19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 31. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 10. Dezember 2018, 11:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf 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. DSAnpUG-EU)

BT-Drucksache 19/4674

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss Digitale Agenda

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Marc Henrichmann [CDU/CSU]
Abg. Saskia Esken [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Ulla Jelpke [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

19. Wahlperiode

Deutscher Bundestag

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		CDU/CSU	
Amthor, Philipp		Berghegger Dr., André	
Bernstiel, Christoph		Gnodtke, Eckhard	
Brand (Fulda), Michael		Gröhler, Klaus-Dieter	
Henrichmann, Marc		Hauer, Matthias	
Irmer, Hans-Jürgen		Heil, Mechthild	
Kuffer, Michael		Heveling, Ansgar	
Lindholz, Andrea		Hoffmann, Alexander	
Middelberg Dr., Mathias		Launert Dr., Silke	
Müller, Axel		Luczak Dr., Jan-Marco	
Nicolaisen, Petra		Pantel, Sylvia	
Oster, Josef		Schimke, Jana	
Schuster (Weil am Rhein), Armin		Sensburg Dr., Patrick	
Seif, Detlef		Ullrich Dr., Volker	
Throm, Alexander		Veith, Oswin	
Vries, Christoph de		Wellenreuther, Ingo	
Wendt, Marian			

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Castellucci Dr., Lars		Fechner Dr., Johannes	
Esken, Saskia		Gerster, Martin	
Grötsch, Uli		Högl Dr., Eva	
Hartmann, Sebastian		Juratovic, Josip	
Heinrich, Gabriela		Kolbe, Daniela	
Kaiser, Elisabeth		Lühmann, Kirsten	
Lindh, Helge		Poschmann, Sabine	
Lischka, Burkhard		Rix, Sönke	
Mittag, Susanne		Rüthrich, Susann	
Özdemir (Duisburg), Mahmut		Vöpel, Dirk	
		Kelber, Ulrich (AOA)	
AfD		**AfD**	
Baumann Dr., Bernd		Elsner von Gronow, Berengar	
Curio Dr., Gottfried		Harder-Kühnel, Mariana Iris	
Haug, Jochen		Hilse, Karsten	
Herrmann, Lars		Maier, Jens	
Hess, Martin		Reusch, Roman Johannes	
Wirth Dr., Christian		Storch, Beatrix von	

3. Dezember 2018

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 2 von 4

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
FDP		**FDP**	
Höferlin, Manuel		Beeck, Jens	
Kuhle, Konstantin		Ruppert Dr., Stefan	
Schulz, Jimmy		Strack-Zimmermann Dr., Marie-Agnes	
Strasser, Benjamin		Thomae, Stephan	
Teutsberg, Linda		Toncar Dr., Florian	
DIE LINKE.		**DIE LINKE.**	
Hahn Dr., André		Akbulut, Gökay	
Jelpke, Ulla		Dağdelen, Sevim	
Pau, Petra		Movassat, Niema	
Renner, Martina		Nastic, Zaklin	
BÜ90/GR		**BÜ90/GR**	
Amtsberg, Luise		Bayram, Canan	
Mihalic Dr., Irene		Brugger, Agnieszka	
Notz Dr., Konstantin von		Haßelmann, Britta	
Polat, Filiz		Lazar, Monika	

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Beratende Mitglieder (§57 Abs. 2 GOBT) des Ausschusses	Unterschrift
Fraktionslos	
Petry Dr., Frauke	

Tagungsbüro

Deutscher Bundestag

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
AFD		
FDP		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Bürczyk, Dirk	LINKE	
Widdish, Teresa	FDP	
Sparr, Jeannette	SPD	
Hollberg, Sebastian	FDP	
Leopold, Nils	Grüne	
Daniela Ordmann	AfD	
Julia Krings	SPD	
Fischer IKEA	Grüne	
Sinnokrot, Carmen	SPD	

Stand: 13. September 2018 / ZT4, Luisenstr. 32-34, Telefon: +49 30 227-32659
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Fraktionsmitarbeiter

Name (bitte in Druckschrift)	**Fraktion**	**Unterschrift**

Tagungsbüro

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Bundesrat

Land	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
Baden-Württemberg	Dr. R. Zeiser		RD
Bayern			
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern			
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz	Schindler		ORR'in
Saarland			
Sachsen	Kühne-Storch		RR'in
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen			

Tagungsbüro

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 10. Dezember 2018, 11:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
BMI	DR. WICHMANN		RD'n
BMI	Schotta		MinR
BMJ	Dr. Griesbeck		MDirig
BMI	v. Wiedtooh.		RD'n
BMI	A. Arno		Referendarin
BMJV	Cur. Fies		Referentin
BMJV	Deffaa		MR
WD ST	Welshop		gepr. RK
BK	DR PETSCH		RR'in
BMJV	Rosenow	Rosenow	RD

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 10. Dezember 2018, 11.00 Uhr
„Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU“

Stand: 29. November 2018

Professor Dr. Hartmut Aden
Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Kirsten Bock
Unabhängiges Landeszentrum für Datenschutz, Kiel

Dr. Stefan Brink
Landesbeauftragter für Datenschutz und Informationsfreiheit des
Landes Baden-Württemberg, Stuttgart

Dr. Malte Engeler
Richter beim Schleswig-Holsteinischen Verwaltungsgericht, Kiel

Jutta Gurkmann
Leiterin Geschäftsbereich Verbraucherpolitik
Verbraucherzentrale Bundesverband e.V., Berlin

Annette Karstedt-Meierrieks
Referatsleiterin Wirtschaftsverwaltungsrecht, Vergaberecht, Datenschutzrecht
Deutscher Industrie- und Handelskammertag, Berlin

Professor Dr. Helmut Köhler
Ludwig-Maximilians-Universität München

Professor Dr. Meinhard Schröder
Universität Passau

Sprechregister der Sachverständigen und Abgeordneten

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf 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. DSAnpUG-EU)

BT-Drucksache 19/4674

Vors. **Andrea Lindholz** (CDU/CSU): Mit Blick auf die Uhr würde ich vorschlagen, wir fangen an mit unserer öffentlichen Anhörung zum Thema Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz. Ich darf Sie alle ganz herzlich heute Morgen hier begrüßen. Besonders bedanken darf ich mich vorab bei den Damen und Herren Sachverständigen, die heute zu uns gekommen sind und den Kolleginnen und Kollegen sozusagen nochmals Rede und Antwort stehen. Wir haben auch schriftliche Berichte angefordert. Ich weiß aber, dass es aufgrund der Kürze der Zeit nicht immer Jedem auch möglich ist, entsprechend vorher einen schriftlichen Bericht einzureichen. Soweit sie schon eingegangen sind, darf ich mich auch an dieser Stelle dafür ganz herzlich bedanken. Begrüßen darf ich auch ganz herzlich die anwesenden Kolleginnen und Kollegen sowie die Zuhörer unserer Anhörung. Wir werden wie üblich von der Anhörung ein Wortprotokoll anfertigen, das auch zur Korrektur übersandt wird. Die Anhörung wird auch im Parlamentsfernsehen übertragen.

Wir werden zunächst jeden Sachverständigen bitten ein fünfminütiges Eingangsstatement abzugeben und sodann in die Fragerunden der Fraktionen eintreten. Bei den Fragerunden der Fraktionen bleibt es beim bisher vereinbarten Modus. Die Kolleginnen und Kollegen werden entweder eine gleiche Frage an zwei Sachverständige stellen oder zwei unterschiedliche Fragen an einen Sachverständigen. Wir haben uns auf die Beibehaltung dieses Modus auch im Ausschuss verständigt. Dadurch sind wir bisher auch immer zumindest auf zwei oder drei Fragerunden gekommen.

Wenn es dazu keine weiteren Fragen gibt, die sehe ich nicht, dann würde ich jetzt anfangen. Zunächst einmal würde ich dann dem Alphabet nach Herrn Prof. Dr. Aden bitten, sein Eingangsstatement zu halten.

SV **Prof. Dr. Hartmut Aden** (HWR, Berlin): Frau Vorsitzende, meine Damen und Herren, vielen Dank für die Einladung und die Gelegenheit, zu diesem sehr imposanten Gesetzentwurf Stellung zu nehmen. Alleine der Umfang ist ja durchaus beeindruckend. Ich verweise auf meine schriftliche Stellungnahme, die Ihnen zugegangen ist, und möchte hier einige wenige Punkte herausheben.

Zunächst einmal ist es aus meiner Sicht begrüßenswert, dass die Bundesregierung jetzt weitere Schritte unternimmt, die längst überfällige Umsetzung bzw. Anpassung, die erforderlich geworden ist aufgrund des EU-Datenschutzpaketes, durchzuführen. Insofern ist es ein Schritt in die richtige Richtung. Wenn man allerdings in die Details dieses sehr umfangreichen Gesetzentwurfes einsteigt, dann gibt es doch eine Reihe von Fragen, die hier kritisch zu erörtern sind. Zunächst einmal fällt auf, dass es einige Elemente gibt in diesem Gesetzentwurf, die mit der Umsetzung des EU-Datenschutzpaketes überhaupt gar nichts zu tun haben. Das heißt, es handelt sich faktisch um das, was man als Omnibus- oder Containergesetz bezeichnet. Es ist zwar verfassungsrechtlich grundsätzlich nicht ausgeschlossen so etwas zu machen, aber im Hinblick auf das Demokratieprinzip sollte das nicht gemacht werden für Inhalte, die mit zusätzlichen Grundrechtseingriffen verbunden sind. Hier sehe ich deswegen zwei Elemente in diesem Gesetzentwurf, die meines Erachtens von Ihnen besser in ein gesondertes Gesetzgebungsverfahren verschoben werden sollten. Nämlich zunächst die Änderungen des BDBOS-Gesetzes. Dort sind umfängliche zusätzliche Datenspeicherungen vorgesehen, die im Hinblick auf den Grundsatz der Verhältnismäßigkeit durchaus problematisch sind: 75 Tage im Hinblick auf die technische Sicherung des Systems und anderer Zwecke. Ich meine, dass gerade im Bereich des Digitalfunks heute auch privacy by design-Lösungen denkbar sein müssen – technische Konzepte also, die es vermeiden, Daten in diesem Umfang auf Vorrat zu speichern. Ich denke, da wären bessere Lösungen möglich als das, was wir jetzt in dem Entwurf haben.

Ähnliches gilt für das BSI-Gesetz. Grundsätzlich ist es sinnvoll, dass auch für den Bereich der IT-Sicherheit spezifischere Datenschutzregelungen geschaffen werden. Allerdings sind die Zweckbestimmungen in dem, was hier vorgeschlagen wird, sehr unbestimmt. Da ist einfach nur von Sammlung,

Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für Informationstechnik die Rede. Auch da sind meines Erachtens wesentlich präzisere, bessere Zielbestimmungen möglich. Und das hat mit der Umsetzung des EU-Datenschutzpakets nur am Rande zu tun, sodass es eigentlich in dieses Gesetz gar nicht hineingehört.

Es gibt dann auch eine Reihe von problematischen Einzelregelungen, hier und da auch handwerkliche Fehler, die sicherlich nicht ganz zu vermeiden sind, wenn ein Gesetzentwurf diese Umfänge annimmt. Ich beginne mit einem Bereich, der stets recht umstritten war, nämlich des Bundesmeldegesetzes. Dort gibt es bekanntlich sehr umfangreiche Datenübermittlungsvorschriften an öffentliche und private Stellen. Diese wurden hier und da nachgebessert im Hinblick auf die Terminologie. Auch die besonders problematische Vorschrift des § 44 Absatz 3, wo es um Datenübermittlung für Werbe- und Adresshandelszwecke an Private geht. Diese Regelungen sind inhaltlich weiterhin problematisch. Sie wurden zwar dem Wortlaut nach ein bisschen an die Anforderungen des Artikels 7 der Datenschutzgrundverordnung (DSGVO), nämlich die informierte Einwilligung, angepasst. Allerdings nicht in dem Maße, wie es eigentlich erforderlich wäre um sicherzustellen, dass die abgebende Behörde auch wirklich prüft, dass diese Daten aufgrund einer informierten Einwilligung abgegeben werden können. Da wären meines Erachtens wesentlich bessere prozedurale Vorschriften nötig, wenn man diese recht problematische Vorschrift bei der Gelegenheit nicht gleich ganz streichen möchte.

Ich habe in meiner schriftlichen Stellungnahme auch auf einige meines Erachtens eher handwerkliche Probleme im Zusammenhang mit dem Postgesetz hingewiesen. Da ist vermutlich an einer Stelle das Widerspruchsrecht nicht durch eine Einwilligungsregelung ersetzt worden für die Postfachinhaber. Da denke ich, sollte man auch im Rahmen des Gesetzgebungsverfahrens noch einmal hinaufschauen, um zu Nachbesserungen zu kommen.

Das, was wir jetzt hier haben, ist nur ein Schritt von mehreren, der dazu beitragen kann, dass es in Zukunft ein moderneres Datenschutzrecht gibt. Es gibt schon die nächsten Projekte, die im Anflug sind. Nämlich insbesondere die ePrivacy-Verordnung, mit der die veraltete Richtlinie aus dem Jahr 2002 abgelöst werden soll. Diese befindet sich derzeit im Gesetzgebungsverfahren im Europäischen Parlament. Dort wird es sicherlich weiteren Anpassungsbedarf geben, wenn die Verordnung eines Tages verabschiedet werden sollte, auch für das deutsche Datenschutzrecht. Gerade für den wichtigen Bereich der elektronischen Kommunikation.

Und schließlich ist mir gerade in diesem sehr umfänglichen Gesetzentwurf aufgefallen, dass wir heute eine große Menge von bereichsspezifischen Datenschutzvorschriften haben, die zwar durch die Terminologieanpassungen etwas einheitlicher werden, die aber doch in gewisser Weise sehr wild gewachsen sind und es fehlt für die Weiterentwicklung an Informationen darüber, was eigentlich mit diesen ganzen Datenübermittlungsvorschriften in der Praxis gemacht wird. Hier wäre meines Erachtens sinnvoll, dass der Bundestag sich stärker darum bemüht, dass diese Gesetze auch evaluiert werden, damit wir mehr darüber wissen, was eigentlich in der Praxis genau an Daten übermittelt wird. Und damit zukünftige rechtliche, aber auch technische Lösungen im Sinne von privacy by design auch gerade auf dieses empirische Wissen aufbauen können.

Im Gesamtfazit möchte ich also dem Bundestag empfehlen, die Omnibus- oder Containerelemente aus diesem Gesetzentwurf herauszunehmen und auch nochmal die handwerklichen Dinge gründlich zu überarbeiten. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kämen wir als nächstes zu Frau Bock, bitte.

SVe **Kirsten Bock** (Kiel): Herzlichen Dank. Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete. Ich bedanke mich für die Einladung zur Anhörung und für die Gelegenheit zur Stellungnahme. Ich möchte auch anmerken, dass ich hier heute als Privatperson spreche und nicht für das unabhängige Landeszentrum für Datenschutz.

In Anbetracht des Umfanges des vorgelegten Gesetzentwurfes beschränke ich mich auf einige ausgewählte Aspekte des Entwurfs zur Anpassung des Datenschutzrechts an die DSGVO und zur Umsetzung der JI-Richtlinie. Die europäische DSGVO ist ja angetreten mit dem Ziel einer Vereinheitlichung des europäischen Rechtsrahmens im Bereich des Datenschutzes in den Mitgliedsstaaten der Union.

Die technische Entwicklung und deren Durchdringung des Lebensalltags sowie unserer internationalen Kontakte stellen auch das Recht und den grundrechtlich zu gewährenden Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten vor wachsende Herausforderungen. Ziel der DSGVO ist es, durch einen soliden, in sich stimmigen und klar durchsetzbaren Rechtsrahmen mehr Sicherheit in rechtlicher und praktischer Hinsicht und vor allem Vertrauen für Bürgerinnen und Bürger, die Wirtschaft und den Staat zu schaffen. Ein solches Ziel ist aber nur dann zu erreichen, wenn bei den durch die DSGVO vorgesehenen Öffnungen, Präzisierungen oder Einschränkungen ihrer Vorschriften durch das nationale Recht, die Mitgliedsstaaten die DSGVO behutsam und sorgfältig in ihr nationales Recht aufnehmen, um diese dann für die Personen, für die sie gelten, auch verständlicher zu machen.

Nun muss man leider sagen, dass mit dem vorgelegten Gesetzentwurf sich diesem Ziel nicht genähert wird. Was nicht gelingt umzusetzen ist das Ziel, das Datenschutzrecht übersichtlicher und für die von ihm betroffenen Personen und Rechtsanwender verständlicher zu machen. Statt auch im bereichsspezifischen Recht auf die DSGVO oder das BDSG zu verweisen, was ja denkbar und durchaus praktikabel wäre, werden wiederum zahlreiche neue und abweichende Datenschutzregelungen geschaffen, die in vielen Fällen den Anforderungen – wie sie in der DSGVO zum Beispiel in Artikel 6, Artikel 9, Artikel 23 geregelt sind – nicht genügen. Ein Beispiel bildet etwa Artikel 8 des Entwurfes, mit dem das BDBOS-Gesetz geändert wird. Das haben wir gerade schon gehört. Die Vorgaben aus Artikel 6 Absatz 2 und 3 erlauben nur spezifische Bestimmungen, die im Ergebnis die Verarbeitungsbefugnisse einschränken, aber nicht erweitern. Die Bundesregierung verpasst damit erneut eine Chance an die Vorreiterrolle, die Deutschland im Datenschutzrecht ja mal innehatte, anzuknüpfen. Dabei bestanden schon vor Gültigkeitsbeginn der DSGVO in einigen Landesgesetzen gute Ansätze, europäische Grundsätze aus der Datenschutzrichtlinie 9546 zum Beispiel zu den technischen und organisatorischen Maßnahmen, die wir ja in der DSGVO wiederfinden, weiter zu präzisieren und für die Rechtsanwender in einer Praxis handhabbarer zu machen, aber dazu komme ich gleich noch.

Auch die vielfältigen Einschränkungen der Betroffenenrechte der Artikel 12 bis 18 DSGVO dienen nicht dem angestrebten Ziel der Vertrauensbildung. Die Schaffung weiterer Rechtsgrundlagen wäre nur dann zu begrüßen, wenn die Anforderungen an gute Gesetzgebungspraxis erfüllt und alles Wesentliche in die Regelungen aufgenommen würde. Dazu gehört in allen Varianten des Artikel 6 Absatz 1 eine hinreichend konkrete Festlegung der Zwecke und eine Präzisierung des öffentlichen Interesses, um sowohl dem Anwender als auch den betroffenen Personen die Erforderlichkeit der Verarbeitung deutlich und nachvollziehbar zu machen. Gerade für den Bereich der öffentlichen Stellen erleichtern klare Rechtsgrundlagen die Verwaltungspraxis und können zum Beispiel über geeignete Once-Only-Verfahren für mehr Bürgerfreundlichkeit der Verwaltung sorgen, ohne dass dabei die Rechte der betroffenen Personen eingeschränkt werden müssen. Bereiche, die auch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz nicht angeht, für die aber Regelungsbedarf besteht, sind vor allem der Beschäftigtendatenschutz über Artikel 88 DSGVO sowie für die Ausübung der Meinungsfreiheit unter Ausfüllung des Artikel 85 DSGVO.

Ich möchte mir nun drei Bereiche aus meiner schriftlichen Stellungnahme herausgreifen und darauf im Folgenden näher eingehen. Das ist zum einen der Grundsatz der Zweckbindung, die unmittelbar aus dem Grundrecht Artikel 8 auf Schutz personenbezogener Daten folgt.

Vors. **Andrea Lindholz** (CDU/CSU): Ich würde nur ganz kurz darauf hinweisen, wir hatten fünf Minuten vereinbart. Es sind schon viereinhalb und ich möchte, dass alle Sachverständigen drankommen und vor allem auch die Kolleginnen und Kollegen die Fragen stellen können, weil die Berichte liegen von allen vor und gehe davon aus, dass alle sie auch gelesen haben sollten.

SVe **Kirsten Bock** (Kiel): Dann möchte ich einfach abschließend noch sagen. Es gibt noch einiges zu tun, um das deutsche Datenschutzrecht wieder an die Spitze und zum Vorreiter zu machen für die Gewährleistung der Grundrechte und insbesondere für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Ich habe nämlich tatsächlich gesehen, alle von

Ihnen haben einen ausführlichen schriftlichen Bericht gemacht. Dafür herzlichen Dank. Dann kämen wir jetzt zu Herrn Dr. Brink.

SV **Dr. Stefan Brink** (LfDI des Landes Baden-Württemberg, Stuttgart): Vielen Dank Frau Vorsitzende. Meine sehr geehrten Damen und Herren Abgeordnete, ich freue mich sehr, hier eine kurze Stellungnahme abgeben zu können und ich habe sie überschrieben mit zehn Vorschläge für ein besseres Datenschutzrecht. Die besondere Stärke der DSGVO besteht darin, dass sie es tatsächlich, schafft zwei Aspekte miteinander zu verbinden. Nämlich einen wirtschaftlichen Aspekt …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielleicht kann Frau Bock das Mikro ausmachen. Dann hallt das nicht so.

SV **Dr. Stefan Brink** (LfDI des Landes Baden-Württemberg, Stuttgart): … einen wirtschaftlichen Aspekt, den man grob umschreiben kann mit moderner Datenverarbeitung oder Digitalisierung auf der einen und einen bürgerrechtlichen Aspekt auf der anderen Seite. Und diese Verknüpfung ist einmalig. Sie ist auch tatsächlich gelungen in der DSGVO und deswegen ist es aus meiner Sicht besonders wichtig, diese Stärke zu betonen und zu sehen, dass wir in manchen Bereichen nicht mit anderen Ländern konkurrieren können. Wir sind nicht so fix und nicht so bedenkenfrei, wie US-amerikanische Anbieter. Wir sind nicht so rücksichtslos wie chinesische Anbieter. Was wir können in Europa ist tatsächlich nachhaltig und bürgerorientiert arbeiten und genau das macht die DSGVO. Sie hat natürlich Schwächen bei allem Positiven, was man über sie sagen kann. Und die wesentliche Schwäche besteht darin, dass sie zu undifferenziert vorgeht. Dass sie Großunternehmen wie Facebook, Amazon und Co. im Prinzip denselben Regeln unterwirft wie kleine, mittlere Unternehmen oder sogar ehrenamtlich tätige Vereine. Das ist ein Fehler, der aber nicht hier in diesem Rahmen durch den Bundestag behoben werden kann, sondern nur auf europäischer Ebene und jeder Versuch, solchen Fehlern national zu begegnen, ist hoch problematisch und stiftet unterm Strich nur Verwirrung. Deswegen wäre mein zweiter Ratschlag, tatsächlich sich zurückzuhalten mit nationalen Korrekturversuchen und mehr den Fokus auf die europäische Ebene zu schieben.

Dritter Punkt: Gerade aktuell ist die Institution des betrieblichen Datenschutzbeauftragten unter Druck gekommen. Sie steht in der politischen Diskussion. Und aus meiner Sicht ist eher die Figur, die sich in Deutschland bewährt hat – für die auch auf europäischer Ebene gekämpft wurde, auch von der Bundesregierung gut gekämpft wurde, der Kampf hat leider nicht zu einem Erfolg geführt – aber jetzt diese hilfreiche Institutionen national in Frage zu stellen, halte ich für hochproblematisch. Unterm Strich ist die See rauer geworden und wir sind drauf und dran mit dem betrieblichen Datenschutzbeauftragten den Lotsen von Bord zu schicken. Das sollten wir im Moment nicht tun.

Vierter Punkt: Wenn man national entlasten möchte, dann hat man durchaus Möglichkeiten. Mein Vorschlag wäre, dort zu schauen bei den kleinen, nicht gewerblich tätigen Vereinen, was man für diese tun kann. Eine Möglichkeit wäre tatsächlich die Bestellungspflicht von Datenschutzbeauftragten an die gewerbliche Verarbeitung von Daten zu knüpfen oder noch besser, um unsere Anwälte und Ärzte und Steuerberater nicht zu vorschnell aus der fürsorglichen und guten Betreuung der Aufsichtsbehörden zu entlassen, an eine geschäftsmäßige Verarbeitung anzuknüpfen.

Den fünften Punkt hat Herr Prof. Dr. Aden eben schon erwähnt. Im Gesetz findet sich das Eine oder Andere, was man dort besser nicht finden würde. Zum Beispiel eine bereichsspezifische Vorratsdatenspeicherung. Auch dazu habe ich das Notwendige bereits geschrieben. Ein allgemeiner Gesichtspunkt, den ich hier ganz bewusst ansprechen möchte. Es ist tatsächlich so, die Unternehmen in Deutschland nehmen die Beratungsleistungen der Aufsichtsbehörden an. Die Aufsichtsbehörden haben sich darauf eingestellt, dass sie dort mehr liefern müssen und wir liefern auch in dem Bereich. Diese Struktur sollte unbedingt erhalten werden und sollte nicht durch vorschnelle Zentralisierungsüberlegungen – so nenne ich es mal vorsichtig – in Frage gestellt werden.

Ein allgemeiner Gesichtspunkt, was die parlamentarische Arbeit und was die Vorbereitung dieses Termins angeht. Ein solcher Gesetzentwurf ist aus meiner Sicht nur ganz schwer zu beraten und in den Griff zu kriegen. Das ist einfach zu viel Holz, was da geliefert wird. Deswegen mein Vorschlag, meine Anregung: Es wäre – glaube ich – sinnvoll, bestimmte Entwürfe der Bundesregierung stärker zu untergliedern zwischen rein terminologischen

Änderungen und tatsächlich inhaltlichen Änderungen, die vorgeschlagen werden und die sollten in besonderer Weise parlamentarisch diskutiert werden.

Dass das BDSG neu in vielen Punkten europarechtliche Zweifel aufwirft, spreche ich hier nur an. Da können wir gerne nochmal im Einzelnen diskutieren. Da ist einiges beim ersten Anpassungsgesetz – aus meiner Sicht jedenfalls – schief gegangen. Wir sehen, dass national in vielen Bereichen, Beispiel Österreich, versucht wird, an den Folgen der DSGVO zu arbeiten. Das ist deswegen so problematisch, weil es rechtlich nicht funktionieren kann. Mein Vorschlag ist, in den Bereichen ganz strickt und konsequent in ein Vertragsverletzungsverfahren vor dem EuGH zu marschieren und alle Mitgliedsstaaten Europas, die sich nicht an die Vorgaben der Grundverordnung halten, dort entsprechend auch wieder einzufangen.

Letzter Punkt: Die DSGVO sieht in Artikel 97 eine Evaluierung vor, die ist sehr sinnvoll. Und mein Vorschlag wäre, dass gerade die Abgeordneten sich da mit ihren Positionen, mit ihrer Dolmetscherfunktion in Bezug auf Vereine, Verbände einbringen und da der europäischen Kommission helfen die Grundverordnung, dort wo sie noch verbessert werden kann, weiter zu verbessern. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, dann kommen wir zu Herrn Dr. Engeler.

SV **Dr. Malte Engeler** (Richter beim Schleswig-Holsteinischen Verwaltungsgericht, Kiel): Frau Vorsitzende, verehrte Damen und Herren. Auch von mir herzlichen Dank für die Einladung und für die Gelegenheit, hier ein paar Anmerkungen zum Zweiten Datenschutz-Anpassungsgesetz mitgeben zu dürfen. Wie schon in meiner Stellungnahme will ich mich auch heute auf zwei wesentliche Punkte beschränken. Erstens die mögliche Umsetzung von Artikel 85 zum Schutz der Meinungsfreiheit und zweitens auf die Frage, ob datenschutzrechtliche Verstöße ausdrücklich aus dem Anwendungsbereich des Gesetzes gegen den unlauteren Wettbewerb (UWG) ausgenommen werden sollten. Die Dringlichkeit einer Umsetzung des Artikels 85 kann aus meiner Sicht gar nicht zu hoch bewertet werden. Ohne sie droht das Datenschutzrecht zu einer Gefahr und zu einem Instrument gegen die Meinungsfreiheit zu werden. Mit dem Datenschutzrecht und der Meinungsfreiheit kollidieren zwei sehr unterschiedliche Regelungsregime. Im Datenschutzrecht ist grundsätzlich erst einmal alles verboten, es sei denn, es ist gesetzlich geregelt oder eine Einwilligung liegt vor. Im Bereich der Meinungsfreiheit hingegen ist grundsätzlich alles erlaubt, es sei denn, es ist gesetzlich verboten. Diese Bereiche kollidieren notgedrungen dort, wo Menschen von ihrer Kunstfreiheit, Meinungsfreiheit, Wissenschaftsfreiheit im digitalen Raum Gebrauch machen. Diskussionen in Foren, Kommentare unter Onlinenachrichten, Digitalfotografie, wissenschaftliche Vorträge, die gestreamt werden, Blogs, Kultur und Literatur im Netz. All das sind Bereiche, sobald das Datenschutzrecht anwendbar ist, braucht es jeweils eine gesetzliche Rechtfertigung. Und eine solche gibt es derzeit nicht. Und das, obwohl Artikel 85 die Mitgliedsstaaten ausdrücklich dazu aufgefordert hat, beide Grundrechte in Einklang zu bringen. Lediglich für die Presse und den Rundfunk haben die Länder und der Bund Regelungen getroffen, die decken aber längst nicht alles ab. Meinungsfreiheit ist schlicht sehr viel mehr als nur Presse.

Umso richtiger ist es deswegen, dass wir heute darüber sprechen, dass es da auch konkrete Pläne für eine Umsetzung gibt. Dieser Umsetzungsbedarf ist leider in der Vergangenheit teilweise kategorisch bestritten worden. Ich meine, die Umsetzung ist auf gar keinen Fall entbehrlich. Sie mögen sich vielleicht fragen, ja wie ist denn dieser Konflikt in der Vergangenheit gelöst worden? Ganz einfach. Die Gerichte konnten abwägen zwischen dem allgemeinen Persönlichkeitsrecht und der Meinungsfreiheit und haben einzelfallgerechte Lösungen gefunden. Die DSGVO schützt aber nicht das allgemeine Persönlichkeitsrecht, sondern das Recht auf Schutz personenbezogener Daten aus Artikel 8 der Charta. Und Artikel 8 der Charta verlangt in Absatz 2 ausdrücklich eine konkrete gesetzliche Regelung. Genauso tut es Artikel 85. Das heißt, die Rechtsprechung kann so wie bisher nicht weitermachen. Genauso reicht es nicht aus auf Artikel 5 Grundgesetz zu verweisen. Auch hier wieder Artikel 8 der Charta und Artikel 85 der Grundverordnung verlangen konkrete gesetzliche Regelungen und zwar nach der Kommentarliteratur Parlamentsgesetze. Das heißt, das Grundgesetz fällt schon deswegen rein formal als Umsetzungsnorm heraus. Auch die Bordmittel der Grundverordnung selbst helfen uns nicht weiter. Da wird ganz gerne auf den Artikel 6 Absatz 1 Buchstabe f verwiesen. Der legitimiert all

solche Datenverarbeitung, für die ein legitimes Interesse besteht und ja, der hilft in einigen Fällen auch weiter, aber längst nicht in allen. Er gilt zum Beispiel nicht für öffentliche Stellen, für die ist er schlicht gesperrt. Das ist misslich, denn auch öffentliche Stellen betreiben – natürlich mittlerweile mit Segen des Bundesverfassungsgerichts – erhebliche umfangreiche Öffentlichkeitsarbeit. Und dann ist da noch Artikel 9, der die Verarbeitung von sogenannten sensiblen Daten unter erhebliche Einschränkungen stellt. Wenn Sie also etwa im Rahmen einer Twitter-Diskussion die politischen Ansichten eines Konkurrenten kritisieren wollen, sind Sie aus Artikel 6 Absatz 1 Buchstabe f sofort raus.

Obendrein haben wir noch Artikel 10. Der stellt auch die Verarbeitung von Daten mit Bezug zu Straftaten unter eine weitere enge Voraussetzung. Auch das kann es zum Beispiel schwierig machen, als freier Journalist, also außerhalb der institutionalisierten Presse, über einen Gerichtsprozess zu berichten. Es ist deshalb ganz herrschende Ansicht unter Datenschutzexperten, dass wir eine Regelung brauchen, die alle Facetten der Meinungsfreiheit abdeckt. Die Frage ist lediglich, wie, nicht ob. Noch viel wichtiger als die Schaffung einer Rechtgrundlage ist aber, dass der ganze Bereich der Betroffenenrechte und der sonstigen Folgepflichten geregelt wird. Jede Datenverarbeitung zieht erhebliche Folgepflichten nach sich. Sie müssen technische Maßnahmen ergreifen. Sie müssen die Zwecke ihrer Datenverarbeitung offenlegen. Kontaktdaten über sich mitteilen. Für die Richtigkeit der Datenverarbeitung einstehen und all das auch noch gegenüber den Aufsichtsbehörden rechtfertigen. Auf die Bereitschaft zur Teilnahme am öffentlichen Meinungsaustausch kann das verheerende, hemmende Wirkung haben und welcher Missbrauch möglich ist, sehen wir leider aktuell schon in anderen Nachbarländern.

Ganz kurz noch zu einem zweiten Punkt, zur Frage der Abmahnfähigkeit. Meines Erachtens nach wird hier derzeit einer allgemeinen DSGVO-Panik aufgesessen. Eine Abmahnwelle ist bisher schlicht ausgeblieben. Was es aber gibt sind auf jeden Fall Unternehmen, die beim Datenschutz sparen. Und da ist das Mittel der Abmahnung manchmal durchaus ein adäquates Mittel, gerade angesichts überforderter Aufsichtsbehörden. Dieser Abmahnmissbrauch muss generell bekämpft werden, keine Frage. Das muss aber strukturell geschehen und nicht durch übereilte Einzelaktionen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir als nächstes zu Frau Gurkmann.

SVe **Jutta Gurkmann** (Verbraucherzentrale Bundesverband e.V., Berlin): Vielen Dank Frau Vorsitzende, meine Damen und Herren. Auch ich bedanke mich für die Einladung und die Möglichkeit heute unsere Position vorzutragen. Der VZBV möchte sich auch nur zu einem Aspekt, nämlich der Frage, ob datenschutzrechtliche Vorschriften Marktverhaltensregelungen sind und dementsprechend wettbewerbsrechtlich verfolgbar sein sollen, äußern.

Nach Ansicht des VZBV sollte es auf jeden Fall weiterhin seriösen, klagebefugten Verbänden möglich sein, Verstöße gegen datenschutzrechtliche Vorschriften als Marktverhaltensregeln mit den Mitteln des Wettbewerbsrechts begegnen zu können. Die steigende Bedeutung von Daten als wesentlichen Bestandteil des markbezogenen Leistungsaustauschs ist kennzeichnend für die fortschreitende Digitalisierung. Wer über Daten verfügt, verfügt über Macht. Wer über mehr Daten verfügt, verfügt über mehr Macht. Wer Daten unbefugt nutzt, erlangt dadurch einen Vorsprung durch Rechtsbruch und diesen muss die Wettbewerbsordnung auch unterbinden können.

Der VZBV sieht die Durchsetzung des Datenschutzrechts durch Datenschutzbehörden und durch die nach Wettbewerbsrecht klagebefugten Einrichtungen als komplementär an. Die Durchsetzung des Datenschutzrechts durch Datenschutzbehörden dient nämlich dem Schutz der Persönlichkeitsrechte. Die Durchsetzung des Wettbewerbsrechts dient dem Schutz der Wettbewerbsordnung, also dem unverfälschten Wettbewerb.

Wegen dieser unterschiedlichen Zielsetzung besteht kein Anlass anzunehmen, dass die DSGVO eine parallele Durchsetzung auf wettbewerbsrechtlichem Weg ausschließen wolle. Das Datenschutzrecht kann im Einzelfall auch Zwecken der Marktverhaltensregelung dienen. Wenn dies der Fall ist, ist Datenschutz Wettbewerbsschutz und muss als solcher durchsetzbar sein. Und die Durchsetzung unterscheidet sich vom behördlichen Datenschutzauftrag und wird im zivilrechtlichen System durch das UWG mit den Mitteln des Wettbewerbsrechts und durch beauftragte qualifizierte Einrichtungen gewährleistet.

Ein Beispiel möchte ich an dieser Stelle nennen, damit wir wissen wovon wir reden. Es ist unser Verfahren gegen Facebook „Freunde finden“, nur eines unserer Verfahren gegen Facebook. Hier hat der BGH auf Klage des VZBV beispielsweise entschieden, dass das Auslesen von Adressbüchern und die Versendung dann von Mails an Nicht-Facebook-Nutzer rechtswidrig war. Facebook musste also diese unbefugte Nutzung aufgrund unserer Klage einstellen und kann daraus keinen ökonomischen Nutzen mehr ziehen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Jetzt kommen wir zu Frau Karstedt-Meierrieks.

SVe **Annette Karstedt-Meierrieks** (Deutscher Industrie- und Handelskammertag, Berlin): Frau Vorsitzende, meine Damen und Herren. Herzlichen Dank für die Einladung. Ich möchte bei unserer Stellungnahme zwei Aspekte herausgreifen. Zunächst mal zurück zu der Basis unseres Hierseins, zu der DSGVO. Die DSGVO hat bei den Unternehmen zu erheblichen Unsicherheiten geführt. Und, das haben wir alle mitbekommen, Sie als Abgeordnete haben sicherlich auch genügend Post aus Ihren Wahlkreisen bekommen und Hinweise von den Unternehmen erhalten, dass die Umsetzung doch mit erheblichem Aufwand verbunden ist. Abgesehen jetzt von der reinen Umsetzung, gibt es aber auch Nebenaspekte, die zu dieser Unsicherheit beigetragen haben. Also die Frage Telemediengesetz. Was ist mit Cookies? Kann man also zukünftig Cookies nur noch mit Einwilligung setzen? KUG, also Kunsturhebergesetz. Was passiert mit Fotos? Und wir sind natürlich auch beim UWG bzw. beim UKlaG (Unterlassungsklagegesetz), also bei der Frage der Abmahnung. Sind Abmahnungen zulässig aufgrund datenschutzrechtlicher Verstöße?

Aufgrund dieser großen Unsicherheit und der großen Belastung, die für die Unternehmen durch die Umsetzung der DSGVO entstanden sind, stellt sich natürlich die Frage, wie können Unternehmen jetzt in dem Gesetzgebungsverfahren Omnibus-Gesetz vielleicht entlastet werden. Und da bietet sich natürlich die Frage an, Bestellung des betrieblichen Datenschutzbeauftragten. Wenn also im Moment eine Entlastung auf europäischer Ebene nicht möglich ist, weil wir die Evaluierung erst ab 2020 sozusagen beginnen lassen, wäre also hier die Möglichkeit kleinere und mittlere Unternehmen doch zu entlasten im Rahmen der Bestellung des betrieblichen Datenschutzbeauftragten. Das kann passieren durch die Anhebung des Schwellenwerts von 10 auf 20 Personen. Das kann passieren, indem man aus dem Begriff Personen Beschäftigte macht. Das kann passieren durch das, was Herr Dr. Brink schon vorgeschlagen hat, um den privaten Bereich, sprich also Vereine, herauszunehmen, den Begriff geschäftsmäßig bzw. gewerblich einzuführen, um eben von privaten Institutionen abzugrenzen. Und man kann natürlich auch durchaus überlegen, ob der risikobasierte Ansatz, den ja die DSGVO trägt, ob man den hier eben auch in das BDSG übernimmt und sich von einem Schwellenwert vollkommen loslöst, sondern auf die Tätigkeit der Beschäftigten abstellt. Also von daher unsere Anregungen hier im BDSG Entlastung für die KMU zu schaffen, indem zumindest der Schwellenwert von 10 auf 20 Beschäftigte angehoben wird.

Zweiter Aspekt: UWG, UKlaG. Ja, die große Abmahnwelle, die auch ich befürchtet habe, ist ausgeblieben. Aber es ist durchaus zu Abmahnungen gekommen. Also man kann nicht sagen, es war „still ruht der See“, sondern es haben sich durchaus einige Personen, Anwälte und auch Verbände darin geübt, hier ein neues Geschäftsmodell aufzulegen. Und man muss sehen, dass natürlich mit Zunahme von Rechtsprechungen auf Basis der DSGVO auch Abmahnungen zunehmen werden, weil dann eine stärkere Rechtssicherheit herrscht. Wir haben unterschiedliche Rechtsprechungen zu der Frage, ob nun Datenschutzregeln Marktverhaltensregeln sind oder nicht. Auch das ist ein Punkt, der natürlich zu Lasten der Unternehmen geht. Von daher wäre es sehr vorteilhaft, wenn der Gesetzgeber hier mit einer Regelung Rechtsklarheit schafft und eben dafür sorgt, dass klargestellt wird, dass Datenschutzverstöße keine Basis für Abmahnungen sind. Also Datenschutzregelungen keine Marktverhaltensregeln darstellen. Das kann im UWG passieren. Wir haben ja im Moment die Diskussion über einen Referentenentwurf zur Änderung des UWG. Ich habe das Gefühl, das dauert etwas lang. Von daher wäre unser Vorschlag, das mit einer Änderung des BDSG zu regeln und dort scheint uns der Bundesratsvorschlag zur Einführung eines 44a durchaus sinnvoll.

Und die Frage, ob das UKlaG geändert werden muss, ich denke Herr Prof. Köhler, da sind Sie wesentlich berufener dazu etwas zu sagen als ich. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann schließen wir auch gleich an und kämen jetzt zu Herrn Prof. Dr. Köhler.

SV **Prof. Dr. Helmut Köhler** (Ludwig-Maximilians-Universität, München): Vielen Dank Frau Vorsitzende, dass ich hier auch meine Stellungnahme abgeben darf. Worum geht es mir? Es geht um das Verhältnis von Datenschutz nach der DSGVO einerseits und dem Verbraucherschutz nach UWG und UKlaG andererseits. Erste These: Vorrang des Unionsrechts vor dem nationalen Recht. Das ist unbestreitbar. Das heißt, wir müssen fragen, was das Unionsrecht zu dieser Frage sagt. Das beginnt schon bei dem primären Unionsrecht, nämlich in dem AEUV, Artikel 16, im EUV, Artikel 39 und in der schon erwähnten Grundrechtecharta Artikel 8. Darin ist der Datenschutz als Regelungsmaterie definiert. Und was den Verbraucherschutz angeht, ist er in Artikel 169 AEUV gesondert definiert. Das heißt, es handelt sich schon aus Sicht des primären Unionsrechts um völlig unterschiedliche Regelungsbereiche mit völlig unterschiedlichen Durchsetzungsmechanismen. Und wie soll das jetzt zusammengehen? Wie es sich Frau Gurkmann vorstellt, dass auf einmal das UWG auch die Funktion des Datenschutzes übernehmen kann? Das ist die Frage.

Die unterschiedlichen Zwecke bestehen darin: Das Datenschutzrecht der DSGVO schützt die Grundrechte der betroffenen Personen vor einer rechtswidrigen Datenverarbeitung ihrer personenbezogenen Daten. Das UWG schützt insbesondere die Interessen der Verbraucher bzw. die UGP-Richtlinie auf EU-Ebene schützt die wirtschaftlichen Interessen der Verbraucher. Und wer ist Verbraucher? Verbraucher ist – vereinfacht gesprochen – jede natürliche Person, die Käufer von Waren oder Dienstleistungen ist. Durch die UGP-Richtlinie und das UWG soll das Interesse der Verbraucher geschützt werden, eine geschäftliche Entscheidung zu treffen, die nicht durch einen Unternehmer unsachlich beeinflusst wird. So und jetzt sage ich noch schnell ein Wort zum § 3a UWG, weil das die Scharniernorm ist, durch die der Verbraucherschutz mit dem Datenschutz verbunden werden könnte. Der § 3a UWG fordert einen Verstoß gegen eine gesetzliche Vorschrift, die auch dazu bestimmt ist, die Interessen der Marktteilnehmer zu schützen. Marktteilnehmer sind nach der Definition des UWG Mitbewerber, Verbraucher und sonstige Marktteilnehmer. Es ist also mit dem § 3a nur der Schutz der wirtschaftlichen Interessen der Verbraucher bezweckt. Der Verbraucher ist aber nicht das gleiche wie die natürliche Person im Sinne des Datenschutzrechts. Deshalb kann man an sich die Frage dahingestellt sein lassen, ob die DSGVO auch den Wettbewerb zwischen Unternehmen regelt. Das tut sie nämlich nicht, aber dazu müssen wir genauer einsteigen in die DSGVO. Das kann ich hier nicht machen.

Also meine These ist: Verbraucherschutz und Datenschutz sind völlig unterschiedliche Regelungskomplexe mit jeweils eigenen Durchsetzungsmechanismen. Der § 3a UWG ist nicht anzuwenden. Seine Anwendung würde gegen höherrangiges Unionsrecht verstoßen und in vergleichbarer Weise gilt das dann auch für das Unterlassungsklagengesetz im Sinne des § 2 Absatz 2 UKlaG. § 2 Absatz 2 Satz 1 Nr. 11 UKlaG hat keine Grundlage im Unionsrecht muss ich sagen, weil auch er nur dem Verbraucherschutz dient und nicht dem Zweck, datenschutzrechtliche Regelungen durchzusetzen. Ich habe selbst Gesetzgebungsvorschläge gemacht. Diese betreffen den § 44 Bundesdatenschutzgesetz. Der Absatz 1 ist völlig „verkorkst“. Diese Vorschrift muss unbedingt geändert werden, weil sie gegen das Unionsrecht verstößt. Für Verbraucherverbände und für Anwälte ergeben sich Betätigungsmöglichkeiten – und zwar ausreichende – im Sinne des Artikel 80 Absatz 2 DSGVO. Diese Bestimmung muss aber erst durch den Gesetzgeber aktiviert werden, weil es sich dabei nur um eine Öffnungsklausel handelt, von der der Bundesgesetzgeber leider noch keinen Gebrauch gemacht hat. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kämen wir abschließend noch zu Herrn Prof. Dr. Schröder.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank Frau Vorsitzende, meine Damen und Herren Abgeordnete. Ich freue mich, dass ich hier meine Stellungnahme zum Entwurf dieses Gesetzes vortragen darf. Zunächst vielleicht aus meiner Sicht: Ich halte das Gesetz für sehr wichtig und richtig im Großen und Ganzen, denn es gibt nichts Schlimmeres für den Rechtsunterworfenen, als wenn er der Rechtsunsicherheit ausgesetzt ist, weil zum Beispiel Begriffe nicht übereinstimmen oder sogar Verweise völlig ins Leere führen.
Von daher war der deutsche Gesetzgeber dazu aufgerufen, hier die Synchronisation zwischen dem Unionsrecht und dem deutschen Recht wieder herzustellen. Ich würde dieses Anliegen auch als

grundsätzlich gelungen betrachten, möchte aber auf einige Punkte hinweisen, die Sie auch in meiner Stellungnahme nachlesen können. Das eine ist der Umgang mit dem Begriff der Verarbeitung. Grundsätzlich hat sich ja der Begriff der Verarbeitung durch das Inkrafttreten der DSGVO etwas gewandelt. Wir hatten vorher einen rein nationalen engen Begriff dessen, was unter Datenverarbeitung zu verstehen ist. Jetzt gibt es nur noch einen europarechtlichen weiten Begriff der Datenverarbeitung. Und wenn man diesen weiten Begriff jetzt in dem Gesetz einfach irgendwo verwendet, muss man sich im Klaren darüber sein, dass je nach Verwendungskontext damit auch eine Befugniserweiterung einhergehen kann. Dieser Entwurf, das wurde bereits angesprochen, ist so umfangreich, dass es mir jetzt auch in der Kürze der Zeit nicht möglich war, das immer unter Abgleich mit dem bereits vorhandenen Gesetz zu überprüfen. Das ist sicherlich die Aufgabe der Damen und Herren Abgeordneten hier, das im Detail zu machen und wahrscheinlich kann man da auch darauf vertrauen, dass das im Entwurf geprüft wurde. Ich sage nur, dass auch in der Begründung nicht immer vollständig klar ist, ob es jetzt wirklich nur eine redaktionelle Änderung ist oder nicht.

