitsgewalt der Union grundsätzlich verlassen würde, dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz nicht mehr im Wesentlichen gleich zu achten oder generell nicht auch weiterhin der Wesensgehalt der Grundrechte verbürgt wäre (ebenso Fremuth EuZW 2018, 723, 730). Der Gestaltungsspielraum der Kirchen wird zwar an tätigkeitsbezogene Merkmale geknüpft und daher in gewisser Weise eingeschränkt (Suttorp/Braun KuR 2018, 270, 274), wodurch umgekehrt das Schutzniveau für die Arbeitnehmer steigt (Fremuth EuZW 2018, 723, 730). Es verletzt aber nicht den Kernbereich des kirchlichen Selbstbestimmungsrechts, wenn diesem im Konflikt mit dem unionsrechtlich verbürgten Diskriminierungsschutz nicht generell der Vorrang eingeräumt wird (aA Greiner NZA 2018, 1289, 1291; Thüsing/Mathy BB 2018, 2805, 2808). Die Religionsgemeinschaften bleiben als Grundrechtsträger vielmehr selbst besonders geschützt, sie können unionsrechtlich lediglich keine Privilegierung im Verhältnis zur gerichtlichen Überprüfbarkeit von Diskriminierungen beanspruchen (Joussen EuZA 2018, 421, 430). Sie dürfen ihren Freiraum auch unionsrechtlich nach eigenen Maßstäben ausfüllen, nur nicht verbindlich selbst über die Reichweite dieses Freiraums im Verhältnis zu den grundrechtlich geschützten Belangen Dritter auf Schutz vor Diskriminierung entscheiden (vgl. Stein ZESAR 2018, 277, 281).

cc) Die Legitimität des Ethos der jeweils betroffenen Religionsgemeinschaft haben die staatlichen Gerichte grundsätzlich auch nach Unionsrecht nicht zu beurteilen (EuGH 17. April 2018 – C-414/16 – [Egenberger] Rn. 61, 64; Menges ZMV 2018, 292, 293). Es trifft daher nicht zu, dass eine Beurteilung des jeweiligen Ethos anhand weltlicher Maßstäbe zu erfolgen hätte (so aber wohl Thüsing/Mathy BB 2018, 2805, 2808; dies. RIW 2018, 559, 562; zutreffend dagegen Schneedorf NJW 2019, 177, 179) bzw. staatliche Gerichte das kirchliche Ethos zu beurteilen hätten. Es bleibt vielmehr die alleinige Angelegenheit der jeweiligen Religionsgesellschaft festzulegen, wie die jeweilige Glaubenslehre zu interpretieren ist und welcher Angebote und Dienste es zur Verwirklichung dieser Glaubenslehre bedarf sowie in welcher Organisationsform die konkrete Umsetzung erfolgt (zutreffend Schneedorf aaO). Bedienen sich kirchliche Einrichtungen – wie insbesondere in Diakonie und Caritas – für die Ausgestaltung ihrer Beschäftigungsverhältnisse des staatlichen Rechts, führt dies auch unionsrechtlich nicht etwa automatisch zu einer Nichtanwendbarkeit der Grundsätze des kirchlichen Arbeitsrechts (Schneedorf aaO). Es hat lediglich ein Ausgleich des kirchlichen Selbstbestimmungsrechts mit dem Recht der Arbeitnehmer stattzufinden, vor Diskriminierung geschützt zu werden. Ein mit dem Grundgesetz deckungsgleicher Schutz in den einzelnen Grundrechtsbereichen ist dagegen nicht erforderlich (vgl. BVerfG 7. Juni 2000 – 2 BvL 1/97 – [Bananenmarktordnung] zu B II 2 c der Gründe, BVerfGE 102, 147). Deshalb kann ein Ausschluss des Anwendungsvorrangs des Unionsrechts entgegen der Auffassung von Thüsing/Mathy (RIW 2018, 559, 562) auch nicht allein damit begründet werden, die Religionsfreiheit sei „im umfassenden Sinne" zu schützen. Wäre dies der Fall, müsste eine Ausgestaltung des Schutzes vor Benachteiligungen wegen der Religion im Bereich der Kirche und der ihr zugeordneten Einrichtungen im gesamten Bereich der Europäischen Union trotz der in Art. 4 RL 2000/78/EG enthaltenen Vorgaben unterbleiben.

IV. Der Senat konnte nicht offenlassen, ob die in unionsrechtskonformer Auslegung von § 9 Abs. 2 AGG geltenden Voraussetzungen an die Rechtfertigung einer Ungleichbehandlung wegen der Religion (vgl. Rn. 32) in Bezug auf die Anforderung, den heiligen und unauflöslichen Charakter der kirchlichen Eheschließung zu achten, erfüllt sind. Bliebe das Recht des Klägers auf Schutz vor Diskriminierung nach der vorgenannten Vorschrift außer Betracht, wäre die Revision der Beklagten begründet. Das Berufungsurteil wäre aufzuheben und die Sache an das Landesarbeitsgericht zurückzuverweisen. Es bedürfte ergänzen-

der Feststellungen zu den nach den Vorgaben des Bundesverfassungsgerichts im Beschluss vom 22. Oktober 2014 (– 2 BvR 661/12 – BVerfGE 137, 273) bei der Interessenabwägung auf Seiten des Klägers zu beachtenden Umständen (ebenso schon der Aussetzungsbeschluss des Senats vom 28. Juli 2016 – 2 AZR 746/14 [B] – Rn. 2 ff.).

1. Der Kläger hätte gegen eine Loyalitätsanforderung verstoßen, die ihm nach der Rechtsprechung des Bundesverfassungsgerichts zulässigerweise auferlegt war und an die er sich freiwillig durch den Abschluss des Arbeitsvertrags mit der Beklagten gebunden hatte. Dies wöge bei ihm als iSd. § 5 Abs. 3 GrO 1993 leitendem Mitarbeiter nach dem zu beachtenden Selbstbestimmungsrecht der römisch-katholischen Kirche besonders schwer. Es handelte sich nicht um ein bloß einmaliges – überwundenes – Fehlverhalten, sondern die Beklagte wäre bei einer Weiterbeschäftigung des Klägers voraussichtlich dauerhaft mit seinem illoyalen Verhalten, dem Leben in einer kirchlich ungültigen Ehe, konfrontiert gewesen (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 182, BVerfGE 137, 273). Demgegenüber könnte allein die Dauer der Beschäftigung des Klägers bei der Beklagten von gut neun Jahren im Zeitpunkt der Kündigung keine Interessenabwägung zu seinen Gunsten rechtfertigen. Es sind bislang auch keine Umstände festgestellt, aufgrund derer das Lebensalter des Klägers bereits eine besondere Schutzbedürftigkeit begründet hätte. Dies gilt auch für die Beurteilung seiner Beschäftigungschancen auf dem Arbeitsmarkt.

2. Soweit der Kläger die Vertragsgestaltung hinsichtlich der Geltung der in der GrO 1993 bestimmten Loyalitätsanforderungen für unklar hält, vermöchte dies nicht zu einer abweichenden Beurteilung zu führen. Ungeachtet der Frage, welche Rechtsfolge sich daraus ergäbe, liegt keine „unklare" Vertragsgestaltung vor.

a) Der Kläger macht nicht geltend, die Unklarheit ergebe sich aus seinem Dienstvertrag selbst. Dafür gibt es auch objektiv keine Anhaltspunkte.

b) Soweit er darauf abstellt, die Unklarheit folge daraus, dass die Beklagte vom Wortlaut her identische Chefarztverträge ebenso mit evangelischen Chefärzten abgeschlossen, diesen aber im Falle einer Wiederheirat nicht gekündigt habe, sind zum einen zum Inhalt anderer Chefarztverträge keine Feststellungen getroffen. Eine zulässige Verfahrens(gegen-)rüge hat der Kläger nicht erhoben. Zum anderen bleibt sein Vorbringen auch im Revisionsverfahren unsubstanziiert. Es ist – bis auf den Fall des schon bei seiner Einstellung durch die Beklagte zum zweiten Mal verheirateten Dr. H – weder dargelegt, um die Verträge welcher Chefärzte es sich handeln soll, noch behauptet, er, der Kläger, habe bereits bei seinem eigenen Vertragsschluss Kenntnis vom Inhalt der fraglichen Verträge und ihrer praktischen Handhabung in anderen Fällen gehabt. Im Übrigen wäre bei identischem Vertragswortlaut auch jeweils die GrO 1993 in Bezug genommen, die für den Loyalitätsverstoß durch Wiederverheiratung gerade zwischen katholischen und nicht-katholischen Mitarbeitern unterscheidet.

3. Ein Verstoß gegen den Gleichbehandlungsgrundsatz, wie ihn das Landesarbeitsgericht zugunsten des Klägers bei der Interessenabwägung berücksichtigt hat, läge ebenfalls nicht vor. Die Beklagte durfte – § 9 Abs. 2 AGG in unionsrechtskonformer Auslegung ausgeklammert – an Katholiken auch bei gleich gelagerter (Leitungs-)Tätigkeit nach deutschem Verfassungsrecht weiter gehende Loyalitätsanforderungen als an Angehörige anderer Konfessionen oder konfessionslose Arbeitnehmer stellen. Ebenso durfte sie das Leben in einer nach kirchlichem Recht ungültigen Ehe als gegenüber dem Zusammenleben in nichtehelicher Gemeinschaft schwerer wiegenden Verstoß werten (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 172 ff., BVerfGE 137, 273) und musste daher nicht schon das eheähnliche Zusammenleben des Klägers mit seiner künftigen zweiten Ehefrau zum Anlass für eine Kündigung seines Arbeitsverhältnisses nehmen. Es sind auch keine Umstände festgestellt oder objektiv ersichtlich, aus denen sich ergäbe, die Beklagte hätte ihr Kündigungsrecht dadurch verwirkt, dass sie die Kündigung erst im März 2009 erklärte, obwohl sie bereits im November 2008 Kenntnis von der zweiten Eheschließung des Klägers erlangte. Das gilt sowohl für das Zeit- als auch für das Umstandsmoment. Die Beklagte musste nicht nur das in der GrO 1993 vorgeschriebene beratende Gespräch mit dem Kläger führen, sondern auch den Aufsichtsrat beteiligen und eine Stellungnahme des Generalvikars einholen. Angesichts der – auch für die Beklagte und das Krankenhaus – weitreichenden Folgen des Kündigungsentschlusses ist es nicht zu beanstanden, dass sie dabei umsichtig und ohne Hast vorging (so bereits BAG 8. September 2011 – 2 AZR 543/10 – Rn. 13, BAGE 139, 144).

4. Der Senat könnte die erforderliche Bewertung der nach den Vorgaben des Bundesverfassungsgerichts bei der Abwägung aller Umstände des Einzelfalls zu beachtenden Interessen des Klägers auf der Basis der bisherigen Feststellungen nicht selbst vornehmen. Dafür bedürfte es weiterer Sachaufklärung.

a) Dies gilt zunächst für die vom Bundesverfassungsgericht verlangte Bewertung, ob die Rechtspositionen des Klägers und seiner zweiten Ehefrau aus Art. 6 Abs. 1 GG und den Wertungen aus Art. 8 Abs. 1 sowie Art. 12 EMRK in einem Maße tangiert sind, das es rechtfertigen würde, den Interessen des Klägers den Vorrang vor den Interessen der Beklagten einzuräumen (vgl. dazu BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 180, BVerfGE 137, 273).

aa) Soweit der Kläger im Personalgespräch am 25. November 2008 mitgeteilt haben soll, mit Rücksicht auf seine beiden Kinder von einer kirchlichen Annullierung der ersten Ehe abgesehen zu haben, bevor er standesamtlich die zweite Ehe geschlossen habe, wäre dies nicht geeignet, besondere Interessen an seiner Wiederheirat zu begründen. Nach dem kirchlichen Selbstverständnis wäre es – solange die Annullierung nicht feststeht – vielmehr unerheblich, ob diese bereits beantragt war oder aus welchen Gründen zunächst nicht. Zudem ist weder vom Kläger dargelegt noch objektiv ersichtlich, dass die kirchenrechtlichen Voraussetzungen für eine Annullierung seiner ersten Ehe gegeben gewesen wären.

bb) Dass die Schließung der zweiten Ehe nach dem Vorbringen des Klägers möglicherweise kein öffentliches Ärgernis ausgelöst hat, wäre nach der hier noch maßgeblichen GrO 1993 für die kündigungsrechtliche Sanktion eines leitenden Mitarbeiters ebenfalls unerheblich.

cc) Soweit der Kläger behauptet hat, er sei von seiner ersten Ehefrau böswillig verlassen worden, ist zwar nicht ausgeschlossen, dass dies – gegebenenfalls unter Berücksichtigung weiterer Umstände – für ein besonderes Interesse am Eingehen einer zweiten Ehe sprach. Ein solcher Sachverhalt ist aber bislang ebenfalls nicht festgestellt.

dd) Soweit das Landesarbeitsgericht ergänzend auf die gewechselten Schriftsätze verwiesen hat, könnten sich zwar auch aus dem damit in Bezug genommenen Vorbringen besondere Interessen des Klägers an der zweiten Eheschließung ergeben haben. Indes fehlt es auch insoweit bislang an Feststellungen.

b) Ebenfalls an ausreichenden Feststellungen mangelt es mit Blick auf die nach der Entscheidung des Bundesverfassungsgerichts etwaig nach dem Gedanken des Vertrauensschutzes zugunsten des Klägers zu berücksichtigenden Umstände.

aa) Das Bundesverfassungsgericht hat im Streitfall die Berücksichtigung des Gedankens des Vertrauensschutzes in Bezug darauf für möglich gehalten, dass § 10 Abs. 4 Nr. 2 des Dienstvertrags in Abweichung von der GrO 1993 unterschiedliche Bewertungen hinsichtlich von Verstößen gegen kirchliche Grundsätze – Verstoß gegen das Verbot des Lebens in kirchlich ungültiger Ehe einerseits und Verstoß gegen das Verbot des Lebens in nichtehelicher Gemeinschaft andererseits – nicht vorsehe und die individualvertragliche Abrede besonderes Vertrauen des Klägers ausgelöst haben könnte (BVerfG 22. Oktober 2014 – 2 BvR 661/12 – Rn. 181, BVerfGE 137, 273).

bb) Es ist jedoch nicht festgestellt, dass der Kläger Kenntnis davon gehabt hätte, zur Kündigung berechtigte Vertreter der Beklagten hätten von dem eheähnlichen Zusammenleben mit seiner späteren zweiten Ehefrau gewusst. Dies wäre Voraussetzung dafür, dass sich bei ihm ein schützenswertes Vertrauen dahingehend hätte bilden können, die Beklagte werde einen solchen Verstoß gegen die Loyalitätsanforderungen und – wegen der gleichgeordneten Aufzählung beider Verstöße als Kündigungsgründe im Arbeitsvertrag – möglicherweise auch eine Wiederheirat nicht zum Anlass für eine Kündigung nehmen. Soweit der Kläger erstmalig im Revisionsverfahren behauptet, ihm sei bekannt gewesen, dass der Geschäftsführung der Beklagten Anhaltspunkte dafür vorlagen, er sei eine nichteheähnliche Lebensgemeinschaft eingegangen, hat die Beklagte diesen – zudem substanzlosen – Vortrag ausdrücklich bestritten.

cc) Die tatrichterliche Würdigung des Landesarbeitsgerichts, die Beklagte habe jedenfalls „seit Herbst 2006 von der nichteheähnlichen Lebensgemeinschaft mit der neuen Lebensgefährtin des Klägers Kenntnis“ gehabt, wird im Übrigen nicht vom wiedergegebenen Ergebnis der Beweisaufnahme getragen. Die diesbezüglich von der Beklagten erhobene Rüge einer Verletzung von § 286 Abs. 1 ZPO wäre begründet. Das Berufungsgericht hat die Kenntnis der Beklagten aus der Aussage eines der ehemaligen Geschäftsführer geschlossen, er sei gegen Ende seiner Dienstzeit von dem weiteren Geschäftsführer „über das Gerücht informiert worden, dass der Kläger eine neue Lebensgefährtin habe“. Dies ist logisch nicht nachvollziehbar. Wer ein Gerücht kennt, weiß deshalb noch nicht, dass die mit ihm verbreiteten Tatsachen wahr sind. Das Landesarbeitsgericht hat seine Schlussfolgerung auch nicht mit weiteren Indizien begründet. Soweit es auf die Angabe des Zeugen verwiesen hat, man habe sich entschlossen gehabt, „diesen Gerüchten nachzugehen, was letztlich dann wohl doch unterblieben sei“, ergibt sich auch daraus nicht, die Beklagte müsse positive Kenntnis von den tatsächlichen Umständen eines eheähnlichen Zusammenlebens des Klägers mit seiner Lebensgefährtin gehabt haben.

Unzulässiger Eingriff in das allgemeines Persönlichkeitsrecht der Arbeitnehmer per Betriebsvereinbarung

(**Bundesarbeitsgericht**, Beschluss vom 11. Dezember 2018 – 1 ABR 12/17 –)

Eine Regelung in einer Betriebsvereinbarung, nach der ein Arbeitgeber zu einem Personalgespräch, das er mit einem Arbeitnehmer führt, bevor er aufgrund eines diesem vorgeworfenen Fehlverhaltens eine arbeitsrechtliche Maßnahme ergreift, gleichzeitig auch den Betriebsrat zu laden hat, ist nach § 75 Abs. 2 BetrVG unwirksam.

Aus den Gründen:

3. Die in § 4 Nr. 4.1 Satz 1 und Satz 3 RBV geregelte Einladung des Betriebsrats und das daran anknüpfende Verfahren zur Beteiligung eines Mitglieds des Betriebsrats an dem vor Ausspruch einer „disziplinarischen“ Maßnahme iSv. § 4 Nr. 4.1 Satz 2 RBV obligatorischen Personalgespräch zwischen Arbeitgeber und Arbeitnehmer beeinträchtigen das allgemeine Persönlichkeitsrecht der zum Gespräch geladenen Arbeitnehmer.

a) Ein Personalgespräch iSv. § 4 Nr. 4.1 RBV dient der Vorbereitung einer „disziplinarischen“ Maßnahme, der typischerweise ein vom Arbeitgeber beanstandetes Verhalten des Arbeitnehmers zugrunde liegt. Da die Einladung an den Betriebsrat als Gremium gerichtet ist, wird die Information einer drohenden „disziplinarischen“ Maßnahme aufgrund eines (etwaigen) fehlerhaften Verhaltens des Arbeitnehmers allen Mitgliedern des Betriebsrats bekannt. Weil die Einladung des Betriebsrats nach § 4 Nr. 4.1 Satz 1 RBV „gleichzeitig“ zu erfolgen hat, hängt es weder vom Willen des Arbeitnehmers ab, ob der Betriebsrat überhaupt von dem konkret bevorstehenden Gespräch erfährt, noch kann er selbst bestimmen, welches oder welche Mitglieder des Betriebsrats hiervon ggf. Kenntnis erlangen sollen.

b) Darüber hinaus sieht § 4 Nr. 4.1 RBV – anders als vom Betriebsrat angenommen – nicht vor, dass der betroffene Arbeitnehmer selbst entscheiden kann, welches Betriebsratsmitglied seines Vertrauens er zum Gespräch hinzuzieht. Weder der Wortlaut dieser Norm noch ihre Systematik lassen den Schluss darauf zu, dass der Arbeitnehmer einen Anspruch darauf hat, das am Gespräch teilnehmende Betriebsratsmitglied selbst zu bestimmen. Vielmehr richtet sich die Einladung zum Gespräch nach § 4 Nr. 4.1 Satz 1 und Satz 4 RBV an den gesamten Betriebsrat. Dieser kann daher im Rahmen seines ihm obliegenden Auswahlermessens dasjenige Mitglied bestimmen, welches sich am Gespräch beteiligt. Das dem Arbeitnehmer in § 4 Nr. 4.1 Satz 3 RBV eingeräumte Wahlrecht beschränkt sich lediglich auf die Befugnis, das Gespräch ohne jegliche Beteiligung eines Betriebsratsratsmitglieds zu führen. Es beinhaltet jedoch nicht das Recht, es nur mit einem bestimmten – vom Arbeitnehmer ausgewählten – Betriebsratsmitglied zu führen.

4. Die durch § 4 Nr. 4.1 Satz 1 und Satz 3 RBV bewirkte Beeinträchtigung des allgemeinen Persönlichkeitsrechts der betroffenen Arbeitnehmer ist gemessen am Zweck der Betriebsratsbeteiligung nicht verhältnismäßig.

a) § 4 Nr. 4.1 RBV verpflichtet den Arbeitgeber, mit dem betroffenen Arbeitnehmer vor Ausspruch einer „disziplinarischen“ Maßnahme zunächst ein Gespräch zu führen. Dem Arbeitnehmer soll damit Gelegenheit gegeben werden, zu den gegen ihn erhobenen Vorwürfen Stellung zu nehmen. Dadurch erhält er die Möglichkeit, ein ihm ggf. zur Last gelegtes Fehlverhalten auszuräumen oder entlastende Umstände vorzubringen und damit die vom Arbeitgeber beabsichtigte Maßnahme entweder gänzlich zu verhindern oder diese zumindest abzumildern. Als Unterstützung in einer Situation struktureller Unterlegenheit des Arbeitnehmers und ggf. zu dessen Beratung wollten die Betriebsparteien ihm hierbei ein Mitglied des Betriebsrats zur Seite stellen.