Dann ein Punkt, auf den ich hinweisen möchte, das ist der geplante § 22 Absatz 1Nr. 1 lit. d) BDSG. Das ist meines Erachtens etwas, was über die Öffnungsklausel, die das Unionsrecht im Artikel 9 gewährt, hinausgeht. Der Artikel 9 erlaubt es zwar, diese besonderen Kategorien personenbezogener Daten, diese sensiblen Daten, aufgrund besonderer Rechtsgrundlage, aufgrund eines wichtigen öffentlichen Interesses zu verarbeiten. Aber er geht doch wohl ersichtlich davon aus, dass der nationale Gesetzgeber konkretisiert, was dieses öffentliche Interesse ist, und zwar in einer Norm. Und wenn man einfach jetzt in das nationale Gesetz nur reinschreibt, die Verarbeitung ist zulässig, wenn das aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist, dann ist das – glaube ich – nicht das, was sich der Unionsgesetzgeber hier vorgestellt hat.

Ein Wort vielleicht noch zu den Erleichterungen für kleinere und mittlere Unternehmen oder Vereine. Sicherlich geht der deutsche Gesetzgeber im Moment darüber hinaus, was das europäische Datenschutzrecht für den betrieblichen Datenschutzbeauftragten vorsieht. Man hat dort von einer Öffnungsklausel Gebrauch gemacht. Ich möchte aber darauf hinweisen, dass wenn man hier eine Erleichterung schafft, diese Erleichterung vielleicht auch nur eine etwas trügerische ist, denn die materiellen Pflichten, Auskunftspflichten, Führen eines Verarbeitungsverzeichnisses usw. bleiben bestehen. Und der Datenschutzbeauftragte ist ja nicht nur irgend ein Ballast, den ein Unternehmen oder ein Verein mit sich herumschleppt, sondern er ist auch eine Hilfestellung. Wenn man sich anschaut, was seine Aufgaben in der DSGVO sind, dann soll er eben auch beraten und darauf hinwirken, dass das Datenschutzrecht eingehalten wird. Und das ist sicherlich etwas, wo man diesen Datenschutzbeauftragten nicht nur als Ballast, sondern auch als Hilfe ansehen kann. Soviel von meiner Seite für den Moment. Ich freue mich auf Fragen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank Herr Prof. Dr. Schröder. Es ist sehr schwierig immer, das nicht als Ballast, sondern als Hilfe zu kommunizieren aus Abgeordnetensicht gesprochen. Dann kommen wir jetzt zur Fragerunde. Herr von Notz, oder technischer Natur?

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Noch eine Geschäftsordnungsfrage.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, bitte.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Wir hatten ja beantragt, dass die Bundesbeauftragte für den Datenschutz geladen wird vor die Klammer. Die wollte nicht kommen, oder?

Vors. **Andrea Lindholz** (CDU/CSU): Nein. Aber das wäre eine Mehrheitsentscheidung gewesen und es kam von keiner anderen Fraktion dazu noch eine Reaktion.

Abg. **Manuel Höferlin** (FDP): Aber es war kein Widerspruch erkennbar. Also ich dachte, wir hätten das einstimmig so im Vorherein, weil es gab keinen der dagegen gesprochen hat. Ich weiß nicht, wie bei Ihnen dieses Verfahren läuft.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Stimmen wir ab? Vielleicht ist Herr Kelber sprachfähig und kann das machen.

Vors. **Andrea Lindholz** (CDU/CSU): Also ich kann jetzt nur aus rein rechtlicher Sicht sagen. Es wäre eine Mehrheitsentscheidung gewesen und es kam von niemanden mehr eine Rückmeldung zu diesem

Thema. Man hätte darüber positiv entscheiden müssen.

Abg. **Manuel Höferlin** (FDP): Unter Protest, Frau Vorsitzende. Ich habe das auch so verstanden, dass wir, da niemand etwas dagegen gesagt hat, …

Vors. **Andrea Lindholz** (CDU/CSU): Ich gebe das dann so weiter ans Sekretariat. Ich habe mir das jetzt heute Morgen angeschaut.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das geht überhaupt nicht.

Vors. **Andrea Lindholz** (CDU/CSU): Ich werde mir den Text anschauen, aber es ist aber auch in der Obleuterunde keinerlei Thema gewesen. In üblicher Weise kommen doch auf diese Anfragen auch von den Fraktionen und von den Obleuten Rückmeldungen zu diesem Punkt. Und diese Rückmeldung ist hier von keiner einzigen Fraktion erfolgt. Es gab noch nicht ein irgendwie geartetes Zeichen der Zustimmung, gar nichts, und Schweigen ist nun mal keine Zustimmung.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Also wir haben das beantragt und damit waren wir dafür. Kann ich nur sagen.

Vors. **Andrea Lindholz** (CDU/CSU): Damit waren Sie auch der Einzige, Herr von Notz. Es tut mir jetzt leid. Ich nehme es mit auf.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Warum haben Sie es denn aufgerufen? Oder wie läuft es denn in der Obleuterunde?

Vors. **Andrea Lindholz** (CDU/CSU): Es ist verteilt worden wie immer. Ihr Antrag ist verteilt worden. In der Obleuterunde werden die Sachverständigen, werden besondere Wünsche angesprochen um das Prozedere zu erklären. Wir machen aber auch gleich dann hier die Runde. Da kam von niemanden der Obleute in der Obleuterunde …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Es ist doch Wahnsinn, dass wir diese Anhörung durchführen, ohne dass die Bundesbeauftragte für den Datenschutz dabei ist.

Vors. **Andrea Lindholz** (CDU/CSU): Diesen Wahnsinn, Herr von Notz, haben Sie als Einziger beantragt und es hat sich niemand diesem Antrag angeschlossen. Ganz einfach. Und es ist eine Mehrheitsentscheidung, so wie üblich, und die ist hier nicht erfolgt.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich habe versucht, den Wahnsinn zu verhindern, Frau Vorsitzende.

Vors. **Andrea Lindholz** (CDU/CSU): Gut, wir nehmen das jetzt so zur Kenntnis. Es ist rechtlich so. Es ist eine Mehrheitsentscheidung wie immer. Wie wir das in anderen Fällen auch haben. Und es ist in Umlauf gegangen an alle Obleute und es ist Null-Komma-Null-Reaktion erfolgt!

So, und jetzt beginnen wir mit der Fragerunde und kommen damit zu Herrn Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank, Frau Vorsitzende. Ich nehme Ihren Satz gerne auf, dass es manchmal schwierig zu kommunizieren ist, um die Vorzüge des Datenschutzes und der DSGVO, wobei ich davon überzeugt bin auch von dem Rechtsgedanken, dass er gut und richtig ist, aber dass wir ihn entsprechend auch mit Leben ausfüllen müssen. Und vor diesem Hintergrund habe ich zwei Fragen an Herrn Prof. Dr. Köhler. Hintergrund der Fragen: Ich komme aus einer Gegend mit ganz vielen kleinen Mittelständlern und ich glaube knapp 1.300 Vereine und Verbände im Wahlkreis, wo also in der Tat die Sorge vor den Abmahnungen die Allergrößte ist und wo niemand sich damit beruhigen lässt, dass es keine Abmahnwelle gegeben hat, sondern allein die Möglichkeit, dass eine Abmahnung ins Haus flattern könnte bzw. die Tatsache, dass der ein oder andere bekannte Verein, Verband oder Gewerbetreibende so eine mal bekommen hat, reicht schon aus für eine riesengroße Verunsicherung. Und die aus der Welt zu kriegen, ist – glaube ich – unsere große Aufgabe. Sie haben thematisiert, dass der Versuch über das UWG das zu lösen, schwierig sei oder unmöglich sei oder auch der falsche rechtliche Weg sei. In diesem Lichte gibt es ja das eine oder andere Urteil. Jetzt Landgericht Würzburg, wenn ich richtig informiert bin, hat das ein bisschen anders gesehen. Aber nochmal zur Klarstellung. Ist der Versuch tauglich, es über das UWG zu lösen?

Oder aber wenn ja – zur Beruhigung – macht es Sinn und falls ja, wie konkret kann im BDSG zum Beispiel noch eine Klarstellung für Ruhe sorgen, sodass die Sorge vor Abmahnungen dementsprechend unbegründet ist. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Wir machen erst die Fragerunde – zur Erklärung – weil es könnte sein, dass ein Sachverständiger auch von

anderen Fragen bekommt, deshalb machen wir erst die komplette Fragerunde und dann jeder Sachverständige kann dann auf alle Fragen, die ihm gestellt worden sind, antworten. Wir kommen als nächstes zu Herrn Haug.

Abg. **Jochen Haug** (AfD): Vielen Dank, Frau Vorsitzende. Ich habe zunächst eine Frage an Herrn Brink. Sie haben in Ihrer Stellungnahme das Thema Videoüberwachung angesprochen. Welchen Nachbesserungsbedarf sehen Sie bei § 4 BDSG, der die Videoüberwachung öffentlich zugänglicher Räume regelt? Und dann habe ich noch eine Frage an Herrn Dr. …

Vors. **Andrea Lindholz** (CDU/CSU): Die gleiche Frage dann.

Abg. **Jochen Haug** (AfD): Achso, stimmt. Habe ich … Fehler meinerseits. Dann werde ich … Dann hätte ich eine andere Frage gehabt. Dann stelle ich dieselbe Frage an Herrn Dr. Engeler.

Vors. **Andrea Lindholz** (CDU/CSU): Okay. Als nächstes kämen wir dann zur Fraktion der SPD.

Abg. **Saskia Esken** (SPD): Der Umfang dieses Monstrums, das auch so einen monströsen Namen hat, dieses Gesetzes ist angesprochen worden. Es ist angesprochen worden die Vermischung von Rechtstechnik und Omnibus, die ziemlich problematisch ist, auch für uns Abgeordnete – wenn Sie schon keine Zeit hatten, es zu lesen, fragen Sie sich, ob wir die hatten – aber ob das tatsächlich jetzt auch noch mit hineingemischt werden soll, dass wir Unsicherheit beseitigen durch weiße Salbe, das finde ich wirklich relativ problematisch. Ich finde den Vorschlag, die Bestellpflicht des Datenschutzbeauftragten, da die Schwelle hochzusetzen oder durch Begriffe da Veränderungen herbeizuführen, relativ problematisch. Einfach deshalb, weil Sie sagten, wir sollten eine Entlastung der Kranken ermöglichen, aber tatsächlich möchten Sie gerne, dass wir den Krankenpfleger wegnehmen. Das halte ich nicht für einen guten Weg. Ich bin der Auffassung, vor allem auch weil wir ja keine Pflichten wegnehmen, abgesehen von der Bestellpflicht, ist es notwendig, dass der Datenschutzbeauftragte die Unternehmen und durchaus auch große Vereine dabei unterstützt, eben die DSGVO gut umzusetzen.

Deswegen geht meine Frage eher in Richtung Klärungsbedarf Artikel 85 und der Aufgabe der Abwägung zwischen dem Schutz personenbezogener Daten und der Meinungsfreiheit an Herrn Dr. Engeler. Wo besteht denn tatsächlich vor dem Hintergrund, der in der Tat sehr uneinheitlichen Umsetzung von Artikel 85 in den Landesmediengesetzen jetzt die Notwendigkeit auf Bundesebene hier zu regeln, etwa mit Blick auf den sogenannten nicht verfassten Journalismus, also etwa Blogger, aber auch in Bezug auf uns alle, die wir uns jeden Tag äußern auch unter Einbeziehung von Namen und anderen Daten von anderen Personen. Wenn ich heute Morgen twittere über die Meinungsäußerung eines anderen Kollegen oder eines Fachmanns in der Presse, inwieweit gerate ich denn da schon unter die Pflichten auch Betroffenenrechte einzuräumen, Auskunftsrechte usw. Wo haben wir da Regelungsbedarf Herr Dr. Engeler?

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann kommen wir zu Herrn Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke Frau Vorsitzende. Ich habe gemäß unseren Regelungen zwei Fragen an Herrn Dr. Brink. Also erstmal vorab als Bemerkung dieser Geschichte, dass man nicht Verfahrensanpassungen in ein Anpassungsgesetz passt und materiell-rechtliche Dinge in ein zweites Gesetz. Das möchte ich auch einfach kritisieren. Das ist sehr nervig. Das kam ja auch von mehreren Sachverständigen. Ich glaube, das ist eine Sache, die nicht nur uns stört, sondern das vor allen Dingen das Thema DSGVO, was ja bei vielen Menschen schon Gänsehaut beim Namen hervorruft – außerhalb dieses Hauses sowieso – noch schwerer macht, Änderungen daran zu transportieren. Also das ist echt schwierig und das macht es jetzt hier nicht einfacher.

Die erste Frage betrifft den Komplex des betrieblichen Datenschutzbeauftragten. Herr Dr. Brink, Sie haben ja gesagt – ich teile die Auffassung auch – dass der einen wertvollen Beitrag zur Umsetzung von Datenschutzrecht in Unternehmen leisten kann. Im Moment ist das Kriterium die Anzahl von Mitarbeitern. Und meine konkrete Frage ist jetzt, gäbe es da nicht andere Kriterien. Sie haben davon gesprochen, dass man vielleicht auch darüber nachdenkt, ob jemand geschäftsmäßig arbeitet. Wäre es nicht vielleicht auch ein Kriterium und eine Überlegung wert darüber nachzudenken, bei Unternehmen nicht Mitarbeiter als Kriterium, sondern die bestimmte datenschutzsensible Bereiche

bearbeiten, die überhaupt mit datenschutzrelevanten Punkten – also sozusagen eine Art Gewichtung einzuführen oder eine Regelung zu führen, die Unternehmen, die überhaupt nichts oder sehr wenig oder mit viel Personal nichts mit datenschutzrelevanten Themen zu tun haben – davon ausnehmen könnte. Also da einen anderen Kriterienmaßstab sozusagen einzuführen.

Und die zweite Frage haben Sie auch darauf angesprochen, ist hier § 22 BDSG neu. Nämlich die Erweiterung der Kategorien personenbezogener Daten, wenn dies aus Gründen eines erheblich öffentlichen Interesses zwingend erforderlich ist. Diese weiche Formulierung, da auch meine Frage. Ist das nicht – Sie haben mal gesagt, wir werden wahrscheinlich von EuGH einige Dinge zu erwarten haben – ist das nicht vorprogrammiert, dass man dort erheblichen Klärungsbedarf hat? Ist es überhaupt europarechtlich vereinbar, solch eine weiche Formulierung national dann zu wählen? Und welcher Anwendungsbereich ist da zu erwarten? Also mir ist noch nicht ganz klar, wie groß da die Tragweite ist für den Anwendungsbereich, was man damit verwenden kann. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, dann kommen wir zur Fraktion DIE LINKE..

Abg. **Gökay Akbulut** (DIE LINKE.): Vielen Dank auch. Ich habe zwei Fragen an Frau Bock. Meine erste Frage richtet sich auf den neuen § 22 Abs. 1 BDSG. Hier soll ja eine Übermittlungsbefugnis von nichtöffentlichen zu öffentlichen Stellen geschaffen werden. Laut Gesetzesbegründung soll das vor allem ermöglichen, dass aus Präventionsprojekten im Bereich islamischer Extremismus personenbezogene Daten zweckändernd an Polizeibehörden übermittelt werden dürfen. Welche Konsequenzen hat hier der fehlende Verweis auf § 22 Abs. 2 BDSG und wie offen ist die Regelung tatsächlich insgesamt? Müssen also noch deutlich mehr nichtöffentliche Stellen damit rechnen, dass die Polizei sich bei der Forderung nach personenbezogenen Daten auf diese Regelung berufen kann.

Können Sie auch nochmal darauf eingehen.

Und meine zweite Frage. Sie schreiben ja zu Beginn Ihrer Stellungnahme, dass Artikel 32 zu den technischen und organisatorischen Maßnahmen zum betrieblichen Datenschutz systematisch unklar sei und empfehlen eine Orientierung an den bislang in den Landesdatenschutzgesetzen vorhandenen Regelungen, diesen Auftrag zum organisatorischen technischen Datenschutz zu übersetzen. Gerade im Blick auf informationstechnische Anwendungen, Stichwort Digitalisierung. Können Sie uns das anhand einzelner Beispiele aus den Ländergesetzen und vielleicht auch Ihrer Prüfpraxis erläutern? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Den Abschluss macht dann Herr von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Meine Damen und Herren Sachverständige, herzlichen Dank für Ihre Stellungnahmen, die schriftlichen und die mündlichen. Ich will vorweg schicken, dass ich es gut fände, wenn die Zeit, die wir hier heute miteinander verbringen, nicht mit der Gefechtslage verbracht wird innerhalb der Groko, sozusagen wie man es jetzt mit den Abmahnungen hält, ja oder nein. Das ist vielleicht auch ein interessantes Thema, wobei ich sagen muss, ich habe lange hier mich mit Abmahnungen im Haus beschäftigt. Da sind Millionen von Verbraucherinnen und Verbraucher über Jahre abgemahnt worden. Familien, die mussten irgendwie tausende von Euro zahlen für 69 Cent Audiodateien, die sie runtergeladen haben. Da hat es hier nie so einen großen Aufriss gegeben. Und hier reden wir nur um irgendeine Angst, die jemand vor Abmahnungen hat. Aber trotzdem soll man das Thema ernstnehmen.

Meine erste Frage geht aber Herrn Dr. Brink und Herrn Prof. Dr. Aden. Nämlich im Hinblick auf das BDBOS-Gesetz. Die Bundesbeauftragte schlägt drei Streichungen für drei Bestimmungen vor im Hinblick auf diesen Behördendigitalfunk, der – wenn ich es richtig verstehe – auch noch um Bundeswehrgeräte erweitert werden soll. Also siebenstelliger Betrag von Leuten, die da betroffen sind von dieser Vorratsdatenspeicherung. Also, ist das offenkundig verfassungswidrig oder ist das erst verfassungswidrig, wenn das Bundesverfassungsgericht in den nächsten Wochen erneut zur Vorratsdatenspeicherung entscheidet oder wie blicken Sie auf diese Frage? Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zur Beantwortung. Wieder in alphabetischer Reihenfolge diesmal nochmal von Anfang des Alphabetes und beginnen mit Herrn Prof. Dr. Aden.

SV **Prof. Dr. Hartmut Aden** (HWR, Berlin): Vielen Dank. Dann fange ich auch gleich mit der letzten Frage an und knüpfe direkt an.

Die Frage, ob der Entwurf der Änderung des BDBOS-Gesetzes verfassungswidrig ist, hängt in der Tat damit zusammen, ob die Speicherung von Verkehrsdaten zu technischen Sicherungszwecken, die dort vorgesehen ist, aber auch zu anderen Zwecken, die zusätzlich vorgesehen sind, dem Grundsatz der Verhältnismäßigkeit genügen. Darum geht es. Und das ist sicherlich eine Frage, die insofern sehr eng verknüpft ist mit der Rechtsprechung des Gerichtshofs der EU zu den Fragen der Verhältnismäßigkeit von diversen Formen von Vorratsdatenspeicherung und auch dem, was wir in Konsequenz daraus auf der nationalen Ebene in Zukunft zu erwarten haben. Ich mag da jetzt keine endgültige Prognose aufstellen, eher etwas differenzieren. Sicherlich ist es grundsätzlich ein legitimer Zweck, dass eine im Sicherheitsbereich tätige Behörde Vorkehrungen trifft, um die Sicherheit ihrer Netze zu kontrollieren. Das ist aus meiner Sicht unbestritten, aber es geht dann darum, was dafür im Zeitalter der Digitalisierung eigentlich die adäquaten Mittel sind. Ist es dafür wirklich erforderlich, wahllos für 75 Tage alle Verkehrsdaten aller Nutzerinnen und Nutzer dieses Systems aufzubewahren? Da habe ich doch erhebliche Zweifel. Es handelt sich um avancierte Technik, die dort eingesetzt wird. Da müsste es doch sehr viel ausgereiftere Techniken geben, damit man etwa mit Stichproben hinkommt und damit man, wenn etwas passiert ist, ein Verfahren hat, um das was gerade passiert ist, zu sichern. Das sind meines Erachtens Alternativen, die dort eingezogen werden sollten und insofern sehe ich keine Erforderlichkeit, die Daten in dem Umfang zu speichern. Und wenn es so wäre, das heißt, wenn der Grundsatz der Verhältnismäßigkeit – so wie ja auch die Bundesdatenschutzbeauftragte das sieht – nicht gewahrt wäre, dann wäre in der Tat diese Regelung auch verfassungswidrig.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann kommen wir zu Frau Bock.

SVe **Kirsten Bock** (Kiel): Vielen Dank. Die Frage drehte sich um den neuen § 22 BDSG. Da haben wir schon gehört, auch in der Fragerunde. Also das geht sicherlich in der jetzt vorliegenden Formulierung über die Öffnungsklausel hinaus. Also es bedarf da dringend einer Konkretisierung des öffentlichen Interesses durch den nationalen Gesetzgeber. Die DSGVO bringt dieses öffentliche Interesse oder das erhebliche öffentliche Interesse als Beispiel in den Raum, aber fordert dann eben die nationalen Gesetzgeber auf, dafür Gründe zu nennen, warum das öffentliche Interesse betroffen sein soll. Und insofern gibt es hier Nachbesserungsbedarf. Insbesondere ist klärungsbedürftig das Verhältnis zu § 24 BDSG, der für nichtöffentliche Stellen eine Übermittlungsbefugnis für besondere Kategorien dadurch schaffen wird. Und hier bleibt eben unklar, ob der Absatz 2 des § 22 auch Anwendung findet. Da geht es ja um die technisch organisatorischen Maßnahmen und gerade in so sensiblen Bereichen Präventionsschutz im Terrorismusbereich. Das ist natürlich von ganz herausragender Bedeutung, auch diese Verarbeitung technisch organisatorisch so zu schützen, dass die Rechte der Betroffenen dabei ausreichend Berücksichtigung finden.

Das bringt mich dann auch zur zweiten Frage. Die Frage nach den technisch organisatorischen Maßnahmen in § 32 BDSG. Hier hätte der Gesetzgeber tatsächlich eine Chance nutzen können weitere Ausführungen zu machen. Wir hatten in den alten Landesdatenschutzgesetzen schon Regelungen, die dahin gingen, die Datenschutz-Schutzziele aufzuführen und zu konkretisieren. Wir finden diese Schutzziele auch in Artikel 5, aber in etwas unsystematischer Reihenfolge. Wir haben in Artikel 5 Grundsätze, Prinzipien, Regeln, alles etwas wild durcheinandergeworfen. Hier hätte man ein wenig ordnend eingreifen können, sozusagen in guter deutscher BDSG-Tradition und Hinweise geben können auf die Schutzziele, wie sie zum Beispiel in Schleswig-Holstein, aber auch in vielen anderen Landesdatenschutzgesetzen eingeführt waren. Im Hinblick auf die klassischen Schutzziele der IT-Sicherheit, also Verfügbarkeit, Integrität und Vertraulichkeit und dann angereichert mit den Datenschutz-Schutzzielen der Transparenz, der Nichtverkettung und der Intervenierbarkeit, also der Rechte der Betroffenen. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Jetzt kommen wir zu Herrn Dr. Brink.

SV **Dr. Stefan Brink** (LfDI des Landes Baden-Württemberg, Stuttgart): Vielen Dank. Ich habe vier Fragen zu beantworten.

Da ist zunächst die Frage von Herrn Abgeordneten Haug zur Thematik Videoüberwachung, § 4 BDSG neu. Zum Hintergrund der Regelung, die ja aus

früheren Zeiten stammt, die ja schon, bevor wir uns mit der Umsetzung der DSGVO befasst haben, ins BDSG hineingekommen ist. Hintergrund war ein offensichtliches Missbehagen des damaligen Innenministers mit der Aufsichtspraxis der Landesbehörden, der Landesdatenschutzbeauftragten. Aus seiner Sicht waren wir zu streng und haben zu viele Videoüberwachungen unterbunden. Deswegen hat man den § 4 ergänzt um eine Hilfestellung für Aufsichtsbehörden bei der Frage, wie wägen wir die Überwachungszwecke mit den gegenläufigen Interessen sinnvollerweise ab. Im Ergebnis hat es in unserer Praxis dazu geführt, dass wir es in vielen Bereichen nur noch schwer haben, Videoüberwachung wieder einzuschränken. Nehmen Sie mal einen Parkplatzbetreiber oder einen Supermarktbetreiber, der uns gegenüber vorträgt, ja, er hätte die Kamera nicht nur gegen Ladendiebstahl und Ähnliches aufgestellt, sondern auch zum Schutz von Leben, Gesundheit oder Freiheit von den Personen, die sich im Supermarkt oder auf dem Parkplatz aufhalten, vor Terroristen, vor Überfällen, vor was auch immer. Unterm Strich haben wir ja größte Probleme, diese Argumente zu entkräften oder damit sinnvoll umzugehen und wir verlagern eine Aufgabe, die ursprünglich unseren Sicherheitsbehörden zugestanden hat. Nämlich zu entscheiden, in welchem Kontext bestimmte eingreifende Maßnahmen geboten sind, wo es tatsächlich eine Gefahr ist – von mir aus auch – eine terroristische Gefahr gibt und wo nicht. Wir verlagern das auf den Parkplatzbetreiber und den Supermarktbetreiber. Das ist eine ganz ungute Entwicklung, die uns in der Praxis erhebliche Schwierigkeiten bereitet.

Zweite Frage, Herr Höferlin. Was für Kriterien finden wir, um die Bestellpflicht für betriebliche Datenschutzbeauftragte abzufedern? Ja, wir haben im Moment in Deutschland eine überschießende Bestellpflicht, ohne jeden Zweifel. Ich würde meinen und da stimme ich der Bundesregierung aus den Jahren 2012, 2013, 2014, 2015, 2016 vollkommen zu. Wir haben gute Erfahrungen damit gesammelt und wir sollten versuchen, dieses Modell weiterhin in Europa zum Standard zu machen und nicht deswegen aus dem Modell auszusteigen, weil es offensichtlich in Europa keine Mehrheit gefunden hat. Ich glaube, das Modell ist gut. Ihr Vorschlag eine Beschränkung vorzunehmen auf solche Unternehmen oder Betriebe, die besonders sensible Daten verarbeiten oder datenschutzrelevante Daten verarbeiten, kann mich allerdings nicht überzeugen. Wenn es um sensible Daten geht, bin ich ohnehin regelmäßig im Bereich der Datenschutzfolgenabschätzung, die vorgenommen werden muss, und dadurch habe ich eine ganz eigene Bestellpflicht. Das heißt, das wäre also kein adäquater Ersatz. Und die Frage, welche Daten sensibel sind, welche belangvoll sind, welche besonders geschützt werden müssen, stellt sich inzwischen eigentlich nicht mehr. Dadurch, dass wir die Verwendungskontexte von Daten nicht mehr vorhersagen können, dass wir keine Ahnung haben, welches personenbezogene Datum sich in dem weiteren Verlauf als relevant oder irrelevant erweist, können wir diese Unterscheidung nicht mehr vornehmen. Das war ja das Gegenmodell, das auch auf europäischer Ebene diskutiert worden ist. Wir steigen ein in einen risikobasierten Datenschutz und kümmern uns nur noch um belangvolle, besonders sensible Daten. Ich bin heilfroh, dass diese Debatte zu einem Ende gekommen ist. Ich bin heilfroh, dass Artikel 6 der DSGVO das Gegenteil geregelt hat und deswegen sollten wir die Debatte auch nicht sozusagen an dieser Stelle wieder einführen.

Zum Thema öffentliches Interesse und Konkretisierungspflicht des nationalen Gesetzgebers. Da hat Frau Bock schon alles gesagt, was man dazu sagen kann. Noch eine Ergänzung von meiner Seite aus. Auch da lernen wir gerade um. Ich würde Ihnen vollkommen zustimmen mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts zur Konkretisierungspflicht des Gesetzgebers. Da würde ich sagen, ja das ist ein Fall. Das wird sozusagen gerichtliche Resonanz haben, wenn wir das so regeln. Wie der EuGH damit umgeht, weiß ich schlicht und ergreifend nicht. Auch da müssen wir dazulernen. Da müssen wir unsere Perspektive vom nationalen in den europäischen Raum lenken und dabei sind wir. Schwer vorherzusagen.

Gleiche Antwort zunächst mal an Sie, Herr von Notz, mit der Frage, wie gehen wir um mit der Vorratsdatenspeicherung, die vorgesehen ist in dem BDBOS. Ganz kurze Antwort darauf. Die Bundesbeauftragte hat Recht. Ja, sie hat Recht, wenn sie sagt, es laufen noch Gerichtsverfahren darüber. Lasst uns doch erstmal abwarten, was dort entschieden wird. Es ist vielleicht nicht so klug, gerade ein solches Gesetzgebungsverfahren dazu zu nutzen oder damit zu belasten eine Thematik anzusprechen, die in absehbarer Zeit reguliert wird.

Und ja, es bestehen erhebliche Zweifel an der Verhältnismäßigkeit einer so langen anlasslosen Speicherung, Zitat Bundesbeauftragte. Da hat sie vollkommen Recht.

Letzter Aspekt: Das wird ja nicht dadurch besser, dass zukünftig nicht das Bundesverfassungsgericht, sondern der Europäische Gerichtshof darüber entscheidet. Der EuGH hat deutlich strengere Maßstäbe, was die Vorratsdatenspeicherung angeht und das finden wir ganz toll. Wir sind dem Bundesverfassungsgericht dankbar, dass er den Datenschutz seit den 80er Jahren gepusht hat. Aber was der EuGH dort macht, ist deutlich weiter. Deswegen man muss – glaube ich – kein Hellseher sein, um die Frage zu beantworten, die Sie gestellt haben. Aber ich überlasse das mal den Gerichten.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Der nächste in der Runde ist dann Herr Dr. Engeler.

SV **Dr. Malte Engeler** (Richter beim Schleswig-Holsteinischen Verwaltungsgericht, Kiel): Ich nehme wahr, dass die Frage ein bisschen zufällig an mich gelangt ist. Von daher beschränke ich mich auf ganz kurze Ergänzungen. Also an Ihrer Frage zu Herrn Dr. Brink. Ich würde nur noch darauf hinweisen wollen, dass meiner Ansicht nach, nach wie vor in Absatz 2 Transparenzpflichten nicht den Anforderungen des Artikels 12 ff. genügen. Da hat die Landesbeauftragte für den Datenschutz in Niedersachsen schon klargestellt, dass sie eine deutlich weitergehende Informationspflicht empfehlen, die also über das hinausgeht und auch verlangen, was § 4 verlangt. Auch unklar ist immer noch, woher diese weitergehende Einschränkung der Transparenzpflicht denn überhaupt, aus welcher Öffnungsklausel die denn folgen soll. Und dann ist immer noch der immer wieder gleiche Hinweis auf die Möglichkeit der Weiterverarbeitung in § 4 Absatz 3 Satz 2, der im Grunde mit Hinblick darauf, dass die Erhebung quasi schwerer zu kontrollieren ist, besonders kritisch zu sehen ist. Denn wenn die Weiterverarbeitung im Grunde zu Zwecken der Verfolgung jedweder Straftaten möglich ist und dann sind da schnell auch Bagatelldelikte drin. Mit Blick darauf, dass die Erhebung also – ich sage mal – schwerer zu kontrollieren ist und dann die Weiterverarbeitung für jede Art von Straftaten ermöglicht werden soll, halte ich das in der Tiefe für unverhältnismäßig.

Frau Esken, auch an Sie vielen Dank für die Frage, wo es Bedarf angesichts der uneinheitlichen Regelungen in den Landesmediengesetzen und Landespressegesetzen gibt. Stichwort Blogger. Die Länder verweisen in ihren Landesmediengesetzen in der Regel auf die Rundfunkstaatsverträge und die privilegieren da solche – ich sage mal – Anbieter von Telemedien mit journalistisch-redaktionellen Inhalten, die Daten zu journalistischen Zwecken verarbeiten. Das Problem ist, dass Blogger in der Regeln nicht journalistisch-redaktionell arbeiten, sind also in aller Regel schon raus. Wären sie drin, könnten sie sich da über eine freiwillige Unterwerfung unter Pressekodex und Presserat ein bisschen dem Datenschutzregime entziehen, aber diese Privilegierung steht ihnen schlicht nicht offen, weil in aller Regel sie nicht häufig genug oder in redaktioneller Form journalistisch tätig sind und deswegen in den Genuss dieser Privilegierung nicht gelangen. Das Gleiche betrifft Landespressegesetze. Die Blogger sind in der Regel nicht als verfasste Presse zu verstehen, so dass sie dort auch nicht erfasst sind. Das heißt, die Privilegierung für Presse und Rundfunk, die greift nicht. Gleichzeitig sind die Blogger aber auch über der Schwelle der rein privaten Tätigkeit. Also auch das hilft ihnen nicht. Das heißt, sie befinden sich da in so einem Schwebezustand zwischen Privilegierung und vollem Datenschutzregime und genau für diesen Bereich braucht es dann eben entsprechende Regelungen.

Das betrifft aber nicht nur Blogger. Das betrifft im Grunde sämtliche Ausübung, der in Artikel 5 GG erfassten Freiheiten. Also PR-Arbeit von Unternehmen, Kunstfreiheit, Literatur, Wissenschaft. Im Grunde alles, was nicht bereits im Landesrecht durch Presse abgedeckt ist, ist bisher noch offen. Das sind Fotojournalisten, Fotodatenbanken. Im Grunde alles, was in Artikel 5 gefasst sein kann. Die Frage ist da im Grunde, wer regelt es. Also es muss unbedingt geregelt werden, die Frage ist nur, wer regelt es. Und da gibt es interessante Diskussionen, wo eigentlich die Kompetenz für den Datenschutz herkommt und wen sie trifft.

Die ganz herrschende Ansicht sagt, das ist eine Annex-Kompetenz, folgt also den einzelnen Kompetenznormen im Grundgesetz als Annex. Und hier würde ich tatsächlich sagen, dass abseits der Presse in der Regel die Kompetenz beim Bund liegt. Man kann da ein bisschen kreativ werden. Also zum Beispiel der ganze Bereich der allgemeinen Meinungsäußerung. Das ist also die normale Person,

die in irgendeinem sozialen Netzwerk eine Meinung äußert. Da würde ich sagen, mit guten Gründen kann man das an das bürgerliche Recht in Artikel 74 Absatz 1 Nr. 1 GG andocken. So dass wir also im Grunde abseits der verfassten Presse und des Rundfunks auf Seiten des Bundesgesetzgebers für sämtliche Bereiche die Kommunikationsgrundrechte betreffend einen Handlungsauftrag sehen.

Und warum ist das noch so entscheidend wichtig? Das würde ich gerne noch erwähnen unter dem Stichwort Chilling effects, die Unwägbarkeiten, dass bei der Ausübung der Meinungsfreiheit, Ausübung der Kunstfreiheit irgendwelche Online-Literaturprojekte auf einmal der gesamte Pflichtenkatalog der DSGVO auf mich einprasselt, kann dazu führen, dass die Bereitschaft zur Ausübung dieses grundrechtlich geschützten Bereichs gemindert wird. Und das Bundesverfassungsgericht spricht in diesem Kontext immer von solchen Vorfeldeinschüchterungen, die mit unserer freiheitlichen Gesellschaft unvereinbar sind. Und die Liste der möglichen – ich sage mal – einschüchternden Effekte der Grundverordnung auf diese ganzen Bereiche sind einfach sehr lang. Ein ganz, ganz entscheidender Punkt ist zum Beispiel Artikel 14. Der verpflichtet jeden Verantwortlichen und verantwortlich, wenn Sie bei Twitter irgendwie eine Meinung äußern, sind Sie. Er verpflichtet also Sie dazu, dass Sie Kontaktdaten des Verantwortlichen offenbaren. Das heißt im Grunde nichts anderes, als eine Klarnamenpflicht in sozialen Netzwerken über den Umweg der DSGVO. Und das ist eine Regelung, die auf den offenen Meinungsaustausch schlicht nicht passt.

Ebenso kritisch Artikel 18, der also auf Hinweis des Betroffenen dazu führt, dass wenn er die Richtigkeit der Daten bestreitet, Sie, solange Sie die Richtigkeit nicht bewiesen haben, die Verarbeitung ja nicht fortführen können. Das ist also ein Instant-Maulkorb im Meinungsäußerungsaustausch, der die Grundverordnung an dieser Stelle zu einem wirklich gefährlichen Werkzeug gegen Meinungsfreiheit machen kann. Ebenso kritisch Schadensersatzansprüche. Kritisch auch Zweckbindungsgrundsatz. Sie wissen schlicht in der nicht verfassten Presse, also im Journalismus, Sie wissen nicht während der Recherche, welche Daten wann wichtig sind. Da ist der Zweckbindungsgrundsatz schlicht nicht angemessen und vor allem am Ende – auch da nochmal der Hinweis – die Möglichkeit, einem mir unliebsamen Meinungsäußernden irgendwie einen Brief zu schreiben und zu sagen, ich zeige Sie jetzt bei der Aufsichtsbehörde an und dann auf die ganzen Pflichten der Aufsichtsbehörde zu verweisen, die kann auch einschüchternd sein. Und wir sehen – wie gesagt – in anderen EU-Mitgliedsstaaten, dass die Aufsichtsbehörden auch instrumentalisiert werden. Gar nicht unbedingt wahrscheinlich absichtlich, aber jedenfalls instrumentalisiert werden, um gegen Journalisten – und das kann man übertragen auf Presse, auf Kunst – vorzugehen und da eben einen einschüchternden Effekt auf diese grundrechtlich geschützten Bereiche auszuüben. Soviel erstmal dazu.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir noch zum Abschluss zu Herrn Prof. Köhler. Er hat noch zwei Fragen zu beantworten.

SV **Prof. Dr. Helmut Köhler** (Ludwig-Maximilians-Universität, München): Herr Henrichmann, Sie haben angedeutet, ob wir vielleicht sagen könnten, dass das UWG in diesen Fällen doch irgendwie zur Anwendung kommen könnte. Dazu auch eine Bemerkung an Sie gerichtet, Frau Gurkmann als Vertreterin der Verbraucherschutzverbände: Es ist mitnichten meine Absicht, die Aktivitäten der Verbraucherschutzverbände einzuschränken. Ich will Sie nur auf den richtigen Weg bringen. Was das UWG angeht, haben Sie mit Recht die „Freunde finden“-Entscheidung des BGH angesprochen, aber das ist – wenn ich mich recht erinnere – nicht eine Entscheidung zu § 3a UWG, sondern zu § 7 UWG zum Tatbestand der belästigenden Werbung, weil die Werbung ohne die Einwilligung der Werbeadressaten erfolgt ist. Das ist der springende Punkt.

Ich will jetzt noch ein anderes Beispiel nennen, weil das sehr wichtig ist, um den Anwendungsbereich der DSGVO von dem Anwendungsbereich des UWG abzugrenzen. Selbstverständlich können die Verbraucherverbände nach UWG vorgehen, auch wenn ein Zusammenhang mit einem Datenschutzverstoß vorliegt, aber nicht isoliert wegen des Datenschutzverstoßes, sondern nur wenn zusätzlich wirtschaftliche Interessen von Verbrauchern beeinträchtigt sind. Ich mache es an einem Beispiel jetzt deutlich, das jeder verstehen wird: Ein Profi-Fußballer verwendet ein bestimmtes Schmerzmittel. Das bekommt der Hersteller dieses Schmerzmittels mit und er verwendet ohne Einwilligung des Fußballers die Tatsache, dass dieser das Schmerzmittel verwendet, in seiner Werbung.

Dann ist das sicher ein Datenschutzverstoß, weil er eben die Daten ohne Einwilligung für einen bestimmten Zweck verwendet, nämlich für den Werbezweck im Sinne der Direktwerbung. Aber sind dadurch wirtschaftliche Interessen von Verbrauchern beeinträchtigt? Was würden Sie meinen?

SVe **Jutta Gurkmann** (Verbraucherzentrale Bundesverband e.V. (VZBV), Berlin): Nicht.

SV **Prof. Dr. Helmut Köhler** (Ludwig-Maximilians-Universität, München): Also, den Verbrauchern ist das doch relativ egal. Genauer: Wenn der Fußballer wirklich dieses Mittel zur Schmerzlinderung einnimmt, dann ist es den Verbrauchern relativ egal, ob dieser in die Werbung eingewilligt hat oder nicht. Das ist eher ein Problem für den Fußballer. Und jetzt ändere ich den Fall ein klein bisschen: Der Fußballer verwendet gar nicht dieses Schmerzmittel, aber der Hersteller glaubt irrtümlich, dass dies so sei, und wirbt jetzt in gleicher Weise. Dann ist es etwas anderes, nämlich ein Fall der irreführenden Werbung im Sinne von § 5 UWG. Sind wir uns einig? Und das ist meine Grundaussage. Diese irreführende Werbung können die Verbraucherverbände selbstverständlich angreifen, weil die Verbraucher durch diese Werbung getäuscht werden.

Und jetzt eben nochmal der Satz: Verbraucherverbände haben für ihr Tätigwerden einen echten Anwendungsbereich im UWG, wenn es sich tatsächlich bei der betreffenden Maßnahme, die man angreift, um einen Verstoß gegen die wirtschaftlichen Interessen der Verbraucher handelt. Und das gleiche entsprechend bei § 7 UWG. Wenn Verbraucher Werbung zugeschickt bekommen, ohne dass sie darin eingewilligt haben, ist es ein selbständiger UWG-Verstoß nach § 7 UWG, aber kein Verstoß gegen § 3a. Das wollte ich dazu sagen.

Jetzt aber nochmal zur Abmahnung. Die Abmahnwelle – Sie haben ja die vielen Unternehmen in Ihrem Einzugsbereich angesprochen – die Abmahnwelle wäre schon längst über uns hereingebrochen, und zwar gegenüber Unternehmen jeder Größenordnung, wenn nicht diese Rechtsunklarheit bestünde: Nämlich, ob Mitbewerber – in erster Linie geht es um Mitbewerber und deren Anwälte – wenn nach § 3a UWG abmahnen können oder nicht. Ich weiß das übrigens aus der Praxis. Da zögern die Anwälte, denn es steht dann viel auf dem Spiel.

Und jetzt gibt es zwei Möglichkeiten, diese Unklarheit zu beseitigen. Entweder man wartet ab, bis einmal ein Rechtsstreit über diese Frage zum BGH kommt und anschließend dann legt der BGH diese Frage mit Sicherheit dem EuGH vor. Dann bekommen wir Rechtsklarheit in wie vielen Jahren etwa? Vier, oder was? Aber damit ist doch niemanden hier im Lande gedient, dass wir eine so lange Rechtsunsicherheit haben. Oder der Gesetzgeber entscheidet die Frage. Dann entweder in dem Sinne, dass man die Verbände auch im Bereich des UWG tätig werden lässt nach Maßgabe des § 3a, was aus meiner Sicht unionsrechtswidrig ist. Das ist übrigens im Referentenentwurf zum Gesetz zur Stärkung des fairen Wettbewerbs vorgeschlagen worden. Ich mache Sie nur darauf aufmerksam. Es sind fünf Worte in der Begründung dieses Gesetzentwurfs enthalten, die das Problem in diesem Sinne lösen, und zwar in einer versteckten Art und Weise, sodass man es eigentlich gar nicht merkt. Denn da steht drin, Abmahnungen dürfen unter anderem dann nicht kostenpflichtig sein, wenn es sich um die Verletzung von datenschutzrechtlichen Regelungen und um kleine Unternehmen handelt. Das ist Schmuggelware, entschuldigen Sie den Ausdruck. Da wird sozusagen durch die Hintertür, ohne dass man es fast merken könnte, eine Entscheidung dieser Grundsatzfrage herbeigeführt. Denn jeder wird doch sagen, wenn er das Gesetz liest: Aha, Datenschutzverstöße sind grundsätzlich kostenlos abmahnfähig, nur ausnahmsweise dann nicht, wenn es sich um ein kleines Unternehmen usw. handelt.

Ich mache Sie nur darauf aufmerksam, wenn Sie diesem Gesetz in dieser Form zustimmen, dann entscheiden Sie diese Frage im Sinne einer Anwendung des UWG auf reine Datenschutzverstöße.

Die andere Möglichkeit ist die, ….

Vors. **Andrea Lindholz** (CDU/CSU): Ich guck ein bisschen auf die Uhr.

SV **Prof. Dr. Helmut Köhler** (Ludwig-Maximilians-Universität, München): Die andere Möglichkeit ist die Klarstellung in der Weise, dass man in das Bundesdatenschutzgesetz eine Regelung einführt – meinetwegen auch in der Gesetzesbegründung – dass Datenschutzverbände (im Sinne des Artikel 80 Absatz 2 DSGVO, das muss man noch ergänzen), nicht berechtigt sind, Datenschutzverstöße nach Maßgabe des § 3a UWG zu ahnden. Dann könnte man auch

noch hinzufügen, dass eine Anwendung anderer UWG-Vorschriften ohne weiteres möglich bleibt. Das wollte ich noch dazu sagen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank.