Auch kann dem am Gespräch beteiligten Betriebsratsmitglied im Hinblick auf das vom Arbeitgeber vorgebrachte Fehlverhalten des Arbeitnehmers eine wichtige Kontroll- und Korrekturfunktion zukommen. Zudem wird durch seine Teilnahme sichergestellt, dass für den Arbeitnehmer eine Person als Zeuge zugegen ist (vgl. hierzu auch BAG 16. November 2004 – 1 ABR 53/03 – Rn. 24, BAGE 112, 341).

b) Im Hinblick auf diesen Zweck sind die Regelungen in § 4 Nr. 4.1 Satz 1 und Satz 3 RBV – ihre Geeignetheit unterstellt – weder erforderlich noch angemessen.

aa) Um dem Arbeitnehmer dem bei der Führung des obligatorischen Personalgesprächs gebotenen Schutz zu gewährleisten, ist die in § 4 Nr. 4.1 Satz 1 und Satz 3 RBV vorgesehene Verfahrensweise nicht erforderlich. Eine im Interesse des Arbeitnehmers liegende Teilnahme eines Betriebsratsmitglieds am Personalgespräch ist auch dann hinreichend gewährleistet, wenn dem betroffenen Arbeitnehmer ein Recht auf Hinzuziehung eines bestimmten Betriebsratsmitglieds eingeräumt und er hierauf in der Einladung zum Gespräch hingewiesen wird. Dies zeigen die Regelungen in § 81 Abs. 4 Satz 3 und § 82 Abs. 2 Satz 2 BetrVG. Nach dem sich aus diesen gesetzlichen Regelungen ergebenden Leitbild ist der durch die Beteiligung eines Betriebsratsmitglieds an den Erörterungen und Gesprächen des Arbeitgebers mit dem Arbeitnehmer über dessen berufliche Fähigkeiten und Leistungen vermittelte Schutz schon dann ausreichend sichergestellt, wenn die Initiativlast für die Hinzuziehung des Betriebsratsmitglieds beim Arbeitnehmer liegt. Dies gilt – wie § 81 Abs. 4 Satz 3 BetrVG erkennen lässt – auch dann, wenn eine Pflicht des Arbeitgebers zur Gesprächsführung mit dem Arbeitnehmer besteht.

bb) Darüber hinaus ist das in § 4 Nr. 4.1 RBV geregelte Verfahren angesichts der Intensität der damit einhergehenden Beeinträchtigung des Persönlichkeitsrechts der Arbeitnehmer in mehrfacher Hinsicht nicht angemessen.

(3) Hinzu kommt, dass die Betriebsparteien in § 4 Nr. 4.1 RBV für das am Gespräch teilnehmende Betriebsratsmitglied keine Pflicht zur Verschwiegenheit über dessen Inhalt geregelt haben. Die Vorschrift des § 79 Abs. 1 Satz 1 BetrVG greift insoweit nicht. Auch eine analoge Anwendung von § 99 Abs. 1 Satz 3 und § 102 Abs. 2 Satz 5 BetrVG bzw. – wie vom Landesarbeitsgericht angenommen – von § 82 Abs. 2 Satz 3 BetrVG scheidet aus. Eine solche setzt eine vom Normgeber unbeabsichtigt gelassene Lücke voraus, deren Planwidrigkeit aufgrund konkreter Umstände positiv festgestellt werden kann (vgl. nur BAG 27. Juni 2018 – 10 AZR 295/17 – Rn. 23). Hieran fehlt es.

c) Die verfahrensrechtlichen Regelungen zum betrieblichen Eingliederungsmanagement (bEM) nach § 167 Abs. 2 SGB IX gebieten keine andere Bewertung. Auch im Rahmen des bEM darf die Hinzuziehung des Betriebsrats nur mit vorheriger Einwilligung des Arbeitnehmers erfolgen (vgl. BAG 22. März 2016 – 1 ABR 14/14 – Rn. 11 und 30 mwN, BAGE 154, 329). Unabhängig davon zielt das bEM darauf ab, eine bestehende und in aller Regel auch betriebsbekannte Arbeitsunfähigkeit zu überwinden, erneuter Arbeitsunfähigkeit vorzubeugen und eine möglichst dauerhafte Fortsetzung des Beschäftigungsverhältnisses zu fördern (vgl. BAG 7. Februar 2012 – 1 ABR 46/10 – Rn. 21, BAGE 140, 350). Damit dient dieses Verfahren anderen Zwecken als das typischerweise an ein pflichtwidriges Verhalten des Arbeitnehmers anknüpfende Personalgespräch nach § 4 Nr. 4.1 RBV.

d) Entgegen der Ansicht des Betriebsrats ergibt sich auch aus seinen Unterrichtungsrechten nach § 99 Abs. 1 Satz 1, § 102 Abs. 1 Satz 2 BetrVG bei einer etwaigen nachfolgenden Versetzung oder Kündigung des Arbeitnehmers vorliegend nichts Gegenteiliges. Die genannten Bestimmungen treffen keine Aussage darüber, wie die Hinzuziehung eines Betriebsratsmitglieds zu einem ggf. im Vorfeld einer solchen personellen Einzelmaßnahme zwischen Arbeitnehmer und Arbeitgeber stattfindenden Gespräch ausgestaltet werden kann.

Anspruch auf Löschung der gespeicherten Kopien eines Personalausweises ohne Passbild

(**Landessozialgericht Berlin-Brandenburg**, Urteil vom 30. April 2019 – L 26 AS 2611/17 –)

Der Speicherung der Kopien des Personalausweises in der elektronischen Akte eines Sozialleistungsträgers steht auch ohne Speicherung des Fotos entgegen, dass dort Angaben zur Augenfarbe und Größe des Betroffenen enthalten sind, die nach § 1 Abs. 2 Nr. 1 Verordnung zur Erhebung von Datennach § 51b SGB IIvom 12. August 2010) gerade nicht zu erheben sind. Es ist auch nicht erkennbar, dass das Vorhalten von Kopien des Personalausweises in der elektronischen Akte der Überprüfung einer korrekten Leistungserbringung und der Bekämpfung von Leistungsmissbrauch dienen kann

(Nicht amtliche Leitsätze)

Aus den Gründen:

Rechtsgrundlage des Anspruchs auf Löschung der in der elektronischen Akte des Beklagten gespeicherten und nach Entfernen des Passfotos nur noch unvollständigen Kopien des Personalausweises ist Art. 17 Abs. 1 a 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 (DS-GVO), in Kraft getreten am 25. Mai 2018. Danach hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

Diese Regelung entspricht im Wesentlichen dem zuvor bis zum 24. Mai 2018 in Deutschland geltenden Recht. Sozialdaten waren nach § 84 Abs. 2 SGB X a. F. auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich war und kein Grund zu der Annahme bestand, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden (vgl. § 84 Abs. 2 Satz 2 SGB X i. d. F. durch Art. 8 § 2 Nr. 18 d des Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001, in Kraft getreten am 23. Mai 2001, <a. F., BGBl. I S. 904>).

Die Norm des Art. 17 Abs. 1 DS-GVO ist auch anwendbar. Maßgeblicher Zeitpunkt für die Beurteilung der Sach- und Rechtslage ist bei einer kombinierten Anfechtungs- und Leistungsklage der Zeitpunkt der letzten mündlichen Verhandlung (vgl. Keller, in: Meyer-Ladewig/Keller/Leitherer/Schmidt, SGG, 12. A. 2017, § 54 RdNr. 34 m.w.N.; s. a. BSG, Urteil vom 18. Dezember 2018 – B 1 KR 31/17 R –, RdNr. 14; abweichend LSG Berlin-Brandenburg, Urteil vom 6. Dezember 2018 – L 32 AS 2045/16 –, RdNrn. 32 ff.; jeweils zitiert nach juris). Es sind schließlich keine Anhaltspunkte dafür ersichtlich, dass die DS-GVO nach ihrem zeitlichen Geltungswillen das streitige Rechtsverhältnis nicht umfassen soll. Dies gilt im vorliegenden Fall erst recht, weil die begehrte Löschung eine in die Zukunft gerichtete Leistung ist.

Nach § 35 Abs. 2 Satz 1 Sozialgesetzbuch Erstes Buch (SGB I) i. d. F. durch Art. 19 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017, in Kraft getreten am 25. Mai 2018, (n. F.; BGBl. I S. 2541) regeln die Vorschriften des Zweiten Kapitels des SGB X und der übrigen Bücher des Sozialgesetzbuchs die Verarbeitung von Sozialdaten abschließend, soweit nicht die DS-GVO unmittelbar gilt. Für die Verarbeitungen von Sozialdaten im Rahmen von nicht in den Anwendungsbereich der DS-GVO fallenden Tätigkeiten finden die DS-GVO und dieses Gesetz entsprechende Anwendung, soweit nicht in diesem oder einem anderen Gesetz Abweichendes geregelt ist (§ 35 Abs. 2 Satz 2 SGB I). Die Speicherung von Kopien eines Personalausweises durch den Beklagten betrifft Sozialdaten im Sinne von § 35 SGB I. Sozialdaten sind personenbezogene Daten (vgl. Art 4 Nr. 1 DS-GVO), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden (vgl. § 67 Abs. 2 Satz 1 SGB X n. F.). Zu den in § 35 SGB I genannten Stellen gehört der Beklagte im Sinne von §§ 12, 19a Abs. 2 SGB I, der als Kreis für die Erbringung von Leistungen nach dem SGB II zuständig ist.

Im Hinblick auf die Auffangregelung in § 35 Abs. 2 Satz 2 SGB I kann der Senat offen lassen, ob die DS-GVO unmittelbare oder entsprechende Anwendung findet (vgl. BSG, Urteil vom 18. Dezember 2018 – B 1 KR 31/17 R –, RdNr. 15, zitiert nach juris). Die Frage stellt sich im hiesigen Fall, weil die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit findet, die nicht in den Anwendungsbereich des Unionsrechts fällt (vgl. Art. 2 Abs. 2a DS-GVO). Nach Art. 4 Abs. 2 b des Vertrags über die Arbeitsweise der Europäischen Union (AEUV oder auch Vertrag von Lissabon vom 26. Oktober 2012) erstreckt sich die von der Union mit den Mitgliedstaaten geteilte Zuständigkeit u.a. auf die Sozialpolitik hinsichtlich der in dem Vertrag genannten Aspekte (dann direkte Anwendung), nicht aber auf die Verwaltungstätigkeit der Sozialbehörden (dann analoge Anwendung).

Nach den übrigen Regelungen in Art. 2 DS-GVO ist die DS-GVO sachlich anwendbar. Die von dem Beklagten durchgeführte Speicherung des Personalausweises der Klägerin stellt eine Verarbeitung (Art. 4 Nr. 2 DS-GVO) personenbezogener Daten dar, die in einem Dateisystem (Art. 4 Nr. 6 DS-GVO) im Sinne von Art. 2 Abs. 1 DS-GVO gespeichert worden sind. Der Ausdruck „personenbezogene Daten" bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (auch: betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DS-GVO). Dazu gehören die Angaben in dem gespeicherten Personalausweis zu Namen, Geburtstag und -ort, Nationalität, Wohnort, Augenfarbe und Größe der Klägerin sowie Personalausweisnummer, Ausstelldatum und ausstellende Behörde. Der Ausdruck „Verarbeitung" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (vgl. Art. 4 Nr. 2 DS-GVO). Der Ausdruck „Dateisystem" bezeichnet jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (vgl. Art. 4 Nr. 6 DS-GVO). Eine elektronische Akte, die den gesamten Ablauf des Verwaltungsverfahrens wiedergibt und auch den kopierten Personalausweis enthält, zählt ohne Zweifel hierzu.

Die Voraussetzungen des Anspruchs aus Art. 17 Abs. 1 a DS-GVO sind erfüllt, denn der Beklagte als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO und § 67 Abs. 4 Satz 1 SGB X n. F. hat den Personalausweis der Klägerin als von der Speicherung ihrer personenbezogenen Daten betroffener Person gespeichert. Die Speicherung soll nach den internen Verwaltungsvorschriften zu den Aufbewahrungs- und Löschungsfristen zehn Jahre ab Beginn des auf die letzte Auszahlung folgenden Jahres dauern. Im Fall der Klägerin, die bis zum 31. August 2012 Arbeitslosengeld II von dem Beklagten bezogen und am 4. Februar 2015 die Löschung beantragt hat, bedeutet dies, dass die Kopien erst am 31. Dezember 2022 gelöscht werden sollen.

Der Löschungsanspruch setzt weiter voraus, dass die gespeicherten Kopien des Personalausweises der Klägerin für die Zwecke, für die er gespeichert wurde, nicht mehr notwendig sind.

Die Rechtsgrundlage zur Feststellung der Zwecke, für die der Verantwortliche, also der Beklagte, die Daten erhoben hat, ergibt sich aus der Regelung der rechtmäßigen Datenverarbeitung in Art. 6 DS-GVO (vgl. dazu BSG, Urteil vom 18. Dezember 2018 – B 1 KR 31/17 R –, zitiert nach juris). Denn die Norm des Art. 17 Abs. 1 a DS-GVO knüpft nach Wortlaut, Regelungssystem (Art. 17 Abs. 1 d DS-GVO) und -zweck an die Beendigung einer rechtmäßigen Datenverarbeitung an. Die Verarbeitung ist nach Art. 6 Abs. 1 c DS-GVO rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Die Rechtsgrundlage hierfür wird u.a. festgelegt durch das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt (Art. 6 Abs. 3 Satz 1 b DS-GVO). Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt sein (vgl. Art. 6 Abs. 3 Satz 2 DS-GVO).

Eine solche Rechtsgrundlage enthält § 67a Abs. 1 Satz 1 und 2 SGB X n. F. Danach ist die Erhebung von Sozialdaten durch die in § 35 SGB I genannten Stellen zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Dies gilt auch für die Erhebung der besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO, die hier jedoch nicht erfolgt ist. Die anschließende Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten durch die in § 35 SGB I genannten Stellen ist nur er-

laubt, soweit datenschutzrechtliche Vorschriften des SGB X oder eine andere Vorschrift des SGB dies erlauben oder anordnen (§ 67b Abs. 1 Satz 1 SGB X n. F.). Hierzu zählen die einschlägigen Regelungen der §§ 50 ff. SGB II. Die dort getroffenen Regelungen enthalten bereichsspezifische Datenschutznormen für die Grundsicherung für Arbeitsuchende. Solche Regelungen des bereichsspezifischen Datenschutzes gehen den allgemeinen Vorschriften des Sozialdatenschutzes der §§ 67 ff. SGB X vor. § 50 SGB II ermächtigt die Grundsicherungsträger zur Datenübermittlung. § 51b SGB II stellt eine Spezialvorschrift über die Datenerhebung und -verarbeitung durch die Träger der Grundsicherung für Arbeitsuchende dar. Ausweislich der Gesetzesmaterialien erfüllt § 51b SGB II auch die Funktion, dass weitere Daten mit Rücksicht auf das Grundrecht auf informationelle Selbstbestimmung der Leistungsempfänger nicht erhoben werden dürfen (vgl. BSG, Urteil vom 19. September 2008 – B 14 AS 45/07 R –, RdNr. 22, zitiert nach juris).

Nach § 51b Abs. 1 SGB II erheben die zuständigen Träger der Grundsicherung für Arbeitsuchende laufend die für die Durchführung der Grundsicherung für Arbeitsuchende erforderlichen Daten. Das Bundesministerium für Arbeit und Soziales wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrats die nach Satz 1 zu erhebenden Daten, die zur Nutzung für die in Abs. 3 genannten Zwecke erforderlich sind, einschließlich des Verfahrens zu deren Weiterentwicklung festzulegen. Die nach den Absätzen 1 und 2 erhobenen [....] Daten dürfen nur [....] für folgende Zwecke verarbeitet und genutzt werden:

1. die zukünftige Gewährung von Leistungen nach diesem und dem Dritten Buch an die von den Erhebungen betroffenen Personen,
2. Überprüfungen der Träger der Grundsicherung für Arbeitsuchende auf korrekte und wirtschaftliche Leistungserbringung,
3. die Erstellung von Statistiken, Kennzahlen für die Zwecke nach § 48a Abs. 2 und § 48b Abs. 5, Eingliederungsbilanzen und Controllingberichten durch die Bundesagentur, der laufenden Berichterstattung und der Wirkungsforschung nach den §§ 53 bis 55,
4. die Durchführung des automatisierten Datenabgleichs nach § 52,
5. die Bekämpfung von Leistungsmissbrauch.

Der Beklagte beruft sich vorliegend auf die Zwecke nach Nrn. 2. und 5.

Danach durfte der Beklagte personenbezogene Daten der Klägerin u.a. zu Familien- und Vornamen, Anschrift, Familienstand, Geschlecht, Geburtsdatum, Staatsangehörigkeit usw. (§ 1 Abs. 2 Nr. 1 der Verordnung zur Erhebung der Daten nach § 51b SGB II vom 12. August 2010, BGBl. I S. 1150) erheben. Dies schließt die Anforderung und Vorlage entsprechender Dokumente zum Nachweis der gemachten Angaben durch die Klägerin nicht aus (vgl. BSG, Urteil vom 19. September 2008 – B 14 AS 45/07 R –, RdNr. 22, zitiert nach juris). Allerdings steht der Speicherung der Kopien des Personalausweises auch nach Löschung des Passbildes bereits entgegen, dass dort Angaben zur Augenfarbe und Größe der Klägerin enthalten sind, die nach § 1 Abs. 2 Nr. 1 der genannten Verordnung gerade nicht zu erheben sind. Es ist auch nicht erkennbar, dass das Vorhalten von Kopien des Personalausweises in der elektronischen Akte der Überprüfung einer korrekten Leistungserbringung und der Bekämpfung von Leistungsmissbrauch dienen kann.

Zunächst ist festzustellen, dass der Beklagte selbst die Vorlage des Personalausweises in seiner Anforderung vom 13. Januar 2009 unter der Rubrik „Ausweispapiere“ nur alternativ neben die Vorlage eines Passes oder Meldebescheinigung gestellt hat. Offenbar sollte die Vorlage dieser Dokumente dem Nachweis des Wohnsitzes der Klägerin und damit der Feststellung der Zuständigkeit zur Leistungserbringung des Beklagten dienen. Die Meldebescheinigung ist – neben den Kopien des Personalausweises – zu den Akten genommen worden. Die Daten des Personalausweises sind außerdem mit Ausnahme von Augenfarbe und Größe auch in dem von der Klägerin unterschriebenen Antragsformular enthalten. Zwar sind die beiden Personalausweise ausstellenden Behörden sowie die Personalausweisnummern nicht im Antragsformular oder an anderer Stelle angegeben. Allerdings ist nicht erkennbar, dass diese Angaben zur Erfüllung der Zwecke in § 51b Abs. 3 Nr. 2 und 5 SGB II erforderlich sind. Zur Vermeidung der Bewilligung von Arbeitslosengeld II an einen Dritten, der sich der echten Ausweispapiere eines anderen bedient, kann die gespeicherte Kopie eines Personalausweises ohne Passbild nicht beitragen. Wenn sich ein Antragsteller mit einem Ausweis Leistungen erschleichen will, lässt sich die Identität des Antragstellers nur durch den Abgleich des Gesichts mit dem vorgezeigten Personalausweisbild feststellen. Ein Dokumentenprüfgerät kann die Echtheit eines gefälschten Personalausweises erkennen. Die unvollständige Kopie eines Personalausweises ist dazu nicht geeignet. Der Auffassung des Beklagten, die Kopie sei auch erforderlich, um gegebenenfalls eine noch zehn Jahre nach der Bewilligung erforderliche Aufhebung nach § 45 SGB X zu prüfen, kann ebenfalls nicht gefolgt werden. Denn die in dem Ausweis enthaltenen Daten sind durch den ausgefüllten Leistungsantrag hinlänglich bekannt.

Schließlich sind nach den obigen Ausführungen weder die internen Verwaltungsvorschriften zu den Aufbewahrungs- und Löschungsfristen noch der Aktenplan II der Bundesagentur für Arbeit vom 1. Oktober 2012 mit den dort jeweils geregelten pauschalen Aufbewahrungsfristen geeignet, ein Recht des Beklagten auf Speicherung der Ausweiskopien der Klägerin über eine Frist von zehn Jahren zu begründen.

Zum Umfang des Auskunftsanspruchs nach § 15 DS-GVO

(**Landgericht Köln**, Teilurteil vom 18. März 2019 – 26 O 25/18 –)

1. **Der Auskunftsanspruch nach § 15 DS-GVO dient nicht der vereinfachten Buchführung des Betroffenen, sondern soll den Betroffene in die Lage versetzen, den Umfang und Inhalt der gespeicherten personenbezogenen Daten zu beurteilen.**
2. **Er erstreckt sich daher nicht auf sämtliche internen Vorgänge des Verantwortlichen, wie z.B. Vermerke, oder darauf, dass sämtlicher gewechselter Schriftverkehr, der dem Betroffenen bereits bekannt ist, erneut ausgedruckt und übersendet werden muss.**
3. **Rechtliche Bewertungen oder Analysen einer Versicherung stellen insofern ebenfalls keine personenbezogenen Daten in diesem Sinne dar**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Gemäß Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein umfassender Anspruch auf Auskunft über verarbeitete sie betreffende personenbezogene Daten sowie weitere Informationen zu. Die Information muss u.a. auch die Verarbeitungszwecke (Ziffer a)), die Empfänger von Daten (Ziffer b)) und die geplante Dauer der Speicherung (Ziffer c)) enthalten. Gemäß Art. 4 Nr. 1 DS-GVO sind „personenbezogene Daten" in diesem Sinne alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Eine „Verarbeitung von Daten" stellt gemäß Art. 4 Nr. 2 DS-GVO jeder Vorgang im Zusammenhang mit personenbezogenen Daten dar. Insofern ergibt sich ein umfassendes Auskunftsrecht bezogen auf die gespeicherten bzw. verarbeiteten personenbezogenen Daten. Dies beinhaltet Daten wie Namen oder Geburtsdatum genauso wie jegliche Merkmale, die die Identifizierbarkeit einer Person ermöglichen können, z.B. Gesundheitsdaten, Kontonummer usw. Nach diesen Grundsätzen und auf Grundlage der Erwägungsgründe stellen ärztliche Unterlagen, Gutachten oder sonstige vergleichbare Mitteilungen anderer Quellen ebenfalls „personenbezogene Daten" dar.

Nach der Auffassung der Kammer bezieht sich der Auskunftsanspruch aber nicht auf sämtliche internen Vorgänge der Beklagten, wie z.B. Vermerke, oder darauf, dass die betreffende Person sämtlichen gewechselten Schriftverkehr, der dem Betroffenen bereits bekannt ist, erneut ausgedruckt und übersendet erhalten kann (so das OLG Köln zu § 34 BDSG a.F., Beschluss vom 26.07.2018, 9 W 15/18). Rechtliche Bewertungen oder Analysen stellen insofern ebenfalls keine personenbezogenen Daten in diesem Sinne dar. Der Anspruch aus Art. 15 DS-GVO dient nicht der vereinfachten Buchführung des Betroffenen, sondern soll sicherstellen, dass der Betroffene den Umfang und Inhalt der gespeicherten personenbezogenen Daten beurteilen kann. Folgerichtig bestimmt Art. 15 Abs. 3 DS-GVO, dass der Betroffene eine Kopie (lediglich) der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, erhält.