Ganz kurz nochmal zur Frage der Bundesdatenschutzbeauftragten, nachdem ich jetzt alle Unterlagen vor mir liegen habe. Die Stellungnahme der Bundesdatenschutzbeauftragten ist am 26. Oktober 2018 eingegangen und zeitgleich an alle Fraktionen verteilt worden. In der Obleuterunde am 7. November 2018 haben wir die Anhörungen besprochen. Insgesamt drei Stück, u. a. auch die Modalitäten für heute und zwar unter 2.c. Es wurde dort der übliche Schlüssel vereinbart. Neun Sachverständige, drei, zwei, eins, eins, eins, eins. Es wurde zusätzlich nicht beantragt, die Bundesdatenschutzbeauftragte vor die Klammer zu ziehen. Es wäre jeder Fraktion darüber hinaus unbenommen gewesen, die Bundesdatenschutzbeauftragte als Sachverständige zu benennen. Zum Verständnis unter Ziffer 2.b haben wir über eine andere Anhörung beraten und dort haben wir auch eine Person oder eine Vertretung vor die Klammer gezogen. Ich empfehle also, dass das vielleicht zukünftig in den Fraktionen abgesprochen wird. Der Grundsatz, jemand vor die Klammer zu ziehen, ist auch nur dann eben möglich, wenn es eine Mehrheitsentscheidung gibt. Darauf haben sich die Obleute auch verständigt. Ein Rechtsanspruch darauf besteht nämlich ansonsten grundsätzlich nicht.

Der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN ist eingegangen am Dienstag um 09:44 Uhr, er ist versandt worden am Dienstag um 12:57 Uhr, wie üblich, wie auch bei allen anderen Anträgen von Fraktionen. Hierauf erfolgte keine Reaktion einer Fraktion. Diesem Antrag hat sich demnach auch keiner angeschlossen. Insofern will ich das nur so für uns festhalten. Bei uns ist das insofern ordnungsgemäß abgelaufen.

Damit setze ich das jetzt hier auch fort und komme dann zur zweiten Fragerunde und dementsprechend …

Herr von Notz, Sie brauchen nicht den Kopf zu schütteln, sondern ich empfehle Ihnen, das einfach an anderer Stelle zu klären.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich lasse mir nicht vorschreiben, wann ich mit dem Kopf schütteln darf!

Vors. **Andrea Lindholz** (CDU/CSU): Naja, es ist ja wirklich, das muss ich jetzt ehrlich sagen, es ist ja …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich sehe es ganz anders.

Vors. **Andrea Lindholz** (CDU/CSU): Dann müssen Sie das aber an anderer Stelle klären. Verfahrenstechnisch ist hier alles ordnungsgemäß abgelaufen.

Und jetzt kommen wir dann zur Fraktion CDU/CSU. Herr Henrichmann nochmal.

Abg. **Marc Henrichmann** (CDU/CSU): Ja, gerne. Ich bleibe nochmal so ein bisschen bei dem Thema KMU, Ehrenamtler, Vereine und Herr von Notz hat vorhin gesagt, die hätten ja bloß Angst, man müsse sich nicht kümmern. Ich halte das für brandgefährlich. Denn ich glaube zum einen, wir setzen damit die ehrenamtlichen Strukturen aufs Spiel, wenn wir die Menschen da alleine lassen und zum zweiten glaube ich, dass der Grundgedanke des Datenschutzes über Bord fällt, wenn wir uns da nicht ein bisschen kümmern und vielleicht auch differenzieren soweit möglich. Und in diesem Geiste möchte ich zwei Fragen an Prof. Dr. Schröder stellen. Zum einen bei den Bußgeldregelungen. Die Österreicher haben sich da ja was Besonderes einfallen lassen. Das wird ja zu Recht sehr kritisch gesehen. Aber sehen Sie hier beispielsweise noch Spielräume für nationale Regelungen, insbesondere eine Differenzierung vielleicht was Verwarnungen angeht, Fahrlässigkeitsfälle angeht. Braucht es diese überhaupt oder ist das vor dem Grundsatz des Verhältnismäßigkeitsgrundsatzes eh alles sozusagen schon immanent? Und das zweite Thema wäre dann eben, gibt es noch Regelungsspielräume, die der nationale Gesetzgeber vielleicht nicht genutzt hat, gerade vor dem Lichte der KMU, Vereine, Ehrenamtler, was Informations- und Auskunftspflichten angeht, Verarbeitungsverzeichnisse hatten Sie selber vorhin genannt. Sehen Sie da in irgendeiner Form überhaupt noch Spiel, um den Betreffenden da entgegen zu kommen? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kämen wir als nächstes zu Herrn Haug.

Abg. **Jochen Haug** (AfD): Dankeschön Frau Vorsitzende. Zwei Fragen an Herrn Dr. Engeler. Und zwar eine nochmal zu der Abmahnproblematik. Sie hatten in Ihrer Stellungnahme vorhin angemerkt, es

gab keine oder es habe keine Abmahnwelle gegeben, aber es bestehe durchaus ein Abmahnrisiko. Und meinten dann, gegen dieses Abmahnrisiko müsse etwas getan werden. Das müsse aber strukturell geschehen. Meine Frage dazu, was verstehen Sie unter strukturell und welche konkreten Vorschläge hätten Sie dazu? Und der zweite Fragekomplex, da geht es darum, dass seit Einführung der DSGVO Unklarheit herrscht, unter welchen Voraussetzungen Fotografien von Personen zulässigerweise erstellt, genutzt und im Internet veröffentlicht werden dürfen. Da wäre meine Frage, sehen Sie gesetzlichen Regelungsbedarf und wenn ja, welchen. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zu Frau Esken.

Abg. **Saskia Esken** (SPD): Lieber Kollege Henrichmann, ich glaube, kein Abgeordneter könnte nicht sagen, in seinem Bereich, in seinem Wahlkreis gäbe es viele kleine und mittlere Unternehmen. Vielleicht der Bonner Abgeordnete, der hat vielleicht ein paar größere und vor allem Bundesbehörden. Aber ansonsten haben wir im Allgemeinen alle kleine und mittlere Unternehmen und Vereine bei uns in den Wahlkreisen und haben selbstverständlich auch die Aufgabe, uns um die zu kümmern und uns auch um deren Verunsicherung zu kümmern. Wir sind uns nur über die Wege uneinig, was da der richtige Weg wäre. Meiner Auffassung nach, das habe ich auch schon öfter so gesagt, hätten wir die Aufgabe gehabt und haben sie auch immer noch – nicht als Gesetzgeber, sondern als ausführendes Organ und damit spreche ich das BMI an, das jetzt leider nicht mehr da ist – eben die Umsetzung von Gesetzen draußen im Lande auch entsprechend zu unterstützen. Und das bedeutet, dass wir zum einen natürlich Informationskampagnen, aber eben auch Beratungs- und Unterstützungskampagnen durchaus finanzieren dürfen auch als Staat, um die Unterstützung in den Unternehmen und Vereinen entsprechend ankommen zu lassen und dann möglicherweise die teils nicht immer hilfreiche Beratung, die von dem einen oder anderen selbst berufenen Berater draußen verbreitet wird und diese zu mehr Unsicherheit als zu Sicherheit führt, eben auch sozusagen zu unterfüttern.

Ich will nochmal zum Thema Abmahnungen jetzt in dem Fall Frau Gurkmann ansprechen. Wir wissen alle, dass der Koalitionsvertrag die wichtige Zielsetzung enthält gegen missbräuchliche Abmahnungen vorzugehen, nicht nur in Bezug auf den Datenschutz eben, sondern auch in Bezug auf andere Tatbestände und wir haben heute Morgen, wer das liest im Tagesspiegel Background, erfahren dürfen, dass dieser Gesetzentwurf, der vom BMJV bereits erarbeitet wurde, auch in dieser Woche in der Koalitionsrunde auf der Tagesordnung steht. Und deswegen frage ich jetzt tatsächlich, wie könnte aus Ihrer Sicht Frau Gurkmann eine sinnvolle gesetzliche Lösung aussehen, die Abmahnungen als Geschäftsmodell auf der einen Seite unattraktiver macht, aber eben keine komplette Bereichsausnahme, auch nicht für DSGVO-Verstöße, beinhaltet. Und wenn wir tatsächlich jetzt so vorgehen würden, wie manche es vorschlagen, welche faktischen Auswirkungen würden Sie sehen für Verbraucherschutzverbände, wenn Abmahnungen nach UWG für DSGVO-Verstöße grundsätzlich nicht mehr möglich wären.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir als nächstes zu Herrn Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke Frau Vorsitzende. Ich habe eine Frage an Herrn Dr. Brink und an Herrn Prof. Schröder. Und zwar, wenn wir jetzt schon mit der Situation konfrontiert sind ein Gesetz zu haben, das Anpassungen und materielle Änderungen hat, wäre es vielleicht nicht möglich gewesen, im Bereich der über die Anpassungen hinausgehenden Bereiche konkrete Vorschläge zu machen, wie zum Beispiel Vereine und kleine mittelständische Unternehmen entlastet würden, dort wo es Öffnungsklauseln gibt. Und meine Frage an Sie ist, wo sehen Sie beide da Möglichkeiten. Gibt es da vielleicht Dinge, die man relativ einfach hätte einpflegen können? Herr Prof. Köhler hat ja gerade eben den Hinweis auch auf das im Referentenentwurf vorliegende Gesetz zu den Abmahnungen nach UWG gemacht. Da hätte man vielleicht auch etwas rausnehmen können, als offene Frage, oder eben in sonstigen Bereichen, sei es jetzt bei Einzelregelungen oder bei ganzen Gestaltungen.
Wo könnte man was machen? An Sie beide, Herrn Prof. Dr. Schröder und Herrn Dr. Brink bitte.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Höferlin, vielen Dank. Jetzt kommen wir noch zu Frau Pau.

Abg. **Petra Pau** (DIE LINKE.): Ja, ich habe noch eine Frage an Frau Bock und ggf., wenn er etwas dazu sagen kann, auch an Herrn Dr. Brink.

Frau Bock, Sie schreiben zu Artikel 5, also Änderung des Rechtsextremismusdateiengesetzes, dass in diesem Entwurf auf die eigentlich geforderte gemeinsame Verantwortlichkeit für die Daten nicht eingegangen wird. Könnten Sie uns nochmal erläutern oder etwas dazu sagen, wie dann die Aufsicht von einer Bundes- oder Landesbehörde gemeinsam aussehen könnte bei einer solchen gemeinsam geführten Datei. Und außerdem interessiert mich in diesem Kontext auch, welche Konsequenzen der Wegfall der bislang beispielsweise im BKA-Gesetz vorgesehenen Errichtungsanordnung in diesem Kontext hat.

Vors. **Andrea Lindholz** (CDU/CSU): Und den Abschluss macht Herr von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Danke Frau Vorsitzende. Ich habe zwei Fragen an Herrn Prof. Aden. Die erste nochmal zu der Bestellpflicht, die ja doch abgesenkt werden soll und ich kann mich ganz gut erinnern, im Jahr 2013 war ja Edward Snowden so ein Thema. Da hat die Bundeskanzlerin im Juni da unten, genau da unten in dem Spreebogen ein Interview gegeben und hat gesagt, alle müssen sich keine Sorgen machen, bald kommt die DSGVO. Jetzt mal neben der Sache, was das Eine mit dem Anderen genau zu tun hat. Ein Versprechen ist von allen gemacht worden seitens der Bundesregierung. Nämlich, dass das deutsche Datenschutzniveau im Kontext der DSGVO nicht abgesenkt wird. Das war das große Versprechen. Das hohe deutsche Datenschutzniveau war übrigens ganz oft ein Argument auch des Bundesinnenministeriums in Europa sehr auf die Bremse zu drücken bei vielen Sachen. Deswegen meine Frage. Wie verträgt sich eigentlich diese Absenkung der Bestellpflicht mit diesem Versprechen?

Und das Zweite ist: Die DSGVO gibt ja vor, eigentlich dass das Verhältnis bezüglich der DSGVO selbst und den bereichsspezifischen Telekommunikationsgesetzen geregelt wird. Wird es aber nicht. Zumindest können wir es nicht erkennen. Und die BfDI, aber auch die europäische Akademie für Datenschutz mahnt das ja an. Und die Frage, wenn eine solche Regelung fehlt, was bedeutet das eigentlich für die Datenschutzaufsicht und wie ist dann die Situation in diesem Bereich? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann gehen wir jetzt im Alphabet in umgekehrter Reihenfolge vor und würden beginnen mit Herrn Prof. Dr. Schröder.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank für die Fragen. Zum Thema Bußgelder: Also sicherlich ist das, was die Österreicher gemacht haben, da nicht mit Europarecht vereinbar. Ich würde sagen, die Bußgeldbestimmungen in der DSGVO sind abschließend. Aber in der Tat ist es nicht so, dass für jeden kleinen Datenschutzverstoß möglicherweise vier Prozent des Jahresumsatzes oder ein zig Millionen betragendes Bußgeld verhängt wird. Wir haben im Artikel 83 detaillierte Vorgaben für die Verhältnismäßigkeitsprüfung und wir haben ja tatsächlich auch in der DSGVO geregelt, dass nicht in jedem Fall ein Bußgeld verhängt werden muss. Der Artikel 83 verweist ja selbst noch auf den Artikel 58, nach dem man es bei einer Verwarnung bewenden lassen darf. Ich glaube nur, was eben nicht geht, ist, dass der Gesetzgeber jetzt den unabhängigen Datenschutzaufsichtsbehörden, die das ja auch dafür sind, um darüber zu entscheiden, eine Vorgabe macht und quasi schon mal vordefiniert, diese Fälle sind so belanglos, dass bitte da nichts verhängt wird. Das ist mit der Regelungsstruktur der Verordnung – glaube ich – nicht vereinbar, sondern man muss letztlich darauf vertrauen, dass die Datenschutzaufsichtsbehörden in diesen Fällen es bei einer Verwarnung seien Bewenden haben lassen, kann sie aber nicht dazu zwingen. Natürlich bleibt es dem betroffenen Unternehmen, das ein Bußgeld bekommt, unbenommen, vor die Gerichte zu ziehen und zu sagen, das wäre aber eigentlich ein Fall gewesen, wo eine Verwarnung gereicht hätte. Das müssen dann die Gerichte entscheiden.

Zu den Erleichterungsmöglichkeiten bei den Informationspflichten, und das beantwortet dann vielleicht auch die zweite Frage gleich mit. Ja, wir haben den Artikel 23 der Verordnung, der es aber nur unter sehr begrenzten Voraussetzungen ermöglicht, von den Betroffenenrechten Abstriche zu machen. Es wird ja teilweise sowieso schon kritisiert, wie das in Deutschland ausgenutzt wird, Stichwort Melderecht. Aber ohne da jetzt näher drauf eingehen zu wollen, glaube ich, dass wir da ziemlich am Ende der Fahnenstange sind und es keine weiteren Möglichkeiten gibt, wie man gerade einzelne Gruppen von Verantwortlichen – sei es KMU, sei es Vereine, sei es Ehrenamtliche – privilegieren kann. Also insbesondere, was ja der Artikel 23 vorsieht,

dass man da sagt, aus allgemeinen öffentlichen Interessen, also dass man als allgemeines öffentliches Interesse vielleicht die Aufrechterhaltung des Ehrenamts oder der Struktur der Wirtschaft versteht, das würde, glaube ich, zu weit gehen. Also da kann man, muss ich sagen, leider nichts machen und da ist man einfach darauf angewiesen Hilfestellung zu geben, die ja durchaus erfolgen kann.

Und zum betrieblichen Datenschutzbeauftragten, der ja auch als Belastung empfunden wird, habe ich schon vorhin gesagt: Klar, das ist europarechtlich in Ordnung, davon wegzugehen von der bisherigen Regelung in Deutschland, aber ob es sich empfiehlt, steht auf einem anderen Blatt. Ich glaube, die Erleichterung wird tatsächlich überschätzt, weil man ja trotzdem den Sachverstand braucht, um datenschutzkonform im Hinblick auf die materiellen Pflichten zu handeln. Da muss man dann irgendwie den Sachverstand extern einkaufen; das kostet auch wieder Geld. Also da ist die Frage, was die bessere Lösung ist, um dieses Ziel zu erreichen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann wäre als nächstes Frau Gurkmann.

SVe **Jutta Gurkmann** (Verbraucherzentrale Bundesverband e.V. (VZBV), Berlin): Vielen Dank, Frau Esken für die Frage bzw. die Fragen. Sie wollten zunächst wissen, was denn eine sinnvolle Lösung sein könnte, um dem Abmahnmissbrauch zu begegnen. Wir haben von Anfang an unterstützt eine generelle Lösung, um dort wirklich angreifen zu können, wo es Probleme gibt. Und diese sehen wir im Datenschutz derzeit nachweislich nicht. Aber es gibt andere Bereiche, in denen uns auch Beschwerden erreichen. Deswegen sind wir sehr stark dafür, eben keine Bereichsausnahmen für den Datenschutz zu treffen, sondern allgemeine Regelungen zu finden, die vor allem bei der Anreizstruktur ansetzen sollten. Also, warum gibt es insbesondere ja die Wettbewerber, die abmahnen, die massenhaft abmahnen. Und da kommt man dann relativ schnell zum Aufwendungsersatzanspruch und deswegen wäre unser erster Ansatz zu sagen, man sieht sich den Aufwendungsersatzanspruch an und reguliert den nochmal und reduziert diesen entsprechend. Bei uns kostet eine Abmahnung 220 Euro. So günstig bekommen Sie keine Rechtsberatung. Ich glaube, das tut dann an der Stelle auch nicht weh. Und wenn man das gleichmäßig macht, dann kann man damit kein Geld verdienen.

Dann hatten Sie als zweites gefragt nach den faktischen Auswirkungen, wenn man sich der Meinung anschließen würde, dass das UWG keine reinen Datenschutzverstöße sanktionieren kann. Das hätte in der Tat aus unserer Sicht schon gravierende Folgen, indem Rechtsdurchsetzung an der Stelle schwerer würde, an der wir tatsächlich Datenschutzverstöße, aber als Markregulierungsregeln hätten. Also nicht das Persönlichkeitsrecht, sondern wenn Daten da abgezogen würden, wie in der Tat auch bei dem Facebook-Fall, und wir die Situation noch nicht haben, dass damit dann unlauter auch noch Emails versendet werden. Also da haben wir ja tatsächlich zwei Handlungen. Wir hatten in der Tat den Facebook-Fall auch auf § 3a UWG gestützt. Der BGH hat sich dazu nicht geäußert. Die Vorinstanz hatte das bejaht und der BGH hatte das dann auch nicht mehr kritisiert. Deswegen war das unsere Hoffnung, dass der BGH das auch so sehen könnte. Jetzt werden wir sehen, ich glaube im Übrigen, wenn Sie mir den Satz noch erlauben. Ich glaube nicht, dass es vier Jahre dauern wird, bis die nächste Entscheidung kommt. Also bei uns stehen demnächst auch wieder Entscheidungen in verschiedensten Facebook- und Twitter-Verfahren an. Deswegen könnte das durchaus schneller gehen.

Ich möchte noch darauf hinweisen, wenn man insgesamt den Datenschutz aus dem Wettbewerbsrecht komplett rausholen würde, dann könnte man solche Dinge, mit denen ja auch tatsächlich Unternehmen, die ihr Geschäftsmodell auf Daten basieren, könnten wir die im wettbewerbsrechtlich überhaupt nicht mehr bekommen, es sei denn in Verbindung mit unlauterer Werbung, Irreführung usw. Das wäre sehr schwierig. Und auch der § 2 UKlaG hilft uns an einigen Stellen nicht so sehr weiter, weil man dafür bestimmte Zwecke, die Verwendung von Daten zu bestimmten Zwecken braucht, und wir erleben es jetzt mehr und mehr, dass die Unternehmen uns sagen, ja wir verwenden aber die Daten ja gar nicht zu Werbezwecken, sondern wir optimieren unser Angebot und das ist rein in Bezug auf das bestehende Vertragsverhältnis. Also wir brauchen diese Daten, um unseren Vertrag bestmöglich zu erfüllen. Und damit wären wir voraussichtlich auch aus dem § 2 UKlaG raus. Deswegen, wir werden sehen, wie die Gerichte entscheiden. Ich fürchte, ich hoffe, in unserem Sinne möglichst bald. Wenn das nicht der Fall wäre, dann muss man sich dringend überlegen, was man dann tun kann, denn ansonsten hätten wir an der Stelle echt

ein Problem.

Vors. **Andrea Lindholz** (CDU/CSU): Als nächster Herr Dr. Engeler bitte.

SV **Dr. Malte Engeler** (Richter beim Schleswig-Holsteinischen Verwaltungsgericht, Kiel): Zu der ersten Frage, wie das Abmahnproblem lösen? Warum nicht spezifisch im Datenschutzrecht, sondern zentral? Ich glaube einfach, nur um das einfach mal vorweg zu schieben, dass der Datenschutz auch ein Stück entwertet wird, wenn man ihn gerade rauspickt. Also ich kann das mal nur als Beispiel empfehlen. Versuchen Sie mal richtig und sauber Creativ Commons zu zitieren. Als Blogger sind Sie da schnell in der urheberrechtlichen Abmahnung. Also warum Urheberrecht schon und Datenschutz auf einmal ausnehmen? Das Problem ist also nicht, dass Datenschutz besonders anfällig wäre, sondern dass das Abmahnwesen derzeit noch davon profitiert, dass es schlicht wirtschaftliche Anreize gibt, auch gegen Bagatellverstöße und missbräuchlich vorzugehen. Die entscheidenden Maßnahmen sollten daher alle die sein, die verhindern, dass es schlicht wirtschaftlich sinnvoll ist, Bagatellverstöße missbräuchlich zu verfolgen. Die Praxis aus dem Wettbewerbsrecht schlägt hier zum Beispiel vor, das ist nur ein Tipp, unter anderem so vorzugehen, dass man – was jetzt in dem Entwurf steht – die Missbräuchlichkeit durch hohe Vertragsstrafen zu definieren, einfach einen anderen Weg geht. Und zwar zu regeln, dass es in notariellen Unterlassungserklärungen samt der Befugnis der Notare auch die Vollstreckbarkeit der Ordnungsmittelandrohung beurkunden zu dürfen, sodass quasi der Abmahner nur den Staat füttert, wenn er Erfolg hat und nicht sich selber. Und das könnte eben dazu führen, dass er wenig Anreize hat, auch Bagatellverstöße zu verfolgen, gleichzeitig aber für den Verstoßenden gegen die Pflichten, die abgemahnt werden, trotzdem spürbar ist, und so eben dazu führt, dass wir den gleichen Effekt haben, ohne aber diese Fehlanreize hin zu Missbrauch zu haben. Also im Grunde alle Instrumente, die dazu führen, dass es schlicht nicht mehr lukrativ ist, dieses Geschäft zu betreiben.

Zur zweiten Frage KUG oder allgemeine Fotografie. Da reden wir immer um personenbezogene Daten in aller Regel. Es sei denn, Sie fotografieren eine Landschaft. Das heißt, Sie sind im Datenschutzrecht drin. Das Problem ist im Grunde, dass es früher den – oder ja immer noch – das Kunsturhebergesetz gibt und die Frage, ob das weiter gilt ist einfach umstritten. Da gibt es gute Argumente für beide Seiten. Im Grunde ist es aber ein Scheinstreit, denn das KUG regelt nur die Veröffentlichung. Das heißt, es hilft Ihnen überhaupt nicht da weiter, wenn Sie Daten erheben. In dem Moment, wo Sie Fotos schießen, veröffentlichen Sie noch nicht. Das heißt, Sie sind dann ohnehin mitten in der DSGVO, und den gesamten Folgepflichten. Also der Fotograf muss eben die gesamte DSGVO einhalten von Dokumentationspflichten bis hin zu Auskunftspflichten usw.. Das hilft Ihnen also auch nicht weiter. Sie können natürlich versuchen, das KUG in den Artikel 6 Absatz 1 Buchstabe f, das ist die Regelung, die dann gerne hilfsweise herangezogen wird, hineinzulesen, auch auf Ebene der Erhebung. Auch das wird Ihnen nicht weiterhelfen, weil der Artikel 6 Absatz 1 Buchstabe f für öffentliche Stellen zum Beispiel gesperrt ist. Und vor allem hilft Ihnen der Artikel 6 Absatz 1 Buchstabe f auch nicht, um den Artikel 9 drum herum. Also der gesamte Bereich besonders schutzwürdigende Informationen. Fotografien, die zum Beispiel Menschen mit gesundheitlichen Auffälligkeiten abbilden usw., sind dann nicht mehr abgebildet. Und zuletzt noch, auch wenn Sie das KUG in den Artikel 6 Absatz 1 Buchstabe f reinlesen wollen im Bereich der Erhebung, dann müssen Sie das mittlerweile – ganz herrschende Ansicht – europarechtskonform auslegen. Das heißt, auch da ist die Frage. Das KUG sieht keine Erforderlichkeitsgrenze vor zum Beispiel. Die DSGVO schon. Das kann also auch sein, dass Sie dann über das Hineinlesen des KUG im Grunde die alte Wertung so gar nicht fortführen können. Deswegen auch im Bereich Fotografie unbedingt Handlungsbedarf.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu den Antworten von Herrn Dr. Brink.

SV **Dr. Stefan Brink** (LfDI des Landes Baden-Württemberg, Stuttgart): Vielen Dank. Ich habe zwei Fragen zu beantworten. Zunächst die von Herrn Abgeordneten Höferlin. Zum Thema, wie schaffen wir das, die Vereine zu entlasten in dem Bereich und ihnen entsprechend weiterzuhelfen. Die DSGVO gibt dafür nicht viel her. Einen Aspekt hat Herr Prof. Schröder eben angesprochen. Ein zweiter Aspekt ist der Artikel 30 Absatz 5 der DSGVO, wo es

so aussieht, als gäbe es eine Freistellung von kleineren Körperschaften von den Pflichten ein Verarbeitungsverzeichnis zu führen. Wenn man sich das genau anschaut stellt man fest, nein, Artikel 30 Absatz 5 hat so gut wie keinen Anwendungsbereich, führt nicht ernsthaft zu einer Entlastung der Vereine, weil Vereine auch nicht nur gelegentlich Daten verarbeiten und das ist die Voraussetzung von Artikel 30 Absatz 5. Sondern jeder Verein, der irgendwo einen Leitz-Ordner stehen hat und halbwegs kontinuierlich arbeitet, wird nicht nur gelegentlich personenbezogene Daten verarbeiten. Also Entlastungsmöglichkeiten auf Basis der DSGVO sehr schwer etwas hinzubekommen.

Was ich anbieten kann und was wir praktizieren und was auch angenommen wird, ist die Entlastung im Vollzug. Das heißt, dass die Aufsichtsbehörden sich darum kümmern, dass sie differenziert vorgehen, nicht nur bei Bußgeldern, das müssen wir, sondern auch im Rahmen der Aufklärung, im Rahmen der Information. Dass wir dort in erster Linie beraten, wo die Not am Größten ist. Und es ist kein Geheimnis, große Unternehmen kommen mit der DSGVO prima zurecht. Die freuen sich über das Marktort-Prinzip. Die freuen sich über den Onestop-Shop. Da gibt es keine Beschwerden, die mir bisher zu Ohren gekommen wären. Die haben natürlich auch andere Mittel, andere personelle Mittel. Wo das Problem groß ist, ist bei den Vereinen, ist bei den Handwerken, ist bei den kleinen Unternehmen. Und da beraten wir schlicht und ergreifend mehr, als wir es früher getan haben. Wir sorgen dafür, dass es Praxishilfen gibt, dass es FAQ-Listen gibt. Wir haben allein in Baden-Württemberg über 200 Veranstaltungen im laufenden Jahr gemacht zur DSGVO mit über 20.000 Teilnehmern, die wir Face to Face geschult haben.

Aber unsere Mittel sind natürlich auch begrenzt in dem Bereich und wir wären sehr dankbar gewesen, wenn auch von Bundesseite da noch mehr Unterstützung gekommen wäre. Auf Landesebene läuft das schlicht und ergreifend so, dass in erster Linie Landtagsabgeordnete sich um ihren Wahlkreis kümmern. Dort 50, 60, 80 Vereinsvorsitzende zusammentrommeln und dann den Abend zum Datenschutz veranstalten. Das funktioniert. Die Stimmung am Anfang ist denkbar schlecht. Am Ende ist sie meistens besser. Und wir versuchen auch tatsächlich hilfreich zu sein, aber das ist eine große Aufgabe und die wird uns noch über Jahre beschäftigen. Also im Vollzug kann man einiges machen. Aber von der rechtlichen Seite her, sehe ich wenig Möglichkeiten.

Frau Abgeordnete Pau, Sie hatten noch gefragt zum Thema Änderung des Rechtsextremismusdateiengesetzes. Eine kurze Vorbemerkung. Frau Bock kann das besser beantworten als ich es kann. Dort ist vorgesehen eine gemeinsame Verantwortung. Gemeinsame Verantwortlichkeit, was das ist, weiß keiner. Das ist ja im Moment der Zauberbegriff. Auch im nichtöffentlichen Bereich. Der EuGH hat sich ja in Sachen Facebook auf dieses Gebiet begeben und offensichtlich meint jetzt jeder, gemeinsame Verantwortlichkeit sei die Lösung für irgendetwas. Nein, es ist keine Lösung. Es ist auch keine Rechtsgrundlage. Es ist auch sehr unklar, was damit im Einzelnen gemeint ist. Sowas im öffentlichen Bereich zu probieren ist noch problematischer. Wo wir eine viel engere Gesetzesbindung brauchen, also im nichtöffentlichen Bereich. Insofern also gewisse Skepsis, aber Frau Bock kann das noch besser sagen.

Vors. **Andrea Lindholz** (CDU/CSU): Jawohl, da gehen wir gleich weiter. Frau Bock bitte.

SVe **Kirsten Bock** (Kiel): Ja, Dankeschön. Ich will das versuchen. Die Frage knüpft ja auch an, an den Wegfall der Errichtungsanordnung und das hängt auch durchaus miteinander zusammen. Errichtungsanordnungen enthalten Verwaltungsvorschriften, wie mit Dateien und Daten umzugehen ist und zwar verbindlich. Also das sind Sollregelungen, die auch bei einer Prüfung in der Vergangenheit dazu dienen konnten abzugleichen, ob das, was tatsächlich getan wird, auch mit dem übereinstimmt, wie das geplant und vorgesehen und eben in diesen Errichtungsanordnungen auch festgehalten worden ist. Für das, was dort geregelt worden ist, nämlich also Zweck der Datei, die Rechtsgrundlage, betroffene Personen, Art der zu speichernden Daten usw., das findet sich jetzt im Verzeichnis der Verarbeitungstätigkeiten wieder. Also da gibt es durchaus Auffangbereiche. Das sollte aber der Gesetzgeber durchaus klarstellen. Und die Frage ist auch, in welchem – und das hat er bisher nicht getan – in welchem Detaillierungsgrad sollen diese Verarbeitungsverzeichnisse geführt werden. Und das ist beim Wegfall der Errichtungsanordnung ganz, ganz wesentlich. Dass man hier klarstellt, was gehört ei-

gentlich in so ein Verzeichnis der Verarbeitungstätigkeiten hinein.

So und nun fällt das ja in der Regel auch zusammen mit einer gemeinsamen Verantwortlichkeit von für sich verantwortlichen Stellen. Und Herr Dr. Brink hat das schon richtig ausgeführt. Also für uns ist der Begriff insofern neu, als dass im alten BDSG die Vorgaben aus der alten Richtlinie nicht umgesetzt waren. Dort gab es nämlich schon lange die gemeinsame Verantwortlichkeit. Also dieser Begriff ist schlichtweg eigentlich für uns hier in Deutschland neu. Und damit müssen wir lernen umzugehen, dass der Gesetzgeber und auch die DSGVO greift das insofern auf, als dass für den Bereich der Informationspflichten da Regelungen getroffen werden. Nämlich, dass die Verantwortlichen jeweils festzulegen haben, wer jeweils zur Auskunft verpflichtet werden soll. Im Übrigen belässt es das Gesetz dabei zu sagen, dass natürlich jeder Verantwortliche entsprechende technisch organisatorische Maßnahmen zur Sicherstellung der Sicherheit der Verarbeitung bei ihm selbst im Rahmen seiner Verpflichtung zur Verantwortlichkeit auch treffen wird. Und nun ist es aber ja so, dass bei Dateien, Dateisystemen, die gemeinsam geführt werden, das Risiko der Verarbeitung durchaus unterschiedlich hoch gelagert ist, weil ja mehr Verantwortliche zugreifen können und die Daten in unterschiedliche Richtungen fließen. Und insofern wäre es hier erforderlich, über besondere Garantieren nachzudenken, die sicherstellen, dass diese technisch organisatorischen Maßnahmen eben nicht nur mit Blick auf den einzelnen Verantwortlichen umgesetzt werden, sondern eben im Blick auf die gemeinsame Verantwortlichkeit. Und da kann es in einzelnen Bereichen durchaus zu unterschiedlichen Ausprägungen kommen im Hinblick zum Beispiel auf Regelungen und Maßnahmen zur Vertraulichkeit, zur Integrität, weil ja unterschiedliche Verantwortliche Zugriff haben. Das muss sich in den Rollenkonzepten zum Beispiel wiederspiegeln, das wäre da sozusagen der praktische Anwendungsrahmen.

Die weitere Frage: Wie gehen wir als Aufsicht eigentlich damit um? Wie prüft man eigentlich gemeinsame Verantwortlichkeit? Das sagte Herr Dr. Brink schon. Da gibt es bislang wenig Erfahrung. Also ich würde nicht sagen, dass es keine Erfahrung gibt, weil es die Zusammenarbeit zwischen den Aufsichtsbehörden ja durchaus in der Vergangenheit schon gab. Was es aber nicht gab, sind gemeinsame Prüfkonzepte. Das ist ein Bereich, der in der Vergangenheit ein bisschen stiefmütterlich behandelt worden ist. Das hat auch sehr viel tun mit Prüftransparenz. Auch die Aufsichtsbehörden unterliegen natürlich gewissen Transparenzpflichten und müssen ihre Arbeit auch nach außen hin vertreten können. Sie sind genauso verantwortlich. Und hier bedarf es also auch im Zuge des europäischen Zusammenwachsens weiteren Bedarf des gemeinsamen Agierens zwischen den Aufsichtsbehörden. Und da ist es natürlich sinnvoll, sich auch zusammen Gedanken zu machen, wie wird eigentlich verlässlich geprüft. Welche Anforderungen bestehen hier und eben insbesondere vor dem Hintergrund der gemeinsamen Verantwortlichkeit? Da gibt es Bestrebungen im technischen Bereich. Der AK-Technik der Datenschutzkonferenz beschäftigt sich seit einigen Jahren mit diesen Fragen. Er hat dazu aufbauend auf den Schutzzielen des Datenschutzrechts das Standarddatenschutzmodell entwickelt, was eine hervorragende Ausgangsposition ist zur Prüfung für diese gemeinsame Verantwortlichkeit. Da wäre es natürlich auch im europäischen Konzert sehr sinnvoll und wiederum auch ein Markenzeichen und ein Vorzeigeaspekt, wenn aus Deutschland hier Anregungen kämen, wie sowas zu prüfen ist. Und da könnte man auch gesetzlich an das Standarddatenschutzmodell anknüpfen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank und dann noch Herr Prof. Dr. Aden bitte.

SV **Prof. Dr. Hartmut Aden** (HWR, Berlin): Vielen Dank für die Fragen. Ich fange mit der Bestellpflicht an. Dazu ist ja schon einiges Wichtiges hier gesagt worden. Ich würde auch sagen, dass die Regelung, wie sie jetzt im BDSG ist, besser praktikabel ist als eine Regelung die ganz weggehen würde von klaren Grenzen und das alles auf Risikokriterien legen würde. Dann hätten wir ja das Problem, dass in jedem Einzelfall entschieden werden müsste, ob die Voraussetzungen erfüllt sind oder nicht. Das heißt, da würde der Verwaltungsaufwand bei denjenigen, die das entscheiden und prüfen müssen, wesentlich höher als er jetzt ist. Es wird auch in der Diskussionen meines Erachtens häufig übersehen, dass die Regelung, so wie wir sie heute haben, recht flexibel ist, weil ja nicht näher bestimmt ist,

wie die Funktion der Beauftragung in Unternehmen oder in Vereinen konkret ausgestaltet werden muss. Denn es kann jemand sein, der das als externer Dienstleister macht. Es kann aber auch intern jemand dafür fortgebildet werden und das machen. Und damit man ja eine sehr große interne Flexibilität. Ich würde mal die Pflichtenintensität vergleichen wollen mit der Buchführungspflicht. Auch da haben wir sehr flexible Regelungen, so dass jedes Unternehmen und jeder Verein selbst entscheiden kann, wie er das genau macht und nichts anderes haben wir hier. Das scheint mir also ganz gut so geeignet zu sein.

Ich selber bin ja auch behördlicher Datenschutzbeauftragter meiner Hochschule und habe deswegen auch diese gewissen Paniken miterlebt, was da jetzt neu käme nach der DSGVO. Ich denke, wenn man vorher schon einen geordneten Datenschutzstandard hatte, hat sich so viel in der Praxis gar nicht geändert. Es gibt einige wenige Bereiche, wo man jetzt ein bisschen genauer hinschauen muss. Das ist zum einen die Frage, ob es für alle Daten, die man hat, eine informierte Einwilligung gibt und man muss die entsprechend dokumentieren. Es gibt außerdem die Berichtspflicht bei Datenschutzvorfällen. Aber das ist ja auch im Sinne der Betroffenen etwas, was wirklich ein großer Fortschritt ist, dass Datenschutzvorfälle nicht mehr einfach unter den Teppich gekehrt werden können. Und ich habe mich auch gefreut, dass ich doch relativ früh schon, also sogar schon vor dem Inkrafttreten der DSGVO, erste Mails von Unternehmen bekam, die mir mitteilten, dass bei ihnen da etwas schief gelaufen ist, was sie mir wahrscheinlich vorher einfach verschwiegen hätten. Insofern finde ich, das sind gute Entwicklungen. Da würde ich auch Herrn Dr. Brink zustimmen, dass es letztendlich jetzt darum geht, den Kleinen Hilfestellungen zu geben. Denn man kann das ja alles sehr stark standardisieren. Man kann dafür Vorlagen entwickeln. Man kann dafür auch elektronische Verfahren entwickeln. Und man sollte sicherlich insbesondere davor warnen, dass dem doch sehr wild blühenden Beratungswesen in dem Bereich zu sehr aufgesessen wird, sondern es geht vor allem darum, dass man pragmatische Lösungen findet und da haben sicherlich die Aufsichtsbehörden, aber auch die Politik und die Ministerien Aufgaben, den Anwendern ihre Arbeit zu erleichtern. Und wenn das so ist, dann ist es sicherlich eine sehr gute Entwicklung, dass die Datenschutzfragen heute doch in einem breiteren Bewusstsein sind.

Die zweite Frage ist indes eine bezüglich des Verhältnisses Datenschutzaufsicht, Telekommunikation, Telemedien. Das ist ein Fragenkomplex, wo ich denke, dass er uns in den nächsten Jahren sehr intensiv beschäftigen wird und muss. Eigentlich war es ja so beabsichtigt, dass quasi parallel mit der DSGVO auch die Regelungen zu ePrivacy mit erneuert werden sollten. Das hat sich nun hingezogen. Es ist weiterhin auch extrem umstritten. Und da wird es sicherlich darauf ankommen, dass für die Bereiche, die für die Verbraucherinnen und Verbraucher, für die Nutzer des Internets wirklich wichtig sind, Fortschritte erzielt werden. Das betrifft insbesondere die Frage des selbstbestimmten Internetnutzens. Das heißt, erfahren wir dann wirklich, was das mit den Cookies jeweils auf sich hat oder wird es weiterhin so sein, dass einem gar nichts anderes übrig bleibt als auf „ja“ zu klicken, wenn man das Internet benutzen will. Da liegen ja die großen Baustellen. Aber auch bezüglich des Trackings, nicht nur im Netz, sondern auch die ganzen trackingfähigen Mobilgeräte. Das sehe ich auch ganz große Herausforderungen, wo im Datenschutzrecht in den nächsten Jahren noch sehr viel passieren muss. Nach meiner Rechtsauffassung gilt dafür die DSGVO, solange es keine spezielleren Regelungen gibt. Aber die Regelungen der DSGVO sind so allgemein, dass sie uns nicht in jedem Fall weiterhelfen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Wir wären dann fast am Ende. Gibt es noch von irgendeiner Kollegin oder irgendeinem Kollegen eine Ihnen auf den Nägeln brennende Nachfrage? Wenn das nicht der Fall ist, dann würden wir unsere Anhörung schließen.

Ich darf mich nochmal im Namen aller für Ihr Kommen bedanken und Ihre Bereitschaft, uns zu unterstützen und wünsche noch einen schönen Tag. Danke.

Schluss der Sitzung: 12:57 Uhr

Andrea Lindholz, MdB
Vorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 A

05. Dezember 2018

Dr. iur. Malte Engeler

Schleswig-Holsteinisches Verwaltungsgericht
Brockdorff-Rantzau-Straße 13
24837 Schleswig
Telefon: 04621/86-0
E-Mail: malte.engeler@ovg.landsh.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin
Nur per E-Mail an: innenausschuss@bundestag.de

Stellungnahme

im Rahmen der öffentlichen Anhörung
des Ausschusses
für Inneres und Heimat
des Deutschen Bundestages
am 10. Dezember 2018

zum

Zweiten Datenschutz-Anpassungs-
und Umsetzungsgesetz EU – 2. DSAnpUG-EU
(BT-Drucksache 19/4674)

vorgelegt von

Dr. Malte Engeler
Richter beim Schleswig-Holsteinischen Verwaltungsgericht

Gliederung

A. Gegenstand der Stellungnahme und Zusammenfassung

Diese Stellungnahme befasst sich mit zwei im Gesetzgebungsverfahren zum 2. DSAnpUG-EU diskutierten Aspekten: Der möglichen Umsetzung des Art. 85 DSGVO, um das Recht auf Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken (im Folgenden „Meinungsäußerung u.a.") in Einklang zu bringen, sowie mit der Frage, ob es einer ausdrücklichen gesetzlichen Ausnahme von DSGVO- und BDSG-Verstößen aus dem Anwendungsbereich des Gesetzes gegen den unlauteren Wettbewerb bedarf.

Diese Stellungnahme kommt dabei zu folgenden Ergebnissen:

- Die Schaffung einer **gesetzlichen Grundlage** für die Verarbeitung von personenbezogenen Daten zu Zwecken der Meinungsäußerung u.a. ist dringend **zu empfehlen**.

- Eine Umsetzung des Art. 85 DSGVO sollte klar als Rechtsgrundlage formuliert werden, in der die Voraussetzungen der zulässigen Verarbeitung von personenbezogenen Daten zu Zwecken der Meinungsäußerung u.a. geregelt werden. Sie sollte **nicht** etwa als generelle **Bereichsausnahme** formuliert werden.

- Die entscheidende tatbestandliche Voraussetzung in dieser zu schaffenden gesetzlichen Grundlage sollte das **Merkmal der Verhältnismäßigkeit** sein, so dass die Datenverarbeitung zulässig ist, wenn diese im Rahmen der Ausübung des Rechts auf Meinungsäußerung u.a. erfolgt und nicht unangemessen in die Rechte der Betroffenen auf Schutz der sie betreffenden personenbezogenen Daten eingreift.

- Wichtiger noch als die Schaffung einer Rechtsgrundlage ist die **Anpassung der Betroffenenrechte** sowie der übrigen datenschutzrechtlichen Folgepflichten und behördlichen Kontrollmöglichkeiten der Kapitel II bis IX DSGVO, um mögliche „**chillings effects**" zu verhindern, die durch die rechtlichen Folgepflichten einer Datenverarbeitung zu Zwecken der Meinungsäußerung u.a. ausgelöst werden könnten, sowie um einem denkbaren **Missbrauch aufsichtsbehördlicher Kompetenzen** gegenüber Meinungsäußernden u.a. zu begegnen.

- Einer ausdrücklichen gesetzlichen Ausnahme von DSGVO- und BDSG-Verstößen aus dem Anwendungsbereich des Gesetzes gegen den unlauteren Wettbewerb **bedarf es nicht**.

B. Stellungnahme zur Umsetzung des Art. 85 DSGVO

Art. 85 DSGVO verpflichtet und ermächtigt die Mitgliedsstaaten, Regelungen zu schaffen, die das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken in Einklang bringen.[1]

Dieser Ausgestaltungsauftrag ist ausgesprochen relevant, weil in der digitalisierten Gesellschaft Meinungsäußerungen, der freie Informationszugang oder auch journalistische, wissenschaftliche, künstlerische sowie literarische Tätigkeiten oft notwendigerweise mit der automatisierten[2] Verarbeitung personenbezogener Daten verbunden sind. Das betrifft Meinungsäußerungen in sozialen Netzwerken[3] genauso wie Digitalfotografie, das Betreiben eines Blogs, literarische Online-Veröffentlichungen und digitale Präsentationen wissenschaftlicher Vorträge oder die Nutzung von Internetsuchmaschinen.

Für Berufsjournalistinnen sowie die institutionelle Presse haben die Länder in den Landespressegesetzen sowie in den Rundfunkstaatsverträgen bereits eigene Regelungen getroffen.[4] Für Journalistinnen außerhalb der institutionellen Presse[5] sowie die genannten weiteren berührten Grundrechtsbereiche fehlen bisher jedoch Regelungen, die Umfang und Grenzen der zulässigen Datenverarbeitung regeln sowie klarstellen, in welchem Umfang die sonstigen Rechte und Pflichten der DSGVO anwendbar sind.

1. Erörterungen zum Regelungsbedarf

Die Notwendigkeit einer gesetzlichen Regelung folgt unmittelbar aus Art. 8 Abs. 2 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta" oder „GRCh"). Dort definiert die Charta, unter welchen Bedingungen das Grundrecht auf Schutz personenbezogener Daten eingeschränkt werden darf. Zulässig ist die Verarbeitung personenbezogener Daten demnach nur nach Treu und Glauben[6] für festgelegte Zwecke

---

[1] Zur Frage, ob und in welchem Umfang Abs. 1 und Abs. 2 selbstständige Öffnungsklauseln darstellen, siehe Abschnitt B. 2. dieser Stellungnahme.
[2] Gemäß Art. 2 Abs. 1 DSGVO ist die DSGVO zwar auch auf die nichtautomatisierte Verarbeitung von in einem Dateisystem gespeicherten personenbezogenen Daten anwendbar, aus Gründen der sprachlichen Vereinfachung und der praktischen Relevanz wird im Folgenden aber vorrangig die automatisierte Datenverarbeitung thematisiert.
[3] Zur Frage der Anwendbarkeit der DSGVO auf Nutzerinnen von Sozialen Medien siehe Abschnitt B. 1. c).
[4] Überblick bei *Cornile*, ZUM 2018, S. 561; *Schiedermair*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 85 Rn. 3.
[5] Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, gemäß Erwägungsgrund 153 DSGVO weit ausgelegt werden; Siehe auch EuGH, EuZW 2009, S. 108, Rn. 56 (Satamedia).
[6] Eine nicht ganz ideale Übersetzung des englischen Begriffs „fair", der nach überwiegender Ansicht das zu beachtende Verhältnismäßigkeitsprinzip betont und Anforderungen an die zu schaffenden Rechtsgrundlagen stellt, nicht jedoch isoliert einen Eingriffstatbestand darstellt, vgl. *Wolff*, in: Frankfurter Kommentar, Art. 8 Rn. 34.

und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage. Daraus wird nach ganz überwiegender Ansicht das sogenannte Verbot mit Regelungsvorbehalt[7] abgeleitet, wonach eine Datenverarbeitung grundsätzlich unzulässig ist, es sei denn die Einwilligung der Betroffenen oder eine gesetzliche Regelung erlauben diese. Eine Einwilligung scheidet für den hier relevanten Bereich in den meisten Fällen praktisch aus oder würde einen unverhältnismäßigen Aufwand bedeuten. Zudem hat der flächendeckende Rückgriff auf die Einwilligung zu einer erheblichen Entwertung ihrer Schutzfunktion und zu einer Einwilligungsmüdigkeit bei Betroffenen gesorgt. Geboten ist folglich die Schaffung einer gesetzlichen Rechtsgrundlage.