Vorliegend hat die Beklagte verschiedene Auskünfte und Informationen erteilt (u.a. Bl. 164 ff. d.A. = Anlage K 10; Bl. 234 d.A. = Anlage B 4, Bl. 359 ff. d.A. = SS vom 20.12.2018 nebst Anlage B 5) und angegeben, dass weitere personenbezogene Daten über die Klägerin nicht gespeichert seien bzw. verarbeitet wurden. Substantiierter Vortrag der Klägerin, welche Informationen seitens der Beklagten darüber hinaus noch verarbeitet worden seien könnten, ist nicht erfolgt. Insofern sind konkrete Anhaltspunkte, dass die Auskunft – nach Maßgabe der Rechtsauffassung der Kammer – unvollständig ist, nicht vorhanden. Aus den Auskünften der Beklagten ergeben sich vielmehr die personenbezogenen Daten sowie die sonstigen Informationen i.S.v. Art. 15 Abs. 1a)-h) wie Gruppen von personenbezogenen Daten, Erfassung der Daten, Speicherdauer usw..

Schwärzung von Drittkonten in der Auskunft des Bundeszentralamts für Steuern durch den Gerichtsvollzieher

(**Landgericht Rostock**, Beschluss vom 7. Mai 2019 – 3 T 66/19 (3) –)

Eine Schwärzung oder Löschung von Auskünften des Bundeszentralamts für Steuern durch den Gerichtsvollzieher über Konten, über die der Schuldner lediglich verfügungsbefugt ist, ist grundsätzlich nicht zulässig.

Sachverhalt:

Die Gläubiger betreiben die Zwangsvollstreckung aus einem Vollstreckungsbescheid. Unter dem 06.11.2017 erteilten die Gläubiger einen kombinierten Sachpfändungsauftrag an die zuständige Verteilerstelle für Gerichtsvollzieher. Da der zuständige Gerichtsvollzieher den Schuldner in seiner Wohnung nicht antraf, bestimmte er auftragsgemäß einen Termin zur Abgabe einer Vermögensauskunft. Der Pflicht zur Abgabe einer Vermögensauskunft kam der Schuldner jedoch nicht nach. Die Gläubiger beauftragten daraufhin den zuständigen Gerichtsvollzieher, eine Drittauskunft nach § 802l Abs. 1 Ziffer 2 ZPO beim Bundeszentralamt für Steuern einzuholen. Der Gerichtsvollzieher leitete die Auskunft des Bundesamtes für Steuern über den Schuldner an die Gläubiger weiter, schwärzte aber die Namen der Kontoinhaber zu bestehenden Konten, an denen der Schuldner lediglich verfügungsberechtigt ist, sodass diese Namen unkenntlich sind.

Hiergegen wendete sich der Gläubiger. Das Vollstreckungsgericht wies die Erinnerung mit Beschluss vom 13.02.2019 – Az.: ... – zurück. Gegen den am 18.02.2019 zugestellten Beschluss wenden sich die Gläubiger mit ihrer am 04.03.2019 eingelegten sofortigen Beschwerde. Das Vollstreckungsgericht hat dem Rechtsmittel nicht abgeholfen und dem Beschwerdegericht zur Entscheidung vorgelegt.

Aus den Gründen:

Die gemäß §§ 567 Abs. 1 Nr. 1, 793 ZPO statthafte sowie form- und fristgerecht eingelegte sofortige Beschwerde gegen die Entscheidung des Vollstreckungsgerichts vom 13.02.2019 ist in der Sache begründet. Sie führt zur Änderung der Entscheidung des Vollstreckungsgerichts dahin, dass auf die Vollstreckungserinnerung der Gläubiger nach § 766 ZPO der zuständige Obergerichtsvollzieher angewiesen wird, die erhaltene Auskunft des Bundesamtes für Steuern über die Namen der Inhaber von Konten, für die der Schuldner eine Verfügungsberechtigung hat, ohne Schwärzungen, Löschungen oder Sperrungen durch den Gerichtsvollzieher mitzuteilen.

Gemäß § 802l Abs. 1 Nr. 2 ZPO darf der Gerichtsvollzieher das Bundeszentralamt für Steuern ersuchen, bei den Kreditinstituten die in § 93b Abs. 1 AO bezeichneten Daten abzurufen (§ 93 Abs. 8 AO), wenn der Schuldner seiner Pflicht zur Abgabe der Vermögensauskunft – wie hier – nicht nachkommt oder bei einer Vollstreckung in die dort aufgeführten Vermögensgegenstände eine vollständige Befriedigung des Gläubigers voraussichtlich nicht zu erwarten ist. Gemäß § 802l Abs. 1 S. 2 ZPO ist dies nur zulässig, soweit dies zur Vollstreckung erforderlich ist. Daten, die für die Zwecke der Vollstreckung nicht erforderlich sind, hat der Gerichtsvollzieher nach § 802l Abs. 2 ZPO unverzüglich zu löschen oder zu sperren.

Es entspricht dem Anwendungsbereich des § 802l Abs. 1 Nr. 2, Abs. 2 ZPO, die vom Bundeszentralamt für Steuern in eigener Verantwortung nach § 93 Abs. 8 AO an den Gerichtsvollzieher übermittelten Auskünfte ohne Löschungen oder Sperrungen der Daten über sogenannte Drittkonten, über die der Schuldner lediglich verfü-

gungsbefugt ist, einschließlich der Namen dieser Kontoinhaber, an die Gläubiger weiter zu leiten. Denn die Weitergabe der vollständigen Daten ist für die Zwecke der Vollstreckung erkennbar erforderlich und entspricht einer effektiven Zwangsvollstreckung. Erst die vollständigen Daten können für den Gläubiger wichtige Informationen darüber enthalten, ob der Schuldner gegebenenfalls eigene Vermögenswerte mit Hilfe anderen Personen, die als Kontoinhaber dem Schuldner eine Verfügungsbefugnis über ein Konto einräumen, der Zwangsvollstreckung entziehen will. Solche Konstruktionen, die die Verschleierung von Vermögenswerten bezwecken und die in verschiedenen Fallgestaltungen auftreten können, werden erst durch eine vollständige Weitergabe der Auskünfte des Bundeszentralamtes für den Gläubiger offenbar. Sie können einer Pfändung und Überweisung von Forderungen des Schuldners gegen den Dritten erst möglich machen.

Ein schützenswertes Interesse der Kontoinhaber, die dem Schuldner eine Verfügungsbefugnis über ein Konto einräumen, an der Nichtweitergabe ihrer Daten, ist nicht ersichtlich. Die beim Bundeszentralamt für Steuern nach § 93 Abs. 1 AO über sie verfügbaren Daten, können nach dieser Vorschrift ohnehin an die dort genannten Verwaltungen und Behörden weiter gegeben werden. Für die Vollstreckung von privaten Gläubigern kann kein anderer Maßstab gelten, denn insoweit besteht kein Unterschied in der Wertigkeit der dort genannten Behörden und sonstigen Gläubigern.

Die genannten Kontoinhaber tragen ferner ebenso wie sonstige Drittschuldner grundsätzlich das allgemeine Risiko, von Vollstreckungsmaßnahmen gegen einen Schuldner, mit dem sie in Rechtsbeziehung stehen, mittelbar betroffenen zu werden. Der Schutzbereich des Rechtes auf informationelle Selbstbestimmung ist in entsprechenden Fällen nicht betroffen.

Zu den Grenzen des Akteneinsichtsrechts eines Ratsmitglieds (Ls)

(**Verwaltungsgericht Düsseldorf**, Urteil vom 3. Mai 2019, – 1 K 3063/18 –)

1. **Das Akteneinsichtsrecht aus § 55 Abs. 5 Satz 1 GO NRW, nach dem jedem Ratsmitglied vom Bürgermeister auf Verlangen Akteneinsicht zu gewähren ist, soweit die Akten der Vorbereitung oder der Kontrolle von Beschlüssen des Rates dient, umfasst nicht die allgemeine Rechtmäßigkeitskontrolle von bereits gefassten Ratsbeschlüssen, für welche dem einzelnen Ratsmitglied auch sonst keine eigenen organschaftlichen Rechte in der Gemeindeordnung eingeräumt sind.**

2. **Das Auskunftsrecht aus § 55 Abs. 1 Satz 2 GO NRW gegenüber dem Bürgermeister wird durch grundrechtlich geschützte Positionen privater Dritter begrenzt. Bestehen solche Belange, hat der Bürgermeister nach pflichtgemäßen Ermessen zu entscheiden, ob er die begehrte Auskunft erteilt oder nicht. Der pauschale Verweis auf datenschutzrechtliche Vorschriften genügt dem nicht.**

Rechtsschutz gegen eine Beanstandung des Landesbeauftragten für Informationsfreiheit (Ls)

(**Verwaltungsgericht Stuttgart**, Urteil vom 21. Februar 2019 – 14 K 17293/17 –)

1. **Die Beanstandung des Landesbeauftragten für die Informationsfreiheit ist einer gerichtlichen Überprüfung weder im Rahmen einer Anfechtungsklage noch einer Feststellungsklage zugänglich. Rechtsschutz gegen eine Beanstandung auf Grundlage des LIFG ist für informationspflichtige Stellen grundsätzlich nicht möglich, da einer Beanstandung nach dem LIFG eine materielle Rechtswirkung nicht zukommt.**

2. **Die Beanstandung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit stellt mangels Regelungswirkung keinen Verwaltungsakt i.S.d. § 35 Landesverwaltungsverfahrensgesetz (LVwVfG) dar.**

3. **Es handelt sich bei der Wahrnehmung der Aufgaben nach dem LIFG nicht um eine Angelegenheit der kommunalen Selbstverwaltung, sondern um staatliche Aufgaben, also um Verwaltungsaufgaben zur Erfüllung nach Weisung.**

Datenschutzrechtliche Zulässigkeit eines Ortungssystems im Beschäftigungskontext (Ls)

(**Verwaltungsgericht Lüneburg**, Teilurteil vom 19. März 2019 – 4 A 12/19 –)

1. **Die GPS-Überwachung der Firmenfahrzeuge der Objektbetreuer, Reinigungskräfte und der Hausmeister einer Reinigungsfirma ist nicht nach § 26 Abs. 1 S. 1 Halbsatz 1 BDSG erforderlich, weil sie für die genannten Zwecke ungeeignet ist.**

a) **Kein Anlass zur pauschalen Überwachung von Wochenendfahrverboten oder eines Verbots von Privatfahrten besteht, wenn Privatfahrten geduldet werden. Zudem genügt anderenfalls die Anweisung, etwa Fahrzeugschlüssel am Firmensitz abzugeben, und/oder die Auflage, Fahrtenbücher zu führen.**

b) **Soweit während wie auch außerhalb der Arbeitszeiten anfallende Daten über das Ortungssystem zu dem Zweck erhoben und gespeichert werden, um Diebstähle zu verhindern bzw. womöglich entwendete Firmenfahrzeuge wieder aufzufinden, ist dies nicht erforderlich da für das Wiederauffinden womöglich entwendeter Firmenfahrzeuge die anlassbezogene Erhebung im Falle eines festgestellten Fahrzeugverlustes ausreicht.**

c) Die Speicherung der Arbeitszeiten kann auch nicht mit der Planung von Touren und der Koordination des Mitarbeiter- und Fahrzeugeinsatzes begründet werden. Die Tourenplanung ist zukunftsorientiert. Informationen über aktuelle und vergangene Standorte der Firmenfahrzeuge sind planungsunerheblich. Für eine womöglich außerplanmäßig (z.B. infolge von Krankheitsausfällen, Staus, Unfällen) akut werdende zentrale Koordination von Mitarbeitern und Fahrzeugen würde die Erreichbarkeit von Mitarbeitern per Mobiltelefon genügen.

d) Zum Nachweis für geleistete Tätigkeiten gegenüber Auftraggebern ist die Speicherung nicht erforderlich, da ein Nachweis über Tätigkeiten am/im Objekt eines Kunden mittels Ortungsdaten nicht geführt werden kann. Über diese Daten könnte allenfalls nachgewiesen werden, dass ein bestimmtes Firmenfahrzeug am Objekt bzw. in dessen Nähe für einen bestimmten Zeitraum anwesend gewesen ist. Somit ist die Erfassung solcher Daten zur Erreichung des Zwecks völlig ungeeignet.

2. Im Rahmen von § 26 Abs. 1 S. 1 BDSG ist darüber hinaus zweifelhaft, ob es insoweit nicht außerdem schon am Bezugspunkt zur Durchführung eines Beschäftigungsverhältnisses mangelt, denn es werden Nachweispflichten des datenverarbeitenden Arbeitgebers gegenüber seinem Kunden als Vertragspartner zum Bezugspunkt gemacht, die mit den Pflichten/Rechten aus dem Beschäftigungsverhältnis nichts zu tun haben. Aber aucht wenn man hier aber auf die allgemeinen Erlaubnistatbestände aus Art. 6 UAbs. 1 c) oder f) DS-GVO zurückgriffe, mangelte es aus den zuvor ausgeführten Gründen an der Erforderlichkeit der Datenverarbeitung.

(Nicht amtliche Leitsätze)

DS-GVO-Vorlagefragen an den EuGH (Ls)

(**Verwaltungsgericht Wiesbaden,** Beschluss v. 28. März 2019 – C-272/19 –)

1. Findet die 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 – DSGVO) – hier Art. 15 DSGVO, Auskunftsrecht der betroffenen Person – auf den für die Bearbeitung von Eingaben von Bürgern zuständigen Ausschuss eines Parlaments eines Gliedstaates eines Mitgliedstaates – hier den Petitionsausschuss des Hessischen Landtages - Anwendung und ist dieser insoweit wie eine Behörde i.S.v. Art. 4 Nr. 7 DSGVO zu behandeln?

2. Handelt es sich bei dem vorlegenden Gericht um ein unabhängiges und unparteiisches Gericht im Sinne von Art. 267 AEUV i.V.m. Art. 47 Abs. 2 CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (GrCH)

(Nicht amtliche Leitsätze)

Zimmer in einer Gemeinschaftsunterkunft ist als Wohnung zu betrachten (Ls)

(**Verwaltungsgericht Hamburg, 9. Kammer,** Urteil vom 15. Februar 2019 – 9 K 1669/18 –)

1. Die beiden Zimmer der Kläger in einer Gemeinschaftsunterkunft nach § 53 AsylG sind als Wohnung im Sinne von § 23 HmbVwVG und Art. 13 Abs. 1 GG zu qualifizieren.

2. Wenn Vollstreckungspersonen eine Wohnung öffnen und betreten, um darin bestimmte Personen aufzufinden und zu ergreifen, handelt es sich um eine Durchsuchung, die bei fehlender richterlicher Anordnung nur bei Gefahr im Verzuge zulässig ist.

(Nicht amtliche Leitsätze)

Bekanntgabe der Benotung einer Pflicht-Modulprüfung eines Bachelorstudiengangs im online-Portal der Hochschule (Ls)

(**Verwaltungsgericht Hamburg**, Urteil vom 18. Dezember 2018 – 2 K 1233/18 –)

1. Die in einem Online-Portal der Hochschule gegenüber dem/der Studierenden bekannt gegebene Benotung einer Pflicht-Modulprüfung eines Bachelorstudiengangs mit „nicht bestanden" stellt einen wirksam bekannt gegebenen Verwaltungsakt dar.

2. Die nach §§ 43 Abs. 1, 41 HmbVwVfG erforderliche Bekanntgabe des Verwaltungsakts, d.h. der Bewertung einer Modulprüfung mit „nicht bestanden", kann zulässigerweise auch über das Onlineportal einer Hochschule erfolgen, wenn dies der normativ geregelte bzw. übliche Weg der Kommunikation zwischen der Hochschule und den Studierenden ist (vgl. ausführlich zu einer ähnlichen Konstellation OVG Münster, Urt. v. 21.3.2017, a.a.O., juris Rn. 45 ff.).

(Nicht amtliche Leitsätze)

Die neue Datenschutz-Grundverordnung für Mitarbeiter

Informieren - Sensibilisieren - Dokumentieren

Die bewährte Mitarbeiterinformation Datenschutz liegt jetzt in neuer aktualisierter Fassung vor. Sie ist auf das neue Datenschutzrecht (DS-GVO und BDSG 2018) ausgerichtet und wurde grafisch neu gestaltet.

Mit dieser Mitarbeiterinformation können Sie alle Ihre Mitarbeiterinnen und Mitarbeiter zu den Grundlagen des Datenschutzes informieren und für dessen Bedeutung und Notwendigkeit sensibilisieren.

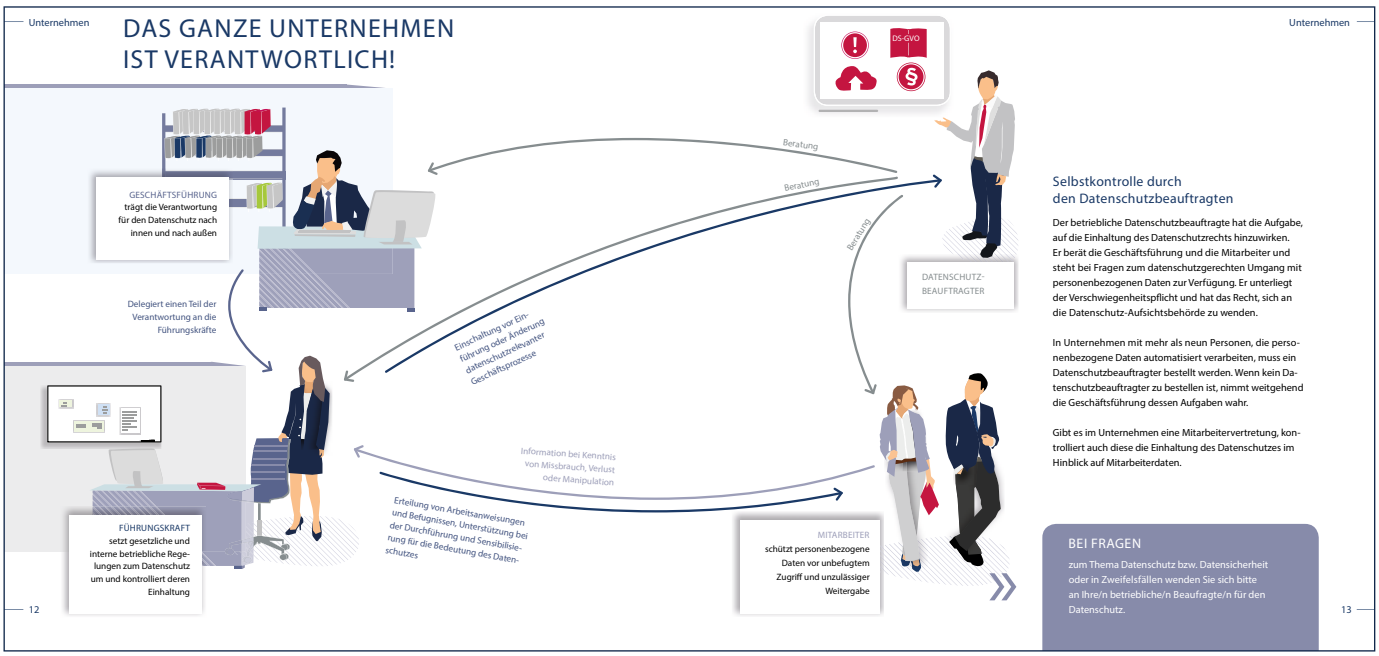
GDD e.V.
Mitarbeiterinformation Datenschutz

Merkblatt für Mitarbeiterinnen und Mitarbeiter
zu DS-GVO und BDSG
28. Auflage 2018 - Broschüre - 21 x 21 cm
ISBN 978-3-89577-790-5
20 Seiten, Staffelpreise

„So informieren Sie Ihre Mitarbeiter einfach und anschaulich zum neuen Datenschutzrecht!“

Judith Todd
Kundenbetreuung

Musterseite



Muster unter www.datakontext.com

DATAKONTEXT GmbH Tel. 02234/98949-30 Fax 02234/98949-32 www.datakontext.com bestellung@datakontext.com

Berichte, Informationen, Sonstiges

Bitkom: Mehrheit wünscht sich digitale Plattformen aus Deutschland

Ob bei der Suche nach einer neuen Wohnung, beim Online-Shopping, der Jobsuche oder beim Austausch mit Freunden in Sozialen Netzwerken – digitale Plattformen sind inzwischen in allen Lebensbereichen verbreitet. Und längst nutzen auch Industrieunternehmen solche Plattformen für Geschäftskunden, um dort Produkte, Dienstleistungen und Herstellungsprozesse zusammenzubringen. Eine große Mehrheit der Bundesbürger wünscht sich, dass dieser Markt nicht den großen Playern aus den USA oder China überlassen wird. Drei Viertel (73 Prozent) sagen, dass deutsche Unternehmen selbst zu Plattformanbietern werden sollten. Und sogar 9 von 10 (90 Prozent) sind der Meinung, dass die Politik den Aufbau deutscher und europäischer digitaler Plattformen stärker fördern sollte. Das ist das Ergebnis einer repräsentativen Befragung im Auftrag des Digitalverbands Bitkom. Gleichzeitig wünscht sich rund jeder Zweite (45 Prozent), dass digitale Plattformen stärker als bislang reguliert werden sollten. Allerdings gibt es dabei deutliche Unterschiede zwischen den Generationen. So sprechen sich jeweils 6 von 10 der Befragten zwischen 50- und 64 Jahre (60 Prozent) sowie ab 65 Jahre (58 Prozent) für mehr Regulierung aus, aber nur eine Minderheit und gerade einmal halb so viele in der Altersgruppe 30 bis 49 Jahre (33 Prozent) und 16 bis 29 Jahre (29 Prozent). „Deutschland muss vom Nachzügler zu einem Vorreiter der Plattformökonomie werden", sagt Bitkom-Präsident Achim Berg. „Es lohnt sich in der Diskussion über die Plattformökonomie einmal mehr, auf die junge Generation zu hören. Wir müssen weg von einer Verhinderungs- und Verbotsdebatte hin zu einer smarten Regulierung, die Innovationen ermöglicht und unterstützt. Regulierung gehört zur traditionellen deutschen und europäischen Wirtschaftspolitik, eine smarte Regulierung gehört zur digitalen Welt. Diese Regulierung muss die Wettbewerbsfähigkeit und den Markteintritt deutscher und europäischer Plattformanbieter unterstützen".