Die Charta bindet dabei die Mitgliedstaaten zwar grundsätzlich nur bei der Durchführung des Rechts der Europäischen Union. Da das Datenschutzrecht aber insbesondere durch Art. 16 AEUV sowie die DSGVO fast vollständig europarechtlich geprägt ist, ist die Charta und damit auch die Schrankenregelung des Art. 8 Abs. 2 GRCh zu berücksichtigen.[8] Die Charta verpflichtet schließlich auch dazu, den Grundrechten zwischen Privaten Wirksamkeit zu verleihen (freilich ohne dass daraus eine unmittelbare Grundrechtbindung zwischen Privaten abzuleiten wäre).[9]

Die Schaffung einer entsprechenden Rechtsgrundlage ist auch weder mit Verweis auf die bisherige deutsche Rechtsprechung (dazu sogleich unter a), auf die allgemeine Abwägung mit Art. 5 GG bzw. Art. 11 GRCh (dazu unter b) oder auf Regelungen der DSGVO selbst (dazu unter c) entbehrlich.

a) Keine Entbehrlichkeit einer Umsetzung mit Verweis auf die deutsche Rechtsprechung

Eine Umsetzung des Art. 85 DSGVO ist nicht mit dem Verweis darauf entbehrlich, dass die deutsche Rechtsprechung den Konflikt zwischen Datenschutz und Meinungsfreiheit in der Vergangenheit im Wege der Abwägung gelöst hat.

---

[7] Ähnliche Grundrechtsschranken finden sich auch an anderer Stelle. So regelt auch das Grundrecht auf körperliche Unversehrtheit gemäß Art. 2 Abs. 2 GG einen Gesetzesvorbehalt, ohne dass daraus im Übrigen abzuleiten wäre, dass dem Recht auf körperliche Unversehrtheit kategorisch der Vorrang gegenüber anderen Grundrechten eingeräumt würde.

[8] Grundlegend: EuGH, Urteil vom 26.02.2013, Rs. C-617/10 (Åkerberg Fransson), Rn. 21; EuGH, Urteil vom 10.07.2014, Rs. C-198/13 (Hernández), Rn. 33; *Schiedermair*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 85 Rn. 9.

[9] Zur Pflicht der Mitgliedsstaaten, Grundrechtsträgerinnen keiner Beeinträchtigung durch andere Private schutzlos ausliefern siehe *Jarass*, in: Charta der Grundrechte der EU, Art. 8 Rn. 10; *Wolff*, in: Frankfurter Kommentar, Art. 8 Rn. 20; Schlussanträgen der Generalanwältin *Kokott* zur Rs. C-275/06 vom 18.07.2007, Slg. 2008, I-271, Rn. 57 (EuGH NJW 2008, 743 - Promusicae); Vertiefend zum drittwirkungsbezogenen Regelungsgehalt des Art. 8 GRCh auch *Streinz/Michl*, EuZW 2011, S. 384.

Dem traditionellen deutschen Verständnis nach ist das Datenschutzrecht vorrangig eine Facette des Allgemeinen Persönlichkeitsrechts,[10] das als offenes Grundrecht stets im Wege der Einzelfallbetrachtung konturiert werden muss und darf.[11] Das führte bisher dazu, dass die Gerichte bei der Abwägung mit der Meinungsfreiheit einen Spielraum für Einzelfalllösungen abseits gesetzlicher Erlaubnistatbestände für sich in Anspruch nahmen. Das Bundesverfassungsgericht[12] entschied beispielsweise in einer Entscheidung aus Juni 2016 (also nach Inkrafttreten, aber vor Geltungsbeginn der DSGVO), dass wahre Tatsachenbehauptungen über Vorgänge aus der Sozialsphäre grundsätzlich hinzunehmen seien. Im dortigen Sachverhalt bemängelte ein Unternehmer in einem Internetportal anhand zutreffender Darstellungen seinen zahlungssäumigen Geschäftspartner. Die Meinungsäußerung erfolgte also mittels der automatisierten Verarbeitung personenbezogener Daten des betroffenen Schuldners. Das Bundesverfassungsgericht löste den Fall dort allein im Wege der Abwägung zwischen dem Allgemeinen Persönlichkeitsrecht des Schuldners und der Meinungsfreiheit des Unternehmers, ohne zu thematisieren, auf welcher gesetzlichen Grundlage die personenbezogenen Daten des säumigen Geschäftspartners verarbeitet werden durften und in welchem Umfang den Meinungsäußernden die datenschutzrechtlichen Folgepflichten seiner Datenverarbeitung trafen (insbesondere Auskunfts-, Lösch- oder Dokumentationspflichten).

Das Bundesverfassungsgericht hätte im Grunde aber bereits selbst nach einer Rechtsgrundlage fragen müssen, da die zu diesem Zeitpunkt geltenden Vorgängerregelungen der DSGVO, die Datenschutz-Richtlinie von 1995 (DSRL)[13] und das auf ihrer Basis erlassene BDSG a.F., ebenfalls an dem spätestens seit 2009[14] verbindlichen Art. 8 Abs. 2 GRCh und dem darin formulierten Gesetzesvorbehalt zu messen gewesen wären. Schon unter Geltung des BDSG a.F. und der DSRL gab es keine Privilegierung für Meinungsäußerungen im Allgemeinen, sondern gemäß § 41 BDSG (als Umsetzung des Art. 9 DSRL) ausschließlich eine für Datenverarbeitungen, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgten.

Hinsichtlich der Datenverarbeitung zu Zwecken der Meinungsäußerung u.a. hat sich mit der DSGVO letztlich nur geändert, dass die Gerichte bei Zweifeln darüber, ob und auf welcher Grundlage entsprechende Datenverarbeitungen zulässig sind, anstelle des Bundesverfassungsgerichts den für die Auslegung der DSGVO und die Vereinbarkeit

---

[10] *Pötters*, in: Gola, DS-GVO, Art. 1 Rn. 8; BVerfG NJW 1984, S. 419 (422); *Wente*, NJW 1984, S. 1446 (1447); *Simitis*, NJW 1984, S. 398 (399).
[11] *Wagner*, in: Münchener Kommentar zum BGB, 7. Aufl. 2017, § 823 Rn. 364.
[12] BVerfG NJW 2016, S. 3362.
[13] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, EU-Amtsblatt Nr. L 281 vom 23.11.1995.
[14] Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (2012/C 326/01), EU-Amtsblatt Nr. C 326 vom 26.10.2012.

nationalen Rechts mit dem Europarecht zuständigen EuGH anrufen müssten.[15] Ein *„weiter so"* mit Verweis auf die bisherige, insofern mit Art. 8 Abs. 2 GRCh nicht vereinbare, deutsche Rechtsprechungspraxis ist also keine Option.

b) Keine Entbehrlichkeit einer Umsetzung mit Verweis auf das deutsche Grundgesetz oder die Charta

Folglich ist auch der Verweis auf die Grundrechte auf Meinungsfreiheit des Art. 5 GG oder Art. 11 GRCh keine Lösung. Vereinzelte Ansätze dahingehend, die Öffnungsklauseln des Art. 85 DSGVO durch Art. 5 GG ausfüllen zu wollen,[16] scheitern ebenso wie die auf eine abstrakte Abwägung gestützte Rechtsprechung an der Forderung des Art. 8 Abs. 2 GRCh nach einer klaren gesetzlichen Regelung. Zwar stimmt es, dass das Grundrecht auf Datenschutz des Art. 8 Abs. 1 GRCh ebenso wie das (insoweit allerdings nicht deckungsgleiche)[17] deutsche Recht auf informationelle Selbstbestimmung keine uneingeschränkten Rechte sind. Das ändert aber nichts an dem durch Art. 8 Abs. 2 GRCh formulierten Gesetzesvorbehalt. Diesem Gesetzesvorbehalt werden alle in einem Gesetzgebungsverfahren erlassenen Akte gerecht, in Deutschland also die Parlamentsgesetze,[18] so dass das Grundgesetz insofern bereits formal ausscheidet.

c) Keine Entbehrlichkeit einer Umsetzung aufgrund bestehender Rechtsgrundlagen der DSGVO

Eine konkrete Umsetzung des Art. 85 DSGVO ist auch nicht deshalb entbehrlich, weil die bestehenden Regelungen der DSGVO hinreichende rechtliche Lösungen bereitstellen, die einen Konflikt mit der Meinungsfreiheit anderweitig verhindern würden.

Zwar ließe sich die in dieser Stellungnahme vorgeschlagene Abwägung als Kernelement der Rechtsgrundlage[19] auch in Art. 6 Abs. 1 S. 1 lit. f) DSGVO umsetzen. Art. 6 Abs. 1 S. 1 lit. f) DSGVO gilt gemäß Art. 6 Abs. 1 S. 2 DSGVO allerdings nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Datenverarbeitung. Ohne Schaffung einer eigenen Rechtsgrundlage wäre damit der gesamte Bereich der behördlichen Public

---

[15] Siehe dazu auch *Stadler*, „Schränkt die Datenschutzgrundverordnung Meinungsäußerungen im Internet ein?", online abrufbar unter http://www.internet-law.de/2018/03/schraenkt-die-datenschutzgrundverordnung-meinungsaeusserungen-im-internet-ein.html.
[16] So aber wohl das Bundesministerium des Innern, für Bau und Heimat in seinen FAQ zur Datenschutz-Grundverordnung, online abrufbar unter: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html.
[17] Grundlegend zu der notwendigen Unterscheidung: *Kokott/Sobotta*, IDPL 2013, S. 222; *Bock/Engeler* DVBl. 2016, S. 593 (595); *Wolff*, in: Frankfurter Kommentar, Art. 8 Rn. 3; *Johannes*, in: Roßnagel DatenschutzR-HdB Kap. 2 Rn. 57.
[18] *Wolff*, in: Frankfurter Kommentar, Art. 8 Rn. 32.
[19] Siehe dazu unter B. 3. a).

Relations Arbeit, die regelmäßig nicht als Presse im Sinne der Landespressegesetze einzustufen ist, erheblicher rechtlicher Unsicherheit ausgesetzt.[20]

Zudem engt Art. 9 Abs. 2 DSGVO den Bereich der zulässigen Datenverarbeitung weiter ein, wenn es um die Verarbeitung personenbezogener Daten geht, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie hinsichtlich der Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DSGVO). Art. 9 Abs. 2 DSGVO stellt insofern eigene, abschließende Rechtsgrundlagen auf, zu denen die allgemeine Abwägung des Art. 6 Abs. 1 S. 1 lit. f) DSGVO nicht gehört. [21] Eine Meinungsäußerung im Online-Kontext, die Informationen zu den von Art. 9 Abs. 1 DSGVO erfassten besonders gesetzlich geschützten Datenarten enthält[22] und die auch nicht offensichtlich von der Betroffenen öffentlich gemacht wurden (Art. 9 Abs. 2 lit. e) DSGVO), wäre also nicht über Art. 6 Abs. 1 S. 1 lit. f) DSGVO zu rechtfertigen, was die Notwendigkeit der Schaffung einer speziellen Rechtsgrundlage zusätzlich belegt.

Schließlich könnte eine Meinungsäußerung mit Bezug zu strafrechtlichen Verurteilungen einer Person auch an den Vorgaben des Art. 10 DSGVO zu messen sein, der abermals besondere, engere Voraussetzungen vorsieht. Demnach darf die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten abseits Art. 6 Abs. 1 DSGVO nur vorgenommen werden, wenn dies u.a. nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Da sich die Verarbeitung von Daten zu Zwecken der Meinungsäußerung in vielen Fällen aber nicht auf Art. 6 Abs 1 S. 1 DSGVO berufen kann, folgt aus Art. 10 DSGVO abermals die Notwendigkeit der Schaffung einer eigenständigen Rechtsgrundlage samt der Schaffung weiterer Garantien.[23]

---

[20] Vertiefend *Mönikes*, Telemedicus vom 14.02.2018, online verfügbar unter http://tlmd.in/a/3265.
[21] Die Bedeutung des Art. 9 Abs. 2 DSGVO ist im Einzelnen strittig. Nach hiesiger Ansicht stellt er einen eigenen abschließenden Katalog an Rechtsgrundlagen auf, der den Rückgriff auf die Erlaubnisnormen des Art. 6 Abs. 1 S. 1 DSGVO sperrt, so auch *Kampert*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 9 Rn. 12.
[22] Insoweit stellt Erwägungsgrund 51 zwar klar, dass die Verarbeitung von Lichtbildern nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden soll, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten" erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Jedenfalls dann, wenn aber mittels Bilder oder Aussagen eindeutige Rückschlüsse auf die gesundheitliche Verfassung einer Person ermöglicht werden, etwa bei Aussagen über oder Bildhinweise auf Krankheiten einer Person, dürfte Art. 9 Abs. 1 DSGVO in aller Regel jedenfalls seinem Wortlaut nach erfasst sein. Ob insoweit eine teleologische Reduktion des Art. 9 Abs. 1 DSGVO möglich ist, wie es *Härting*, CR-online.de Blog vom 06.09.2018, online abrufbar unter https://www.cr-online.de/blog/2018/09/06/von-brillentraegern-pegida-demonstranten-und-csd-teilnehmern-wann-sind-daten-besonders-geschuetzt/, andeutet, muss angesichts der Intention des Verordnungsgebers zurückhaltend bewertet werden.
[23] Dazu Näheres in Abschnitt B. 3. c).

d) Keine Entbehrlichkeit mit Verweis auf die *Household Exemption* des Art. 2 Abs. 2 lit. c) DSGVO

Auch ein Verweis auf Art. 2 Abs. 2 lit. c) DSGVO macht die Umsetzung des Art. 85 DSGVO nicht entbehrlich. Gemäß dieser als *Household Exemption* bezeichneten Ausnahmeregelung werden jene Datenverarbeitungen von der Anwendbarkeit der DSGVO ausgenommen, die durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgen. Die Frage, ob Nutzerinnen von sozialen Medien, also Inhaberinnen z.B. eines Twitter-, Instagram- oder Facebook-Kontos unter diese Ausnahme für private Datenverarbeitungen fallen, ist noch ungeklärt. Der EuGH hat bisher einerseits in seiner Lindqvist-Entscheidung[24] entschieden, dass die *Household Exemption* ausscheidet, wenn eine Veröffentlichung von Daten im Internet vorliegt und die Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden. Da Meinungsäußerungen z.B. in Sozialen Medien in der Regel öffentlich sind, geht auch die Literatur verbreitet davon aus, dass die dortigen Datenverarbeitungen nicht der *Household Exemption* unterfallen.[25] In seiner Wirtschaftsakademie-Entscheidung[26] hat der EuGH allerdings in einem (nicht entscheidungsrelevanten) Nebensatz angemerkt, dass der bloße Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich genommen eine Facebook-Nutzerin nicht für die von diesem Netzwerk vorgenommene Verarbeitung personenbezogener Daten (mit)verantwortlich mache. Ob der EuGH daraus nun ableiten will, dass Datenverarbeitungen in sozialen Netzwerken durch Privatnutzerinnen nicht der DSGVO unterfallen und wie der damit ausgelöste Widerspruch zu seiner Lindqvist-Entscheidung aufzulösen wäre, macht er nicht deutlich.[27] Aber selbst wenn man die Anwendbarkeit der *Household Exemption* unterstellen wollte, würde diese die Schaffung einer Rechtsgrundlage für die Datenverarbeitung zu Zwecken der Meinungsäußerung u.a. nicht entbehrlich machen, da sie sich in jedem Fall nicht auf Meinungsäußerungen von juristischen Personen[28], mittels beruflich genutzter Accounts oder etwa von Politikerinnen beziehen würde, denn Meinungsäußerungen in diesem Kontext erfolgen in keinem Fall allein zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

---

[24] EuGH, Urteil vom 06.11.2003, Rs. C-101/01 (Lindqvist).
[25] So etwa *Gola*, in: Gola, Datenschutzgrundverordnung Kommentar, Art. 2, Rn. 21; *Schulz/Heilmann* in: Gieschmann u.a., Datenschutz-Grundverordnung, Art. 85 Rn. 28.
[26] EuGH, Urteil vom 05.06.2018, Rs. C-210/16 (Wirtschaftsakademie), Rn. 56.
[27] Der EuGH dürfte hier letztlich nur die (Mit-) Verantwortlichkeit für die im Hintergrund des Social Media Auftritts stattfindende Datenverarbeitung zu Zwecken der Reichweitenmessung und Personalisierung von Inhalten meinen, nicht die Verantwortlichkeit für die veröffentlichen Inhalte selbst.
[28] Zur Anwendbarkeit des Art. 5 GG auf Unternehmen siehe *Schulz/Heilmann* in: Gieschmann u.a., Datenschutz-Grundverordnung, Art. 85 Rn. 20.

2. Möglicher Umsetzungsspielraum für eine Rechtsgrundlage

Zur konkreten Form der Umsetzung des Art. 85 DSGVO werden im Wesentlichen drei Ansätze diskutiert.[29] Neben der bereits als unzulänglich dargestellten Nichtregelung (bei Verweis auf Art. 5 GG und die Rechtsprechung) ist sowohl eine komplette Bereichsausnahme[30] als auch die Schaffung einer konkreten Rechtsgrundlage[31] denkbar.

Die Form der Umsetzung des Art. 85 DSGVO hängt maßgeblich davon ab, welchen Spielraum die Regelung eröffnet. Nach einer Ansicht enthält Art. 85 Abs. 1 DSGVO eine sehr weite Kann-Regelung, die sogar eine Bereichsausnahme ermöglichen soll,[32] während Art. 85 Abs. 2 DSGVO einen konkreten Ausgestaltungsauftrag dahingehend beinhalten soll, die genannten Grundrechtsbereiche vor unangemessenen rechtlichen Folgewirkungen der DSGVO zu schützen.[33] Vereinzelt wird dem Art. 85 Abs. 1 DSGVO generell der Charakter als Öffnungsklausel abgesprochen.[34] Andere Stimmen führen schließlich mit Verweis auf die Entstehungsgeschichte des Art. 85 DSGVO aus, dass es sich bei Art. 85 Abs. 1 DSGVO zwar um eine Öffnungsklausel handle, diese allerdings restriktiv auszulegen sei.[35]

Dafür, dass Art. 85 Abs. 1 DSGVO keine eigene Öffnungsklausel enthalten soll, spricht nach hiesiger Auffassung wenig. Die Historie des Gesetzgebungsverfahrens zur DSGVO ist insoweit eindeutig. Der Kommissionsvorschlag sah in Abs. 1 vor, dass die Mitgliedstaaten Ausnahmevorschriften erlassen, „um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen" und Abs. 2 enthielt die Verpflichtung der Mitgliedstaaten, die Rechtsvorschriften, die sie nach Abs. 1 erlassen haben, der Kommission mitzuteilen und sie unverzüglich auch von allen weiteren Änderungsgesetzen oder diese Rechtsvorschriften betreffenden Änderungen in Kenntnis zu setzen.[36] Die Kommission wollte also nicht derart streng zwischen einer Öffnung betreffend der allgemeinen Meinungsfreiheit (jetzt nur in Abs. 1 genannt) und ihren besonderen Schutzbereichen,

---

[29] Siehe dazu die Übersicht von *Assion*, DSGVO Fachkonferenz - Tagungsbericht des Bundesverband deutscher Pressesprecher (BdP) vom 22.03.2018, S. 6, online abrufbar unter https://www.bdp-net.de/sites/default/files/tagungsbericht_dsgvo-fachkonferenz_22032018.pdf.
[30] Vgl. § 7 des schwedischen Datenschutzgesetzes.
[31] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Entschließung vom 09.11.2017, https://www.datenschutz-bayern.de/dsbk- ent/DSK_94-Art_85_DSGVO.html; ebenso Stellungnahme des Deutschen Anwaltsvereins durch den Ausschuss Informationsrecht - Stellungnahme Nr. 34/2018.
[32] *Golz/Gössling*, ITRB 2018, S. 68 (72), schreiben diesbezüglich von „wünschenswert aber nicht zwingend"; *Schulz/Heilmann* in: Gieschmann u.a., Datenschutz-Grundverordnung, Art. 85 Rn. 34 halten eine Bereichsausnahme nicht für ausgeschlossen.
[33] *Pauly*, in: Paal/Pauly, DS-GVO BDSG 2. Auflage 2018, Art. 85 Rn. 5.
[34] *Schack/Dregelies*, Stellungnahme „Fotografieren in der Öffentlichkeit", LT-SH Drucks. 19/1294.
[35] *Specht/Bienemann*, Sydow DSGVO, Art. 85 Rn. 9.
[36] *Specht/Bienemann*, Sydow DSGVO, Art. 85 Rn. 9.

etwa journalistischen, wissenschaftlichen und literarischen Tätigkeiten, trennen, wie es jetzt in Abs. 2 deutlich wird. Auch die nur auf den jetzigen Art. 85 Abs. 2 DSGVO verweisende Mitteilungspflicht des Art. 85 Abs. 3 DSGVO ist für eine derartige Auffassung unergiebig, da die DSGVO insoweit auch an anderer Stelle nicht frei von redaktionellen Fehlern war.[37] Dass aus der Öffnungsklausel ein in den Mitgliedsstaaten unterschiedliches Schutzniveau und eine unterschiedliche Gewichtung des Verhältnis zwischen Meinungsfreiheit und Datenschutz erwächst, führt ebenso zu keinem anderen Ergebnis, schließlich folgt das gleiche Resultat zwingend auch aus Art. 85 Abs. 2 DSGVO, dem seine Abweichungsbefugnis deswegen ebenfalls nicht abgesprochen wird, obwohl das Maß der Abweichung von Mitgliedstaat zu Mitgliedstaat gleichermaßen unterschiedlich ausfallen kann.

Überzeugender ist letztlich, dass Art. 85 Abs. 1 DSGVO eine eigenständige Öffnungsklausel enthält, die aber nicht so weit reicht, dass damit eine gänzliche Ausnahme der Datenverarbeitung zu den Zwecken des Art. 85 Abs. 1 DSGVO einhergeht. Eine derartige Privilegierung entsprechender Datenverarbeitungen würde weder dem Stellenwert des Rechts auf Schutz personenbezogener Daten noch dem Abwägungsauftrag des Art. 85 Abs. 1 DSGVO gerecht werden.

Eine gänzliche Bereichsausnahme würde außerdem abermals den Gesetzesvorbehalt des Art. 8 Abs. 2 GRCh missachten und könnte zudem erhebliche rechtliche Folgefragen nach sich ziehen, wenn etwa zu Zwecken der Meinungsäußerung Dritte als Auftragsverarbeiter oder gemeinsame Verantwortliche im Sinne des Art. 4 Nr. 7 und 8 DSGVO eingebunden würden. Anbieterinnen z.B. von Plattformen oder Hostingdiensten würden bei einer Bereichsausnahme unter Umständen reflexartig ebenfalls aus dem Anwendungsbereich der DSGVO fallen. Zuletzt erscheint es auch nicht nachvollziehbar, andere, ebenso der Meinungsbildung dienende Inhalte auf Blogs, in Foren oder auf Online-Plattformen so viel weitgehender zu privilegieren als die institutionelle Presse im Sinne der Landespressegesetze und sie im Rahmen einer Bereichsausnahme von datenschutzrechtlichen Pflichten generell freizustellen. Ihre Wirkung auf die Rechte der Betroffenen ist oft ähnlich intensiv und ihre Bedeutung für die öffentliche Meinungsbildung ebenso gewichtig.[38]

---

[37] *Specht/Bienemann*, Sydow DSGVO, Art. 85 Rn. 9 verweisen hier zurecht auf den nunmehr korrigierten Verweis des Art. 15 Abs. 4 DSGVO auf den nicht existenten Art. 15 Abs. 1 b DSGVO.

[38] Gegen ein derartiges allgemeines Medienprivileg auch *Specht/Bienemann*, Sydow DSGVO, Art. 85 Rn. 13, die zu Recht darauf verweisen, dass dies abermals für den Charakter des Art. 85 Abs. 1 DSGVO als selbstständige Öffnungsklausel spricht.

Diese Stellungnahme empfiehlt vor diesem Hintergrund die Schaffung einer konkreten Rechtsgrundlage, die sich hinsichtlich des eingeräumten Umsetzungsspielraums an den Grenzen des Art. 85 Abs. 2 DSGVO orientiert.[39]

3. Konkreter Inhalt einer Rechtsgrundlage als Umsetzung des Art. 85 Abs. 1 DSGVO

Eine Umsetzung des Art. 85 DSGVO sollte klar als Rechtsgrundlage formuliert werden, deren wesentliche Voraussetzung die Verhältnismäßigkeit der Datenverarbeitung unter Abwägung des Grundrechts auf Meinungsfreiheit u.a. mit dem des Rechts auf Schutz personenbezogener Daten ist (dazu unter a). Bei der Gestaltung der Rechtsgrundlage ist auf die Beweislastverteilung zu achten (dazu unter b) und es sind die Forderungen der DSGVO nach der Schaffung spezieller Garantien zu berücksichtigen (dazu unter c) und d).

a) Die Abwägung als Tatbestandsvoraussetzung

Wesentliche Tatbestandsvoraussetzung einer Rechtsgrundlage muss die Verhältnismäßigkeit sein. Eine derartige Regelung ermöglicht es, die reichhaltige Rechtsprechung der deutschen Gerichte,[40] des EuGH sowie des EGMR[41] als Ausgangspunkt zu erhalten, verschließt sich gleichzeitig aber auch nicht vor möglichen neuen Gewichtungen unter Berücksichtigung des Art. 8 GRCh. Konkret geeignet wäre insofern eine Formulierung, wie sie unter anderem der Deutsche Anwaltsverein[42] vorgeschlagen hat:

> *Formulierungsvorschlag 1*
> *„Die Verarbeitung zum Zweck der Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit ist grundsätzlich zulässig, es sei denn, dem steht ein überwiegendes legitimes Interesse der Betroffenen entgegen. Dies gilt insbesondere für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.*"

Eine hinsichtlich der Zwecke und des Umfangs der erlaubten Datenverarbeitung strengere Formulierung, könnte wie folgt lauten:

---

[39] So im Ergebnis zur Reichweite des Art. 85 Abs. 1 DSGVO auch *Buchner/Tinnefeld*, in: Kühling/Buchner, DS-GVO BDSG 2. Auflage 2018, Art. 85 Rn. 12.
[40] Zuletzt etwa BVerfG, NVwZ 2016, S. 761; BVerfG, EUGRZ 2016 S. 491; BGH, NJW 2015, S. 778; zum Thema Bewertungsportale im Überblick auch *Petruzzelli*, MMR 2017, S. 800.
[41] Übersicht bei *Schiedermair*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 85 Rn. 10.
[42] Stellungnahme des Deutschen Anwaltsvereins durch den Ausschuss Informationsrecht - Stellungnahme Nr. 34/2018, S. 16.

Formulierungsvorschlag 2
„Die Verarbeitung personenbezogener Daten im angemessenen Umfang zum Zwecke des Rechts auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken stattfindet, ist zulässig, es sei denn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen."

Mit dieser Formulierung würde die Abwägung zusätzlich bei der Zweckbestimmung aufgeführt.

b) Die Beweislastverteilung

Beide obigen Formulierungen räumen dem Grundrecht auf Meinungsfreiheit grundsätzlich den Vorrang gegenüber den widerstreitenden Interessen der Betroffenen ein. Mit der Formulierung „es sei denn" wird klargestellt, dass es grundsätzlich an der betroffenen Person ist, darzulegen und im Zweifel gerichtlich nachzuweisen, dass ihre Interessen überwiegen.[43]

Denkbar ist allerdings auch, die Beweislast auf die meinungsäußernde Person zu verlagern. Eine entsprechende Formulierung könnte lauten:

Formulierungsvorschlag 3
„Die Verarbeitung personenbezogener Daten ist nur zulässig, sofern sie im angemessenen Umfang zum Zwecke des Rechts auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen."

Mit dieser Formulierung läge es zunächst an der Meinungsäußernden, darzulegen, dass ihre Datenverarbeitung sowohl im angemessenen Umfang erfolgt, um dem Zweck der Datenverarbeitung zu erreichen, als auch, dass die Interessen der betroffenen Person nicht überwiegen. Eine solche Verteilung der Darlegungslast hätte ohne Zweifel aber einen stärkeren negativen Effekt auf die Bereitschaft zur Ausübung der Meinungsfreiheit mittels automatisierter Datenverarbeitung. Mit Blick auf die schlechthin konstituierende Bedeutung der Meinungsfreiheit für die Demokratie und der grundsätzlichen Vermutung

[43] Siehe zu einer ähnlichen Diskussion um die Darlegungslast im Rahmen einer Abwägung bereits *Simitis*, in: Simitis, Bundesdatenschutzgesetz 8. Auflage 2014, § 28 Rn. 130f.

für die Freiheit der Rede in allen Bereichen[44] sollte von einer solchen Beweislastverteilung daher nur sehr zurückhaltend Gebrauch gemacht werden.

Eine solche Beweislastverteilung könnte dort angezeigt sein, wo es tatsächlich nicht nur um rein private Meinungsäußerungen geht, sondern um journalistische Tätigkeiten (außerhalb der Presse im Sinne der Landespressegesetze). Eine derartige Regelung, die bewusst die private Meinungsäußerung privilegiert, könnte sich wie folgt darstellen:

> *Formulierungsvorschlag 4*
> *„Die Verarbeitung personenbezogener Daten zum Zwecke des Rechts auf freie Meinungsäußerung und Informationsfreiheit ist zulässig, es sei denn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Erfolgt die Verarbeitung personenbezogener Daten im angemessenen Umfang zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, ist sie nur zulässig, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen.*"

Im Rahmen dieser Formulierung läge die Beweislast nur solange bei der betroffenen Person, wie diese sich einer privaten Meinungsäußerung gegenübersieht, während es hinsichtlich der übrigen Verarbeitungszwecke an der Datenverarbeiterin wäre, die Rechtmäßigkeit ihrer Verarbeitung darzulegen. Auch eine solche Regelung sähe sich aber erheblichen Bedenken hinsichtlich ihrer einschränkenden Wirkung auf u.a. freie journalistische Tätigkeiten ausgesetzt, da das Bundesverfassungsgericht nicht nur die Meinungsäußerung, sondern auch den gesamten – auch den journalistisch geprägten – öffentlichen Meinungsbildungsprozess als Grundprinzip der Demokratie anerkennt.

Im Rahmen dieser Stellungnahme wird daher dafür plädiert, eine Beweislastverteilung zu schaffen, die im Zweifel für die Meinungsfreiheit streitet.

c) Zu schaffende Garantien im Sinne des Art. 10 DSGVO

Da auch Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO Gegenstand von Meinungsäußerungen bzw. journalistischen oder literarischen Tätigkeiten usw. sein können, sind geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen. Erforderlich sind über die Betroffenenrechte hinausgehende besondere materielle Schutzstandards, die den Verhältnismäßigkeitsgrundsatz und das Resozialisierungsinteresse der betroffenen Person berücksichtigen.[45] Eine mögliche Umsetzung könnte darin bestehen, die etablierten medienrechtlichen Instrumente der Richtigstellung, Gegendarstellung und der

[44] BVerfGE 7, S. 198 (Lüth); BVerfGE 20, S. 56 (97).
[45] *Schiff*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung 2. Auflage 2018, Art. 10 Rn. 8.

Unterlassungsansprüche ausdrücklich ihrerseits zu privilegieren. Als Vorbild könnte dabei die Regelung in § 12 des Hamburgischen Datenschutzgesetzes dienen, die sicherstellt, dass eine für die Wahrnehmung dieser Ansprüche und Rechte nötige Datenverarbeitung nicht nur zulässig ist, sondern auch den Umgang mit den dafür erforderlichen Daten regelt.

> *Formulierungsvorschlag 5*
> *„Führt die Verarbeitung personenbezogener Daten gemäß Absatz 1 zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Gerichtsentscheidungen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen, Gerichtsentscheidungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren, wie die Daten selbst sowie bei einer Offenlegung der Daten gemeinsam offenzulegen.*"

Auch die gemäß den obigen Ausführungen[46] nur ganz zurückhaltend angezeigte Beweislastregelung zu Lasten der Meinungsfreiheit könnte im Kontext des Art. 10 DSGVO als zusätzliche Garantie in Betracht kommen. Ein rein klarstellender Hinweis der Art

> *Formulierungsvorschlag 6*
> *„Bei der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO ist im Rahmen der Abwägung des Rechts der Meinungsäußerung der Verantwortlichen mit dem Recht auf Schutz personenbezogener Daten der Betroffenen insbesondere das Resozialisierungsinteresse der betroffenen Person zu berücksichtigen.*"

dürfte hingegen nicht den Aufforderungen des Art. 10 DSGVO zur Schaffung konkreter Schutzstandards gerecht werden.

d) Kein zusätzlicher Regelungsbedarf hinsichtlich Art. 89 DSGVO

Hinsichtlich der ebenfalls von Art. 85 DSGVO erfassten Datenverarbeitung zu wissenschaftlichen Zwecken bestehen gewisse Abgrenzungsprobleme gegenüber Art. 89 DSGVO. Die Kommentarliteratur verweist insofern zu Recht darauf, dass die Öffnungsklauseln des Art. 85 Abs. 1 und Abs. 2 DSGVO weiter als die des Art. 89 Abs. 2 DSGVO sind.[47] Dies hat zur Folge, dass Art. 85 DSGVO den Mitgliedsstaaten hinsichtlich der Datenverarbeitung zu wissenschaftlichen Zwecken einen viel weiteren Öffnungsspielraum einräumt als Art. 89 DSGVO, der in seinem Abs. 1 geeignete Garantien vorsieht und in Abs. 2 nur sehr viel engere Abweichungen von den

[46] Abschnitt B. 3. b).
[47] *Specht/Bienemann*, in: Sydow DSGVO, Art. 85 Rn. 14.

Betroffenenrechten vorsieht, als dies bei Art. 89 Abs. 2 DSGVO der Fall ist. Dieser Widerspruch würde entweder dazu führen, dass die Öffnungsklausel des Art. 89 Abs. 2 DSGVO überflüssig ist,[48] weil sie komplett in der viel weitergehenden Öffnungsklausel des Art. 85 DSGVO aufginge oder sie würde, etwa wenn man Art. 89 Abs. 2 DSGVO für die Datenverarbeitung zu Wissenschafts- und Forschungszwecken als spezieller und vorrangig annimmt, die Nennung der wissenschaftlichen Zwecke in Art. 85 Abs. 1 DSGVO als weitgehend sinnlos erscheinen lassen. Mit Blick auf die englische Sprachfassung wird aber deutlich, dass Art. 85 DSGVO im Anwendungsbereich anders gelagert ist. Er erfasst die „academic expression", also Publikationen, Vorträge und Lehre, während Art. 89 DSGVO die „scientific research", also originäre Forschung erfasst.[49] Die deutsche Sprachfassung macht diese Unterscheidung mit den fast identischen Begriffen „wissenschaftliche Zwecke" (Art. 85 Abs. 1 DSGVO) und „wissenschaftliche Forschungszwecke" (Art. 89 Abs. 1 DSGVO) nur unzureichend klar und suggeriert, dass letzteres in ersterem enthalten sei.

Soweit die Literatur dennoch eine Überschneidung annimmt, löst sie den Widerspruch zu Lasten der Bedeutung des Art. 89 Abs. 2 DSGVO dahingehend, dass zwar grundsätzlich bei der Umsetzung des Art. 85 DSGVO ein gegenüber Art. 89 Abs. 2 DSGVO weiterer Spielraum angenommen wird, der Forderung nach Garantien des Art. 89 Abs. 1 DSGVO aber dennoch Rechnung zu tragen sei.[50] Dieser Anforderung könnte verhältnismäßig einfach dadurch gerecht werden, dass auch im Rahmen der Umsetzung des Art. 85 Abs. 1 DSGVO auf § 22 Abs. 2 BDSG Bezug genommen wird, der zusammen mit § 27 BDSG die geforderten Garantien des Art. 89 Abs. 1 DSGVO abbildet. Eine Formulierung könnte lauten:

> *Formulierungsvorschlag 7*
> *„Werden Daten zu wissenschaftlichen Zwecken im Sinne des Absatz 1 verarbeitet, so gelten die Vorgaben des § 22 Abs. 2 BDSG entsprechend.*"

Eine solche Formulierung ist nach hier vertretener Ansicht aber entbehrlich, da der Art. 89 DSGVO nach richtiger Lesart für die Kundgabe wissenschaftlicher Ansichten in Publikationen und freiem Vortrag bereits nicht anwendbar ist und daher die Forderung nach entsprechenden Garantien des Art. 89 Abs. 1 DSGVO schon gar nicht greift. Sinnvoller wäre stattdessen eine Formulierung, die das Verhältnis zu Art. 89 DSGVO und § 27 BDSG klarstellt und etwa wie folgt formuliert werden könnte:

---

[48] *Pötters*, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, 89, Rn. 17.
[49] *Golla*, in: Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, Kapitel 23 Rn. 6.
[50] *Specht/Bienemann*, in: Sydow DSGVO, Art. 85 Rn. 14; *Pötters*, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, 89, Rn. 17.

Formulierungsvorschlag 8
„Als Datenverarbeitung zu wissenschaftlichen Zwecken im Sinne des Abs. 1 gilt insbesondere die Kundgabe wissenschaftlicher Ansichten, etwa in Form von Publikationen und Lehre. Hinsichtlich der Verarbeitung zu wissenschaftlichen Forschungszwecken bleibt § 27 BDSG unberührt."

Mit dieser Klarstellung wäre zudem erreicht, dass Unsicherheiten im Bereich der Datenverarbeitungen zu wissenschaftlichen Zwecken ausgeräumt werden. Diese entstehen unter anderem daraus, dass in § 27 BDSG nur die Verarbeitung von besonderen Kategorien von Daten im Sinne des Art. 9 Abs. 1 DSGVO privilegiert wird, was bisher zu dem wenig überzeugenden Ergebnis führt, dass z.B. die Datenverarbeitung im wissenschaftlichen Kontext nur dann nicht die Informationspflichten der Art. 13 ff. DSGVO auslöst, wenn darin Daten im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet werden. Sind derartige „sensiblen" Daten hingegen nicht betroffen, greifen beispielsweise die Informations- und Auskunftspflichten voll. Dies könnte den Willen der Verantwortlichen zur kritischen wissenschaftlichen Auseinandersetzung hemmen. Durch die vorgeschlagene Klarstellung wäre erreicht, dass jedenfalls hinsichtlich Publikations-, Vortrags- und Lehrtätigkeiten dieses unsinnige Ergebnis ausgeräumt wird.

4. Konkreter Inhalt einer Anpassung der datenschutzrechtlichen Folgepflichten als Umsetzung des Art. 85 Abs. 1 DSGVO

Die bisherigen Überlegungen zeigen, dass neben der Schaffung einer eindeutigen und klarstellenden Rechtsgrundlage vor allem die Regelung der Betroffenenrechte sowie der sonstigen datenschutzrechlichen Folgepflichten von großer Bedeutung ist. Die aus ihnen mittelbar ableitbare Klarnamenpflicht, die mögliche hemmende Wirkung auf die Bereitschaft zur Meinungsbildung und -kundgabe sowie ein möglicher Missbrauch aufsichtsbehördlicher Kompetenzen gegenüber Einzelmeinungen (dazu sogleich unter a) machen eine Anpassung zwingend erforderlich. Die konkrete Anpassung der datenschutzrechtlichen Folgepflichten muss dies berücksichtigen (dazu unter b).

a) Zur Notwendigkeit der Anpassung der Betroffenenrecht und datenschutzrechtlichen Folgepflichten

Wie bereits dargestellt,[51] besteht Grund zu der Annahme, dass Meinungsäußerungen in sozialen Netzwerken, in Online-Foren oder in den Kommentaren eines Blogs eine Datenverarbeitung im Anwendungsbereich der DSGVO darstellen. Damit würde auch die Pflicht des Art. 14 Abs. 1 lit. a) DSGVO gelten, wonach die Kontaktdaten des Verantwortlichen zu benennen wären. Eine Privilegierung für Datenverarbeitungen zu

[51] Siehe Abschnitt B. I. d).

Zwecken der Meinungsäußerung fehlt bisher und wurde auch nicht in Umsetzung des Art. 22 Abs. 1 lit. i) DSGVO in § 33 BDSG aufgegriffen.[52] Damit kommt Art. 14 Abs. 1 lit. a) DSGVO im Endeffekt einer Klarnamenpflicht gleich, die sich erheblich nachteilig auf die Bereitschaft auswirken könnte, Meinungen online zu kommunizieren.[53]

Aber nicht nur der Verlust der Möglichkeit anonymer Meinungsäußerung im Online-Bereich hätte unter Umständen hemmende Wirkung („*chilling effects*"). Auch die übrigen Pflichten, beispielsweise zur Auskunftserteilung (Art. 15 DSGVO), zur Berichtigung (Art. 16 DSGVO), zur Einschränkung der Verarbeitung (Art. 18 DSGVO), zur Berücksichtigung eines Widerspruchs (Art. 21 DSGVO) oder zur Zahlung von Schadensersatz bei Verstößen gegen die Vorgaben der DSGVO (Art. 82 DSGVO) könnten im Meinungskampf instrumentalisiert werden und die Bereitschaft zur Teilnahme an online geführten Diskussionen schmälern.[54]

Schließlich würde die Datenverarbeitung im Rahmen der Zwecke des Art. 85 DSGVO auch voll der Kontrolltätigkeit der Aufsichtsbehörden im Sinne des Kapitel VI und VIII der DSGVO unterliegen. Aktuelle Entwicklungen in anderen europäischen Staaten zeigen eindrücklich, dass diese Kompetenzen auch genutzt werden, um etwa Journalisten zur Offenlegung ihrer Quellen zu zwingen.[55] Gleichermaßen wäre es denkbar, die behördlichen Aufsichtskompetenzen auch gegen Meinungsäußernde, Wissenschaftlerinnen oder Künstlerinnen einzusetzen.[56]

b) Mögliche Anpassungen der datenschutzrechtlichen Folgepflichten

Die konkrete Anpassung der Betroffenenrechte bzw. der sonstigen datenschutzrechtlichen Folgepflichten kann auf unterschiedliche Weise erfolgen. Sie gänzlich abzubedingen, würde den möglichen nachteiligen Folgen für die Betroffenen allerdings nicht gerecht, so dass als denkbare Minimallösung erst die Option erscheint, ihre Geltung allgemeinen unter einen Abwägungsvorbehalt zu stellen.

---

[52] Zu einer diesbezüglichen Forderung auch bereits *Veil*, in: Gieschmann u.a., Datenschutz-Grundverordnung, Art. 85 Rn. 28.
[53] Vgl. insoweit die Diskussion um den § 13 Abs. 6 TMG; Dazu etwa *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 Rn. 21 mit weiteren Nachweisen; *Müller-Broich*, Telemediengesetz, 1. Auflage 2012, § 13 Rn. 10, der auf die Bedeutung der anonymen Nutzung für den Erfolg des Internets hinweist.
[54] Hierzu auch die Darstellung bei *Schulz/Heilmann* in: Gieschmann u.a., Datenschutz-Grundverordnung, Art. 85 Rn. 28.
[55] Siehe etwa das Vorgehen der rumänischen Datenschutzaufsichtsbehörde gegen die Journalisten des RISE Project, https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/dsgvo-rumaenien-missachtet-quellenschutz/.
[56] Derartige Szenarien sind zusätzlich relevant, wie Bund und Länder weiterhin davon absehen, transparente Verfahren für die Besetzung der Leitungspositionen der Datenschutzaufsichtsbehörden gemäß Art. 53 Abs. 1 DSGVO zu schaffen und somit rechtsstaatlichen Fehlentwicklung nicht im Rahmen des Möglichen begegnen, siehe *Engeler*, CR-online.de Blog vom 06.08.2018, https://www.cr-online.de/blog/2018/08/06/die-ernennung-der-beauftragten-fuer-den-datenschutz-und-das-transparente-wahlverfahren-nach-art-53-abs-1-dsgvo/.

In Umsetzung des oben vertretenen Gleichklangs zwischen Art. 85 Abs. 1 und Abs. 2 DSGVO hinsichtlich des Umfangs der Abweichungsmöglichkeiten[57] ließe sich eine entsprechende Regelung wie folgt formulieren:

> *Formulierungsvorschlag 9*
> *„Die Vorgaben der Kapitel II bis VII sowie IX gelten nur, sofern sie unter Abwägung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu wissenschaftlichen, künstlerischen, journalistischen oder literarischen Zwecken angemessen sind.*"

Als etwas weniger weitgehende Reduzierung wäre auch denkbar, einzelne Regelungen, deren Anwendbarkeit in jedem Fall als notwendig erachtet wird, von der Abwägungsklausel des Formulierungsvorschlags 9 rückauszunehmen. Damit würde zudem ein höheres Maß an Bestimmtheit im Verhältnis zu einer reinen Abwägungslösung erreicht. Eine entsprechende Regelung könnte wie folgt lauten:

> *Formulierungsvorschlag 10*
> *„Die Vorgaben der Betroffenen des Kapitel II bis VII sowie IX gelten nur, sofern sie unter Abwägung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu wissenschaftlichen, künstlerischen, journalistischen oder literarischen Zwecken angemessen sind. Satz 1 gilt nicht für [Aufzählung stets anwendbarer Vorschriften].*"

Im Idealfall würde hingegen der gesamte Katalog der datenschutzrechtlichen Nebenpflichten der DSGVO auf ihre Vereinbarkeit mit den Kommunikationsgrundrechten des Art. 85 DSGVO überprüft und jeweils ihre Geltung und die Umstände ihrer Geltung konkret klargestellt.

Zu erörtern ist abschließend die Reduzierung der Kontroll- und Aufsichtsbefugnisse der Aufsichtsbehörden, insbesondere, ob insoweit auch Ausnahmen von Kapitel VIII zulässig sind. Will man Art. 85 Abs. 1 DSGVO in seinem Öffnungsumfang ähnlich lesen, wie Art. 85 Abs. 2 DSGVO,[58] so bliebe dafür kein Raum, da dort Kapitel VIII gerade ausgenommen ist. Damit wäre es nicht möglich, das Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO), das Recht auf wirksame Rechtsbehelfe gegen Verantwortliche (Art. 79 DSGVO) oder Haftung und Schadensersatzansprüche (Art. 82 DSGVO) anzupassen. Insbesondere das Recht auf Beschwerde bei einer Aufsichtsbehörde

[57] Abschnitt B. 2.
[58] So die hiesige Auffassung, siehe Abschnitt B. 2.

würde aber ohnehin ins Leere laufen, sofern die diesbezüglichen Aufsichts- und Kontrollbefugnisse des Kapitel VI reduziert werden.[59]

Praktisch relevant bleibt damit vorrangig die Frage der Schadensersatzpflichten. Will man Art. 85 Abs. 1 DSGVO insoweit als weitergehende Öffnungsklausel verstehen, würde auch eine Anpassung des Kapitel VIII möglich werden mit der Folge, dass auch die Regelungen hinsichtlich der Schadensersatzpflicht modifiziert werden könnten. Die datenschutzrechtlichen Folgeansprüche und -pflichten könnten so weitgehend zugunsten der etablierten zivilrechtlichen Rechte und Pflichten rund um das Allgemeine Persönlichkeitsrecht reduziert werden. Dies könnte insofern vorteilhaft sein, als dass die Rechtsprechung zu Verletzungen des Allgemeinen Persönlichkeitsrechts sehr restriktiv an eine tatsächliche Persönlichkeitsrechtsverletzung anknüpft, während Art. 82 DSGVO unabhängig von einer Persönlichkeitsrechtsverletzung jedweden Verstoß gegen die DSGVO ausreichen lässt.[60] Letztlich kann, auch mangels hinreichender Erfahrung mit der Vorgängernorm der DSRL, derzeit nur schwer beurteilt werden, inwiefern sich aus Art. 82 DSGVO in der Praxis tatsächlich gegenüber der bisherigen Rechtslage weitergehende Ersatzpflichten ergeben.[61]

5. Zur Gesetzgebungskompetenz des Bundes

Entscheidend für eine Umsetzung des Art. 85 Abs. 1 DSGVO ist schließlich die Gesetzgebungskompetenz des Bundes. Der Grundregel des Art. 70 Abs. 1 GG folgend, ist dabei stets nach einer ausdrücklichen Gesetzgebungskompetenz des Bundes zu fragen, andernfalls steht das Recht der Gesetzgebung den Ländern zu. Den Kompetenzkatalogen des Art. 73 GG (ausschließliche Gesetzgebung des Bundes) und Art. 74 GG (konkurrierende Gesetzgebung des Bundes) ist allerdings keine abstrakte Kompetenz für die Meinungsfreiheit oder das Datenschutzrecht zu entnehmen. Ausdrückliche Kompetenzen finden sich nur für einzelne Bereiche, etwa das Urhebergesetz, womit jedenfalls Regelungen entsprechend der bisher vom KUG[62] erfassten Bereiche der Veröffentlichung von Bildnissen von Personen im Rahmen einer Umsetzung des Art. 85 Abs. 1 GG möglich sind.[63] Für den Bereich der Öffentlichkeitsarbeit öffentlicher Stellen des Bundes hat das Bundesverwaltungsgericht zudem klargestellt, dass die

---

[59] *Pauly*, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, Art. 85 Rn. 11; *Specht/Bienemann*, in: Sydow DSGVO, Art. 85 Rn. 16.
[60] *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 82 Rn. 7.
[61] Für weitergehende Ersatzpflichten aber Gola/Piltz, in Gola, Datenschutz-Grundverordnung 2. Auflage 2018, Art. 82 Rn. 12.
[62] Zum Streitstand um die (fehlende) Fortgeltung des KuG nach Geltungsbeginn der DSGVO vgl. *Hansen/Brechtel*, GRUR-Prax 2018, S. 369.
[63] Kritisch diesbezüglich aber der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, LT-SH Drucks. 19/1246, S. 3.

Gesetzgebungskompetenz bei dem Bund, nicht bei den Ländern liegt, sofern es um presserechtliche Angelegenheiten der Bundesbehörden geht.[64]

Im Übrigen hat bereits das 1. DSAnpUG in seiner Begründung weitgehend auf eine Annexkompetenz verwiesen, die aus den jeweiligen Sachkompetenzen der Art. 73 bis 74 GG folgt.[65] Für eine wirtschaftliche, auch eine literarische oder künstlicher Betätigung, ließe sich eine Kompetenz insofern aus Art. 74 Abs. 1 Nr. 11 GG ableiten.[66] Der Bereich der allgemeinen Meinungsfreiheit steht zweifelsohne auch in einem Sachzusammenhang mit der Kompetenz des Art. 74 Abs. 1 Nr. 1 GG (bürgerliches Recht).[67] Die ebenfalls in Art. 74 Abs. 1 Nr. 1 GG geregelte Kompetenz für das Strafrecht betrifft mit dem Straftatbestand des § 185 StGB ebenfalls die Zulässigkeit von Meinungsäußerungen. Die Kompetenz für das Vereinsrecht (Art. 74 Abs. 1 Nr. 3 GG) könnte im Annex schließlich die Datenverarbeitung zu Zwecken der Öffentlichkeitsarbeit von Vereinen, Verbänden und Parteien[68] erfassen.

Jedenfalls im Ergebnis dürfte es nicht zu bestreiten sein, dass es zweckmäßig ist, den Schutz der Meinungsfreiheit und seiner besonderen Schutzbereiche bundeseinheitlich zu regeln, um zu verhindern, dass eine Meinungsäußerung, eine literarische Datenverarbeitung oder ein wissenschaftlicher Vortrag in den einzelnen Bundesländern unter abweichenden Bedingungen zulässig sind.

---

[64] BVerwG, NVwZ 2013, S. 1006.
[65] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BT-Drucks. 18/11325, S. 71.
[66] *Kühling/Martini*, EuZW 2016, S. 448 (453).
[67] *Simitis*, in: Simitis, Bundesdatenschutzgesetz 8. Auflage 2014, § 1 Rn. 6.
[68] *Degenhart*, in: Sachs, Grundgesetz 8. Auflage 2018, Art. 74 Rn. 30, sieht insoweit den Art. 21 GG als lex specialis an, was am Ergebnis der Bundeskompetenz aber nichts ändert.

C. Stellungnahme bezüglich einer Ausnahme datenschutzrechtlicher Verstöße aus dem Anwendungsbereich des UWG

Im September 2018 veröffentlichte das Bundesministerium der Justiz und für Verbraucherschutz den Referentenentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs,[69] der das Abmahnwesen grundlegend überarbeiten soll. Geplant sind u.a. Anpassungen der Klagebefugnis, der Gegenstands- und Streitwerte sowie die Einführung einer Bagatellgrenze, womit insgesamt der Missbrauch durch Abmahnungen verhindert werden soll, die einzig auf die Geltendmachung von Gebühren gerichtet sind. Vor allem kleine Unternehmen und Selbstständige sollen so entlastet werden.

Um und nach dem Geltungsbeginn der DSGVO wurde eine DSGVO-„Abmahnwelle" befürchtet und eine gesetzliche Klarstellung (sei es im Rahmen des Gesetzes zur Stärkung des fairen Wettbewerbs oder im BDSG) dahingehend gefordert, dass datenschutzrechtliche Verstöße nicht als Verstöße im Sinne des UWG anzusehen seien.[70] Eine derartige ausdrückliche Ausnahme ist aber weder nötig (dazu unter 1.) oder sinnvoll (dazu unter 2.), noch als Ausdruck einer ohnehin bestehenden Sperrwirkung geboten (dazu unter 3.) und begegnet nicht zuletzt europarechtlichen Bedenken hinsichtlich der grundsätzlichen Zulässigkeit einer solcher Einzelausnahme für datenschutzrechtliche Verstöße (dazu unter 4.). Zu berücksichtigen ist schließlich auch, dass eine mögliche Klarstellung bezüglich des UWG die Regelungen des UKlaG unberührt ließe, was eine Konzentration der zivilrechtlichen Ahndung von Datenschutzverstößen bei wenigen klagebefugten Verbänden zur Folge haben könnte (dazu unter 5.).

1. Eine „Abmahnwelle" ist bisher ausgeblieben

Die tatsächliche Notwendigkeit eines derartigen Ausschlusses ist bisher nicht ersichtlich. Von einer Abmahnwelle kann auch sechs Monate nach Geltungsbeginn der DSGVO keine Rede sein. Die Praxis berichtet vielmehr übereinstimmend von nur vereinzelten – und zum Teil überwiegend inhaltlich zweifelhaften bis unseriösen – Abmahnungen wegen Datenschutzverstößen.[71] Im Gegenteil berichten Praktikerinnen davon, dass der Aufwand für erfolgreiche Abmahnungen aufgrund der hohen Komplexität datenschutzrechtlicher Anforderungen hoch und entsprechende Mandate keineswegs erfolgversprechend sind. Stattdessen scheint die derzeitige Sorge auf eine allgemeine „DSGVO-Panik" zurückzuführen zu sein, die auch mit dem medialen Fokus auf immer neue

---

[69] Antrag der Fraktionen der CDU/CSU und SPD vom 12.06.2018, Ausschuss für Recht und Verbraucher Drs. 19(6)10; Referentenentwurf vom 11.09.2018, online abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_fairerWettbewerb.pdf?__blob=publicationFile&v=1.

[70] Siehe dazu etwa *Asshoff*, CR 2018, S. 720 (721) Fn. 4, mit Verweis auf Forderungen von *Bender* in der Lebensmittelzeitung vom 20.09.2018.

[71] *Schreiber*, GRUR-Prax 2018, S. 371 (371); *Asshoff*, CR 2018, S. 720 (721); *Laoutoumai/Hoppe*, K&R 2018, S. 533 (536).

datenschutzrechtliche Kuriositäten zusammenhängen dürfte, die den Rechtsfolgen der DSGVO zugeschrieben werden. Die diesbezügliche Berichterstattung beruht in Einzelfällen zwar zweifelsohne auf zu diskutierenden Ungereimtheiten der DSGVO, ist in seiner Gesamtheit aber kein tragfähiger Ausgangspunkt für elementare Kritik am datenschutzrechtlichen Status quo.

2. Datenschutzrechtliche Vorgaben haben hohe Wettbewerbsrelevanz

Ein gesetzlicher Ausschluss von Verstößen gegen DSGVO und BDSG aus dem Schutzbereich des UWG wird der wettbewerbsrechtlichen Bedeutung datenschutzrechtlicher Vorgaben nicht gerecht. Insbesondere sprechen gewichtige Argumente dafür, dass die ineffiziente Aufsichtstätigkeit der Landes- und Bundesdatenschutzaufsichtsbehörden in vielen Fällen zu Schutzlücken für Mitbewerberinnen führt und geradezu danach verlangt, dass die aufsichtsbehördliche Durchsetzung der DSGVO durch die Geltendmachung wettbewerbsrechtlicher Ansprüche flankiert wird.[72] Ersparter Aufwand hinsichtlich der Gestaltung von rechtskonformen Datenschutzerklärungen, der Einbindung von Drittinhalten oder der Umsetzung einer angemessenen Transportverschlüsselung („https") in Onlineangeboten, kann Mitbewerberinnen bevorteilen, ohne dass in vielen Fällen dafür ein effektiver Rechtsschutz vorhanden wäre. Die Selbstregulierung mittels des Lauterkeitsrechts kann hier das Schutzregime der DSGVO sinnvoll ergänzen.

Unangemessene Belastungen durch die Ahndung von Bagatellverstößen oder missbräuchliche „Abmahngeschäfte" sind hingegen kein Sonderproblem datenschutzrechtlicher Verstöße (sie sind nach jetzigem Stand sogar eher noch eine Ausnahme), sondern insbesondere im Urheberrecht verbreitet. Eine grundlegende Unausgewogenheit des UWG sollte daher allgemein und strukturell behoben werden, statt mittels sektorspezifischer Ausnahmen, wie sie derzeit hinsichtlich einer Ausklammerung der DSGVO diskutiert werden. Ansätze dafür liefert der angesprochene Entwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs, der insgesamt eine Entlastung herbeiführen will, ohne einzelne Bereiche einer effektiven wettbewerbsrechtlichen Ahndung zu entziehen.

3. Die DSGVO sperrt die Regelungen des UWG nicht

Einige Stimmen aus der Literatur und der Rechtsprechung vertreten, dass die DSGVO ohnehin Sperrwirkung gegenüber den Regelungen des UWG entfalte, während die wohl überwiegende Ansicht in der Literatur sowie ein Teil der Rechtsprechung dem

[72] *Diercks*, CR 2018 (nur online), Rn. 62; *Laoutoumai/Hoppe*, K&R 2018, S. 533 (535).

entgegentreten.[73] Überzeugend ist nach hiesiger Auffassung, dass die DSGVO lediglich die Rechtsbehelfe natürlicher Personen regelt (Art. 77 ff. DSGVO) und gerade keinerlei Aussagen zu anderen Sanktionsregimen trifft. Sanktionsmechanismen zugunsten Dritter, etwa Unternehmen, die aufgrund datenschutzrechtlicher Verstöße von Mitbewerberinnen einen Nachteil erleiden, sieht die DSGVO in den Art. 77 ff. DSGVO nicht vor, [74] sie sind der DSGVO schlicht gleichgültig.[75] Für eine abschließende Regelungswirkung gegenüber anderen Sanktionsregimen, wie sie etwa im § 69 SGB V oder § 44 TKG festgehalten ist, ist in der DSGVO ebenfalls nichts ersichtlich. [76] Die DSGVO bezweckt andererseits ausdrücklich die Förderung des freien Waren- und Dienstleistungsverkehr, so dass auch insoweit nicht ersichtlich ist, weshalb ihren Regelungen eine wettbewerbliche Relevanz abgesprochen werden sollte.[77] Der teilweise geforderte Ausschluss von DSGVO-Verstößen aus dem Anwendungsbereich des UWG stellt vor diesem Hintergrund also keineswegs lediglich eine Klarstellung unstreitiger dogmatischer Verhältnisse dar. Er würde zuletzt auch weder der tatsächlichen Bedeutung des Datenschutzrechts für die Digitalwirtschaft gerecht werden noch dem erklärten politischen Ziel, die Einhaltung datenschutzrechtlicher Vorgaben zu einem Standortvorteil Deutschlands und Europas zu machen.

4. Eine Einschränkung der wettbewerblichen Rechtsbehelfe des UWG steht im Widerspruch zu den Zielen der UGP-Richtlinie

Eine Sperrwirkung folgt auch nicht aus einem Vorrangverhältnis der DSGVO gegenüber der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken (UGP-Richtlinie). Weder ergibt sich aus den Regelungsarten „Richtlinie" und „Verordnung" ein Rangverhältnis, noch hebt die DSGVO die UGP-Richtlinie auf, noch regelt die DSGVO Aspekte unlauterer Geschäftspraktiken im Sinne des Art. 3 Abs. 4 UGP-Richtlinie.[78]

Es wäre letztlich vielmehr zu fragen, inwiefern es Deutschland überhaupt eingeräumt ist, unlautere Praktiken, die im Zusammenhang mit der Verletzung von datenschutzrechtlichen Vorgaben stehen, kategorisch dem Regelungsziel des Art. 1 UGP-Richtlinie zu entziehen, der seinerseits gerade beabsichtigt, durch Angleichung der

---

[73] Siehe zum Meinungsstand statt vieler *Diercks*, CR 2018 (nur online), Rn. 3; Insbesondere *Köhler*, WRP 2018, S. 1269 (dem folgend das LG Bochum, Urteil vom 07.08.2018 – I 12 O 85-18 – sowie das LG Wiesbaden, Urteil vom 05.11.2018 – Az. 5 O 214/18 –) vertritt eine Sperrwirkung; In der Literatur dem folgend: *Baumgartner/Sitte*, ZD 2018, S. 555 (557); *Spittka*, GRUR-Prax 2018, S. 561; Anders hingegen das OLG Hamburg, Urteil vom 25.10.2018 – 3 U 66/17, BeckRS 2018, 27136 sowie das LG Frankfurt, Beschluss vom 08.10.2018 – 2-06 O 349/18 –; In der Literatur gegen eine Sperrwirkung zudem *Asshoff*, CR 2018, S. 720; *Laoutoumai/Hoppe*, K&R 2018, S. 533; *Schreiber*, GRUR-Prax 2018, S. 371 (371); Übersicht zum Diskussionsstand auch bei *Löffel/Abrar*, online verfügbar unter: https://loeffel-abrar.com/newsblog/sind-verstoesse-gegen-die-datenschutz-grundverordnung-wettbewerbswidrig/.
[74] *Asshoff*, CR 2018, S. 720 (726).
[75] *Laoutoumai/Hoppe*, K&R 2018, S. 533 (535).
[76] *Diercks*, CR 2018 (nur online), Rn. 51.
[77] So auch *Schreiber*, GRUR-Prax 2018, S. 371 (373); *Asshoff*, CR 2018, S. 720 (727).
[78] *Diercks*, CR 2018 (nur online), Rn. 28f.

Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über unlautere Geschäftspraktiken, die die wirtschaftlichen Interessen der Verbraucher beeinträchtigen, zu einem reibungslosen Funktionieren des Binnenmarkts und zum Erreichen eines hohen Verbraucherschutzniveaus beizutragen. Dieses Ziel würde gerade verhindert, wenn die Einhaltung datenschutzrechtlicher Vorgaben und die ihnen innewohnenden wettbewerbsrechtliche Relevanz für den digitalen Binnenmarkt ignoriert würden.

5. Konzentrationswirkung auf das UKlaG

Zum Abschluss ist darauf hinzuweisen, dass die Ausnahme von DSGVO-Verstößen aus dem Anwendungsbereich des UWG, die Regelungen des UKlaG unberührt ließe. Insbesondere § 2 Abs. 2 Nr. 11 UKlaG, der all jene Vorschriften zu Verbraucherschutzgesetzen erklärt, welche die Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer oder (in ausgewählten Geschäftsbereichen) die Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, betreffen, würde unverändert die Durchsetzung von Unterlassungs- und Widerrufsansprüchen erlauben. Diese Rechte würden allerdings nur noch anspruchsberechtigten Stellen im Sinne des § 3 UKlaG zustehen, was eine Konzentration der zivilrechtlichen Ahndung datenschutzrechtlichen Verstöße in Person dieser Stellen zur begünstigen würde.[79] Die Selbstregulierungsmöglichkeiten mittels des UWG würden damit entzogen und Mitbewerberinnen wären ebenso wie bei dem Verweis auf die Aufsichtstätigkeit des Datenschutzbehörden auf das Einschreiten Dritter angewiesen, deren Ziele – abgesehen von fehlenden Kapazitäten – jedoch nicht in jedem Fall den eigenen entsprechen müssen.

[79] Zum bisherigen Nebeneinander von UKlaG und UWG siehe auch *Podszun/de Toma*, NJW 2016, S. 2987 (2989).

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 B

STELLUNGNAHME

Berlin, 05. Dezember 2018

Deutscher Industrie- und Handelskammertag

Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestags zum Gesetzentwurf der Bundesregierung Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. Datenschutz-Anpassung- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) BT-Drucksachen 19/4674,19/5414

I. Vorbemerkung

Die Anpassung der bereichsspezifischen Datenschutzregelungen ist erforderlich. Sie gibt Gelegenheit, die Vorschriften auch daraufhin zu überprüfen, ob sie den Anforderungen des Art. 6 Datenschutz-Grundverordnung (DSGVO) an eine ausreichende Rechtsgrundlage genügen.

Der Gesetzentwurf war zunächst nur unter dem Aspekt der formalen, redaktionellen Anpassung an die DSGVO formuliert worden. Nach mehr als einem halben Jahr Gültigkeit der DSGVO stellt sich jedoch die Frage, ob diese Gelegenheit genutzt werden sollte, um gewisse Entlastungen für die Verantwortlichen im Sinne des Datenschutzes zu schaffen.

Die DSGVO ist von dem Grundsatz „one size fits all“ ausgegangen. Wie die Praxis zeigt, trifft dieses Prinzip nur teilweise zu: kleinere und mittlere Unternehmen (KMU) sind verhältnismäßig stärker belastet mit der Umsetzung als größere und große Unternehmen. Sie können häufig nicht auf internen Sachverstand in Person eines betrieblichen Datenschutzbeauftragten zurückgreifen, sondern müssen externen Rat in Anspruch nehmen. Dieser ist aber momentan schwer zu bekommen, da alle kompetenten Berater eine sehr hohe Anzahl an Mandaten zu betreuen haben.

II. Konkrete Vorschläge

1. Betrieblicher Datenschutzbeauftragter

Das Institut des betrieblichen Datenschutzbeauftragten hat sich seit seiner Einführung bewährt. Es ist Ausdruck der Selbstverantwortung und der effektiven Selbstkontrolle der Unternehmen. Das Konzept des Datenschutzbeauftragten ist daher auch mit der DSGVO EU-weit eingeführt worden. Die DSGVO sieht jedoch die Bestellung eher als Ausnahme vor, während das BDSG die Bestellung als Regel ausgestaltet (hat).

Durch die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten entstehen den KMU erhebliche Belastungen zusätzlich zu denen der DSGVO (Dokumentations-, Informationspflichten).

DIHK | Deutscher Industrie- und Handelskammertag e.V.
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Fax 030-20308-1000 | Internet: www.dihk.de

Der Spielraum des nationalen Gesetzgebers, im nichtöffentlichen Bereich von der DSGVO abzuweichen, ist sehr eng. Das BDSG eröffnet aber die Möglichkeit zur Erleichterung bei § 38 mit der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten.

Bei der Änderung des BDSG zur Anpassung an die DSGVO wurde der bisher geltende Schwellenwert im Wesentlichen (nun: 10 Personen) beibehalten. Damit muss eine hohe Anzahl an Unternehmen einen betrieblichen Datenschutzbeauftragten bestellen. Die Zahl der zu berücksichtigenden Personen erhöht sich schnell bei Teilzeitbeschäftigungen oder auch bei Saisonbetrieben.

Ferner ist die Voraussetzung „ständig…" mit Rechtsunsicherheit verbunden, da die Verarbeitung personenbezogener Daten bereits durch das Versenden von E-Mails häufig erfüllt ist. Zwar können sich auch durch die Nutzung von E-Mail-Verteilern datenschutzrechtliche Risiken ergeben. Dennoch geht der Gesetzgeber wohl eher von anderen Risikoszenarien aus. Daher scheint eine Formulierung angebracht, die solchen Risikosituationen entgegenwirken kann.
In etlichen Unternehmen besteht die „ständige Verarbeitung" z. B. nur im Aufrufen der Kundendatei, um Lieferungen oder Dienstleistungen zu erbringen, die heute üblicherweise elektronisch bearbeitet werden. In einem Großteil der Unternehmen werden personenbezogene Daten eigentlich nur als Nebenprodukt, in Form von Lesen genutzt, z. B. ein Lagerarbeiter, der ein Versandetikett auf das Paket klebt, oder Transporteur, der eine Ware ausliefert und sich eine Unterschrift auf dem Tablett geben lässt.

Vorschlag:
1. Zunächst sollte die Pflicht zur Bestellung auf den gewerblichen Bereich beschränkt werden. Momentan trifft die Pflicht zur Bestellung auch Vereine. Zwar wird auch dort eine Vielzahl von personenbezogenen Daten verarbeitet. Damit Idealvereine nicht erfasst werden, die durchaus wirtschaftliche Tätigkeit ausüben können, die aber dem Vereinszweck untergeordnet ist, sollte der Anknüpfungspunkt der Gemeinnützigkeit geprüft werden. Wie Erwägungsgrund 18 der DSGVO zeigt, sollen von der DSGVO nicht-berufliche Tätigkeiten in Bezug auf den Datenschutz ausgenommen werden. Daher erscheint es sinnvoll, die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten auf die Fälle zu beschränken, in denen Verantwortliche personenbezogene Daten geschäftsmäßig verarbeiten oder – alternativ – die Verarbeitung gewerblichen Zwecken dient, wobei letzteres auch Freiberufler ausnehmen würde, die zu einem großen Teil ohnehin ihrem Berufsgeheimnis unterliegen.

2. Für eine Anhebung des Schwellenwertes von 10 auf 20 Beschäftigte spricht, dass viele der kleineren und mittleren Unternehmen personalintensiv wegen Teilzeitbeschäftigten oder Saisonarbeitern sind. Mit der Klarstellung von Verantwortlichkeiten nimmt die DSGVO verstärkt die Unternehmer („Verantwortliche) in die Pflicht. Inhaber/Geschäftsführer sind im Zweifel ohnehin die Verantwortlichen, müssen also für die Festlegung des Schwellenwertes nicht berücksichtigt werden. Insofern macht es gerade bei KMU Sinn, dass diese nicht dauerhaft einen Datenschutzbeauftragten bestellen müssen, sondern punktuell bei Bedarf entsprechende Dienste in Anspruch nehmen können. Dies trägt zur Kostenreduzierung bei und entschärft die Nachfrage nach fachlich qualifizierten Datenschutzbeauftragten, ohne dass dies zu qualitativen Einbußen führen muss.

3. Generell ist jedoch zu fragen, ob ein Schwellenwert für die Bestellung eines betrieblichen Datenschutzbeauftragten sinnvoll ist. Angesichts der neuen Möglichkeiten, mit – sehr – kleinen Einheiten erhebliche Mengen von Daten verarbeiten zu können, wäre es sinnvoller, die Idee der DSGVO zu übernehmen, anhand der Tätigkeit des Unternehmens („Kerntätigkeit") bzw. der Beschäftigten zu differenzieren, um damit dem durch ein hohes Maß an Datenverarbeitung steigenden Risiko zu begegnen.

Der DIHK schlägt daher folgende Formulierung für § 38 Abs. 1 BDSG vor:

§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen
(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit in der Regel mindestens **zwanzig Beschäftigte ständig personenbezogene Daten automatisiert verarbeiten und die Verarbeitung gewerblichen Zwecken dient**. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Hilfsweise käme auch noch folgende Änderung in Betracht, wenn der Schwellenwert der Beschäftigten nicht geändert werden sollte:
§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen
(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit in der Regel mindestens zehn **Beschäftigte ständig personenbezogene Daten automatisiert verarbeiten und die Verarbeitung gewerblichen Zwecken dient**. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Unabhängig von einem Schwellenwert könnte folgende Formulierung genutzt werden. Allerdings birgt sie neue Rechtsunsicherheiten bzgl. des Begriffs „wesentlich“:

§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen
(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit **die Verarbeitung gewerblichen Zwecken dient und die wesentliche Tätigkeit der Beschäftigten in der automatisierten Verarbeitung personenbezogener Daten besteht**. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

2. Abmahnungen

Zwar ist die befürchtete Abmahnwelle durch Inkrafttreten der DSGVO ausgeblieben. Es hat aber durchaus Versuche flächendeckender Abmahnungen gegeben. Wie die Entscheidungen des LG Würzburg und des LG Bochum zeigen, besteht auch bei Gerichten eine unterschiedliche Rechtsauffassung zu der Frage, ob die DSGVO eine abschließende Regelung ist. Um Unternehmen vor

dieser Rechtsunsicherheit wirksam zu schützen, muss der Gesetzgeber Klarheit schaffen. Insofern schlagen wir vor, klarzustellen, dass weder die DSGVO noch das BDSG Vorschriften im Sinne von § 3a UWG sind.

Datenschutz ist nicht Verbraucherschutz, sondern ein Individualgrundrecht, das sich kollektiver Wahrnehmung entzieht.

Unternehmen nehmen zunehmend die Beratungsleistung der Datenschutzaufsichtsbehörden in Anspruch. Diese positive Zusammenarbeit hat bisher auch dazu geführt, dass wenige Klagen im Bereich des Datenschutzes erhoben wurden. Behörden arbeiten mit verschiedenen Maßnahmen eher unterstützend als bestrafend nicht nur auf die Beseitigung, sondern schon auf die Verhinderung von Datenschutzverstößen hin. In vielen Fällen verhängen sie nicht sofort Bußgelder und sonstige Strafen, sondern wirken im ersten Schritt durch Hinweise auf die Korrektur des Fehlers hin sowie mittels Orientierungshilfen, Informationsblättern und Veranstaltungen präventiv Verstößen entgegen und erhöhen das Bewusstsein bei den Unternehmen.

Im Internet gibt es sicherlich viele Datenschutzerklärungen, die abmahnfähig sind, weil die vielen Informationspflichten inzwischen kaum zu überblicken und einzuhalten sind. In den meisten Fällen liegt aber trotz fehlerhafter Datenschutzerklärung tatsächlich kein Datenmissbrauch vor. Eine sofortige Abmahnung ist überzogen und führt zu einer unnötigen Zusatzbelastung für Unternehmen. Flächendeckende Kontrollen durch die Behörden dagegen führen nicht nur zu einer Beseitigung von eventuellen datenschutzrechtlichen Defiziten bei dem geprüften Unternehmen, sondern lenken auch die Aufmerksamkeit der anderen Unternehmen auf den Datenschutz und die Beseitigung der in der jeweiligen Prüfung festgestellten Mängel (z. B. durch die Tätigkeitsberichte der Datenschutzaufsichtsbehörden).

Das Nebeneinander von Datenschutzaufsicht und Verbandsklagerecht führt zu einer Rechtszersplitterung durch unterschiedliche Rechtswege. Damit erhöht sich die Rechtsunsicherheit für die Unternehmen, weil auch die Ergebnisse gerichtlicher Auseinandersetzungen unterschiedlich sein werden. Zwar ist eine Klärung von Rechtsfragen im Datenschutz durch Gerichte durchaus wünschenswert, diese sollte aber einheitlich in einem Rechtsweg erfolgen. Die momentane Rechtslage schafft die Gefahr widerstreitender Entscheidungen.

Ferner droht im Zivilverfahren immer das Damoklesschwert der einstweiligen Verfügung, die im Zweifel vorläufig vollstreckbar ist, ohne dass der Abgemahnte vorher angehört wird. Von einer echten „Anhörung“ des Betroffenen im Rahmen einer Abmahnung kann in den meisten Fällen kaum gesprochen werden. Die einstweilige Verfügung wird jedenfalls bei wettbewerbsrechtlichen Abmahnungen praktisch standardmäßig als Druckmittel eingesetzt. Es bringt aber gerade Kleinunternehmer oft dazu, selbst bei unberechtigten oder zweifelhaften Abmahnungen schnell die Unterlassungserklärung zu unterschreiben und die Kosten zu bezahlen.

Demgegenüber ist das Verwaltungsverfahren bei Maßnahmen der Aufsichtsbehörde völlig anders strukturiert: Bevor ein (vorläufig) vollstreckbarer Verwaltungsakt seine Wirkung entfaltet, ist eine vorherige Anhörung des Betroffenen verpflichtend. Ein verwaltungsinternes Prüfungsverfahren erzeugt für den Betroffenen zunächst keine Kosten. Kommt der Fall vor Gericht, geht er in der Regel ins Hauptsacheverfahren. Denn Eilmaßnahmen kann die Behörde bei Eilbedürftigkeit selbst treffen.

Der Ansatz der DSGVO zu einem one-stop-shop (Kohärenzverfahren), bei dem die Unternehmen EU-weit eine Auskunft zu datenschutzrechtlichen Fragen erhalten, und das analoge nationale Verfahren würde durch die Möglichkeit von Abmahnungen konterkariert.

In der DSGVO wird die Unabhängigkeit der Aufsichtsbehörden als ein wichtiges Regelungsziel in Umsetzung der Rechtsprechung des EuGH gesehen. Private Verbände unterliegen hingegen anderen Interessen und Abhängigkeiten.

Der DIHK schlägt daher folgende Formulierung für eine Regelung im BDSG vor:

„Vorschriften der Verordnung (EU) 679/2016 und Vorschriften der Teile 1 und 2 dieses Gesetzes stellen keine Vorschriften im Sinne von § 3a des Gesetzes gegen den unlauteren Wettbewerb dar."

3. Öffnungsklausel des Art. 10 DSGVO

Nach dem Wortlaut des Art. 10 ist die Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen nur „unter behördlicher Aufsicht" zulässig. Unternehmen benötigen aber in etlichen Zusammenhängen z. B. Auskünfte aus dem Bundeszentralregister von ihren Beschäftigten oder von anderen Vertragspartnern. Das gilt z. B. bei Bewachungsunternehmen, die im Sicherheitsbereich öffentlicher Einrichtungen tätig sind oder für Versicherungsunternehmen bei leitenden Personen oder Personen in Schlüsselfunktionen. Da diese Verarbeitung auf einer Rechtsgrundlage basiert, ist sie nach Art. 6 Abs. 1 lit. b DSGVO zulässig, scheint aber durch Art. 10 wiederum verboten. Zur Schaffung von Rechtsklarheit für die Unternehmen wäre es daher sinnvoll zu regeln, dass Unternehmen Daten über Straftaten und strafrechtliche Verurteilungen verarbeiten dürfen, wenn sie dazu durch gesetzliche Vorschriften verpflichtet sind oder es im Rahmen von Verträgen erforderlich ist.

Ansprechpartnerin im DIHK

Annette Karstedt-Meierrieks
Bereich Recht
Leiterin des Referats Wirtschaftsverwaltungsrecht,
Öffentliches Auftragswesen, Datenschutz
DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin
Telefon 030 20308-2706
Fax 030 20308-52706
E-Mail: karstedt-meierrieks.annette@dihk.de
www.dihk.de

Wer wir sind:

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.
Auf Bundes- und Europaebene setzt sich der DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.
Darüber hinaus koordiniert der DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.

Er ist im Register der Interessenvertreter der Europäischen Kommission registriert (Nr. 22400601191-42).

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 C

Richter Sandy PA4

Von: Prof. Dr. Helmut Köhler <h.koehler.neusaess@t-online.de>
Gesendet: Dienstag, 4. Dezember 2018 23:00
An: Innenausschuss PA4
Betreff: Anhörung am 10.12.2018 - Stellungnahme Köhler
Anlagen: BT-Innenausschuss_10.12.2018 - Köhler.docx

Sehr geehrter Herr Dr. Heynckes,

haben Sie vielen Dank für die Einladung zur Anhörung im Innenausschuss am 10.12.2108. Anbei darf ich Ihnen meine Stellungnahme übersenden.

Aus meiner Sicht wäre es zweckmäßig, wenn die Ausschussmitglieder einen Auszug aus der DS-GVO bekommen könnten, der die Art. 9, 17, 42, 57, 58, 77 – 84 DS-GVO umfasst. Auch § 44 BDSG wäre von Interesse. Damit würde die bessere Verständlichkeit meines Textes gewährleistet.

Für Rückfragen stehe ich gerne zur Verfügung, vorzugsweise per Mail an H.Koehler.Neusaess@t-online.de.

Mit besten Grüßen

Helmut Köhler

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR INTERNATIONALES RECHT
EUROPÄISCHES UND INTERNATIONALES
WIRTSCHAFTSRECHT
PROF. EM. DR. HELMUT KÖHLER

Prof. em. Dr. Helmut Köhler · Ludwigstr. 29/II · 80539 München

2. Datenschutzanpassungs- und Umsetzungsgesetz EU
Anhörung des Innenausschusses des Deutschen Bundestags am 10.12.2018

Stellungnahme zum Thema

„Durchsetzung des Datenschutzrechts mit den Instrumenten des Wettbewerbs- und Verbraucherschutzrechts?“

Zusammenfassung

1. Die DS-GVO bezweckt den Schutz des Grundrechts natürlicher Personen auf Schutz ihrer personenbezogenen Daten (Art. 1 II DS-GVO). Sie bezweckt dagegen nicht den Schutz der kollektiven Verbraucherinteressen wie die UGP-Richtlinie (und das UWG) und die Unterlassungsklagenrichtlinie (und das UKlaG).

2. Die Durchsetzung der allgemeinen Vorschriften der DS-GVO ist alleinige Aufgabe der nationalen Aufsichtsbehörden (Art. 57 I lit. a DS-GVO). Diese Regelung des *public enforcement* ist abschließend. Sie kann nicht durch ein *private enforcement* von Mitbewerbern oder Verbänden mittels der §§ 3a, 8 III UWG oder der § 2 II 1 Nr. 11, § 3 UKlaG ergänzt werden. *Beispiel:* Eine Partnervermittlung speichert von Kunden/Kundinnen ohne deren Einwilligung Daten, aus denen ihre ethnische Herkunft, ihre religiösen oder weltanschaulichen Überzeugungen hervorgehen, sowie Daten zu ihrem Sexualleben. Genau dies ist nach Art. 9 I DS-GVO untersagt. Ein generelles Verbot dieser Art der Datenverarbeitung kann nur von den Aufsichtsbehörden ausgesprochen, nicht dagegen von Verbänden oder Mitbewerbern im Klagewege durchgesetzt werden.

3. UWG und UKlaG kennen keinen Individualschutz der Verbraucher. Die DS-GVO gewährt dagegen den „betroffenen Personen" individuelle Rechte insbesondere auf Auskunft, Berichtigung und Löschung, Datenübertragung und Widerspruch. Die betroffenen Personen können ihre Rechte selbst durchsetzen (Art. 79 DS-GVO), aber auch eine Einrichtung i.S. des Art. 80 I DS-GVO zu diesem Zweck beauftragen und bevollmächtigen. *Beispiel:* Kundin K kann von der Partnervermittlung Löschung der sie betreffenden gespeicherten Daten verlangen (Art. 17 I lit. d DS-GVO). Die Aufsichtsbehörden müssen die betroffenen Personen bei der Ausübung ihrer Rechte unterstützen und sich mit ihren Beschwerden befassen (Art. 57 I lit. e, f DS-GVO).

4. Die Mitgliedstaaten können außerdem nach Art. 80 II DS-GVO vorsehen, dass eine Einrichtung i.S. des Art. 80 I DS-GVO das Recht hat, die Rechte betroffener Personen ohne deren Auftrag geltend zu machen. Von dieser Öffnungsklausel hat der deutsche Gesetzgeber bisher noch keinen Gebrauch gemacht.

5. Die Öffnungsklausel des Art. 80 II DS-GVO ist nicht weit, sondern als Ausnahmevorschrift eng auszulegen. Ihr ist nicht zu entnehmen, dass die Mitgliedstaaten darüber hinaus sonstige Dritte (wie etwa Mitbewerber, Verbraucherschutzbehörden, Ombudsleute) ermächtigen dürften, die Rechte betroffener Personen wahrzunehmen.

6. Die Einschaltung von Mitbewerbern und Verbänden in die Durchsetzung der DS-GVO würde überdies zu einem unabgestimmten Nebeneinander von *public* und *private enforcement* führen. Es wären völlig unterschiedliche Entscheidungen der auf den Datenschutz spezialisierten Aufsichtsbehörden (§ 58 II DS-GVO)

einerseits und der zahlreichen jeweils angerufenen Zivilgerichte andererseits und damit im Ergebnis eine unionsweite Rechtszersplitterung zu befürchten.

7. Ein zusätzliches *private enforcement* würde auch zu einer Mehrbelastung der Gerichte führen, ohne dass dem eine Entlastung der Aufsichtsbehörden entspräche. Die Mehrkosten fielen dem Bund und den Ländern zur Last. Dies gilt auch für die Mittelausstattung der Verbraucherverbände.

8. Zugleich käme es zu einer Mehrbelastung der wegen eines Datenschutzverstoßes in Anspruch genommenen Unternehmen, weil sie sich sowohl gegenüber der Aufsichtsbehörde als auch gegenüber privaten Klägern verteidigen müssten. Davon wären insbesondere kleine Unternehmen betroffen, die nicht anwaltlich beraten sind und einer Abmahnung zumeist hilflos gegenüberstünden.

9. Der Gesetzgeber sollte die derzeit bestehende Rechtsunsicherheit beseitigen. Dazu würde sich eine Ergänzung des § 44 DS-GVO empfehlen. Es sollte erstens die Regelung des Art. 80 I DS-GVO konkretisiert werden. Zweitens sollte von der Öffnungsklausel des Art. 80 II DS-GVO Gebrauch gemacht werden. Dann wären auch und gerade *Verbraucherverbände* bei entsprechender Satzungsänderung befugt, im eigenen Namen gebündelt die Individualrechte betroffener Personen mit deren Zustimmung, aber ohne deren Auftrag außergerichtlich und gerichtlich durchzusetzen. Darüber hinaus sollte drittens zumindest in der Gesetzesbegründung klargestellt werden, dass die Durchsetzung der allgemeinen Vorschriften der DS-GVO allein Aufgabe der Aufsichtsbehörden ist.

10. Die Regelungen in § 2 I 3, II 1 Nr. 11 und II 3 UKlaG sind mit der DS-GVO als dem höherrangigen Unionsrecht nicht vereinbar und dürfen daher von den Gerichten ab dem 28.05.2018 nicht mehr angewendet werden. Der Gesetzgeber sollte sie im Interesse der Rechtsklarheit und Rechtssicherheit für alle Beteiligten daher aufheben.

A. Das Problem

In Rspr.[1] und Schrifttum[2] ist umstritten, ob Verstöße von Unternehmen gegen die DS-GVO nicht nur von den Aufsichtsbehörden (*public enforcement*), sondern darüber hinaus auch noch von Mitbewerbern und Verbänden nach den §§ 3a, 8 III UWG und den §§ 2, 3 UKlaG (*private enforcement*) verfolgt werden können. Die Lösung dieses Problems hängt entscheidend davon ab, ob die unionsrechtlichen Regelungen der DS-GVO dies zulassen oder nicht.

Diese Auslegungsfrage muss letztlich der EuGH entscheiden. Auf der Ebene der deutschen Gesetzgebung kann es daher nur darum gehen, ob der Gesetzgeber die derzeit und möglicherweise noch lange bestehende Rechtsunsicherheit durch eine Regelung pro oder contra eines *private enforcement* beseitigen sollte.

Die nachfolgende Analyse soll dazu beitragen, dem Innenausschuss eine sachliche Grundlage für seine Entscheidung zu geben.

B. Darstellung der Unterschiede zwischen Wettbewerbsrecht (UWG), Verbraucherschutzrecht (UKlaG) und Datenschutzrecht (DS-GVO)

I. Wettbewerbsrecht (UWG)

1. Wer wird geschützt?

Das UWG schützt drei Gruppen von Marktteilnehmern vor unlauteren Handlungen, nämlich Mitbewerber, Verbraucherinnen und Verbraucher sowie sonstige Marktteilnehmer (§ 1 S. 1 UWG).

2. Was bedeutet Verbraucherschutz im UWG?

Die verbraucherschützenden Verbote der §§ 3 ff. UWG dienen dem Schutz der *wirtschaftlichen Interessen* der Verbraucher (Erwägungsgrund 6, 8 UGP-Richtlinie). Verbraucher sollen ihre *geschäftlichen Entscheidungen* (§ 2 I Nr. 9 UWG) frei und „informiert“ (in Kenntnis der erforderlichen Informationen) treffen können (Erwägungsgrund 7, 14, 16 UGP-Richtlinie).

3. Wer ist als Rechtsverletzer verantwortlich?

[1] Die Anwendbarkeit des UWG und des UKlaG wird bejaht von OLG Hamburg, WRP 2018, 1510 (mit krit. Anmerkung Köhler); LG Würzburg (ohne nachvollziehbare Begründung), dagegen verneint vom LG Bochum und vom LG Wiesbaden.

[2] Die Anwendbarkeit des UWG und des UKlaG wird bejaht von Wolff, ZD 2018, 248 ; Laoutoumai/Hoppe, K&R 2018, 533; dagegen verneint von Köhler, in: Köhler/Bornkamm/Feddersen, UWG, 37. Aufl. 2019, § 3a Rn. 1.40a;Schaffert, in: MünchKommUWG, 3. Aufl. 2018, § 3a Rn. 71; Köhler, ZD 2018, Köhler WRP 2018, 1269; Barth, WRP 2018, 790; Schreiber, GRUR-Prax 2018, 371, 372.

Unternehmer verstoßen gegen die §§ 3 ff. UWG, wenn sie geschäftliche Entscheidungen der Verbraucher unlauter beeinflussen, z.B. durch irreführende oder aggressive Geschäftspraktiken (Erwägungsgrund 7 UGP-Richtlinie). Gegen sie können Unterlassungs- und Beseitigungsansprüche zum Schutz der Kollektivinteressen der Verbraucher geltend gemacht werden.

4. Wer setzt den Verbraucherschutz im UWG durch?

Unionsrechtliche Grundlage der Durchsetzung ist Art. 11 I UGP-Richtlinie von 2005. Danach können die Mitgliedstaaten zwischen einem privatrechtlichen und einem verwaltungsrechtlichen Schutzsystem wählen. Deutschland hat sich 2008 für die privatrechtliche Durchsetzung entschieden. Die Durchsetzung erfolgt daher nicht durch Verbraucherschutzbehörden, sondern aufgrund privater Initiative von Mitbewerbern, Unternehmens- und Verbraucherverbänden (§ 8 III UWG) durch die ordentlichen Gerichte. Es gilt also das Prinzip: *„Wo kein Kläger, da kein Richter“.*

Nicht klagebefugt sind hingegen die von unlauteren Handlungen betroffenen Verbraucher. Sie haben keine eigenen individuellen Unterlassungs-, Beseitigungs- und Schadensersatzansprüche nach dem UWG. Individualrechte der Verbraucher ergeben sich lediglich aus dem Bürgerlichen Recht.

II. Verbraucherschutzrecht (§ 2 UKlaG)

1. Wer wird geschützt?

Verbraucherschutzgesetze i.S. des § 2 I UKlaG dienen, wie schon der Wortlaut deutlich macht, dem Schutz der Verbraucher i.S. des § 13 BGB. Der Verbraucherschutz braucht nicht der alleinige Schutzzweck zu sein, darf jedoch keine nur untergeordnete oder nur zufällige Nebenwirkung sein. Keine Verbraucherschutzgesetze sind beispielsweise Vorschriften zum Schutz des Allgemeinen Persönlichkeitsrechts oder das AGG, weil sie alle natürlichen Personen, nicht aber speziell Verbraucher schützen.[3]

Die Regelung in § 2 II 1 Nr. 11 UKlaG qualifiziert zwar bestimmte Datenschutzgesetze als Verbraucherschutzgesetze. Sie ist aber auf das BDSG a.F. zugeschnitten.[4] Jedenfalls nach dem Wirksamwerden der DS-GVO am 28.05.2018 ist indessen davon auszugehen, dass im Anwendungsbereich dieser Verordnung die Durchsetzung der allgemeinen Datenschutzvorschriften den Aufsichtsbehörden vorbehalten ist und die gerichtliche Durchsetzung der Rechte der betroffenen Personen nach Maßgabe der Art. 79, 80 DS-GVO zu erfolgen hat. Wegen des Vorrangs des Unionsrechts dürfen die Gerichte § 2 I 3, II 1 Nr. 11 und

[3] OLG Hamm NJW-RR 2017, 684; Palandt/*Grüneberg*, BGB, 77. Aufl. 2018, § 2 Rn. 3 UKlaG.
[4] Vgl. *Köhler*/Bornkamm/Feddersen, UWG, 36. Aufl. 2018, § 2 Rn. 18 UKlaG; zu Einzelheiten vgl. *Micklitz/Rott,* in: MüKoZPO, 5. Aufl. 2017, § 2 Rn. 30, 31 UKlaG.