Neufassung der Orientierungshilfe „Selbstauskünfte für Mietinteressenten"

Infolge der Geltung der Datenschutz-Grund-verordnung und der Berücksichtigung neuerer Rechtsprechung wurde eine Überarbeitung der Orientierungshilfe der Aufsichtsbehörden zu „Selbstauskünfte für Mietinteressenten" erforderlich (Neufassung der Orientierungshilfe „Selbstauskünfte für Mietinteressenten"; www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuen). Vor der Vermietung von Wohnraum werden von den Mietinteressenten verschiedene personenbezogene Angaben erhoben, wobei nur solche Daten verarbeitet werden dürfen, für die der Vermieter berechtigte Interessen vorweisen kann oder sich eine Erforderlichkeit der Datenerhebung für die Durchführung des Mietvertrags ableiten lässt. Es kann zwischen drei Zeitpunkten differenziert werden, nämlich dem Besichtigungstermin, der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine bestimmte Wohnung anmieten zu wollen, und dem Stadium, in welchem die Entscheidung über den auszuwählenden Mietinteressenten fallen soll. Im Rahmen dieser drei Zeitpunkte kann die Erhebung bestimmter Angaben zulässig sein. Wesentliche Ergänzungen wurden in der Orientierungshilfe insbesondere im Rahmen des Stadiums vorgenommen, in welchem der Vermieter sich für einen Mietinteressenten entscheidet. Fragen zu Kontaktinformationen aktueller oder früherer Vermieter der Mietinteressenten sind zunächst mangels einer Erforderlichkeit zur Durchführung des Mietverhältnisses unzulässig. Erfragt werden dürfen aber Angaben zur Erfüllung mietvertraglicher Pflichten, sofern diese Aufschluss über die Zahlungsfähigkeit der Mietinteressenten geben. Solche Angaben können sich etwa auf die Zahlung der vereinbarten Miete und der Nebenkosten beziehen. Auch Fragen nach Pflichtverletzungen aus dem bisherigen Mietverhältnis über Wohnraum können zulässig sein, allerdings unter der Bedingung, dass die Pflichtverletzung eine Kündigung rechtfertigt und solche Pflichtverletzungen für die Zukunft zu erwarten sind. Die Kündigung muss u.a. rechtskräftig oder in tatsächlicher Hinsicht unbestritten sein. Bezüglich der Anforderung einer Selbstauskunft der Mietinteressenten ist zu berücksichtigen, dass diese nach der Rechtsprechung nicht verpflichtet sind, eine Mietschuldenfreiheitsbescheinigung zu erstellen. Daher kann eine solche Bescheinigung vom Mietinteressenten bei der beabsichtigten Neuanmietung von Wohnraum nicht verlangt werden. Zulässig wäre es hingegen, vom Mietinteressenten wahlweise entweder von Vorvermietern geschuldete Quittungen über empfangene Zahlungen oder geschwärzte Kontoauszüge und Mietverträge als Beleg zu geleisteten Mietzahlungen an Vorvermieter sowie zur Höhe des Mietzinses und damit zum Nachweis einer bestehenden Bonität zu erbitten. Bereits in der Erstfassung der Orientierungshilfe wurde erläutert, dass die Einholung von Einwilligungen der Mietinteressenten zur Erhebung von Angaben nicht das richtige Mittel für den Vermieter darstellt. Die Freiwilligkeit von Einwilligungserklärungen als zentrales Wirksamkeitskriterium hat mit Geltung der Datenschutz-Grundverordnung nochmals besonderes Gewicht erhalten. Demnach läge im Bereich der Anmietung von Wohnraum keine freiwillige und damit eine unwirksame Einwilligungs-

erklärung vor, wenn der Abschluss des Mietvertrags von der Einwilligung in die Erhebung nicht erforderlicher Angaben abhängig gemacht wird.

Neufassung des „Code of Conduct“der Versicherungswirtschaft

Im Jahre 2012 war die Versicherungswirtschaft in Deutschland die erste Branche, die zur Förderung der Beachtung datenschutzrechtlicher Regelungen durch den Berliner Beauftragten für den Datenschutz förmlich anerkannte Verhaltensregeln erlassen hat. Auf Grundlage einer in den Verhaltensregeln enthaltenen Klausel sollte bei jeder den Regelungsinhalt betreffenden Rechtsänderungund spätestens fünf Jahre nach Abschluss der Überprüfung der Verhaltensregeln durch die zuständige Datenschutzaufsichtsbehörde eine Evaluierung stattfinden. Infolge des Stichtags für die Geltung der Datenschutz-Grundverordnung, dem 25.05 2018, und dem Ablauf der Evaluierungsfrist im Jahre 2017 bestanden gleich zwei Gründe, eine Überarbeitung der Verhaltensregeln vorzunehmen. Die vorgenommene Aktualisierungen beurteilt die für die förmliche Anerkennung der Verhaltensregeln zuständige Berliner Beauftragte für den Datenschutz und die Informationsfreiheit als eine mit den Vorgaben der Datenschutz-Grundverordnung für die Versicherungswirtschaft branchenspezifische Konkretisierung. (abrufbar:www.gdv.de/resource/blob/23938/4aa2847df2940874559e51958a0bb350/download-code-of-conduct-data.pdf). Angepasst wurden etwa Regelungen zur Einwilligung und zum Umgang mit besonderen Datenkategorien wie Gesundheitsdaten, zu den Informationspflichten gegenüber betroffenen Personen, zur gemeinsamen Verantwortung von zwei oder mehreren Unternehmen, zu den Rechten betroffener Personen wie z.B. Auskunft, Berichtigung, Einschränkung der Verarbeitung und Datenübertragbarkeit, zur Datenschutz-Folgenabschätzung, zur Benennung von Datenschutzbeauftragten und zur Meldung.

Literaturhinweise

Fritz Schmidt/Harald Schweißguth/Jan Heiner Hoffmann/David Hummel, **Datenschutz in der Wohnungswirtschaft – inkl. Arbeitshilfen online;** Haufe-Verlag, 2018, 320 S., 49,95 €

Die neue Datenschutz-Grundverordnung (DS-GVO) hat erhebliche Auswirkungen auf Wohnungsunternehmen, die das vorliegende Buch im Einzelnen abhandelt. Es zeigt, in nachfolgenden Themen auf wie die Daten von Mitgliedern oder Mietern künftig rechtskonform zu verarbeiteiten sind:

- Grundzüge- und Prinzipien des Datenschutzes
- Überblick über die Änderungen durch die DS-GVO
- Dokumentationspflichten
- Informationspflichten
- Datenschutzbeauftragte
- Datenschutz in einzelnen Geschäftsprozessen von Wohnungsunternehmen
- Auskunftspflichten gegenüber Betroffenen
- Einzuhaltende technisch-organisatorische Maßnahmen und Löschungskonz

(Redaktion)

Christian Weiß/Nico Reisener, **Datenschutz in der Insolvenzkanzlei,** ZIP-Praxisbuch 13, RWS Verlag, Köln, 2019, Brosch. 322 S., 68,– €

Der Datenschutz hat in Insolvenzkanzleien einen besonderen Stellenwert und spielt eine immer wichtigere Rolle: Daten sind aus den schuldnerischen Betrieben nicht mehr wegzudenken und stellen oftmals Vermögenswerte dar, die der Insolvenzverwalter zu verwerten hat. Viele insolvenzspezifische Aspekte des Datenschutzes sind im Zuge der DS-GVO nun in der Diskussion: z.B. die Frage, ob bzw. ab wann ein (vorläufiger) Insolvenzverwalter verantwortliche Stelle i.S.v. Art. 4 Nr. 7 DS-GVO sein kann, Überlegungen zur verschlüsselten Übersendung der Insolvenztabelle per E-Mail oder ob in Zukunft die datenschutzkonforme Abwicklung von Insolvenzverfahren für Gerichte ein Gradmesser für eine qualitätsbewusste Insolvenzverwaltung sein wird.

Das Werk greift diese Aspekte auf und stellt die Grundsätze des Datenschutzrechts in der Insolvenzkanzlei dar. Es erläutert den Datenschutz in der Kanzlei des Insolvenzverwalters, etwa im Antragsverfahren, im eröffneten Verfahren, bei der Betriebsfortführung oder bei Arbeitnehmer- und Kundendaten. Viele Beispiele vertiefen das Thema und helfen effizient dabei, offene Fragen aus der täglichen Praxis zu klären.

(Redaktion)

Norbert Pohlmann, **Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung,** Springer Verlag, Berlin, 1. Aufl. 2019, 488 S., 306 Abb., 34,99 €

Die Digitalisierung verändert Geschäftsmodelle, Verwaltungsprozesse und viele weitere Lebensbereiche radikal. Dadurch eröffnet der digitale Wandel auf der einen Seite viele neue und interessante Möglichkeiten. Auf der anderen Seite sorgen Hacker mit Cyber-Angriffen immer wieder für Aufsehen. Die fortschreitende Digitalisie-

rung bringt neben vielen Vorteilen auch weitere Gefahren. Für eine erfolgreiche Zukunft unserer Gesellschaft ist es daher entscheidend, eine sichere und vertrauenswürdige IT zu gestalten.

Prof. Dr. Norbert Pohlmann, IT-Sicherheitsexperte, Informatikprofessor und Leiter des renommierten Instituts für Internet-Sicherheit, gibt mit seinem Lehrbuch eine umfassende Einführung in den Themenkomplex der Cyber-Sicherheit. Erklärt werden Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen. Der Autor vermittelt aber nicht nur theoretisches Fachwissen, sondern befähigt den Leser, die Cyber-Sicherheit aus der anwendungsorientierten Perspektive und unter neuen Blickwinkel auf die relevanten Themen zu betrachten.

Eine Besonderheit des Buches ist die Breite der adressierten Zielgruppe: Nicht nur Lehrende können das Lehrbuch in die Unterrichtsgestaltung einfach einbinden, sondern auch Studierende festigen und erweitern damit ihr Wissen in allen Belangen der Cyber-Sicherheit. Weiterhin holt es auch Arbeitnehmer der IT-Branche dort ab, wo ergänzende und unterstützende Informationen von Belang sind. Auch IT-Affine ohne Security Background finden in dem Lehrbuch zahlreiche Anwendungsbeispiele und Lösungen für Problemstellungen, die eine schnell voranschreitende Digitalisierung mit sich bringt.

Im einführenden Abschnitt des Lehrbuchs vermittelt Autor Pohlmann zunächst die Grundlagen der Cyber-Sicherheit und schärft den Blick des Lesenden für folgende Aspekte: Strategien, Motivationen, Bedürfnisse, Probleme, Herausforderungen, Wirksamkeitskonzepte der IT-Sicherheit.

In den darauffolgenden Kapiteln wird das Wissen dezidierter und beleuchtet Kryptografie, Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen, Digitale Signatur, elektronische Zertifikate sowie PKIs und PKAs, Identifikation und Authentifikation, Enterprise Identity und Access Management, Trusted Computing, Cyber-Sicherheit Frühwarn- und Lagebildsysteme, Firewall-Systeme, E-Mail-Sicherheit, Blockchain-Technologie, Künstliche Intelligenz und Cyber-Security sowie Social Web Cyber-Sicherheit.