II 2 UKlaG nicht mehr anwenden.[5] Diese Vorschriften sollten daher im Interesse der Rechtsklarheit und Rechtssicherheit für alle Beteiligten aufgehoben werden.

2. Wer setzt den Verbraucherschutz im UKlaG durch?

Die Durchsetzung der Verbraucherschutzgesetze mittels Unterlassungs- und Beseitigungsansprüchen dient dem kollektiven Schutz der Verbraucherinteressen und nicht der Durchsetzung von Individualansprüchen.[6] Anspruchsberechtigt sind nur die in § 3 UKlaG aufgelisteten Verbände, nicht aber die Mitbewerber des Verletzers.

III. Datenschutzrecht (DS-GVO)

1. Wer wird geschützt?

Geschützt werden nicht Verbraucher (i.S. des § 13 BGB), sondern ganz allgemein *natürliche Personen* (Art. 1 DS-GVO), unabhängig davon, ob sie im geschäftlichen Verkehr Verbraucher oder Unternehmer sind.

2. Welche Rechtsgüter schützt die DS-GVO?

In der DS-GVO geht es nicht um den Schutz wirtschaftlicher Interessen der Verbraucher, sondern um den Schutz der Grundrechte und Grundfreiheiten aller natürlichen Personen und insbesondere um den Schutz ihres *Rechts auf den Schutz personenbezogener Daten* (Art. 1 II DS-GVO).

Grundlage dafür ist Art. 8 I und II Grundrechte-Charta, dem im deutschen Recht das Grundrecht auf *informationelle Selbstbestimmung* entspricht. Die Konkretisierung dieser Bestimmungen ist in der DS-GVO erfolgt. Die allgemeinen Bestimmungen für die Datenverarbeitung sind insbesondere in Kapitel II (Art. 5 bis Art. 11 DS-GVO), die Rechte der von der Datenverarbeitung „betroffenen Personen“ sind in Kapitel III (Art. 12 – 23 DS-GVO) geregelt.

3. Wer ist für Datenschutzverstöße verantwortlich?

Für Verstöße gegen die DS-GVO müssen der *Verantwortliche* (Art. 4 Nr. 7 DS-GVO) und der *Auftragsverarbeiter* (Art. 4 Nr. 8 DS-GVO) einstehen. Der Kreis der Verantwortlichen ist nicht auf Unternehmen beschränkt, sondern erstreckt sich auch auf Behörden, Einrichtungen und sonstige Stellen.

4. Wer setzt den Datenschutz durch?

[5] Vgl. Gola/*Werkmeister,* DS-GVO, 2. Aufl. 2018, Art. 80 Rn. 18.
[6] Palandt/*Grüneberg* ,(Fn. 2), § 2 Rn. 1 UKlaG.

„Die Einhaltung der Datenschutzvorschriften wird von einer unabhängigen Stelle überwacht“ (Art. 8 III Grundrechte-Charta). Dies wird in Kapitel VI der DS-GVO über *„Unabhängige Aufsichtsbehörden“* näher geregelt (Art. 51 bis 59 DS-GVO). Ihre Hauptaufgabe ist die Überwachung und Durchsetzung der Anwendung der DS-GVO (Art. 57 I lit. a DS-GVO). Dazu werden ihnen umfangreiche Beratungspflichten auferlegt und Untersuchungs- und Abhilfebefugnisse (Art. 58 DS-GVO) eingeräumt.

Die Aufsichtsbehörde kann den Sachverhalt „von Amts wegen“ aufklären und beratend tätig werden. Die Abhilfebefugnisse (Art. 58 II DS-GVO) ermöglichen es ihr, abgestufte, nämlich dem Grundsatz der Verhältnismäßigkeit entsprechende Maßnahmen zu verhängen. Dies geht bis von einer bloßen Verwarnung bis zur Verhängung von drakonischen Geldbußen in Höhe von 20 Mio. Euro oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes (Art. 83 DS-GVO).

Im Gegensatz zum UWG und zum UKlaG, die nur Unterlassungs- und Beseitigungsansprüche kennen, liegt der DS-GVO also ein differenziertes verwaltungsrechtliches System der Durchsetzung zugrunde, das dem Grundsatz der Verhältnismäßigkeit entspricht (*public enforcement*).

5. Durchsetzung der Rechte betroffener Personen

a) Recht der betroffenen Person auf Beschwerde bei der Aufsichtsbehörde

Wird eine betroffene Person in ihren subjektiven Rechten, die ihnen die DS-GVO gegen Verantwortliche und Auftragsverarbeiter gewährt, beeinträchtigt, hat sie das Recht auf eine Beschwerde bei der *Aufsichtsbehörde* (Art. 77 DS-GVO) und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen die Untätigkeit der *Aufsichtsbehörde* (Art. 78 II DS-GVO).

b) Recht der betroffenen Person auf gerichtliche Geltendmachung ihrer Rechte

Außerdem hat die betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen den Verantwortlichen oder Auftragsverarbeiter (Art. 79 I DS-GVO) zur Durchsetzung ihrer aufgrund einer rechtswidrigen Datenverarbeitung verletzten Rechte. Der Gesetzgeber hat die Regelungen in Art. 79 I und II DS-GVO mittels des § 44 BDSG in das deutsche Recht übernommen.

c) Recht der betroffenen Person auf Beauftragung und Bevollmächtigung einer Einrichtung zur Durchsetzung ihrer Rechte

Ferner hat die betroffene Person das Recht auf Bevollmächtigung und Beauftragung einer Einrichtung usw., die im Namen der betroffenen Person deren Rechte geltend macht (Art. 80 I DS-GVO). Hierfür kommen nicht nur, aber vor

allem Verbraucherschutzverbände, wie etwa der *vzbv* in Betracht, wenn sie die in Art. 80 I DS-GVO genannten Voraussetzungen erfüllen. Allerdings werden sie dann nicht zum Schutz der kollektiven wirtschaftlichen Interessen der Verbraucher, sondern zum *Individualschutz* einzelner betroffener Personen tätig.

d) Eigenes Recht einer Einrichtung zur Durchsetzung der Rechte betroffener Personen

Schließlich enthält Art. 80 II DS-GVO eine *Öffnungsklausel* für die Mitgliedstaaten. Danach können Einrichtungen i.S. des Art. 80 I DS-GVO die Rechte einer oder mehrerer betroffener Personen auch ohne deren Auftrag im eigenen Namen wahrnehmen. Das kommt einer echten Verbandsklage nahe; allerdings geht es auch insoweit nur um den *Individualschutz* einzelner betroffener Personen. Auf den Punkt gebracht: **Art. 80 II DS-GVO räumt Verbänden keine weitergehenden Klagebefugnisse ein, als sie die betroffenen Personen haben.** Um das Selbstbestimmungsrecht dieser Personen zu wahren, darf dies aber nicht gegen deren Willen geschehen. Der nationale Gesetzgeber sollte daher ggf. eine opt-in- oder zumindest eine opt-out-Klausel vorsehen.

Würde der Gesetzgeber von dieser Öffnungsklausel Gebrauch machen, so könnten auch und vor allem Verbraucherverbände, wie insbesondere der *vzbv,* und die *Wettbewerbszentrale* eine gesellschaftspolitisch wichtige Aufgabe bei der Durchsetzung der Rechte betroffener Personen übernehmen.

Dazu müssten sie ggf. ihre Satzung ändern, weil es um eine Erweiterung ihres Aufgabenbereichs ginge. Ihre Aufgabe wäre insoweit nämlich nicht die Durchsetzung der wirtschaftlichen Interessen der Verbraucher gegen unlauter handelnde Unternehmen. Vielmehr ginge es ganz allgemein um die Durchsetzung des Grundrechts auf informationelle Selbstbestimmung *aller Bürger*, gleichgültig, welche Stellen (Unternehmen, Vereine, NGO, Parteien, Kirchen usw.) ihre Daten rechtswidrig verarbeitet haben.

6. Keine Befugnis der Mitgliedstaaten zu weitergehenden Regelungen

a) Keine erweiternde, sondern enge Auslegung der Öffnungsklausel des Art. 80 II DS-GVO

Die DS-GVO enthält keine weitere Öffnungsklausel dahingehend, dass die Mitgliedstaaten, zusätzlich zum *public enforcement* der Aufsichtsbehörden, ein *private enforcement* des objektiven Datenschutzrechts der DS-GVO einführen könnten. Entgegen manchen Bestrebungen im Schrifttum und in einzelnen Gerichtsentscheidungen lässt sich aus Art. 80 II DS-GVO eine derartige Befugnis

der Mitgliedstaaten auch nicht im Wege einer erweiternden Auslegung herauslesen. Dies widerspräche dem unionsrechtlichen Grundsatz der engen Auslegung von Ausnahmevorschriften,[7] wie sie eine Öffnungsklausel darstellt.

b) Keine Grundlage in den Art. 82 und 84 DS-GVO

Eine derartige Befugnis lässt sich auch nicht den Art. 82 und 84 DS-GVO entnehmen. Art. 82 DS-GVO regelt nur den Anspruch einer (betroffenen) Person auf Schadensersatz, also ebenfalls nur ein subjektives Recht, das ggf. – bei entsprechender nationaler Regelung – nach Art. 80 I DS-GVO von Einrichtungen im Namen und Auftrag der betroffenen Person durchgesetzt werden kann. Art. 80 II DS-GVO ist insoweit nicht anwendbar. Art. 84 DS-GVO regelt nur verwaltungsrechtliche und strafrechtliche Sanktionen (Geldbußen, Geldstrafen; vgl. dazu §§ 41 – 43 BDSG).

c) Keine Rechtfertigung durch den Grundsatz des effet utile

Ebenso wenig lässt sich der Grundsatz des *effet utile* heranziehen, um eine ergänzende Anwendung der § 3a UWG, § 2 UKlaG auf Verstöße gegen die DS-GVO zu rechtfertigen. Dieser unionsrechtliche Grundsatz bezieht sich nur auf die Auslegung bestehender unionsrechtlicher Normen im Sinne ihrer praktischen Wirksamkeit. Er ermöglicht nicht die beliebige Ergänzung der DS-GVO durch nationale Normen. Der Grundsatz des *effet utile* hat in Art. 52 IV DS-GVO seinen Ausdruck gefunden. Danach sind die Mitgliedstaaten rechtlich verpflichtet, die Aufsichtsbehörden so auszustatten, dass sie ihre Aufgaben und Befugnisse *„effektiv wahrnehmen können".* Es sind also Bund und Länder gefordert, zusätzliche Mittel und Ressourcen für die Aufsichtsbehörden bereitzustellen, wenn die erforderlich würde. – Ein zusätzliches *private enforcement* hätte die gegenteilige Wirkung eines *effet inutile.* Es bestünde die Gefahr unterschiedlicher Entscheidungen. Damit würde die vom Unionsgesetzgeber ausdrücklich gewollte *einheitliche Durchsetzung* der DS-GVO innerhalb der Union durch die Aufsichtsbehörden unterlaufen (vgl. u.a. Art. 57 I lit. g, 61 I, 63 I DS-GVO; Erwägungsgrund 11, 13, 129, 133 DS-GVO).

Darum wird in der DS-GVO größter Wert auf eine Zusammenarbeit der nationalen Aufsichtsbehörden gelegt. Andernfalls könnte jeder Mitgliedstaat nach Belieben bestimmte Einrichtungen, wie etwa Ombudsleute oder Verbraucherschutzbehörden, zusätzlich zur Durchsetzung der DS-GVO ermächtigen. Dem will der Unionsgesetzgeber aber gerade vorbeugen. Denn auch hier gilt das Sprichwort: *„Viele Köche verderben den Brei".* Daher hat sich auch die *Kommission* gegen solche zusätzlichen Befugnisse von Privaten ausgesprochen (s. Anhang).

[7] St. Rspr. des EuGH; vgl. *EuGH,* WRP 2015, 1206 Rn. 54 – Abcur/Apoteket Farmaci.

d) Keine Ausschöpfung bestehender Möglichkeiten zum Tätigwerden der Verbraucherverbände

Der deutsche Gesetzgeber hat im Übrigen noch nicht einmal die Möglichkeiten ausgeschöpft, die die DS-GVO den Mitgliedstaaten in Art. 80 II DS-GVO auch für Verbraucherverbände eröffnet.

7. Ergebnis

Eine zusätzliche, die Ermächtigung nach Art. 80 II DS-GVO überschreitende privatrechtliche Durchsetzung der DS-GVO durch Mitbewerber und Verbände ist mit der Zielsetzung des Unionsgesetzgebers nicht vereinbar.

C. Gesetzgeberische Möglichkeiten zur Optimierung des Rechtsschutzes im Anwendungsbereich der DS-GVO

I. Einführung einer zusätzlichen privatrechtlichen Durchsetzung der DS-GVO?

1. Gefahr eines Vertragsverletzungsverfahrens

Der Gesetzgeber könnte sich über die genannten Bedenken hinwegsetzen und ein *private enforcement* auch bei Verstößen gegen objektives Datenschutzrecht einzuführen, etwa um Forderungen aus der Anwaltschaft oder von bestimmten Verbänden entgegenzukommen. Dies wäre aber nicht empfehlenswert, weil die DS-GVO als vorrangige und abschließende unionsrechtliche Regelung dies nicht zulässt. Es wäre daher höchstwahrscheinlich mit einem *Vertragsverletzungsverfahren* zu rechnen. Auch bestünde das Risiko, dass die Gerichte die betreffenden nationalen Vorschriften wegen des Vorrangs des Unionsrechts nicht anwenden und aus diesem Grund den *EuGH* anrufen würden.

2. Nachteile und Probleme eines gleichzeitigen private enforcement

Davon abgesehen würde eine privatrechtliche Durchsetzung der DS-GVO zusätzlich zur verwaltungsrechtlichen Durchsetzung durch die Aufsichtsbehörden eine Reihe von Nachteilen und Problemen mit sich bringen.

a) Nebeneinander von behördlichen und zivilgerichtlichen Verfahren

Die Folge wäre nämlich ein Nebeneinander von behördlichen und zivilgerichtlichen Verfahren. Die (angeblichen) Verletzer von Vorschriften der DS-GVO könnten sich dann gegenüber der Aufsichtsbehörde nicht darauf berufen, sie seien bereits von einem Mitbewerber und/oder Verband abgemahnt und verklagt worden; ebenso wenig könnten sie gegenüber den Mitbewerbern und/oder

Verbänden geltend machen, die Aufsichtsbehörde habe gegen sie ein Verfahren eröffnet. Es gäbe keinen Einwand etwa der Rechtshängigkeit und es bestünde auch keine Möglichkeit der Aussetzung des zivilgerichtlichen Verfahrens nach § 148 ZPO, weil die behördliche Entscheidung nicht vorgreiflich ist. Aus diesem Grund könnte es auch zu widersprechenden Entscheidungen von Aufsichtsbehörden und ordentlichen Gerichten kommen.[8] Dies widerspräche wiederum dem erklärten Ziel des Unionsgesetzgebers, eine einheitliche Durchsetzung der DS-GVO zu gewährleisten. Hinzu käme, dass im Grundsatz *jedes Landgericht* in Deutschland für Klagen von Mitbewerbern und Verbänden zuständig wäre. Dieses Nebeneinander von Verfahren wäre umso misslicher, als es dadurch zu einer unerwünschten Rechtszersplitterung schon innerhalb Deutschland´s kommen könnte.

b) Mehrbelastung der Zivilgerichte und der (angeblichen) Verletzer

Zu bedenken ist weiter die *Mehrbelastung der Zivilgerichte* durch zahlreiche Verfahren, dem keine entsprechende Entlastung der Aufsichtsbehörden gegenüberstünde. Das würde entweder die Gefahr von Verfahrensverzögerungen mit sich bringen oder aber entsprechende Mehrkosten für zusätzliche Richter verursachen, für die wiederum Bund und Länder aufkommen müssten.

Aber auch die Mehrbelastung der *(angeblichen) Verletzer* durch eine *doppelte* Inanspruchnahme seitens der Aufsichtsbehörde und seitens der Mitbewerber und Verbände ist zu bedenken. Das *private enforcement* würde vor allem kleine Unternehmen, insbesondere Start-ups, empfindlich treffen. Sie könnten auch bei einem vergleichsweise geringfügigen Datenschutzverstoß auf ihrer Homepage nicht nur von der Aufsichtsbehörde verwarnt, sondern auch von einem oder mehreren Mitbewerbern und Verbänden abgemahnt und ggf. verklagt werden, und müssten sich allen gegenüber verteidigen.

Geplante gesetzliche Abmilderungen, etwa eine Kostenfreiheit der ersten Abmahnung und der Begrenzung der Höhe der Vertragsstrafe unter bestimmten Voraussetzungen, helfen nicht wirklich. Denn eine Abmahnung stellt für kleine Unternehmen schon für sich gesehen eine Belastung dar. Dies kann sie ggf. dazu verleiten, vorsichtshalber, nämlich ohne anwaltliche Beratung, eine strafbewehrte Unterlassungserklärung abzugeben, um sich nicht dem Risiko einer einstweiligen Verfügung mit entsprechender Gebührenbelastung auszusetzen. Entsprechende Gesetzgebungsvorschläge geben gerade im Datenschutzrecht kleinen Unternehmen *„Steine statt Brot“.*

Mitbewerber, die sich durch einen Datenschutzverstoß eines Unternehmens beeinträchtigt glauben, sind im Übrigen nicht schutzlos. Denn sie können diesen Verstoß der Aufsichtsbehörde anzeigen und sie um Abhilfe bitten.

[8] Dem stünde auch § 12a S. 1 UKlaG nicht wirklich entgegen, weil das Gericht nicht an die Auffassung der Aufsichtsbehörde gebunden ist. Auch ist die für die Praxis wichtige Ausnahmeregelung in § 12a S. 2 UKlaG zu bedenken.

II. Herstellung von Rechtssicherheit für alle Beteiligten

Die von vielen befürchtete „Abmahnwelle“ wegen Verstößen gegen die DS-GVO ist vermutlich schlicht deshalb ausgeblieben, weil die an Abmahnungen interessierten Unternehmen und Anwälte sich nicht sicher sein konnten, ob sie wirklich nach §§ 3a, 8 III Nr. 1 UWG vorgehen konnten. Gleichwohl ist die derzeitige Rechtsunsicherheit aufgrund unterschiedlicher Gerichtsentscheidungen für alle Beteiligten (Aufsichtsbehörden, Gerichte, Anwälte, Unternehmen, Verbände, betroffene Personen) und kontroversen Diskussionen im Schrifttum in hohem Maße unbefriedigend. Dies sollte den Gesetzgeber zu einem Eingreifen veranlassen.

III. Vorschläge für die Gesetzgebung

1. Übernahme der Regelungen des Art. 80 DS-GVO in das BDSG

Da es sich um Datenschutzrecht *pur* handelt, sollten Gesetzesänderungen zweckmäßigerweise im BDSG erfolgen. Hierfür bietet sich das *Kapitel Rechtsbehelfe* an, das bisher nur den § 44 BDSG enthält. Die Änderungen sollten entweder in Folgeparagraphen oder, wie hier vorgeschlagen, in § 44 BDSG erfolgen.

2. Beschränkung des § 44 I 1 BDSG hinsichtlich seines Anwendungsbereichs

Bei dieser Gelegenheit sollte der Wortlaut des § 44 I 1 BDSG geändert werden. Die derzeitige Fassung geht über die durch Art. 79 I DS-GVO eröffnete Möglichkeit der betroffenen Person zu einer Klage gegen einen Verantwortlichen oder einen Auftragsverarbeiter hinaus. Sie ermöglicht nämlich Klagen

„wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 <u>oder</u> der darin enthaltenen Rechte der betroffenen Person“.

Damit wird eine Popularklage natürlicher Personen gegen Datenschutzverstöße ermöglicht. Dies ist weder von Art. 79 I DS-GVO gedeckt noch mit dem Vorrang der Befugnisse der Aufsichtsbehörden vereinbar. § 44 I 1 BDSG könnte daher wie folgt gefasst werden:

„Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen einer Verletzung ihrer Rechte aus der Verordnung (EU) 2016/679 infolge einer gegen diese Verordnung verstoßenden Verarbeitung ihrer personenbezogenen Daten können ….“

3. Einfügung eines neuen § 44 IV BDSG

Die neue Vorschrift könnte lauten:

„Klagen nach Absatz 1 Satz 1 können auch von einer Einrichtung im Sinne des Absatzes 5 sowohl im Namen und Auftrag von betroffenen Personen, die in ihren Rechten verletzt wurden, als auch im eigenen Namen ohne deren Auftrag erhoben werden."

Diese Regelung würde zum einen Art. 80 I DS-GVO konkretisieren. Ein Verstoß gegen das sog. Wiederholungsverbot[9] läge darin nicht, da es nur darum geht, den Art. 80 I DS-GVO an die deutsche Rechtsterminologie anzupassen. Zum anderen würde von der Öffnungsklausel des Art. 80 II DS-GVO Gebrauch gemacht, nach Einrichtungen im Sinne des Art. 80 I DS-GVO die Rechte betroffener Personen im eigenen Namen und ohne deren Auftrag wahrnehmen können. Damit würde u.a. Verbraucherverbänden und der Wettbewerbszentrale die Möglichkeit eröffnet, über ihr bisheriges Aufgabengebiet hinaus im Interesse des Datenschutzes *aller* Bürger tätig zu werden.

4. Einfügung eines neuen § 44 V BDSG

Ergänzend käme eine Definition in § 44 V BDSG hinzu, die dem Art. 80 I DS-GVO entspräche und wie folgt lauten könnte:

„Einrichtung im Sinne des Absatzes 4 ist jede juristische Person ohne Gewinnerzielungsabsicht, deren satzungsmäßiges Ziel im öffentlichen Interesse liegt und die im Bereich des Schutzes und der Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogener Daten tätig ist."

Selbstverständlich könnte der Gesetzgeber diese Definition dadurch präzisieren, dass eine Liste klagebefugter „qualifizierter Einrichtungen", vergleichbar der Regelung in § 4 UKlaG, geschaffen würde, in die sich Verbände eintragen lassen müssten.

5. Klarstellender Hinweis auf die alleinige Befugnis der Aufsichtsbehörden zur Durchsetzung der DS-GVO

Um Missverständnissen zu vorzubeugen, sollte zumindest in der **Gesetzesbegründung** ein **klarstellender Hinweis** erfolgen, dass für die Durchsetzung der allgemeinen Verpflichtungen der Verantwortlichen und der Auftragsverarbeiter nach der DS-GVO ausschließlich die Aufsichtsbehörden zuständig sind.

6. Konkretisierung der Vorgaben aus Art. 80 I DS-GVO hinsichtlich der Rechte der betroffenen Person gegenüber der Aufsichtsbehörde

Zu erwägen ist schließlich, ob der Gesetzgeber aufgrund der Vorgaben aus Art. 80 I DS-GVO auch die Befugnis der Einrichtungen i.S. des Art. 80 I DS-GVO zur

[9] Verbot der Wiederholung von unionsrechtlichen Normen im nationalen Recht.

Geltendmachung der Rechte der betroffenen Person aus **Art. 77, 78 DS-GVO** in deren Auftrag und Namen regeln müsste. Dies könnte sinnvollerweise in einem § 44a BDSG geschehen. Eine entsprechende Regelung im Sinne des Art. 80 II DS-GVO ist zwar aufgrund der Öffnungsklausel möglich, aber nicht notwendig.

7. Aufhebung der datenschutzbezogenen Regelungen in § 2 UKlaG

Die datenschutzbezogenen Regelungen in § 2 I 3, II 1 Nr. 11 und II 2 UKlaG sind mit der DS-GVO nicht vereinbar. DS-GVO ist kein Verbraucherschutzgesetz und stellt eine abschließende Regelung dar. Wegen des Vorrangs des Unionsrechts vor dem nationalen Recht dürfen die Gerichte diese Regelungen seit dem 28.05.2018 nicht mehr anwenden. Der Gesetzgeber sollte sie daher aufheben.

IV. Eröffnung von Betätigungsmöglichkeiten für die Verbraucherverbände

Die vorgeschlagene Ergänzung des § 44 BDSG um einen Absatz 4 eröffnet für Verbraucherverbände, neue sinnvolle Betätigungsmöglichkeiten im Bereich der Wahrnehmung der Rechte von betroffenen Personen, unabhängig davon, ob sie in ihrer Eigenschaft als Verbraucher im Rechtssinne betroffen sind oder nicht. Es geht um das Interesse aller Bürger am Schutz ihrer personenbezogenen Daten vor einer rechtswidrigen Verarbeitung dieser Daten durch alle denkbaren Verantwortlichen und Auftragsverarbeiter. Damit die Verbände diese zusätzliche Aufgabe übernehmen können, müsste ihnen lediglich der Gesetzgeber durch Umsetzung des Art. 80 II DS-GVO einen Schritt entgegenkommen.

Anhang

Parliamentary questions

PDF 105k WORD 18k
3 October 2018
E-004117/2018(ASW)
Answer given by Ms Jourová on behalf of the European Commission
Question reference: E-004117/2018
The General Data Protection Regulation (GDPR) (1) grants individuals several remedies in case of an alleged infringement of their rights, such as the right to lodge a complaint with a supervisory authority or to bring proceedings before the courts.

They may mandate a not-for-profit body to exercise their rights on their behalf. Additionally, Member States may provide that a not-for-profit organisation, which has been properly constituted in accordance with the national law, pursues public interests and is active in the field of the data protection, may lodge a complaint and start proceedings in courts independently of a data subject's mandate.

Except where this is allowed pursuant to Article 80 GDPR, other persons wishing to act independently of a data subject's mandate do not have standing to exercise the rights granted to individuals under the GDPR.

The Commission does not currently have any overview of the illegal practices mentioned by the Honourable Member. Article 97 of the regulation provides that by May 2020 the Commission shall submit a report on the evaluation and review of the regulation. The Commission will assess during the coming year of application whether there is a need to evaluate such practices in its forthcoming report on the application of the new rules.

Under the GDPR, the promotion of public awareness in relation to the processing of personal data is primarily a task for the independent national supervisory authorities(2).

The Commission has undertaken several actions to ensure appropriate information is disseminated in all the Member States about the new rules(3). The Commission has also issued a call for proposals for an amount of EUR 2 million to support data protection authorities in their awareness-raising activities(4).

(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.
(2) Article 57(1)(a) of the GDPR.
(3) In January 2018, the Commission published its communication on the guidance for the direct application of the GDPR, together with an online toolkit targeting citizens and small and medium-sized enterprises (SMEs) to raise their understanding of the new rules.
(4) http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

Prof. Dr. Meinhard Schröder

Lehrstuhl für Öffentliches Recht, Europarecht
und Informationstechnologierecht

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 D

Telefon Prof. Dr. Meinhard Schröder
0851 509-2381

Telefax 0851 509-2382

E-Mail Meinhard.Schroeder
@uni-passau.de

Datum 6.12.2018

Stellungnahme zum Entwurf eines
Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 – 2. DSAnpUG-EU

Primäres Ziel des Gesetzes ist es, die zahlreichen bereichsspezifischen Datenschutzregelungen des deutschen Rechts mit dem europäischen Unionsrecht, d.h. mit der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680, (redaktionell) in Einklang bringen. Nach eingehender Durchsicht des Entwurfs erscheinen folgende Bemerkungen veranlasst.

1. Umgang mit Öffnungsklauseln

Die Verordnung (EU) 2016/679 beabsichtigt in ihrem Anwendungsbereich eigentlich eine Vollharmonisierung des europäischen Datenschutzrechts; es soll unionsweit ein gleichwertiges Schutzniveau herrschen (insbes. ErwGr 10). Gleichwohl enthält die Verordnung zahlreiche Öffnungsklauseln, in deren Anwendungsbereich die Mitgliedstaaten beispielsweise zwischen bestimmten Optionen wählen dürfen oder bestimmte Konkretisierungen vornehmen dürfen oder müssen.

Eine Durchsicht des vorliegenden Gesetzesentwurfs zeigt, dass im deutschen Recht vor allem in dreierlei Hinsicht von den Öffnungsklauseln Gebrauch gemacht wird: Erstens bestehen zahlreiche Regelungen i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) der Verordnung (EU) 2016/679 – dazu im Folgenden a). Zweitens geht es in einigen Fällen um die Verarbeitung besonderer Kategorien personenbezogener Daten, wobei Art. 9 Abs. 2 lit. g) und Abs. 4 der Verordnung (EU) 2016/679 bedeutsam sind – dazu b). Drittens wird mehrfach von der Möglichkeit Gebrauch gemacht, gem. Art. 23 der Verordnung (EU) 2016/679 Betroffenenrechte einzuschränken – dazu im Folgenden c). Ergänzend wird auf die im Entwurf nicht angesprochene, aber in der öffentlichen Diskussion häufig in Zusammenhang mit den Betroffenenrechten gebrachte Frage des deutschen Sonderwegs für den Datenschutzbeauftragten für nichtöffentliche Stellen eingegangen – dazu d).

a) Regelungen i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) der Verordnung (EU) 2016/679

In Ausnutzung von Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) können durch nationales Recht Rechtsgrundlagen für eine Datenverarbeitung geschaffen werden. Beide Öffnungsklauseln sind durch weitgehende Parallelen geprägt, die aus der Verwendung des Begriffs der Erforderlichkeit sowie aus den in beiden Fällen anwendbaren Vorgaben der Abs. 2 und 3 des Art. 6 resultieren. Gemäß diesen Vorschriften können im mitgliedstaatlichen Recht auch „spezifische Bestimmungen“ vorgesehen werden, die den Umgang mit Daten nur in geringerem Umfang erlauben, als er sonst in der Verordnung vorgesehen ist; hierzu zählen etwa Beschränkungen der Verarbeitungserlaubnis auf bestimmte Kategorien von Daten, Zweckverbote oder über Art. 5 Abs. 1 lit. e) der Verordnung hinausgehende Löschungspflichten für den Verantwortlichen.

Das in Ausnutzung von Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) entstehende „bereichsspezifische Datenschutzrecht“ muss insbesondere

- gesetzlich vorgesehen sein,
- den Zweck der Datenverarbeitung angeben, und
- verhältnismäßig sein

Bedenken, dass der Gesetzentwurf diesen nicht neuen und auch verfassungsrechtlich seit jeher anerkannten Anforderungen entspricht, bestehen mit Blick auf diejenigen Befugnisnormen, die nur sprachlich modifiziert werden, nicht (siehe aber noch unten 3.). Soweit neue Befugnisse zur Datenverarbeitung geschaffen werden oder der Anwendungsbereich der bestehenden erweitert wird, ist vor allem auf die Verhältnismäßigkeit zu achten.

b) Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verordnung (EU) 2016/679 unterwirft die Verarbeitung von besonders sensiblen personenbezogenen Daten besonders strengen Anforderungen. Sie ist nur in den in Art. 9 Abs. 2 genannten Fällen zulässig. Als Ausnahmeregelung zu Abs. 1 sind die in Abs. 2 genannten Bestimmungen restriktiv auszulegen.

Als Öffnungsklausel wirkt Art. 9 Abs. 2 lit. g) der Verordnung (EU) 2016/679, der die Verarbeitung unter folgenden Voraussetzungen ermöglicht:

- Rechtsgrundlage im Recht der Mitgliedstaaten (oder im Unionsrecht)
- Gründe eines erheblichen öffentlichen Interesses
- angemessenes Verhältnis zu dem verfolgten Ziel
- Wahrung des Wesensgehalts des Rechts auf Datenschutz, und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person

Zweifelhaft erscheint, ob sich ein Mitgliedstaat darauf beschränken kann, im nationalen Recht eine Generalklausel zu schaffen, nach der im Fall eines erheblichen öffentlichen Interesses eine Datenverarbeitung zulässig ist, wie dies im neuen Art. 22 Abs. 1 Nr. 1 lit. d) BDSG der

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

Fall sein soll (Art. 12 Nr. 7 des Änderungsgesetzes). Für die Zulässigkeit eines solchen Vorgehens spricht zwar, dass die Einhaltung der Voraussetzungen des Art. 9 Abs. 2 lit. g) der Verordnung (EU) 2016/679 letztlich nur im konkreten Einzelfall beurteilt werden kann. Allerdings hat der Unionsgesetzgeber das erhebliche öffentliche Interesse im Unterschied zu den anderen Buchstaben in Art. 9 Abs. 2 gerade nicht als unmittelbar anwendbare Ausnahme vom dem in Art. 9 Abs. 1 etablierten grundsätzlichen Verbot der Verarbeitung besonders sensibler Daten anerkannt, sondern es der Ausgestaltung durch das Recht der Mitgliedstaaten (oder der Union) überlassen. Auch die Formulierung „Gründe eines erheblichen öffentlichen Interesses“ in der Norm spricht dafür, dass der nationale Gesetzgeber eine konkrete Situation, eben einen Grund, vor Augen haben muss, aus dem er die Verarbeitung für geboten hält. Letztlich sollen – ähnlich wie durch Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e) – bereichsspezifische Datenschutznormen ermöglicht werden. Das „erhebliche öffentliche Interesse“ kann bei dieser Lesart nur als Grund für die Einführung dieser Normen dienen, ohne nähere Präzisierung aber nicht als Rechtfertigung für die Verarbeitung der besonders sensiblen Daten. Das Minimum an Präzisierung, das man verlangen müssen wird, ist eine Angabe des Bezugs zu einer bestimmten Aufgabe (so geschehen etwa in Art. 1 des Änderungsgesetzes für § 31 des Staatsangehörigkeitsgesetzes oder in Art. 48 des Änderungsgesetzes für § 7 des Asylgesetzes); die allgemeine Querschnittsregel im BDSG lässt dies vermissen.

Die Öffnungsklausel des Art. 9 Abs. 4 der Verordnung (EU) 2016/679 erlaubt nicht die Schaffung zusätzlicher Befugnisse zur Verarbeitung besonders sensibler Daten, sondern nur die Einschränkung der sich aus Abs. 2 ergebenden Befugnisse durch die Mitgliedstaaten im Hinblick auf ganz bestimmte Daten (Bedingungen und Beschränkungen). Der Entwurf macht hiervon mehrfach Gebrauch, wenn beispielsweise die Einwilligung in die Verarbeitung von Gesundheitsdaten in einer bestimmten Form erfolgen muss.

c) Einschränkungen von Betroffenenrechten gemäß Art. 23 der Verordnung (EU) 2016/679

Die Betroffenenrechte sind in Art. 12–22 der Verordnung (EU) 2016/679 geregelt. Hierzu gehören nicht nur Bestimmungen, aufgrund derer die betroffene Person bestimmte Ansprüche gegen den Verantwortlichen geltend machen kann, wie etwa das Auskunftsrecht nach Art. 15, sondern auch Bestimmungen, nach denen der Verantwortliche ohne Aufforderung tätig werden muss, namentlich die Informationspflichten gemäß Art. 12–14.

Die Betroffenenrechte können gemäß Art. 23 der Verordnung (EU) 2016/679 eingeschränkt werden. Solche Einschränkungen müssen fünf Voraussetzungen erfüllen

- Regelung in einem Gesetz
- Achtung des Wesensgehalts der Grundrechte und Grundfreiheiten
- Notwendigkeit in einer demokratischen Gesellschaft und Verhältnismäßigkeit
- Mindestens ein legitimes Ziel aus dem Katalog in Art. 23 Abs. 1 lit. a) – j)
- Falls möglich, alle Schutzmaßnahmen gem. Art. 23 Abs. 2

Wo nach deutschem Recht Betroffenenrechte eingeschränkt werden, nennt der Entwurf in den meisten Fällen mindestens ein legitimes Ziel aus dem Katalog des Art. 23 Abs. 1 unter

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

Angabe des relevanten Buchstabens; wo dies nicht der Fall ist, ist zumindest das Ziel erkennbar. Auch die Verhältnismäßigkeit der Einschränkung wird durchweg begründet.

Überzeugend ist, dass der Entwurf nicht Forderungen nachgibt, KMU, Vereine oder andere Akteure, für die die Befolgung der Vorgaben der Verordnung (EU) 2016/679 einen bisher nicht gekannten Aufwand verursacht, von einzelnen Pflichten der Art. 12–22 auszunehmen, denn für eine solche Privilegierung kann angesichts des Katalogs in Art. 23 Abs. 1 lit. a) – j) keine unionsrechtskonforme nationale Rechtsgrundlage geschaffen werden. Insbesondere ist das Interesse an weniger Aufwand beim Datenschutz kein wichtiges Ziel des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats im Sinne von lit. e). Auch sonst ist keine Öffnungsklausel ersichtlich, mit der eine Befreiung einzelner Verantwortlicher von den datenschutzrechtlichen „Grundpflichten“ erreicht werden könnte.

d) Öffnungsklausel zum Datenschutzbeauftragten (Art. 37 Abs. 4 S. 1 Hs. 2 der der Verordnung (EU) 2016/679

Deutschland hat bereits mit dem 1. DSAnpUG-EU von der durch Art. 37 Abs. 4 S. 1 Hs. 2 der Verordnung (EU) 2016/679 eingeräumten Möglichkeit Gebrauch gemacht, die Bestellung eines Datenschutzbeauftragten auch in anderen Fällen als den in Art. 37 Abs. 1 der Verordnung genannten vorzuschreiben, und die Regelung des § 4f BDSG-alt in § 38 Abs. 1 BDSG-neu sinngemäß fortgeschrieben. Diese Regelung könnte selbstverständlich ohne einen Verstoß gegen Unionsrecht gestrichen werden. Möglicherweise wird der „Gewinn“ einer solchen Streichung für die Verantwortlichen aber aus mehreren Gründen überschätzt:

- Die materiellen datenschutzrechtlichen Pflichten des Verantwortlichen oder Auftragsverarbeiters bleiben auch ohne die Pflicht zur Bestellung eines Datenschutzbeauftragten unverändert bestehen.
- Wegen dieser Pflichten müssen Beratung und Unterrichtung, die sonst der Datenschutzbeauftragten gemäß Art. 38 Abs. 1 lit. a) der Verordnung (EU) 2016/679 übernehmen würde, wohl durch andere sachkundige Personen übernommen werden.
- Bei einem Verantwortlichen, der mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, stellt sich überdies die Frage, ob nicht eine „Kerntätigkeit“ 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 (Art. 37 Abs. 1 lit. b) der Verordnung (EU) 2016/679. Die Reichweite dieser Norm ist völlig ungeklärt und wird erst durch die Rechtsprechung des Europäischen Gerichtshofs Konturen erlangen; mit der Regelung des § 38 Abs. 1 BDSG ist man demgegenüber „auf der sicheren Seite“.

2. Berücksichtigung der unmittelbaren Geltung der Verordnung (EU) 2016/679

Zu Recht weist die Gesetzesbegründung darauf hin, dass aus der unmittelbaren Geltung der Verordnung grundsätzlich ein „Normwiederholungsverbot“ im nationalen Recht resultiert, da

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

ansonsten die Provenienz der Norm verschleiert werden könnte. Vor diesem Hintergrund erscheint die Streichung von Bestimmungen beispielsweise zum Widerruf einer Einwilligung, zu allgemeinen Löschpflichten oder zu technischen und organisatorischen Schutzmaßnahmen geboten, weil diese Themen in der Verordnung (EU) 2016/679 selbst abschließend geregelt sind: Art. 7 Abs. 3 regelt den Widerruf der Einwilligung, Art. 5 Abs. 1 lit. e) und Art. 17 Abs. 1 lit. a) regeln die Löschpflicht, Art. 24, 25, 32 die technischen und organisatorischen Schutzmaßnahmen.

Von dem Normwiederholungsverbot sind in der Rechtsprechung des EuGH allerdings Ausnahmen anerkannt, auf die die Gesetzesbegründung ebenfalls Bezug nimmt. Diese Ausnahmen gehen über den in ErwGr. 8 der Verordnung (EU) 2016/679 genannten Fall der Präzisierung oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten hinaus und erfassen generell die Situation, dass eine Wiederholung des Unionsrechts bzw. ein Verweis darauf für die Rechtsklarheit notwendig sind. Grundsätzlich sind Verweise unproblematischer als echte Normwiederholungen, weil sie nicht den genannten Verschleierungseffekt verursachen.

Daran gemessen erscheinen die deklaratorischen Verweise auf die Verordnung (EU) 2016/679, insbesondere hinsichtlich der Schutzmaßnahmen nach Art. 24, 25 und 32 oder der Bußgeldandrohung in Art. 83 unproblematisch, weil erst sie dem Rechtsunterworfenen ein vollständiges Bild seines Pflichtenprogramms und der allfälligen Sanktionen in einer Kodifikation ermöglichen. Besonders unproblematisch und gleichzeitig eine gewisse Warnfunktion erfüllend erscheint insofern die Formulierung „unbeschadet der weiteren Vorgaben der Verordnung (EU) 2016/679“, wie sie mitunter zur Anwendung kommt. Nicht ganz klar ist, nach welchen Kriterien solche Hinweise oder Verweise manchmal vorgesehen sind und manchmal nicht.

Zu Recht werden Bußgeldbestimmungen, die allein an Datenschutzverstöße anknüpfen, aufgehoben, weil Art. 83 der Verordnung (EU) 2016/679 abschließender Natur ist, wie sich neben dem Ziel der Vollharmonisierung (s.o.) auch im Umkehrschluss aus seinem Abs. 7 ergibt. Deshalb ist es auch überzeugend, dass der Entwurf nicht auf Forderungen eingeht, ergänzende nationale Regelungen zur (Nicht-)Verhängung von Geldbußen zu schaffen. Die Verordnung (EU) 2016/679 selbst sieht in Art. 83 Abs. 2 S. 1 vor, dass Geldbußen je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und j verhängt werden, und enthält in Art. 83 Abs. 2 S. 2 einen nicht abschließenden, aber auch nicht für Konkretisierungen durch die Mitgliedstaaten offenen Katalog von Verhältnismäßigkeitsaspekten, der bei der Entscheidung über eine Geldbuße zu berücksichtigen ist. Insofern liegt es allein in der Hand der unabhängigen Datenschutzaufsichtsbehörden, die Entscheidung zu treffen, ob bei einem nach unionsrechtlichen Maßstäben geringfügigen Verstoß eine Verwarnung nach Art. 58 Abs. 2 lit. b) der Verordnung (EU) 2016/679 anstelle eines Bußgelds ausreicht.

3. Anpassung von Begriffsbestimmungen, insbes. Verarbeitungsbegriff

Grundsätzlich erscheint es im Interesse der Kohärenz des Datenschutzrechts und zur Vermeidung von Unklarheiten bei der Auslegung von Begriffen geboten, die Begrifflichkeiten des

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

deutschen Rechts an die der Verordnung (EU) 2016/679 anzupassen; dies gilt insbesondere im Anwendungsbereich des bereichsspezifischen Datenschutzrechts gemäß Art. 6 Abs. 1 UAbs. 1 lit. c) und lit. e). Solche Änderungen machen das Gros der „redaktionellen Änderungen“ des Gesetzentwurfs aus, und die meisten von ihnen (z. B. „betroffene Person“ statt „Betroffener“, „Verantwortlicher“ statt „verantwortliche Stelle“) erscheinen völlig unproblematisch.

Deutlich komplizierter ist der Umgang mit dem Begriff der „Verarbeitung“ von Daten. Durch die Aufhebung des BDSG-alt ist die Differenzierung zwischen einem weiten europarechtlichen, schon in der Richtlinie 95/46/EG verwendeten und in der Verordnung (EU) 2016/679 ähnlich übernommenen Begriff der „Verarbeitung“ von personenbezogenen Daten einerseits und einem engeren, rein nationalen, in § 3 Abs. 4 BDSG a.F. verwendeten Begriff der Datenverarbeitung andererseits entfallen. Es gibt jetzt nur noch den weiten, europarechtlich geprägten Begriff aus Art. 4 Nr. 2 der Verordnung (EU) 2016/679 bzw. Art. 3 Nr. 2 der Richtlinie (EU) 2016/680. Dieser Begriff meint

> „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“,

ist also ein Oberbegriff für praktisch jede Form des Datenumgangs. Vor diesem Hintergrund kann in allen Fällen, in denen im deutschen Recht bisher umfassend der Datenumgang geregelt werden sollte, der Begriff der Verarbeitung ohne Bedenken verwendet werden; dies ist insbesondere der Fall, wenn die alte Trias „erheben, verarbeiten und nutzen“ oder auch das Begriffspaar „erheben und verwenden“ durch „verarbeiten“ ersetzt wird.

Nicht selten soll nach dem Entwurf der Begriff der Verarbeitung aber auch verwendet werden, wo vorher nur einzelne Formen des Datenumgangs genannt waren. Art. 1 Nr. 1 DSAnpUG-EU soll beispielsweise die Formulierung „erheben, speichern, verändern und nutzen“ durch den Begriff „verarbeiten“ ersetzen, der offensichtlich weiter zu verstehen ist. Die Begründung zum 2. DSAnpUG-EU geht mit diesem sich durch den gesamten Entwurf ziehenden Thema uneinheitlich um. Insbesondere im Bereich des SGB wird stets genau begründet, warum es trotz der Änderung der Begrifflichkeit nicht zu einem Bedeutungswandel und insbesondere einer Befugniserweiterung des Verantwortlichen kommt. Andernorts wird dies bloß (aber auch immerhin) behauptet, an wieder anderen Punkten wird schlicht von einer redaktionellen Anpassung gesprochen, ohne die Frage überhaupt zu thematisieren.

Der Begründung zu den Änderungen des SGB lassen sich in der Gesamtschau drei Konstellationen entnehmen, in denen trotz Verwendung eines weiteren Verarbeitungsbegriffs der Bedeutungsgehalt der Norm unverändert bleibt. Dies ist der Fall,

- wenn die Norm (eigentlich entgegen ihrem Wortlaut) schon bisher so weit verstanden wurde,
- wenn es sich bei der Norm um eine solche handelt, die Datenverarbeitung nicht autorisiert, sondern beschränkt,

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

- oder wenn auch in einer Befugnisnorm der weite Verarbeitungsbegriff aufgrund der Gesetzessystematik keine über die bisherige, eventuell engere Auslegung hinausgehende Bedeutung erlangt.