Thematisiert werden außerdem IPSec-Verschlüsselung, Transport Layer Security (TLS)/Secure Socket Layer (SSL) sowie Sicherheitsmaßnahmen gegen DDoS-Angriffe. Anschauliche Grafiken und Tabellen bilden Prozesse und Zusammenhänge verständlich ab. Didaktisch gut aufbereitet, können die Inhalte mit zahlreichen Übungsaufgaben vertieft werden.

(Schriftleitung)

Johannes Knaut, **Die Bedeutung des Datenschutzrechts bei Beweisverboten in Zivil- und Arbeitsgerichtsbarkeit** – eine Darstellung anhand der Rechtsprechung zu „Dash-Cams", Verlag Dr. Kovać, Beiträge zu Datenschutz und Informationsfreiheit, Band 25, Hamburg 2019, 280 S. 89,90 €

In den letzten Jahren ist verstärkt diskutiert worden, inwieweit Zivil- und Arbeitsgerichte rechtswidrig erlangte Beweismittel zur Grundlage ihrer Entscheidung machen dürfen. Besonders umstritten ist dabei die Fallgruppe der Dash-Cams gewesen – kleine Kameras im Inneren von Fahrzeugen, die laufend ihre Umgebung filmen, um Beweismaterial für etwaige Unfälle zu sammeln.

Der Verfasser beleuchtet die Diskussion hierzu und ordnet die seiner Ansicht nach überzeugende Grundsatzentscheidung des Bundesgerichtshofs aus dem Jahr 2018 ein, der zufolge der Einsatz von Dash-Cams der datenschutzrechtlichen Rechtfertigung bedarf. Eine solche Rechtfertigung soll nur möglich sein, wenn die Dash-Cam in technischer Hinsicht datenschutzfreundlich konfiguriert ist.

Hiervon ausgehend gibt der Verfasser einen Überblick über die in Literatur und Rechtsprechung vertretenen Auffassungen zum Umgang mit rechtswidrig erlangten Dash-Cam-Aufnahmen und Beweismitteln allgemein. Anhand der Dash-Cam-Rechtsprechung kritisiert er die von der herrschenden Meinung angewandte „Abwägungslösung", wonach in ZPO und ArbGG kein Beweisverwertungsverbot zu finden sein und die Verwertbarkeit daher von einer Abwägung der grundgesetzlich geschützten Parteiinteressen abhängen soll.

In der Studie wird eine datenschutzrechtliche Lösung der Problematik entwickelt. Diese basiert auf der Annahme des Verfassers, die Verwertung eines rechtswidrig erlangten Beweismittels unterfalle regelmäßig dem Datenschutzrecht. Sie müsse sich deswegen mittels der datenschutzrechtlichen Normen rechtfertigen lassen. Sowohl für die Rechtslage vor Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) als auch für danach untersucht der Autor, ob das Datenschutzrecht hier allgemein gültige Lösungen bereithält.

(Redaktion)

Lutz Bergmann/Roland Möhrle/Armin Herb, **Datenschutzrecht: Bundesdatenschutzgesetz – Europäische Datenschutz-Grundverordnung – Datenschutzgesetze der Länder – Bereichsspezifischer Datenschutz,** Kommentar, Stuttgart, Verlag Boorberg, Loseblattwerk mit 54. Aktualisierung 2018, 3760 S., mit CD-ROM. In 3 Ordnern, 96,00 €

Nach dem Tode von Bergmann setzen Möhrle/Herb die Arbeit an der vor 40 Jahren begründeten Kommentierung schrittweise fort. Die letzte Lieferung erfolgte im Februar 2019. Wenn auch noch größere Teile des neuen Rechts unkommentiert sind, ist insbesondere hinzuweisen auf die Schemata und Checklisten zur EU-DSGVO-Kommentierung (z.B. zu Datenpannen nach Art. 33; Benachrichtigungen nach Art. 34; Joint-Controller-Vereinbarungen nach Art. 26; Verpflichtung auf die Vertraulichkeit) und die ausführlichen Erläuterungen des Beschäftigtendatenschutzes (Art. 88 DSGVO und § 26 BDSG).

(Redaktion)

Neuerscheinungen

Aufsätze

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

Boehme-Neßler, Volker, **Gläserne Prostituierte? Das ProstSchG und der Datenschutz,** DuD 2019, S. 342
Mit dem Prostituiertenschutzgesetz des Jahres 2017 wollte der Gesetzgeber verstärkt gegen Zwangsprostitution vorgehen, wobei jedoch nach Ansicht des Verfassers manche Regelungen mit der DS-GVO und der Grundrechte-Charta der EU unvereinbar sind.

Fuhlrott. Michael, **Data Incident Management: Rechtlicher Umgang mit „Datenpannen",** NZA 2019, S. 649
Der Beitrag widmet sich den notwendigen unternehmensseitigen (arbeits)rechtlichen Schritten nach Bekanntwerden einer sog. „Datenpanne", wobei die Einschaltung des Datenschutzbeauftragten, obwohl nicht ausdrücklich gesetzlich vorgesehen, als „praktisch nahezu unumgänglich" empfohlen wird.

Indenhuck, Moritz/Britz, Thomas, **Vom Datenschutzrecht zum Datenschuldrecht. Neue Leitlinien zur Verarbeitung personenbezogener Daten bei Online-Dienstleistungen,** BB 2019, S. 1091
Neue Leitlinien des european data protection boards zur Datenverarbeitungen bei Onlinedienstleistungen sehen eine autonome datenschutzrechtliche Inhaltskontrolle von Verträgen vor, die nach der Befürchtung der Autoren zu einem datenschutzrechtlichen „Schattenvertragsrecht" außerhalb der klassischen Grundsätze des Privatrechts führen könnte.

Kühling, Jürgen/Sackmann, Florian, **Die Musterfeststellungsklage nach Datenschutzverstößen – ein unkalkulierbares Risiko für Unternehmen?** DuD 2019, S. 347
Die neue Möglichkeit der Musterfeststellungsklage bietet im Zusammenspiel mit dem materiellen Datenschutzrecht erhebliche Chancen für Verbraucher und spiegelbildlich erhebliche Herausforderungen in der Datenschutzpraxis auf Unternehmensseite.

Lücke, Oliver, **Die Betriebsverfassung in Zeiten der DS-GVO,** NZA 2019, S. 658
Dargestellt wird das Verhältnis von Betriebsverfassungs- und Datenschutzrecht, insbesondere mit der datenschutzrechtlichen Stellung des Betriebsrats, der Rolle des Datenschutzbeauftragten im Hinblick auf den Betriebsrat und den Datenverarbeitungen des Betriebsrats. Die als Untertitel des Aufsatzes gestellte Frage nach dem „Bermuda-Dreieck" zwischen Arbeitgeber, Betriebsräten und Datenschutzbeauftragten versucht der Autor aufzulösen, indem er einerseits an der Rolle des Betriebsrats als Teil der verantwortlichen Stelle festhält, andererseits dem Datenschutzbeauftragen ein Kontrollrecht zugesteht.

Meinhold, Stefan, **Stellung des Personalrats als Verantwortlicher nach der DS-GVO,** NZA2019, S. 670
Erörtert werden die Konsequenzen aus der Entscheidung des thüringischen Gesetzgebers, den Personalrat als „Verantwortlichen" zur Bestellung eines eigenen Datenschutzbeauftragten zu verpflichten (§ 80 I 2. HS 1 ThürPersVG) und Pflichten eines Verantwortlichen gegenüber den Beschäftigten aus der DS-GVO zu erfüllen.

Schnebbe, Maximilian, **DSB-Bestellpflicht und Datenschutzfolgeabschätzung,** DuD 2019, S. 373
Der Autor zeigt an einem Beispiel auf, wann Unternehmen, auch wenn sie weniger als 10 Personen bei der Verarbeitung personenbezogener Daten beschäftigten, einen Datenschutzbeauftragten bestellen müssen, weil – was oft unklar ist – sie ihre Verarbeitungen einer Datenschutzfolgenabschätzung unterziehen müssen.

Stück, Volker, **Betriebsrat oder Geheimrat? Beschäftigtendatenschutz beim Betriebsrat,** ZD 2019, S. 256
Verneint wird u.a. die Rolle des Betriebsrats als eigener Verantwortlicher und dann konsequenterweise seine Kontrolle durch den betrieblichen Datenschutzbeauftragten bejaht.

Ulber, Daniel, **Arbeitszeiterfassung als Pflicht des Arbeitgebers,** NZA 2019, S. 677
Der Autor erörtert die Entscheidung des EuGH vom 14.05.2019 – C- 55/18, die jeden Arbeitgeber zur Erfassung der Arbeitszeit der Beschäftigten als verpflichtet ansieht, positiv dahingehend, dass der EuGH Arbeitnehmerrechten damit zur praktischen Wirklichkeit verhelfe.

Der intelligente Einkaufswagen

Preise müssen nicht gleich sein

Wer beim Gebrauchtwagenhändler ein Auto kauft, der möchte einen guten Preis bekommen. Vielleicht legt er für die Preisverhandlung seine teure Uhr ab, zieht einen alten Anzug an, und der Verkäufer taxiert auf dieser Basis den hoffentlich günstigen Kaufpreis. Kauft man einen Gebrauchtwagen im Internet, helfen solche Tricks nicht. Hier kann der Preis am Verhalten des Interessenten gemessen werden. Wer über ein teures Endgerät bestellt, im Onlinekaufhaus häufig ohne Preisvergleich und langes Überlegen kauft, der wird einen höheren Preis akzeptieren als ein Sparfuchs. Algorithmen werten zahlreiche Parameter aus. Sie können Zahlungsbereitschaft und oft auch Zahlungsfähigkeit präzise voraussagen und ein entsprechendes Angebot machen. Solche Prüfungen sind nicht grundsätzlich verboten. In der Regel lässt die Vertragsfreiheit individuelle Preise zu, und jeder kann selbst entscheiden, wo die Grenze liegt. Ein ungutes Gefühl bleibt dennoch: zum einen, weil man anders als beim Gebrauchtwagenkauf nichts davon bemerkt, dass man anders behandelt wird. Transparenz ist eine Frage der Fairness. Zudem muss es dort Grenzen geben, wo der Verkäufer eine Notlage ausnutzt, etwa weil er weiß, dass der Kunde krank ist und deshalb ein überteuertes Medikament kauft. Wenn der Algorithmus aber eine Zahlung per Kreditkarte ablehnt, weil er erkennt, dass die Karte nicht gedeckt ist, differenziert er aus nachvollziehbaren Gründen.

Digital Shift

AKARION
Innovating Trust

Die Konferenz für Compliance und neue Technologien

-25%

auf den Ticketpreis, **Code „RDV2019"** auf der Website eingeben und Rabatt sichern!

25. Sept. 2019
München

www.digitalshift.xyz

Einführung in den Datenschutz

Mitarbeiter schulen via E-Learning.

- ✓ Moderation in TV-Studioqualität
- ✓ Rechtssicher gemäß DS-GVO
- ✓ von einem Experten entwickelt
- ✓ Dauer: 45 Minuten
- ✓ animierte Schaubilder und Grafiken
- ✓ interaktive Quizfolgen
- ✓ Abschlusszertifikat
- ✓ auch in englischer Sprache verfügbar

Sehen Sie sich jetzt unseren Trailer an:
www.datakontext.com/eLearning

DATAKONTEXT