Es ist der Natur eines Änderungsgesetzes geschuldet, dass im Normtext nicht erkennbar ist, ob eine und wenn ja, welche dieser Konstellationen gegeben ist. Nur in den genannten Fällen ist eine sprachliche Anpassung aber unproblematisch, andernfalls muss geprüft werden, ob ggf. eine Erweiterung der Verarbeitungsbefugnisse gewollt (und zulässig) ist. Ist dies nicht der Fall, sollten – wie ebenfalls in einigen Änderungen zum SGB vorgeführt – die relevanten Verarbeitungsteilschritte entsprechend der Terminologie des Art. 4 Nr. 2 der Verordnung (EU) 2016/679 bzw. des Art. 3 Nr. 2 der Richtlinie (EU) 2016/60 konkret benannt werden.

Passau, den 6.12.2018

gez. Prof. Dr. Meinhard Schröder

Besucheradresse Innstraße 39, Raum 114
Internetadresse www.uni-passau.de/schroeder

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 E

Dr. Stefan Brink

LfDI Baden-Württemberg

6.12.2018

Stellungnahme gegenüber dem Deutschen Bundestag

zur BT-Drucksache 19/4674 vom 1. Oktober 2018

Die mühsame Anreise durch das Datenschutz-Deutschland des 2. DSAnpUG-EU

Seit dem 25. Mai 2018 reguliert europäisches Recht den Datenschutz. In den 70er Jahren in Deutschland entwickelt und seit 1995 mit einer umsetzungsbedürftigen europäischen Richtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) ausgestaltet, endet so die jahrzehntelange Reise der Idee von der individuellen Entscheidung über persönliche Informationen – seit 1983 „Grundrecht auf informationelle Selbstbestimmung“ genannt – an einem absoluten Ziel- und Höhepunkt: Durch europäischen Verordnung (VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016, ABl. L 119 vom 4.5.2016, S. 1) sind jetzt alle Informationsbeziehungen zwischen Privatpersonen auf der einen und Unternehmen und Behörden auf der anderen Seite eindeutig und abschließend geregelt. Und zwar durch unmittelbar geltendes, in der ganzen Europäischen Union gleichlautendes und mit Anwendungsvorrang vor nationalen Normen ausgestattetes Recht.

Damit ist die „Reise nach Europa“ für den Datenschutz aber noch nicht an ihrem Ende. Denn gerade wegen des Anwendungsvorrangs der Europäischen Verordnung müssen jetzt noch nationale Altbestände des Datenschutzrechts aus dem Weg geräumt werden – in Deutschland waren dies etwa das „gute alte“

Bundesdatenschutzgesetz und die – zeitlich noch älteren – Landesdatenschutzgesetze.

Soweit – so einfach. Aber das Reisen in Europa ist aus zweierlei Gründen doch etwas komplizierter als das einfache Umsteigen vom nationalen D-Zug in den Trans-Europa-Express: Zum einen ist das neue europäische Verordnungsrecht sachlich nicht umfassend anwendbar, es spart etwa Bereiche wie die Datenverarbeitung durch Parlamente (Art. 2 Abs. 2 lit. a DSGVO), durch Privatpersonen für persönliche Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO, etwa das Fotografieren fürs Familienalbum) oder durch Behörden zum Zwecke der Strafverfolgung oder Strafvollstreckung (Art. 2 Abs. 2 lit. d DSGVO) aus. Hier wird weiter national geregelt. Zum anderen ist die DSGVO leider gar keine Vollregelung. Sie lässt zahlreiche Lücken, deren Ausfüllung sie ausdrücklich den Mitgliedsstaaten der EU überlässt (sog. „Öffnungsklauseln“). Damit stellt die DSGVO ihr großes Ziel, gleiches Recht in Europa gleichmäßig anzuwenden, zwar in Frage; aber so entlasteten sich Europäisches Parlament und Rat im ohnehin langwierigen und fragilen Gesetzgebungsprozess. Anstatt eine europaweit einheitliche Lösung für die Fragen der Verarbeitung von Beschäftigtendaten oder für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten zu finden, überließ man es den Mitgliedsstaaten, hier jeweils nationale Antworten zu geben. Daraus erklärt sich, warum es auch nach dem 25. Mai 2018 noch nationales Datenschutzrecht gibt – und im föderalen Deutschland gleich in doppelter Ausführung (BDSGneu/16 LDSGneu).

1. Aufschlag

In einem ersten Aufschlag haben die Deutschen Gesetzgeber (mit leichter Verspätung) schon mal die dicksten nationalen Brocken von der Straße geschoben, sie haben das Bundesdatenschutzgesetz und die entsprechenden Ländergesetze an die Vorgaben der DSGVO angepasst und von den verbliebenen Regulierungsmöglichkeiten ausgiebig Gebrauch gemacht (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der

Richtlinie (EU) 2016/680 - Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU – vom 30. Juni 2017, BGBl. I S. 2097). Dabei haben die nationalen Gesetzgeber allerdings nicht nur gut geräumt, sie haben auch ganz erhebliche Kollateralschäden am Straßenkörper verursacht: Die Strecke nach Europa wurde nicht schneller, sondern holperiger. Zu nennen wären da etwa ganz offensichtliche Kompetenzüberschreitungen zu Lasten der DSGVO, etwa mit § 4 BDSG zur Videoüberwachung. Mit dieser Vorschrift wird jetzt jeder Parkplatzbetreiber zum Terrorfahnder heraufgestuft und die Arbeit der Aufsichtsbehörden in den Ländern ganz erheblich (und gezielt) erschwert. Zu nennen ist auch die absurde Vorschrift des § 43 Abs. 4 BDSG, wonach Bußgelder bei Datenpannen nur noch verhängt werden können, wenn der Verantwortliche dem zustimmt (!). Auch beim Versuch, die wackeren Rechtsanwälte, Ärzte und Steuerberater dem Zugriff der furchtbaren Landesdatenschützer zu entziehen (§ 29 BDSG), leistete der Bundesgesetzgeber ganze Arbeit – die nun vom Europäischen Gerichtshof in mühsamer Kleinarbeit wieder glattgezogen werden muss. Vertragsverletzungsverfahren sind dem deutschen Gesetzgeber schon mal sicher.

Ansonsten nutzte der Bundestag tatsächliche oder vermeintliche Öffnungsklauseln dazu, die Rechte der Betroffenen wo immer möglich weiter einzuschränken (§§ 32 ff. BDSG); lediglich bei der Bestellpflicht eines betrieblichen Datenschutzbeauftragten überbot der nationale Gesetzgeber die laschen Vorgaben der DSGVO (Art. 37 f.), was er aber jetzt schon wieder bereut (vgl. Bundesrats-Drucksache 430/1/18).

Als tröstlich mag man empfinden, dass noch eindeutigere Verstöße gegen Wortlaut und Geist der DSGVO anderen Regierungen überlassen blieben, etwa Österreich mit der Freistellung von Erstverstößen von der Bußgeldpflicht (Art. 83 DSGVO) oder dem Bayerischen Kabinett mit der rechtsgrundlosen Herausnahme von Vereinen aus der Bestellpflicht von Datenschutzbeauftragten. Hier endet die Reise nach Europa offensichtlich in der Sackgasse.

2. Aufschlag

Mit weitaus erheblicherer Verspätung - mehr als ein halbes Jahr nach Wirksamwerden der DS-GVO - bemüht sich nun die Bundesregierung darum, in einem zweiten (und vermeintlich letzten) Anlauf die gesamte bundesdeutsche Restrechtsmaterie DSGVO-konform zu gestalten. Sie tut dies in einem vom Innenministerium federführend zu verantwortenden „Omnibus-Gesetz“, das in einem Artikelgesetz mehr als 150 Bundesgesetze Huckepack nimmt und abändert. Es dient der Anpassung sogenannter „bereichsspezifischer Datenschutzvorschriften“ des Bundes an die DSGVO, mit dabei sind Gesetze aus allen Ressortbereichen der Bundesregierung. Dass es sich beim Datenschutzrecht mittlerweile um eine echte Querschnittsmaterie handelt, erfährt jeder, der die 563 Seiten der Bundesrats-Drucksache 430/18 vom 7. September 2018 durchblättert; betroffen sind so unterschiedliche Rechtsmaterien wie das Antiterrordatei-Gesetz, das Anti-Doping-Gesetz und das Prostituiertenschutz-Gesetz.

Dieser Mammut-Regierungsentwurf wurde am 5.9.2018 vom Bundeskabinett beschlossen und zunächst dem Bundesrat zur Beratung zugeleitet, die 1. Lesung im Deutschen Bundestag (BT-Drucksache 19/4674 vom 1. Oktober 2018) fand am 12.10.2018 statt.

Wohin geht die Reise?

Großteils bestehen die Änderungen lediglich darin, die bisherigen Vorschriften an die Terminologie der DS-GVO anzupassen. Wenig spektakulär, aber absolut notwendig sind etwa die Ersetzung der Wörter „erheben, speichern, verändern und nutzen“ durch das Wort „verarbeiten“. Dieser DS-GVO-Sprech betrifft nicht nur die Gesetzesfassade, er verdeutlicht auch den fundamentalen Wechsel der Rechtsquelle, der mit dem 25.5. vollzogen wurde: Wir alle wenden nicht länger wohlbekanntes deutsches Recht an, das der Verwaltung vertraut, von zahlreichen Kommentatoren ausgeleuchtet und von nationalen Gerichten ausgeformt wurde. Wir ergründen die europäische Bedeutung nur scheinbar bekannter Rechtsbegriffe.

„Verarbeiten“ nach § 3 Abs. 4 BDSG alter Fassung ist eben nicht identisch mit der „Verarbeitung“ des Artikel 4 Nr. 2 DSGVO. Das alte Verständnis aus den Köpfen der erfahrenen Datenschützer herauszubekommen und Platz zu machen zumindest für die Bereitschaft, vermeintlich Wohlbekanntes neu und richtig zu verstehen, ist eine Herausforderung.

Materielle Änderungen finden sich im Gesetzentwurf natürlich auch: Wieder nutzt die Bundesregierung die Öffnungsklauseln der DS-GVO, um Betroffenenrechte auf Auskunft oder Löschung einzuschränken. Dabei ist wie bereits beim 1. Anpassungsgesetz nicht immer ganz klar, ob die Voraussetzungen für diese Beschränkungen, wie sie in Artikel 23 Absatz 1 DS-GVO festgelegt sind, auch in jedem Falle vorliegen. Solche Unterschreitungen des Schutzniveaus der DSGVO sind nämlich nur dann zulässig, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt“. Das wäre in jedem Einzelfall zu prüfen. Zudem muss jede einschränkende Gesetzgebungsmaßnahme „insbesondere gegebenenfalls spezifische Vorschriften enthalten“, jedenfalls hinsichtlich der Zwecke der Verarbeitung und mittels Garantien gegen Missbrauch oder unrechtmäßige Übermittlung der Daten (Art. 23 Abs. 2 DS-GVO). Es liegt sehr nahe, dass der EuGH in den kommenden Jahren klare Vorgaben für solche Rechtsbeschränkungen entwickeln wird – und dass auch der deutsche Gesetzgeber hiervon betroffen sein wird.

Erster Kandidat für solche Korrekturen wird der im 2. DSAnpUG-EU an zahlreichen Stellen zu findende Ausschluss des Auskunftsrechts nach Artikel 15 DS-GVO sein, der unser Bürgerrecht auf Kenntnis von Verarbeiter und Verarbeitung bereits dann einschränkt, „wenn die Auskunftserteilung die ordnungsgemäße Aufgabenerfüllung gefährden würde“. Dieser Maßstab ist offensichtlich so niedrig angesetzt, dass zahllose Datenverarbeitungen durch öffentliche Stellen künftig „unter dem Radar“ segeln würden. Das kann nicht richtig sein – und ist von der DS-GVO auch nicht gewollt. Wie schon beim 1. DSAnpUG-EU verpasst die Bundesregierung damit

erneut die Chance, den Datenschutz als Grundrechtsschutz auf ein insgesamt höheres Niveau zu heben.

Darüber hinaus finden sich breit über die 563 Seiten des Gesetzentwurfs verteilt Einzelbestimmungen zu Datenverarbeitungen, die der Bundesregierung schon immer „ein Anliegen“ waren. Aus der Vielzahl problematischer Einzelregelungen seien nur die datenschutzrechtlich problematischsten hervorgehoben:

- Teilweise werden bei Gelegenheit der Rechtsanpassung eigenständige Rechtsgrundlagen mit dem Ziel geschaffen, weitreichendere Verarbeitungen personenbezogener Daten zu gestatten als bislang erlaubt, etwa nach dem Telekommunikationsgesetz. Mit § 19 Absatz 4 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz - BDBOSG) soll so zugunsten der Bundesanstalt für den Digitalfunk eine Vorratsdatenspeicherung für Verkehrsdaten eingeführt werden, die sage und schreibe alle Daten der vergangenen 75 Tage umfasst. Das ist eine – auch mit Blick auf vorliegende und noch ausstehende Entscheidungen des Bundesverfassungsgerichts und des EuGH zur Grundproblematik jeder anlasslosen massenhaften Datenspeicherung – steile Ansage.

- Zumindest unschön ist eine Neuregelung im Soldatengesetz, die vorsieht, dass Meldebehörden personenbezogene Daten deutscher Staatsangehöriger, die im nächsten Jahr volljährig werden, an das Bundesamt für Personalmanagement der Bundeswehr übermitteln dürfen. Gedanklich scheint die Bundesregierung die allgemeine Wehrpflicht also noch nicht realisiert zu haben. Dass Betroffene der Übermittlung vorab widersprechen können, ist da nur ein schwacher Trost.

- Ähnlich unsauber ist die vorgesehene Neuregelung im IHK-Gesetz, wonach die Industrie- und Handelskammern personenbezogene Daten ihrer Kammermitglieder an nicht-öffentliche Stellen übermitteln dürfen, wenn die

Kammermitglieder dem nicht widersprechen. Zu Zeiten, in denen der Kammerzwang keineswegs völlig akzeptiert ist, tun sich die IHKs mit solchen Eingriffen in Mitgliederrechte sicherlich keinen Gefallen.

- Manches Mal ist auch das Schweigen des Gesetzentwurfes beredt: Anders als noch im Referentenentwurf vorgesehen, findet sich im Regierungsentwurf zur Änderung des SGB V nicht mehr die Möglichkeit, gegen die gesetzlichen Krankenkassen bei Datenschutzverstößen erhebliche Bußgelder zu verhängen. Glückwunsch an die erfolgreichen Lobbyisten.

- Das gilt auch für den mit Blick auf die gerade scheiternden Verhandlungen zur ePrivacy-Verordnung besonders relevanten Anpassungen und Neuregelungen des Telekommunikationsgesetzes TKG. Anders als noch im Referentenentwurf vorgesehen, findet man im Entwurf nun keinerlei Regelungen zum Verhältnis von TKG und DSGVO mehr – und damit hängt eine unabhängige Datenschutzaufsicht in diesem wichtigen Bereich weiter in der Luft.

- Mehrfach wird die durch die DS-GVO grundsätzlich verbotene Verarbeitung sensitiver Daten (vgl. Art. 9 Abs. 1 DS-GVO) durchbrochen. So sollen nun auch nicht-öffentliche Stellen zur Verarbeitung solcher Daten grundsätzlich befugt sein, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist (§ 22 Absatz 1 Nummer 1 Buchstabe d BDSG). Damit werden etwa die Voraussetzungen dafür geschaffen, dass sensible Informationen durch zivilgesellschaftliche Träger im Rahmen von Deradikalisierungsprogrammen verarbeitet und im Einzelfall an die Sicherheitsbehörden weitergegeben werden können. Auch wenn man dies vom Grundansatz als legitimes Interesse ansieht, lässt die ungewöhnlich weite sprachliche Fassung erheblich weitergehende Anwendungsbereiche erwarten und befürchten.

Im Asylgesetz und im Aufenthaltsgesetz soll zudem die Verarbeitung sensitiver Daten freigegeben werden, „soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist“. Diese weite und strukturlose Formulierung widerspricht eindeutig der Öffnungsklausel des Artikel 9 Absatz 1 Buchstabe g DSGVO. Zudem sind nirgends spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der Betroffenen vorgesehen.

Auch hier zeigt sich wieder: Wer Grundrechte einschränken möchte, fängt damit bei Außenseitergruppen an: Bei Straftatverdächtigen, Asylsuchenden, Ausländern. Der weitere Weg solche Grundrechtsverluste ist dann vorgezeichnet: über „extensive“ Grundrechtsnutzer wie Demonstranten, Meinungsinhaber und Reisende bis hinein in den Kern unserer Gesellschaft.

Fazit

Insgesamt gesehen bleiben beim geneigten Leser dieses Werkes drei Eindrücke hängen:

1. Ein solches Mammutprojekt vollständig zu durchdringen, ist weder dem Parlament, noch der kritischen Öffentlichkeit möglich. Ob dies nun der komplexen Materie oder dem überschießenden Regulierungsinteresse der Bundesregierung geschuldet ist, bleibt letztlich gleich. Rationale Gesetzgebung wird so nicht funktionieren. Abhilfe wäre nur möglich, indem sich die Regierung jeder materiellen Nutzung von Öffnungsklauseln enthält (ja, das wäre durchaus möglich!) oder zumindest eine klare Trennung von terminologischen und ideologischen Änderungsanliegen vornimmt.

2. Anstatt den Schwung der DSGVO aufzugreifen und zu begreifen, dass die Zukunft der Datenverarbeitung aus europäischer Sicht und als globales Alleinstellungsmerkmal nur in einer unauflöslichen Verbindung von Digitalisierung und Datenschutz liegen kann, ergeht sich der Entwurf in einem Kleinklein der Beschränkung von Betroffenenrechten. So agieren nicht inspirierte Gestalter, so agieren Kleinkrämer.

3. Der lange Weg des Datenschutzes nach Europa kann nur gelingen, wenn die nationalen Straßen von Ballast und Unrat geräumt werden und der „Omnibus zur EU“ freie Fahrt bekommt. Dabei sind alle nationalen Vorschriften, die nicht EU-rechtskonform ausgestaltet sind, von Übel, denn sie verzögern, wo Tempo gefragt ist und sie verunsichern, wo Klarheit Not tut. Auch mit diesem 2. Gesetzentwurf steht die Bundesregierung weiter auf der Bremse.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
zu 19(4)187 E

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Dr. Stefan Brink

LfDI Baden-Württemberg

7. Dezember 2018

Stellungnahme gegenüber dem Innenausschuss des Deutschen Bundestags
zum 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU
(BT-Drucksache 19/4674 vom 1. Oktober 2018)

10 Vorschläge für ein besseres Datenschutzrecht

1. Die Stärke der DS-GVO besteht in der unauflöslichen Verbindung von moderner Datenverarbeitung und Bürgerrechten, von **Digitalisierung und Datenschutz**. Nicht zwingend gebotene nationale Sonderregelungen, insbesondere Beschränkungen von jenen Betroffenenrechten, welche den europäischen Weg in die Digitalisierung gerade charakterisieren, sollten unterbleiben.

2. **Schwächen der DS-GVO**, etwa die unterschiedslose Regulierung von kleinen Betrieben und Großkonzernen, sollten dort behoben werden, wo das rechtlich möglich und sinnvoll ist: **auf EU-Ebene**. Nationale Korrekturversuche sind nutzlos und tragen erheblich zur bestehenden Verunsicherung der Verantwortlichen bei.

3. Die Axt an die **Institution des betrieblichen Datenschutzbeauftragten** zu legen würde bedeuten, eine bewährte Einrichtung des deutschen Datenschutzes gerade in dem Moment zu beschneiden, wo sie am dringendsten gebraucht wird. Es kann nur darum gehen, die Belastungen durch die DS-GVO angemessen zu gestalten – und nicht darum, die dabei für die Unternehmen hilfreichste Institution nach dem Motto zu beschädigen: „Die See wird rauer, wir sollten den Lotsen von Bord schicken!“

4. Möglich bleibt die **Entlastung von nationalen Vorgaben**, etwa die Freistellung **kleinerer, nicht gewerblich tätiger Vereine** von der Bestellpflicht eines Datenschutzbeauftragten. Die Beschränkung der Bestellpflicht auf Verarbeitungen zu gewerblichen Zwecken würde Rechtsanwälte, Ärzte und Steuerberater ausnehmen, was sachlich nicht zu rechtfertigen und zudem europarechtswidrig ist. Möglich wäre demgegenüber eine Beschränkung auf „**geschäftsmäßige Verarbeitungen**“.

5. Datenschutzwidrige Vorhaben wie die Einführung bereichsspezifischer **Vorratsdatenspeicherungen** sollten fallengelassen werden.

6. Unternehmen nehmen zunehmend die **Beratungsleistungen der Datenschutzaufsichtsbehörden** in Anspruch. Auch deshalb ist die **föderale Struktur** der Datenschutzaufsicht in Deutschland zu erhalten, denn nur sie gewährleistet eine ortsnahe, effektive und pragmatische Beratung der Verantwortlichen.

7. Zur Unterstützung der Arbeitsfähigkeit des Parlamentes sollte die Regierung künftig bei **Gesetzentwürfen eine klare Trennung** von rein terminologischen und inhaltlich bedeutsamen Änderungsanliegen vornehmen.

8. Der Bundestag sollte **europarechtswidrige Regelungen des BDSGneu**, wie etwa das Verwertungsverbot bei Datenpannen-Meldungen oder die weitgehende Freistellung der freien Berufe von der Datenschutz-Aufsicht zurücknehmen.

9. Soweit **andere Mitgliedstaaten** der EU, wie etwa Österreich, offensichtlich **europarechtswidrige nationale Regelungen** in Kraft setzen, etwa zur Aussetzung von Bußgeldern durch die Datenschutz-Aufsichtsbehörden oder zur Bestellpflicht von Datenschutzbeauftragten, sollte der Bundestag auf die Einleitung von **Vertragsverletzungsverfahren vor dem EuGH** dringen. Dies sorgt für Rechtssicherheit und baut rechtswidrige Wettbewerbsvorteile innerhalb Europas ab.

10. Bei der **Evaluierung der DS-GVO** nach Art. 97 sollten die **Abgeordneten des Deutschen Bundestages** eine **aktive Rolle** einnehmen und ihre Erfahrungen als Ansprechpartner von Betrieben und Vereinen gegenüber der Europäischen Kommission einbringen – ganz unabhängig von den Positionen der Bundesregierung.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 F

verbraucherzentrale
Bundesverband

ZU EINEM FAIREN WETTBEWERB GEHÖRT AUCH DER DATENSCHUTZ

Stellungnahme
des Verbraucherzentrale Bundesverbands (vzbv)
zum Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(BT-Drucksachen 19/4674, 19/5414)

anlässlich der öffentlichen Anhörung
im Ausschuss für Inneres und Heimat des Deutschen Bundestages
am 10. Dezember 2018

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Recht und Handel

Markgrafenstraße 66
10969 Berlin

Recht-und-Handel@vzbv.de

Inhalt

I. ZUSAMMENFASSUNG

Diese Stellungnahme betrifft die Frage, ob der Gesetzgeber die wettbewerbsrechtlichen Klagebefugnisse für Verstöße gegen Datenschutzrecht einschränken sollte und inwieweit Verstöße gegen Datenschutzrecht überhaupt wettbewerbsrechtlich verfolgt werden können.

Der Verbraucherzentrale Bundesverband e.V. (vzbv) positioniert sich zu dieser Frage folgendermaßen:

- **Der Gesetzgeber sollte keine Regelung des Inhalts treffen, dass datenschutzrechtliche Vorschriften nicht als Marktverhaltensregel im Sinn des § 3a UWG anzusehen seien.**

  Die steigende Bedeutung von Daten als wesentlicher Bestandteil des marktbezogenen Leistungsaustauschs ist kennzeichnend für die Digitalisierung. Wer über Daten verfügt, verfügt auch über ökonomische Macht. Wer Daten unbefugt nutzt, erlangt einen ökonomischen „Vorsprung durch Rechtsbruch“. Diesen muss die Wettbewerbsordnung unterbinden können.

- **Der vzbv sieht die Durchsetzung des Datenschutzrechts durch Datenschutzbehörden und durch die nach Wettbewerbsrecht klagebefugten Verbände und Personen als komplementär an.**

  Die Durchsetzung des Datenschutzrechts durch Datenschutzbehörden dient dem Schutz der Persönlichkeitsrechte, die Durchsetzung des Wettbewerbsrechts dient dem Schutz des unverfälschten Wettbewerbs. Wegen dieser unterschiedlichen Zielsetzung besteht kein Anlass anzunehmen, dass die Datenschutz-Grundverordnung (DSGVO) eine parallele Durchsetzung auf wettbewerbsrechtlichem Weg ausschließe.

  Das Datenschutzrecht kann im Einzelfall auch Zwecken der Marktverhaltensregelung dienen. Wenn dies der Fall ist, ist Datenschutz auch Wettbewerbsschutz und muss als solcher durchsetzbar sein. Diese Durchsetzung unterscheidet sich vom behördlichen Datenschutzauftrag und wird im zivilrechtlichen System durch das UWG und damit beauftragten qualifizierten Einrichtungen – einschließlich der Verbraucherverbände - gewährleistet.

- **Die vom vzbv erfolgreich geführten und noch laufenden Verfahren im Bereich des Datenschutzes belegen, dass das Klagerecht der Verbraucherverbände von hoher Bedeutung ist, um Verbraucherinnen und Verbraucher[1] vor einer unbefugten Nutzung ihrer Daten zu schützen und gleichzeitig im Interesse der Marktteilnehmer einen „Vorsprung durch Rechtsbruch“ zu verhindern.**

  Im Verfahren „Freundefinder“ gegen Facebook hat der BGH auf Klage des vzbv beispielsweise entschieden, dass die Auslesung der Adressbücher von Facebook-Nutzern und das Versenden von Einladungs-Mails rechtswidrig war. Facebook musste diese unbefugte Nutzung von Nutzerdaten einstellen und kann keinen weiteren ökonomischen Nutzen mehr daraus ziehen.

[1] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

II. DAS DATENSCHUTZRECHT IN DER DEBATTE ÜBER ABMAHNMISSBRAUCH

1. GESETZENTWURF DES BMJV ZUR STÄRKUNG DES FAIREN WETTBEWERBS

Ob und inwieweit Datenschutzverstöße auch mit den Mitteln des Wettbewerbsrechts verfolgt werden können, ist rechtlich schon seit längerem umstritten. In die politische Aufmerksamkeit ist das Thema gerückt, seit mit Inkrafttreten der Datenschutzgrundverordnung die Sorge vor einer datenschutzrechtlichen Abmahnwelle um sich greift.

Insofern ist die Diskussion über die Klagebefugnis im Datenschutzrecht Teil der generellen Debatte über Abmahnmissbrauch. Der vzbv erkennt an, dass dem Missbrauch von Abmahnungen insbesondere zu Zwecken der Gewinnerzielung durch entsprechende Gesetzesänderungen zu begegnen ist. Der vzbv hat den Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) für ein Gesetz zur Stärkung des Wettbewerbs[2] in den wesentlichen Punkten begrüßt.

Das System einer zivilrechtlichen Kontrolle des Wettbewerbs und der Beachtung verbraucherschützender Gesetze hat sich bewährt. Darin ist sich der vzbv mit der Wirtschaft einig. Gerade deshalb ist es wichtig, einen Missbrauch der zivilrechtlichen Rechtsdurchsetzungsbefugnisse zu verhindern. Der Missbrauch droht ansonsten die zivilrechtliche Rechtsdurchsetzung insgesamt in Misskredit zu bringen.

Der Gesetzentwurf des BMJV geht das Problem des Abmahnmissbrauchs insgesamt an, ohne danach zu differenzieren, auf welche Rechtsvorschriften sich eine Abmahnung bezieht. Das ist aus Sicht des vzbv der richtige Ansatz.

2. SONDERREGELUNGEN FÜR DIE KLAGEBEFUGNIS IM DATENSCHUTZRECHT?

Im Unterschied zum gesetzgeberischen Ansatz des BMJV wird verschiedentlich erwogen, die zivilrechtlichen Klagebefugnisse speziell im Bereich des Datenschutzrechts einzuschränken. Das Land Bayern hatte im Bundesrat eine entsprechende Gesetzesinitiative eingebracht[3] und außerdem eine entsprechende Änderung des Zweiten Datenschutz-Anpassungsgesetzes beantragt[4]. Die beiden Anträge haben im Bundesrat keine Mehrheit gefunden. Dennoch sollen die entsprechenden Überlegungen hier kommentiert werden, weil sie voraussichtlich auch in der Bundestagsdebatte zum Zweiten Datenschutz-Anpassungsgesetz eine Rolle spielen werden.

Der vzbv warnt davor, eine Regelung des Inhalts zu treffen, dass das Datenschutzrecht generell keine Marktverhaltensregel im Sinn des § 3a UWG sei. Eine solche gesetzgeberische Regelung wäre – anders als teilweise behauptet - keine Klarstellung, sondern eine drastische Einschränkung der wettbewerbsrechtlichen Klagebefugnisse. Angesichts der rasch voranschreitenden Digitalisierung wäre es nicht hinnehmbar, dass ein wettbewerblicher „Vorsprung durch Rechtsbruch“ dann wettbewerbsrechtlich irrelevant ist, wenn sich der Rechtsbruch auf das Datenschutzrecht bezieht.

---

[2] Referentenentwurf des Bundesministeriumns der Justiz und für Verbraucherschutz: Entwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs vom 11.09.2018.

[3] BR-Drs. 304/18 vom 26.06.2018

[4] BR-Drs. 430/1/18 vom 5.10.2018

Es wäre auch rechtsstaatlich problematisch, wenn die Reichweite der Klagebefugnis davon abhinge, welche Rechtsvorschriften durchgesetzt werden. Ein Signal, dass Marktverhaltensregeln aus dem Bereich des Datenschutzrechts weniger stringent durchgesetzt werden als andere verbraucherrechtlich relevante Vorschriften, stünde in einem Widerspruch zu der wachsenden Bedeutung der Persönlichkeitsrechte als „Währung“ im Leistungsaustausch der digitalen Wirtschaft.

Schließlich besteht für eine datenschutzspezifische Einschränkung der wettbewerbsrechtlichen Klagebefugnis auch kein Anlass, weil es bislang gar keine Anzeichen für eine Abmahnwelle wegen Verletzungen der DSGVO gibt.

> Die steigende Bedeutung von Daten als wesentlicher Bestandteil des marktbezogenen Leistungsaustauschs ist kennzeichnend für die Digitalisierung. Wer über Daten verfügt, verfügt auch über ökonomische Macht. Wer Daten unbefugt nutzt, erlangt einen ökonomischen „Vorsprung durch Rechtsbruch“. Diesen muss die Wettbewerbsordnung unterbinden können.

III. WETTBEWERBSWIDRIGKEIT VON DATENSCHUTZVERSTÖßEN NACH GELTENDEM RECHT

1. DATENSCHUTZ ALS MARKTVERHALTENSREGEL

Die eben dargestellte ökonomische Bedeutung des Datenschutzrechts findet ihre Entsprechung auch auf der rechtlichen Ebene.

Soweit Vorschriften des Datenschutzes auch dazu bestimmt sind, Marktverhalten zu regeln, kann deren Nichtbeachtung spürbare Folgen für den Wettbewerb und die Akteure am Markt haben. Verbraucher können hiervon unmittelbar betroffen sein, etwa wenn es um eine Kommerzialisierung des Rechts auf informationelle Selbstbestimmung geht. Darüber hinaus sind Verbraucher indirekt betroffen, wenn sich Unternehmen durch Missachtung von Datenschutzregeln Vorteile vor Mitbewerbern verschaffen (Vorsprung durch Rechtsbruch) und damit Druck auf Wettbewerber ausüben (Fehlanreize).

Das primäre Ziel bei der Durchsetzung von Datenschutzrecht mit den (privatrechtlichen) Mitteln des Lauterkeitsrecht liegt dementsprechend nicht im Datenschutz selbst, sondern in der Lauterkeit des Wettbewerbs. Mit anderen Worten: Über § 3a UWG wird nicht primär Datenschutzrecht, sondern Wettbewerbsrecht durchsetzt.

2. DSGVO NICHT ABSCHLIEßEND IM HINBLICK AUF WETTBEWERBSRECHTLICHE UNTERLASSUNGSANSPRÜCHE

Die Durchsetzung des Datenschutzrechts durch Datenschutzbehörden dient dem Schutz der Persönlichkeitsrechte, die Durchsetzung des Wettbewerbsrechts dient dem Schutz des unverfälschten Wettbewerbs. Wegen dieser unterschiedlichen Zielsetzung besteht kein Anlass anzunehmen, dass die Datenschutz-Grundverordnung eine parallele Durchsetzung auf wettbewerbsrechtlichem Weg ausschließe[5].

[5] Eine solche Ausschließlichkeit nimmt insbesondere Köhler an, vgl. WRP 2018, Seite 1269 ff.

Die DSGVO beinhaltet gerade keine wettbewerbsrechtlichen Regelungen und Rechtsbehelfe und kann deshalb gar nicht abschließend sein. Die grundsätzliche Eignung einzelner Regelungen der DSGVO als wettbewerbsrelevante Marktverhaltensregel kann auch vor dem Hintergrund der Entstehungsgeschichte der DSGVO und dem Vollharmonisierungsansatz zur Vermeidung von Wettbewerbsverzerrung kaum ernsthaft bestritten werden. Gerade die sich aus der Datenschutzrichtlinie von 1995 ergebenen Unterschiede führten nach Ansicht des Verordnungsgebers zu Wettbewerbsverzerrungen im Binnenmarkt.[6] Soweit Datenschutzregeln gleichzeitig Marktverhaltensregeln sind, kann deren Verletzung deshalb *auch* eine Störung des lauteren Wettbewerbs darstellen, die dann auch mit den Mitteln des Lauterkeitsrechts – einschließlich der Verbraucherverbandsklage - abzustellen ist.

3. ZUM AUSBLEIBEN DER BEFÜRCHTETEN „ABMAHNWELLE“

Dass es bislang keine Hinweise auf vermehrte Abmahnungen wettbewerbsrechtlicher Art wegen Datenschutzverstößen gibt, dürfte nicht zuletzt darauf zurückzuführen sein, dass gerade nicht jeder Datenschutzverstoß gleichsam automatisch über § 3a UWG auch einen wettbewerbsrechtlichen Unterlassungsanspruch begründet. Denn eine Durchsetzung des Datenschutzrechts mit Hilfe des wettbewerbsrechtlichen Unterlassungsanspruchs ist nur möglich, wenn neben der verletzten datenschutzrechtlichen Norm, die weiteren Voraussetzungen des Wettbewerbsrecht vorliegen. Das bedeutet im Sinne eines klassischen Prüfungsschemas:

- Die datenschutzrechtliche Norm muss zugleich das Marktverhalten regeln;
- Der Schutz der Marktteilnehmen (Verbraucher) muss zumindest Nebenzweck sein (§ 2 Absatz 1 Nr. 3 UWG);
- Das beanstandete Verhalten muss eine geschäftliche Handlung im Sinne von § 2 Absatz 1 Nr. 1 UWG sein;
- Der Verstoß gegen den datenschutzrechtlichen Tatbestand muss vollständig gegeben sein und
- Die konkrete Handlung muss geeignet sein, die Interessen der Verbraucher spürbar zu beeinträchtigen.

Dabei liegt die Erfüllung der oben genannten Tatbestandsmerkmale nicht auf der Hand und ihre Darlegung vor Gericht kann sich nicht auf Floskeln beschränken. Verbraucherverbände müssen in jedem Einzelfall begründen, dass eine konkrete Norm des Datenschutzes auch eine Marktverhaltensregel ist und der Datenschutzverstoß im konkreten Fall auch einen Wettbewerbsverstoß begründet. Soweit dieser Nachweis aber gelingt und zur Überzeugung des Gerichts eine unterlassungspflichtige Beeinträchtigung des lauteren Wettbewerbs gegeben ist, müssen Verbraucherverbände und andere qualifizierte Einrichtungen auch weiterhin in der Lage sein, diese Verstöße abzustellen.

[6] So in Bezug auf die Richtlinie 95/46/EG ausdrücklich Erwägungsgrund 9, Satz 3 DSGVO: „Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeit darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern“; vgl. hierzu im Einzelnen auch Laoutoumai/Hoppe, Kommunikation & Recht, 2018, Seite 533, 534.

4. NOTWENDIGKEIT DER WETTBEWERBSRECHTLICHEN DURCHSETZUNG VON DATENSCHUTZVORSCHRIFTEN

Die Notwendigkeit, diese Klagebefugnis de lege lata zu erhalten, folgt damit unmittelbar aus dem gesetzlichen Auftrag an die qualifizierten Einrichtungen, als einzige Akteure im zivilrechtlichen Durchsetzungsregime Verletzungen des Lauterkeitsrechts zu ahnden. Aus der Perspektive der Verbraucherverbände ist das Datenschutzrecht dabei Teil einer wettbewerbsrechtlichen Gesamtbetrachtung des Marktverhaltens und der Interessen der Verbraucher. Dies ist ein anderer Fokus als der deutlich umfassendere Schutzauftrag des allgemeinen Persönlichkeitsrechts durch die Datenschutzbehörden. Insoweit umfasst die DSGVO auch spezifische Regeln zur vorwiegend behördlichen Durchsetzung, nicht allerdings im Hinblick auf Marktverhaltensregeln, die überhaupt nicht Gegenstand der DSGVO sind, so dass diese insoweit auch keinesfalls als „abschließend“ betrachtet werden kann.

> Datenschutz kann im Einzelfall auch Zwecken der Marktverhaltensregelung dienen. Wenn dies der Fall ist, ist Datenschutz auch Wettbewerbsschutz und muss als solche durchsetzbar sein. Diese Durchsetzung unterscheidet sich vom behördlichen Datenschutzauftrag und wird im zivilrechtlichen System durch das UWG und damit beauftragten qualifizierten Einrichtungen – einschließlich der Verbraucherverbände - gewährleistet.

IV. AKTIVITÄTEN DES VZBV ZUR DURCHSETZUNG DES DATENSCHUTZRECHTS

Abschließend soll anhand einiger Beispielfälle illustriert werden, dass Marktverhaltensregeln des Datenschutzes innerhalb der wettbewerbsrechtlichen Klagebefugnisse der Verbraucherverbände für die Marktbereinigung in einer digitalen Wirtschaft sehr hohe Relevanz haben. Der vzbv hat sein Klagerecht gegenüber Unternehmen der Digitalwirtschaft stets in einer Weise genutzt, die Verbraucher vor einer unbefugten Nutzung ihrer Daten schützt und gleichzeitig im Interesse der Marktteilnehmer einen ökonomischen „Vorteil durch Rechtsbruch“ verhindert.

1. FACEBOOK (FREUNDEFINDER I)[7]

Facebook ließ Einladungs-E-Mails im Namen der Nutzer an Menschen verschicken, die nicht bei Facebook registriert sind – und die sich jedenfalls teilweise bewusst gegen eine Nutzung von Facebook entschieden haben. Der Bundesgerichtshof (BGH) sah darin unlautere Werbung und einen Verstoß gegen Datenschutzrecht. Kern des Verstoßes war belästigende Werbung gegenüber Dritten. Nutzer wurden damals durch eine Funktion namens „Sind Deine Freunde schon bei Facebook“ dazu gebracht, ihre Adressbücher auf Facebook hochzuladen, damit das Netzwerk abgleichen konnte, welche Kontakte auch schon angemeldet sind. Daraufhin erhielten auch Kontakte, die nicht bei Facebook waren, ungefragt mehrere E-Mails mit einer Einladung, dem Netzwerk beizutreten. Die entsprechenden E-Mails erweckten den Anschein, sie seien vom Nutzer versandt und nicht vom Netzwerk. Über eine derartige Verwendung der E-Mailadressen wurde in Nutzungs- und Datenschutzbedingungen, wenn überhaupt, nur unzureichend

[7] Pressemitteilung des vzbv vom 14.01.2016, https://www.vzbv.de/pressemitteilung/wegweisendes-bgh-urteil-facebooks-einladungs-e-mails-waren-unlautere-werbung (abgerufen am 05.12.2018).

informiert. Facebook erlangte damit unbefugten Zugang zu einer Vielzahl von Kontaktdaten, ein enormer Wettbewerbsvorteil durch Rechtsbruch.

Auf Klage des vzbv hat der BGH diese Praxis für rechtswidrig erklärt, weil er die Einladungsemails für belästigende Werbung und die Information über die Datenverwendung für irreführend hielt. Die Vorinstanz hatte auch noch einen Verstoß gegen Datenschutzrecht über § 4 Nr. 11 a. F. (jetzt § 3a) UWG festgestellt. Der BGH hat diese Rechtsauffassung nicht beanstandet.

2. STAYFRIENDS[8]

Das Schulfreunde-Portal StayFriends hatte im Profil neuangemeldeter Nutzer die Voreinstellung getroffen, dass Profilbilder automatisch auf Suchmaschinen und Partnerwebseiten angezeigt werden. Diese Voreinstellung hielt das OLG Nürnberg auf Klage des vzbv für rechtswidrig. Für eine Veröffentlichung außerhalb des Netzwerks fehlte die erforderliche Einwilligung der Verbraucher. Nach Berufungsrücknahme wurde das Urteil des Landgerichts rechtskräftig.

Der Zweck des Portals liegt aus Sicht des vzbv darin, mit ehemaligen Schulfreunden in Verbindung zu bleiben. Hierzu wählt man bei der Anmeldung konkrete Jahrgänge an konkreten Bildungseinrichtungen aus, gibt im Profil persönliche Informationen preis und lädt regelmäßig ein Profilbild von sich hoch. Es entspricht jedenfalls nicht dem engeren Vertragszweck, dass ein Teil dieser sehr persönlichen Informationen oder das Profilbild auch außerhalb des Netzwerkes auffindbar sind. Letzteres dient eher der Absatzförderung des Unternehmens als dem Verbraucher, der ja genau weiß, in welchen Bildungseinrichtungen er war. Für eine solche Erweiterung bedurfte es auch nach Auffassung der Gerichte einer informierten und freiwilligen Einwilligung, die hier nicht vorlag. Auch hier hat das beklagte Unternehmen durch den Datenschutzverstoß einen unbefugten Wettbewerbsvorteil erlangt.

3. PLANET49[9]:

Die Klage des vzbv gegen „Planet49“ liegt derzeit dem EuGH zur Entscheidung vor. Grundlage ist folgender Sachverhalt: Im Rahmen eines Gewinnspiels, an dem man mittels einer eigens dafür eingerichteten Webseite teilnehmen konnte, sollten Verbraucher unter anderem in das Setzen eines Tracking-Cookies und die damit verbundene Auswertung ihres Nutzerverhaltens „einwilligen“. Die Zustimmung war bereits durch ein Häkchen voreingestellt, mit Informationen flankiert und musste eigens deaktiviert werden. Ob dann eine Teilnahme am Gewinnspiel überhaupt noch möglich war, blieb unklar. Der vzbv hofft mit dem Verfahren die Ausgestaltung der ubiquitären, aus Verbrauchersicht aber lästigen Cookie-Banner zu verbessern und Rechtssicherheit in Bezug auf das bislang ungeklärte sogenannte Koppelungsverbot in der DSGVO zu gewinnen.

[8] Pressemitteilung des vzbv vom 14.05.2018, https://www.vzbv.de/pressemitteilung/stayfriends-verstoesst-gegen-datenschutzrecht (abgerufen am 05.12.2018)

[9] Rechtssache C-673/17, Anhörung am 13.11.2018, Schlussanträge angekündigt für 28.02.2018

Folgende Verfahren wurden seit dem Inkraftttreten der Datenschutzgrundverordnung am 25.05.2018 neu eingeleitet:

4. TIKTOK:

TikTok ist eine bei Teenagern und jungen Erwachsenen sehr beliebte Karaoke-App mit einer aus Sicht des vzbv besonders datenschutzunfreundlichen Voreinstellung: Peinliche Videos aus den Kinderzimmern werden sofort anderen - ggf. mehr als hundert Millionen - Nutzern weltweit angezeigt.

Eine derartig weite und nicht zu beherrschende weltweite Anzeige von sensiblen personenbezogenen Daten Minderjähriger verstößt aus Sicht des vzbv gegen die DSGVO, insbesondere, weil die Veröffentlichung der Daten standardmäßig voreingestellt ist.

Der Anspruch wird auch über § 3a UWG verfolgt, weil aus Sicht von TikTok die Veröffentlichung Teil der vertraglichen Leistung ist, was einen Anspruch aus § 2 Absatz 1 Satz 2 Nr. 11 Unterlassungsklagengesetz (UKlaG) gefährden könnte.

5. TWITTER (FREUNDEFINDER II):

Der vzbv beanstandet, dass Twitter Nutzer durch fortlaufende Aufforderungen dazu bringt, auf dem Endgerät gespeicherter Kontakte hochzuladen. Diese werden dann bis zur Deaktivierung dieser Funktion fortlaufend von Twitter synchronisiert und auf Servern des Unternehmens verarbeitet. Betroffen sind regelmäßig auch solche Kontakte, die gar nicht bei Twitter sind und vielleicht nicht einmal wissen, dass sie in einem fremden Adressbuch gespeichert sind. Twitter verfügt in der Regel nicht über eine Einwilligung dieser dem Unternehmen völlig unbekannten Personen.

Die konkrete Ausgestaltung ist nach Auffassung des vzbv dazu geeignet, Twitternutzer zum Rechtsbruch zu verleiten und könnte zudem gegen die Grundsätze von „privacy by design“der „Datenminimierung“ verstoßen. Das Verfahren hat Symbolwirkung, weil es diese Funktion in vielen Apps gibt.

Der Anspruch wurde wegen der engen Voraussetzungen von § 2 UKlaG auch hier vor allem auf § 3 a UWG gestützt. Wie in den zuvor dargestellten Verfahren wird aus der Fallgestaltung deutlich, dass Twitter erhebliche ökonomische Vorteile aus der vom vzbv angegriffenen Nutzung von Kontaktdaten zieht, somit die Beachtung des Datenschutzrechts auch hier von hoher ökonomischer Relevanz ist.

6. GOOGLE - STANDORTANZEIGE[10]

Wenn man auf einem Computer ein neues Google-Konto einrichtet, sieht man in den Privatsphäreneinstellungen eine standardmäßig deaktivierte Funktion „Standort freigeben“. Dazu gibt es die Information, dass der Standort derzeit „für niemanden bei Google“ angezeigt wird.

Mittels einer nach Einschätzung des vzbv völlig unscheinbaren weiteren Einstellung (Web- und App-Aktivitäten), die anders als die Standortfreigabe standardmäßig aktiviert ist, werden dann aber doch Standortdaten in diversen Einzeldiensten von Google aufgezeichnet. Über diesen Umstand wird nur sehr versteckt in einer umständlich verlinkten Hilfedatei informiert.

---

[10] Gemeinsames Vorgehen von Verbraucherverbänden aus mehreren europäischen Staaten, siehe hierzu die Pressemitteilung des europäischen Verbraucherverbands BEUC vom 27.11.2018, https://www.beuc.eu/press-media/news-events/gdpr-complaints-against-google%E2%80%99s-deceptive-practices-track-user-location (abgerufen am 05.12.2018)

Auch hier kritisiert der vzbv eine fehlende Einwilligung und einen Verstoß gegen die Grundsätze von „privacy by design“ und der Datenminimierung.

Der Anspruch wird wegen der rechtlichen Unwägbarkeiten von § 2 Absatz 2 Satz 1 Nr. 11 UKlaG zugleich auf § 3 a UWG gestützt.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 G

Ass. jur. Kirsten Bock

info@kirsten-bock.de
www.kirsten-bock.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin
Per E-Mail an: innenausschuss@bundestag.de

08. Dezember 2018

Stellungnahme zum Gesetzentwurf der Bundesregierung,
Entwurf 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. DSAnpUG-EU)
vom 01.10.2018

Vorgelegt zur Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 10. Dezember 2018 in Berlin

Sehr geehrte Frau Ausschussvorsitzende Lindholz,
Sehr geehrte Damen und Herren,

ich bedanke mich für die Einladung zur Anhörung und für die Gelegenheit zur Stellungnahme. In Anbetracht des Umfangs des vorgelegten Gesetzentwurfes beschränkt sich meine Stellungnahme auf einige ausgewählte Punkte und Aspekte des Entwurfs zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL). Im Folgenden nehme ich zunächst in einer Gesamtschau zu dem umfassenden Entwurf Stellung (A), betrachte sodann ausgewählte Aspekte und Regelungsbereiche (B) und wende mich abschließend einzelnen Artikeln des vorliegenden Gesetzentwurfs zu (C).

A. Gesamtschau des Entwurfs

Die europäische Datenschutzgrundverordnung ist angetreten mit dem Ziel einer Vereinheitlichung des europäischen Rechtsrahmens im Bereich des Datenschutzes in den Mitgliedstaaten der Union. Die technische Entwicklung und deren Durchdringung des Lebensalltags sowie eine weltumspannende informationstechnische Vernetzung stellen auch das Recht und den grundrechtlich zu gewährenden Schutz natürlicher Personen vor wachsende Herausforderungen. Ziel der DSGVO ist es durch einen „soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen“ mehr „Sicherheit in rechtlicher und praktischer Hinsicht“ und Vertrauen für Bürgerinnen und Bürger, die Wirtschaft und den Staat zu schaffen.[1] Ein solches Ziel ist aber nur zu erreichen, wenn bei den durch die DSGVO vorgesehenen Öffnungen, Präzisierungen oder Einschränkungen ihrer Vorschriften durch das nationale Recht, die Mitgliedstaaten die DSGVO behutsam und sorgfältig in ihr nationales Recht aufnehmen, um die „nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.“[2]

Mit dem vorgelegten Gesetzentwurf wird sich diesem Ziel nicht genähert. Auch das 2.Umsetzungs- und Anpassungsgesetz (2. DSAnpUG-EU) verfehlt das Ziel, das Datenschutzrecht übersichtlicher und für die von ihm betroffenen Personen und Rechtsanwender verständlicher zu machen. Statt auch im bereichsspezifischen Recht auf die

[1] S. DSGVO, EWG 7.
[2] S. DSGVO, EWG 8.

DSGVO oder das BDSG zu verweisen, werden wiederum zahlreiche neue und abweichende Regelungen geschaffen, die in vielen Fällen den Anforderungen, wie sie in der DSGVO z.B.

- für Art. 6 Abs. 1 UAbs. 1 lit. c und e in Art. 6 Abs. 2 und 3 DSGVO,
- in Art. 9 Abs. 2 lit. g und Abs. 4 DSGVO sowie
- in Art. 23 DSGVO

bestimmt sind, nicht genügen. Ein Beispiel bildet etwa Art. 8 des Entwurfs, mit dem das BDBOS-Gesetz geändert wird. So erlauben die Vorgaben aus Art. 6 Abs. 2 und 3 DSGVO nur „spezifischere Bestimmungen“, die im Ergebnis die Verarbeitungsbefugnisse einschränken, aber nicht erweitern. Die Bundesregierung verpasst damit erneut eine Chance, an die Vorreiterrolle, die Deutschland im Datenschutzrecht innehatte, anzuknüpfen. Dabei bestanden schon vor Gültigkeitsbeginn der DSGVO in einigen Landesgesetzen gute Ansätze dafür, europäische Grundsätze aus der Richtlinie 95/46/EG, z.B. zu den technischen und organisatorischen Maßnahmen, die von der DSGVO übernommen wurden, weiter zu präzisieren und für den Rechtsanwender in der Praxis handhabbarer zu machen (s. dazu unter B.). Auch die vielfältigen Einschränkungen der Betroffenenrechte der Art. 12 bis 18 DSGVO dienen nicht dem angestrebten Ziel der Vertrauensbildung. Die Schaffung weiterer Rechtsgrundlagen wäre nur dann zu begrüßen, wenn die Anforderungen an gute Gesetzgebungspraxis erfüllt und alles Wesentliche in die Regelungen aufgenommen würde. Dazu gehört in allen Varianten des Art. 6 Abs. 1 DSGVO eine hinreichend konkrete Festlegung der Zwecke und eine Präzisierung der öffentlichen Interessen, um sowohl dem Anwender als auch den betroffenen Personen die Erforderlichkeit der Verarbeitung deutlich und nachvollziehbar zu machen. Gerade für den Bereich der öffentlichen Stellen erleichtern klare Rechtsgrundlagen die Verwaltungspraxis und können über geeignete Once Only-Verfahren für mehr Bürgerfreundlichkeit der Verwaltung sorgen, ohne dass dabei die Rechte der betroffenen Personen eingeschränkt werden müssen.

Über das 2. DSAnpUG-EU hinaus bestehen weiterhin Möglichkeiten und Regelungsbedarf für die Bereiche des Beschäftigtendatenschutz über Art. 88 DSGVO sowie für die Ausübung der Meinungsfreiheit über Art. 85 DSGVO (dazu s. u. C.).

B. Stellungnahme zu einzelnen Grundsatzfragen des Entwurfs

Die **Zweckbindung** folgt unmittelbar aus dem Grundrecht auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechte-Charta). Sie ist ein zentraler Grundsatz für die Rechtmäßigkeit der Datenverarbeitung. Aus der Logik des Datenschutzrechts wird unmittelbar das ihm zugrunde liegenden Verbots mit Regelungsvorbehalt abgeleitet, demzufolge für einen bestimmten Zweck erhobene Daten nicht nach Belieben, sondern nur unter sehr engen, den Voraussetzungen des Art. 6 Abs. 4 DSGVO unterliegenden Bedingungen, weiterverarbeitet werden dürfen. Denn jede Verarbeitung zu einem neuen Zweck berührt den Schutzbereich und stellt damit einen (weiteren) Grundrechtseingriff dar, den es für sich zu rechtfertigen gilt. Dazu bedarf es jeweils einer eindeutigen Rechtsgrundlage. Der Kanon möglicher Rechtsgrundlagen wird in Art. 6 Abs. 1 DSGVO abschließend aufgezeigt. Die in Art. 6 Abs. 2 bis 4 DSGVO bestimmten Anforderungen entsprechen dem grundgesetzlichen Bestimmtheitsgebot. Eine pauschale Verweisung auf die Aufgaben eines Verantwortlichen genügt diesen Anforderungen nicht. Auch allgemein formulierte Zwecke, wie „öffentliches Interesse“ sind unzureichend. Zwar sei dem Bundesgesetzgeber nicht empfohlen, das Datenschutzrecht weiter durch sich wiederholende Regelungen in zahlreichen Rechtsgebieten zu zerfasern, sondern auf die DSGVO und das BDSG zu verweisen. Jedoch besteht im Bereich möglicher Zweckänderungen ein konkreter Reglungsbedarf, um den Anforderungen an die Bestimmtheit zu genügen, den der Gesetzentwurf nicht erfüllt.

An vielen Stellen erfolgt eine sprachliche Anpassung an den **Verarbeitungsbegriff** aus Art. 4 Abs. 2 DSGVO, wobei überwiegend die Begriffe „erheben, verarbeiten und nutzen“ durch den Begriff „verarbeiten“ ersetzt werden. Dabei ist zu bedenken, dass der bislang im BDSG a.F. verwendete Begriff der Verarbeitung nicht mit dem Verarbeitungsbegriff der DSGVO identisch ist. Zwar enthält Art. 4 Abs. 2 DSGVO keine echte Definition der Verarbeitung, sondern beschreibt beispielhaft Vorgänge oder Vorgangsreihen, die im Zusammenhang mit personenbezogenen Daten ausgeführt werden. Die Art der Beispiele macht aber deutlich, dass der gesamte Lebenszyklus einer personenbezogenen Information erfasst werden soll: vom Erheben über das Verändern bis zum Löschen oder Anonymisieren (Entketten von Informationsbezügen). Abweichungen ergeben sich damit in den Bereichen des Rechts, in denen der Verarbeitungsbegriff des § 3 Abs. 4 BDSG a.F. erhalten bleibt bzw. (noch) nicht geändert wurde. Dies hat besondere Auswirkungen auf Erlaubnisnormen, bei denen

nunmehr auch die Erhebung und Nutzung erfasst wird und damit der Erlaubnistatbestand erweitert wird. Regelungen mit verarbeitungsbeschränkendem Charakter trifft das gegenteilige Schicksal. Soweit nur bestimmte Formen der Verarbeitung geregelt werden sollen, ist dies kenntlich zu machen und es kann nicht auf den allgemeinen Verarbeitungsbegriff zurückgegriffen werden, wie dies beispielsweise in Art. 2 Nr. 1 des Entwurfs (Änderung des Gesetzes zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet) erfolgt. Dort werden die Wörter „verarbeiten und nutzen“ durch die Wörter „speichern, verändern, nutzen, übermitteln oder in der Verarbeitung einschränken“ gleichsam „rückübersetzt“. Erfolgt eine solche Anpassung nicht, verändert sich der erfasste Gegenstandsbereich einer Regelung.

In vielen Artikeln des Entwurfs zum 2. DSAnpUG-EU wird auf „**technische und organisatorische Maßnahmen**“ nach den „Artikeln 24, 25 und 32“ der DSGVO verwiesen, z.B. in Art. 49 Nr. 9, 18, Art. 96 Nr. 2, Art. 105 Nr. 3, Art. 107 Nr. 1, Art. 123 Nr. 19, Art 153 Nr. 6 c. Hervorzuheben ist hierbei, dass eine Zusammenführung der Art. 24, 25 und 32 DSGVO insoweit sinnvoll erscheint, als die Regelungen sich komplementär ergänzen und stets nebeneinander Anwendung finden. Während Art. 24 DSGVO primär auf organisatorische Maßnahmen Bezug nimmt (sog. Compliance Management) und Art. 32 DSGVO die eigentliche Verarbeitung regelt (Sicherheit der Verarbeitung), zielt Art. 25 Abs. 1 DSGVO auch auf das Stadium vor Anwendbarkeit der DSGVO (Vorbereitung der Verarbeitung) und bezieht dieses Stadium *ex tunc* in den Anwendungsbereich der DSGVO (Verarbeitung personenbezogener Daten) ein und konkretisiert dies für die zu treffenden Voreinstellungen in Art. 25 Abs. 2 DSGVO. Gleichwohl mangelt es in Art. 32 DSGVO an systematischer Klarheit. Hier hätte der Entwurf aufbauend auf den ehemals bestehenden Regelungen zu den Schutzzielen des Datenschutzes in den Datenschutzgesetzen der Länder[3] den Rechtsanwendern vor allem für die „Übersetzung“ der rechtlichen Regelungen der DSGVO in informationstechnische Anwendungen präzisierende Hilfestellungen leisten können.

Die **Verarbeitung besonderer Kategorien** personenbezogener Daten, wie etwa von Gesundheitsdaten (Allergiker*in, Brillenträger*in), stellt nicht in jedem Fall für die

[3] S. § 5 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000, GVOBl. Schl.-H. S. 169.

betroffenen Personen einen besonders schweren Grundrechtseingriff dar. Jedoch können Verarbeitungen solcher Kategorien, wie sie z.B. in Art. 12 Nr. 8 des Entwurfs zur Änderung des Bundesdatenschutzgesetzes, in Art. 91 Nr. 4 zur Änderung des Kreditwesengesetzes oder in Art. 88 Nr. 5 lit c zur Änderung des Strahlenschutzgesetzes vorgesehen sind, typischerweise zu besonders erheblichen Folgen für die betroffenen Personen führen, die bei ihrer erstmaligen Verarbeitung nicht ohne Weiteres absehbar sind. So kann beispielsweise die Erhebung eines biometrischen Fingerabdrucks im Rahmen einer späteren Forschungsarbeit zu nachteiligen Feststellungen führen, die zum Zeitpunkt der erstmaligen Verarbeitung noch nicht denkbar waren. Die Verarbeitung der Mitgliedschaft in einer Partei oder einer Religionsgemeinschaft, kann z.B. nach einem Regierungswechsel zu Verfolgung oder zu Repressalien führen. Wesensmerkmal dieser Kategorien ist zudem, dass ein Wechsel oder eine Veränderung der Merkmale für die betroffene Person nur schwer bzw. unmöglich sind. Wird beispielsweise der Fingerabdruck gefälscht und gerät dadurch in polizeiliche Dateien, so kann die betroffene Person sich dessen nicht in zumutbarer Weise entledigen oder diesen ändern. Die Verarbeitung besonderer Kategorien der Verarbeitung soll daher nur unter besonderen Vorkehrungen erfolgen. Art. 9 Abs. 2 lit g DSGVO verlangt für gesetzliche Grundlagen insoweit, dass

- für die Regelung ein erhebliches öffentliches Interesse besteht,
- die Regelung der Verarbeitung in einem angemessenen Verhältnis zu dem verfolgten Ziel steht,
- der Wesensgehalt des Rechts auf Datenschutz gewahrt wird und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen

vorgesehen werden. Dazu ist zunächst das erhebliche öffentliche Interesse zu konkretisieren bzw. zu begründen. Ein allgemeiner Verweis auf ein erhebliches öffentliches Interesse wie in Art. 12 Nr. 7 a des Entwurfs zur Änderung des § 22 Abs. 1 Nr. 1 lit. d BDSG, das dann bei der Anwendung zu bestimmen ist, reicht dafür nicht aus. I.d.R. wird ebenso ein bloßer Verweis auf eine gesetzliche Aufgabenerfüllung zur Begründung, wie in Art. 1 Nr. 1 des Entwurfs zur Änderung von § 31 S. 2 Staatsangehörigkeitsgesetz, nicht ausreichen. Nur durch die Konkretisierung kann dann auch beurteilt werden, ob die Regelung in einem angemessenen Verhältnis zum angestrebten Ziel steht. Das erhebliche öffentliche Interesse an der

Verarbeitung darf nicht zu Verarbeitungserlaubnissen führen, durch die der Wesensgehalt des Grundrechts auf Datenschutz berührt wird.[4] Dies ist immer dann der Fall, wenn eine Regelung eine unbegrenzte Erhebung oder Speicherung oder andere Verarbeitung zulässt oder die betroffenen Personen in einem Lebensbereich einer uneingeschränkten Beobachtung ausgeliefert[5] wird, wie es beispielsweise der Entwurf für das BSI-Gesetz vorsieht (s.u.). Die zu treffenden spezifischen Maßnahmen sind entweder direkt gesetzlich festzulegen, s. etwa in Ansätzen Art. 16 Nr. 9 c des Entwurfs, oder mit Verweis auf die Schutzziele des Datenschutzes[6] zur

- Vertraulichkeit, Integrität, Verfügbarkeit,
- Nichtverkettung (zur Umsetzung der Zweckbindung)
- Intervenierbarkeit (Kontrollfähigkeit und Rechte der Betroffenen) sowie
- Transparenz der Verarbeitung

und den umzusetzenden Schutzbedarf (z.B. normal, hoch oder sehr hoch) zur Gewährleistung der Rechte natürlicher Personen zu konkretisieren. Auch solche Festlegungen lässt der Entwurf vermissen.

Erfolgt ein **Ausschluss des Auskunftsrechts** nach Art. 15 DSGVO, müssen gem. Art. 23 DSGVO besondere Gründe dargelegt werden. Mit dem Ausschluss wird das Recht auf Kenntnis des Verarbeiters und den Umständen der Verarbeitung einschränkt. Erfolgt dies bereits „wenn die Auskunftserteilung die ordnungsgemäße Aufgabenerfüllung gefährden würde“, wie z.B. in Art. 13 zur Änderung des BSI-Gesetzes, so bleibt dies hinter den Art. 23 Abs. 1 DSGVO benannten Gründen zurück. Dieser Maßstab ist offensichtlich so niedrig, und im Hinblick auf die oft weitreichenden oder unklar beschriebenen gesetzlichen Aufgaben, dass es nicht nur für den Betroffenen, sondern auch für die Verantwortlichen und nicht zuletzt die Datenschutzaufsichtsbehörden, schwer ist, die Voraussetzungen zu prüfen.

[4] EuGH Urt. v. 06.10.2015 (Schrems), NJW 2015, 3151, 3157.
[5] S. dazu Bock/Engeler, DVBL 2016, 593.
[6] S. Bock/Meissner, DuD 2012, 425ff; Robrahn/Bock, DuD 2018, 7ff.

C. Stellungnahme zu einzelnen Änderungen

Zu Art. 1: Änderung des Staatsangehörigkeitsgesetzes

Nach Art. 1 Nr. 3 b des Entwurfs zu § 33 Abs. 4 S. 3 zur Änderung des Staatsangehörigkeitsgesetzes soll eine Übermittlung auch dann zulässig sein, „wenn das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Verarbeitung erheblich überwiegt." Diese Regelung widerspricht dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. d DSGVO und erweitert die Übermittlungsbefugnisse. Art. 89 Abs. 1 DSGVO verlangt für wissenschaftliche und historische Forschungszwecke geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen durch technische und organisatorische Maßnahmen. Auch bei wissenschaftlichem Interesse sollte daher im Regelfall eine Übermittlung durch Maßnahmen der Pseudonymisierung abgesichert werden, wenn eine Anonymisierung nicht möglich ist. Insoweit könnte der Entwurf für § 33 Abs. 4 S. 3 auf § 22 Abs. 2 BDSG verweisen.

Zu Art. 5: Änderung des Rechtsextremismus-Datei-Gesetzes

Die Änderung in Nr. 7 zu § 13 enthält eine Änderung der Überschrift. Das Wort „Errichtungsanordnung" wird durch die Wörter „Festlegungen für die gemeinsame Datei" ersetzt, mit der auf das Vorliegen einer gemeinsamen Verantwortlichkeit bei dem Betrieb einer gemeinsamen Datei hingewiesen wird, ohne aber materiell rechtlich auf die für das deutsche Datenschutzrecht neue gemeinsame Verantwortlichkeit, Art. 3 Nr. 8 RL (EU) 2016/680, einzugehen. Zwar regelt § 9 RED-G die datenschutzrechtliche Verantwortlichkeit für die Erhebung und „Pflege", für die Errichtung und den Betrieb einer gemeinsamen Datei sind diese Regelungen jedoch nicht hinreichend. Ein gemeinsamer Betrieb erfordert besondere Garantien, die sicherstellen, dass technische und organisatorische Maßnahmen bestehen, die in § 13 RED-G Erwähnung finden. Ein Verweis auf § 10 RED-G allein, wird hierfür nicht genügen, es sei denn, die spezifischen Anforderungen werden in einem neuen § 10 Abs. 4 aufgenommen. Alternativ könnte ein Verweis auf die Anforderungen an die Sicherheit der Datenverarbeitung nach § 64 BDSG und das Verzeichnis von Verarbeitungstätigkeiten nach § 70 BDSG erfolgen mit einer Ergänzung der Besonderheiten einer gemeinsamen Verantwortlichkeit. Für das Verzeichnis der Verarbeitungstätigkeiten sollten über den § 70 Abs. 1 BDSG hinaus die zwingenden Angaben zur gemeinsamen

Verantwortlichkeit einschließlich eines Rollen- und Berechtigungskonzeptes sowie deren Detaillierungsgrad festgelegt werden.

Zu Art. 8: Änderung des BDBOS-Gesetzes

Der Entwurf zu § 19 Abs. 2 erlaubt Verkehrsdaten bei Vorliegen tatsächlicher Anhaltspunkte für eine rechtswidrige Inanspruchnahme von Verkehrsdaten zu verarbeiten, „soweit dies erforderlich ist, um die rechtswidrige Inanspruchnahme des Digitalfunk BOS festzustellen und zu unterbinden“. Im Hinblick auf die Nichtöffentlichkeit des Dienstes erscheint diese weitreichende Verarbeitungserlaubnis nicht in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck zu stehen. Zumindest erscheint eine Einschränkung geboten, die eine rechtwidrige Inanspruchnahme auf für den Betrieb und die Sicherstellung des Betriebs relevante Inanspruchnahmen beschränkt.

Der Entwurf zu § 19 Abs. 3 eröffnet eine Zweckänderung und damit quasi eine unbegrenzte Speicherung von Verkehrsdaten zur Weiterentwicklung des Digitalfunks BOS. Die Regelung ist selbst bei Zugrundelegung eines hohen Schutzbedarfs für ein kritische Infrastruktur unverhältnismäßig und genügt zudem nicht den Bestimmtheitsanforderungen.

Eine Speicherung über 75 Tage, wie sie der Entwurf zu § 19 Abs. 4 vorsieht, geht über die allgemein schon weitreichende Vorratsdatenspeicherung von 70 Tagen hinaus, an der ihrerseits bereits erhebliche Zweifel im Hinblick auf die Verhältnismäßigkeit bestehen.[7] Zwar ist zu begrüßen, dass die Einholung einer Einwilligung verworfen wird, die zu Recht weder als praktikabel noch im Hinblick auf die Konkretisierung der Zwecke als möglich betrachtet werden muss. Eine Speicherung von Verkehrsdaten sollte entsprechend dem Grundsatz der Datenminimierung nur soweit erfolgen, wie dies für den Betrieb einschließlich der Störungsbeseitigung erforderlich ist.

Der Entwurf wie auch die Gesetzesbegründung lassen des Weiteren eine Auseinandersetzung mit den Interessen der betroffenen Personen vermissen.

Zu Art. 11: Änderung des Bundesbeamtengesetzes

Die Auslagerung von Personalakten im öffentlichen Bereich stellt für den Staat und seine Beamten und Beamtinnen einen besonders sensiblen Bereich dar. Bei der Zulässigkeit der

[7] BVerfG 1 BvR 141/16.

Verarbeitung von Personalaktendaten im Auftrag in § 111a (Art. 11 Nr. 8 des Entwurfs) sollte daher ein Abs. 3 angefügt werden, der beim Verarbeiter besonders zu garantierende technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Intervenierbarkeit zur Umsetzung der Rechte der Betroffenen und des Verantwortlichen, der Nichtverkettung (Zweckbindung, Mandantenfähigkeit) und Integrität vorsieht. Bei der Auswahl eines Verarbeiters ist dabei, wie stets im öffentlichen Bereich, sicherzustellen, dass dieser keinen Zugriffsrechten durch Geheimdienste oder anderen, in Drittstaaten belegenen, Stellen ausgesetzt ist.[8]

Zu Art. 12 Änderung des Bundesdatenschutzgesetzes

Die vorgesehenen Änderungen des Bundesdatenschutzgesetzes sind im Hinblick auf den Korrekturbedarf, der sich durch das 1. DSAnpUG-EU bspw. durch die Einschränkung der Rechte der betroffenen Personen bei der Videoüberwachung im öffentlichen Raum (§ 4 BDSG), den Rechten der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten (§ 29 Abs. 1 BDSG) sowie beim Recht auf Löschung (§ 35 Abs. 1 BDSG) ergibt, zurückhaltend geblieben. Auch die Einschnitte bei den Rechten der Betroffenen (§§ 32 ff. BDSG) bleiben bestehen. Hier sollte die Gelegenheit genutzt werden, auf die Ausnahmen zu verzichten, aber zumindest die Regelungen zu konkretisieren und damit in Übereinstimmung mit den Anforderungen aus Art. 23 Abs. 2 DSGVO zu bringen.

Zu Nr. 4: § 9 BDSG

Durch den Verweis auf § 115 Abs. 4 Telekommunikationsgesetz (TKG) bleibt es nach wie vor unklar, ob dieser Bestand haben soll. Zwar lässt auch die Gesetzesbegründung erkennen, dass „Bereiche“ des TKG, durch die DSGVO unmittelbar geregelt werden und diese aus dem TKG gestrichen würden, inwieweit davon aber der Regelungsgehalt des § 115 Abs. 4 TKG erfasst wird, bleibt durch den Verweis in dem Entwurf für § 9 Abs. 1 S. 1 BDSG unklar. Es sollte klargestellt werden, dass die Zuständigkeit bei der oder dem Bundesbeauftragten liegt, der Verweis auf § 114 Abs. 4 TKG erscheint zumindest zum gegenwärtigen Zeitpunkt überflüssig.

[8] Vgl. EuGH Urt. v. 06.10.2015 (Schrems), NJW 2015, 3151, 3157.

Zu Nr. 7. a) cc): § 22 Abs. 1 lit. d

Die Regelung genügt den Anforderungen des Art. 9 Abs. 2 lit. g DGSVO nicht. Mit dem Wechsel aus der Nr. 2 in die Nr. 1 wird die Verarbeitung aufgrund eines zwingenden erheblichen öffentlichen Interesses nunmehr auch für nichtöffentliche Stellen eröffnet. Mit der Regelung wird über den Verweis in § 24 Abs. 2 BDSG für nichtöffentliche Stellen eine Übermittlungsbefugnis von besonderen Kategorien personenbezogener Daten zu anderen Zwecken geschaffen. Dabei bleibt unklar, ob § 22 Abs. 2 BDSG Anwendung findet, da § 24 Abs. 2 lediglich auf den Ausnahmetatbestand verweist. Eine Anwendung ist auch schon deswegen notwendig, um sicherzustellen, dass die erforderlichen, angemessenen und spezifischen Maßnahmen für die Verarbeitung im Sinne des Art. 9 Abs. 2 lit g DSGVO, bei den nichtöffentlichen Stellen getroffen werden.

Zu Nr. 8: § 86 BDSG

In Satz 1 sollte klargestellt werden, dass sich der Anwendungsbereich des § 86 allein auf „staatliche“ Auszeichnungen und Ehrungen beschränkt.

Die Formulierung „als auch andere öffentliche und nicht-öffentliche Stellen“ in Abs. 1 des Entwurfs ist zu unkonkret, insbesondere da sich die Regelung auch auf besondere Kategorien personenbezogener Daten bezieht. Hier wären zumindest näher bestimmte Kategorien von Empfängern, z.B. Dienstherr*in oder Arbeitgeber*in, zu nennen.

Der Ausschluss der Betroffenenrechte, Art. 13 bis 16 DSGVO, in Abs. 2 geht über das gebotene Maß hinaus. Es kann noch nachvollzogen werden, dass eine aktive Informationspflicht bei Ehrungen entbehrlich sein kann, nicht jedoch, dass ein Recht auf Auskunft nach Art. 15 DSGVO insbesondere gegenüber „anderen Stellen“ ausgeschlossen sein soll.

Zu einer aufzunehmenden Regelung zum Schutz der allgemeinen Meinungs- und Informationsfreiheit sowie zum Schutz von künstlerischen und literarischen Zwecken

Es bedarf nach wie vor einer Regelung zum Schutz der allgemeinen Meinungs- und Informationsfreiheit sowie zum Schutz von künstlerischen und literarischen Zwecken. Die z.T.[9] vertretene Auffassung, dass Art. 85 Abs. 1 DSGVO bereits durch Art. 5 GG ausgefüllt

[9] Bmi.bund.de, FAQs zur Datenschutz-Grundverordnung.

werde und daher keine weitere Anpassung erfolgen müsse, übersieht, dass neben dem professionellen Journalismus, für den bereits durch den Bundes- und die Landesgesetzgeber[10] spezielle Vorschriften erlassen wurden, weiterer Regelungsbedarf für Datenverarbeitungen zu künstlerischen (z.B. Fotografen*, Hobbyfotografen*, Künstler*) und für die öffentliche Meinungsäußerung Privater (z.B. Blogger*, Podcaster*, Politiker*, Pressesprecher*, Twitter-Nutzer*, YouTuber*) besteht, die nicht bereits durch eine Anwendung des Art. 5 GG oder das KUG gewährleistet wird. Ein Anpassungsbedarf wird auch schon daraus deutlich, dass das 2. DSAnpUG-EU in Art. 41 für den Bereich der Deutschen Welle eine Ausnahme vorsieht. Ein Anpassungsbedarf besteht, weil auch die o.g. Gruppen sich regelmäßig öffentlich äußern und dadurch einen wichtigen Beitrag zum öffentlichen Diskurs leisten. Ein Anpassungsbedarf kann auch nicht deswegen verneint werden, weil es sich bei den o.g. Verantwortlichen nicht um professionelle Journalisten handelt. Die DSGVO führt dazu in EG 153 aus, dass Begriffe, die im Zusammenhang mit der Meinungsäußerungsfreiheit stehen, wie beispielweise der Begriff „Journalismus“ weit auszulegen seien.

Die Aufforderung, zur Schaffung von Ausnahmen oder Abweichungen, um das Recht auf freie Meinungsäußerung mit dem Recht auf Datenschutz in Einklang zu bringen, bezieht sich daher nicht nur auf den professionellen Journalismus, sondern auch auf die o.g. Aktivitäten. Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[11] müssen sich Ausnahmen zur DSGVO auf konkrete und spezifische Regelungen stützen. Rechtliche Unsicherheiten im Bereich der Meinungsäußerungsfreiheit stellen schon an sich eine erhebliche Beeinträchtigung[12] des Rechts auf freie Meinungsäußerung und der Kommunikationsfreiheit dar. Anzustreben wäre in diesem Bereich eine Rechtsgrundlage, die neben den bestehenden Rechtsgrundlagen aus Art. 6 Abs. 1 lit e und f DSGVO, das Verhältnis bzw. die Bedingungen der Verarbeitung bei Datenverarbeitungen unter Art. 9 und 11 DSGVO sowie im Hinblick auf die Informationspflichten nach Art. 13 und 14 DSGVO sowie des Betroffenenrechts nach Art. 15 DSGVO für alle in Art. 85 DSGVO genannten Zwecke regelt. Dabei sollte ein besonderes Gewicht auf die grundlegende Bedeutung der Möglichkeiten zur

[10] Übersicht bei emr-sb.de, Synopse zu den geplanten Änderungen landesrechtlicher Regelungen zur Umsetzung des 21. RÄndStV und der DS-GVO.
[11] Entschließung vom 09.11.2017.
[12] S. dazu z.B. telemedicus.info/article/3307-Braucht-die-DSGVO-ein-Medienprivileg-auch-fuer-Blogger,-Fotografen-und-Pressesprecher.html.

freien Meinungsäußerung und zur Teilnahme am öffentlichen Diskurs gelegt werden, die mit dem Recht der natürlichen Personen bei der Verarbeitung personenbezogener Daten in Ausgleich zu bringen sind. Es kann dabei auf die bisherige Rechtsprechung des BVerfG und des EUGH aufgebaut werden, wobei jedoch die Besonderheiten der Verarbeitung durch informationstechnische Systeme auch vor dem Hintergrund deren technischer Weiterentwicklung sowie den Möglichkeiten der Manipulation und Dekontextualisierung mit besonderer Aufmerksamkeit bedacht werden sollten.

Zu Art. 13 Änderung des BSI-Gesetzes

Das BSI-Gesetz sieht erhebliche Verarbeitungsbefugnisse einhergehend mit umfangreichen Einschränkungen der Rechte der betroffenen Personen vor, wobei die Anforderungen an Einschränkungen aus Art. 23 Abs. 2 DSGVO nur unzureichend erfüllt werden. Selbst die Gesetzesbegründung führt aus, dass es sich bei der Einfügung des § 3a Abs. 1 und 2 um eine datenschutzrechtliche Ermächtigungsgrundlage handele, die „nur für Aufgaben und Tätigkeiten [gelte], die nicht unmittelbar durch die speziellen datenschutzrechtlichen Ermächtigungen […] erfasst“ sei. Damit handelt es sich um einen „Auffangtatbestand“.

Zu Nr. 3: § 3a Abs. 2

Die Vorschrift bedeutet eine fast konturenlose Ausweitung der Verarbeitungsbefugnisse. Insbesondere die Zwecke der „Sammlung“ in Abs. 2 Nr. 1 lit. a und „Unterstützung“ in Abs. 2 Nr. 1 lit b stellen keine hinreichend konkreten Zwecke im Sinne der Art. 5 Abs. 1 lit b und 23 Abs. 2 lit a DSGVO dar.

Zu Nr. 6 und 7: §§ 6-7

Für das BSI-Gesetz wird mit den Nr. 6 und 7 eine umfangreiche Beschränkung der Rechte der betroffenen Personen eingeleitet. Zwar ist die Verarbeitung personenbezogener Daten zum Betrieb und Schutz informationstechnischer Systeme nachvollziehbar, damit muss aber nicht ein so weitreichender Ausschluss der Betroffenenrechte verbunden sein. Die Regelungen belassen es im Belieben des BSI, wann und mit welchem Inhalt eine Auskunft erteilt wird. Es ist nachvollziehbar, dass die umfangreichen Rechte der Betroffenen im Zusammenhang mit der Sicherstellung der technischen Infrastruktur für das BSI eine zusätzliche Belastung und unter bestimmten Bedingungen auch eine Gefahr für die Erfüllung dessen Aufgaben darstellen. Gerade aber vor diesem Hintergrund, wäre eine konkrete Positivregelung

dahingehend, in welchen Fällen und unter welchen Bedingungen eine Auskunft erteilt wird, für alle Beteiligten hilfreicher und würde den Aufwand und Umfang von den - nunmehr erforderlichen - Abwägungsentscheidungen abmildern.

Zumindest die Regelung des § 6f S. 2 ist mit den Anforderungen des Art. 23 insbesondere Abs. 2 lit. f) DSGVO nicht vereinbar. Es bedarf zumindest einer Maximalfrist für die Speicherdauer. Keinesfalls kann es dem BSI anheimgestellt werden, ob zwingende Gründe für eine Verarbeitung bestehen. Eine solche Prüfung sollte unverzüglich erfolgen müssen.

Zu Art. 15 Änderung des E-Government-Gesetzes

Art. 15 zur Änderung des E-Government-Gesetzes sieht in erster Linie sprachliche Anpassungen an die DSGVO vor. Ziel des Gesetzes zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Es soll eine gesetzliche Grundlage für die elektronische Verwaltungstätigkeit des Bundes, der Länder und Kommunen bei der Erfüllung von Bundesaufgaben schaffen. Die Anpassung an den Wortlaut der DSGVO zu § 5 in Art. 15 Nr. 1 lit. a des Entwurfs soll verdeutlichen, dass für Verarbeitungen im sog. Once Only-Verfahren[13] die Regelungen der DSGVO zur Einwilligung, Art. 4 Nr. 1 und Art. 7 DGVO, direkt gelten. Zu beachten ist in diesem Zusammenhang, dass die Einwilligung im Bereich der öffentlichen Verwaltung nur in bestimmten Zusammenhängen eingeholt werden darf. Im Verhältnis Staat – Bürger*in besteht ein Ungleichgewicht, das einer freien Entscheidung zunächst entgegensteht. Es ist daher jeweils darzulegen, dass dieses Ungleichgewicht in der konkreten Anwendungssituation ausgeglichen ist oder ausgeglichen wird. Dies ist z.B. dann der Fall, wenn die Nichterteilung der Einwilligung keine nachteiligen Folgen für die betroffene Person hat oder der Zugang zu der Verwaltungshandlung auf herkömmlichen, analogen Weg nicht künstlich, z.B. durch ein höheres Entgelt, erschwert wird.

In Art. 15 Nr. 2 d oder e des Entwurfs zu § 11 Abs. 3 oder Abs. 4 sollte klargestellt werden, dass im Rahmen der gemeinsamen Vereinbarung nach Maßgabe des Art. 26 DSGVO sichergestellt wird, dass ein höherer Schutzbedarf bei einem Verantwortlichen auf das gemeinsame Verfahren übertragen wird und, soweit erforderlich, auch bei dem

[13] Vgl. Bock „Datenschutz in der Verwaltung von Bund, Ländern und Kommunen“ in Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, i.E., § 20 Rn 27ff.

Verantwortlichen oder Verarbeiter Anwendung findet, für die oder den dieser Schutzbedarf nicht ermittelt wurde.

Zu Art. 16 Änderung des Bundesmeldegesetzes (BMeldG)

Das Melderecht wird gerne als informationelles Rückgrat der modernen Verwaltung bezeichnet, weil es die Rechtsgrundlagen und Regelungen für einen Grundbestand an Informationen über die Bürgerinnen und Bürger in staatlicher Hand darstellt.[14] Einerseits muss der Staat über verlässliche Informationen zur Planung und Daseinsvorsorge verfügen. Andererseits verlangt die verpflichtende Hergabe der personenbezogenen Daten an den Staat einen vertrauensvollen Umgang und Schutz. Bestand in der Vergangenheit ein gewisser faktischer Schutz in der dezentralen, mehr oder weniger analogen Verwaltung der Bürger*innendaten bei den örtlichen Meldeämtern, so sind mit der Digitalisierung der Meldedatenhaltung und des Meldeverfahrens die Zugriffsmöglichkeiten durch den Staat gestiegen. Damit einher gehen Möglichkeiten einer effizienteren Gestaltung der Verwaltungsverfahren über die Zuständigkeiten einzelner Behörden hinweg. Positiv betrachtet können damit eine Vereinfachung der Verfahren und Entbürokratisierung erfolgen. Die Kehrseite, ist die Zunahme der Zugriffs- und Verkettungsmöglichkeiten über zahlreiche Schnittstellen und eine virtuelle Zentralisierung bei wenigen Datenzentralen.[15] Dies führt zu einer virtuellen und tatsächlichen Verwundbarkeit, nicht nur individueller Bürger*innen, sondern auch der Verwaltung und damit des Staates. Die Anpassung des Bundesmeldegesetzes sollte vor diesem Hintergrund nicht nur eine formale Anpassung an die Begrifflichkeiten der DSGVO vornehmen, sondern die Erfordernisse in einer sich technisch und politisch wandelnden Welt berücksichtigen und die Voraussetzungen für ein entsprechend robustes Meldewesen zum Schutz der Rechte natürlicher Personen bei der Verarbeitung von Meldedaten schaffen. Diese Voraussetzungen sollten über technische und organisatorische Anforderungen ergänzend z.B. in Art. 16 Nr. 3 erfasst werden.[16]

[14] S. Bock, DuD 2005, 360ff.

[15] So verarbeitet beispielsweise der Informations- und Kommunikationsdienstleister Dataport mittlerweile Meldebestände aus sechs Bundesländern.

[16] Vgl. oben unter B. zu den technischen und organisatorischen Maßnahmen.

Zu Art. 16 Nr. 2 b

Es sollte in Ergänzung zu § 2 Abs. 4 S. 2 bestimmt werden, ob alle oder nur bestimmte Angaben nicht meldepflichtiger Personen erfasst werden dürfen und aus welchem Grund und zu welchen Zwecken diese verarbeitet werden dürfen. Liegen diese Informationen der betroffenen Person nicht vor, kann keine gem. Art. 7 DSGVO wirksame Einwilligung erteilt werden. Zudem gilt das oben zur Freiwilligkeit der Einwilligung im öffentlichen Bereich Ausgeführte.

Zu Art. 16 Nr. 10 a

Der Entwurf sieht für § 11 Abs. 1 Nr. 1 vor, dass das Recht auf eine Auskunft nach Art. 15 Abs. 1 lit. b und lit. c DSGVO u.a. nicht für nicht automatisierte einfache Melderegisterauskunft bestehen soll. In der Begründung des Entwurfs wird dazu ausgeführt, es handele sich bei einfachen Melderegisterauskünften um Massenauskunftsverfahren. Manuelle, d.h. nicht automatisierte Melderegisterauskünfte würden wegen des Protokollierungsaufwandes nicht erfasst, sondern „nur aufbewahrt“. Vor dem Hintergrund, dass einer einfachen Melderegisterauskunft nicht widersprochen werden kann, kann der Begründung für den Ausschluss der Auskunft aus aktueller Sicht nicht gefolgt werden. Die manuelle Melderegisterauskunft stellt schon lange nicht mehr den Regelfall der einfachen Melderegisterauskunft dar. Manuelle Auskünfte oder manuelle Nachbearbeitungen werden, schon aus Kostengründen, nur dann eingeholt, wenn eine elektronische Auskunft nicht erteilt wurde, weil z.B. ein unvollständiger oder fehlerhafter Datensatz vorlag, § 49 Abs. 4 BMG. Gerade in diesen Fällen, besteht ein begründetes Interesse der betroffenen Person auf ihr Auskunftsrecht. Gerade das Recht auf Auskunft ist für das Grundrecht auf Datenschutz wesentlich, weil nur darüber eine Transparenz für die betroffene Person hergestellt werden kann, die ihr eine Kontrolle über die über sie verarbeiteten personenbezogenen Daten ermöglicht. Der entstehende Aufwand für eine Protokollierung beim Verantwortlichen überwiegt gegenüber diesem Interesse nicht.

Zu Art. 16 Nr. 26

Der Entwurf für § 44 Abs. 3 sieht vor, dass eine einfache Melderegisterauskunft nach wie vor, unter der Bedingung erteilt wird, dass die Identität der betroffene Person aufgrund der vom Anfragende mitgeteilten Angaben nach Abs. 3 Nr. 1 lit. a bis lit. f von der Meldebehörde

eindeutig festgestellt werden kann. Der in S. 1 HS. 1 vorgesehen Fall der Einwilligung sollte nicht darüber hinwegtäuschen, dass diese nicht den Regelfall für die Auskunftserteilung darstellen wird. Bei der Vorschrift dürfte es sich in erster Linie um Makulatur handeln. Sie lädt geradezu dazu ein, sich mit Hilfe einer geschickten optischen oder textlichen Vertragsgestaltung, Verbraucher in eine „Einwilligungsfalle“ zu locken. Zwar sind die Anforderungen an die Einwilligung mit der DSGVO gestiegen. Nichtsdestotrotz ist es aber aufgrund übermäßiger Nutzung von Einwilligungen als Rechtsgrundlage nach Art. 6 Abs. 1 lit. a DSGVO bei Verbrauchern und Verbraucherinnen zu einer sog. Einwilligungsermüdung gekommen. Datenschutzrechtliche Einwilligungen, zumal wenn sie als Pop-up erscheinen, werden häufig angeklickt, weil sie als lästig empfunden werden. Der datenschutzrechtliche Wert für die Selbstbestimmung und die Schutzwirkung, die die Einwilligung eigentlich entfalten soll, geht damit verloren. Daher wird empfohlen, die Einwilligung aus § 44 Abs. 3 HS.1 zu streichen. Die Anforderungen der korrekten Identifizierbarkeit sind insbesondere im elektronischen Verfahren hoch. Die betroffenen Personen werden dadurch, auch im Verhältnis zu dem Informationsgehalt des in Frage stehenden Datensatzes, ausreichend geschützt.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 H

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Prof. Dr. Hartmut Aden
Fachbereich 5
Polizei und Sicherheitsmanagement
Professur für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft

Stv. Direktor, Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin)

Behördlicher Datenschutzbeauftragter der HWR Berlin

Alt-Friedrichsfelde 60
D-10315 Berlin
T +49 (0)30 30877-2868

privat:
Postfach 580601
D-10415 Berlin

E-Mail: Hartmut.Aden@hwr-berlin.de

www.hwr-berlin.de/prof/hartmut-aden

www.foeps-berlin.org

Prof. Dr. Aden, HWR Berlin • Alt-Friedrichsfelde 60 • 10315 Berlin

An den
Ausschuss für „Inneres und Heimat“ des
Deutschen Bundestages

Per E-Mail an: innenausschuss@bundestag.de

Datum: 08. Dezember 2018

**Stellungnahme zum
Gesetzentwurf der Bundesregierung:
Entwurf 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. DSAnpUG-EU), Bundestags-Drucksache 19/4674,
vorgelegt zur Anhörung des Ausschusses für „Inneres und Heimat“ des Deutschen Bundestags am 10. Dezember 2018 in Berlin**

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Mitwirkung an der Anhörung. Wegen des großen Umfangs des Gesetzentwurfs beschränkt sich meine Stellungnahme auf grundsätzliche Erwägungen und ausgewählte Einzelfragen.

A) Notwendige Anpassungen an das EU-Datenschutzrecht und problematische Nutzung als „Omnisbus“- /„Container“-Gesetz

Die EU-Datenschutzgrundverordnung (EU) 2016/679 (im Folgenden: DSGVO) gilt seit dem 25. Mai 2018 unmittelbar verbindlich (Art. 99 Abs 2). Die Richtlinie (EU) 2016/680 war ebenfalls bereits bis zum 6. Mai 2018 in das mitgliedstaatliche Recht umzusetzen. Daher ist es grundsätzlich zu begrüßen, dass die Bundesregierung jetzt (verspätete) Anstrengungen unternimmt, die noch ausstehenden Anpassungen und Umsetzungen auf den Weg zu bringen. Die Vereinheitlichung der Terminologie, die das neue EU-Datenschutzrecht mit sich bringt, ist für die weitere Harmonisierung und Fortentwicklung des Datenschutzrechts grundlegend. Die überfällige Anpassung weiterer Fachgesetze des Bundes ist daher ein wichtiges Anliegen.

Berliner Volksbank
Konto 884 101 52 40

Allerdings enthält der Gesetzentwurf – anders als sein Titel suggeriert – keinesfalls nur Anpassungen an die DSGVO und Umsetzungsbestimmungen für die Richtlinie (EU) 2016/680. Vielmehr sind für einige der insgesamt 154 in den Entwurf einbezogenen Gesetze weitreichende zusätzliche Änderungen vorgesehen, die nicht auf die EU-Datenschutzreform zurückgehen, sondern mit denen rein bundespolitische Anliegen verfolgt werden.

Die Integration solcher Inhalte in einen Gesetzentwurf, die nicht mit dem eigentlichen Gesetzeszweck zu tun haben („Omnisbus"- oder „Containergesetz"), ist grundsätzlich verfassungsrechtlich zulässig. Allerdings sollte diese Gesetzgebungstechnik nur für Regelungen von geringer inhaltlicher Reichweite eingesetzt werden. Für inhaltlich weitreichende Regelungen, insbesondere für solche, die zusätzliche Grundrechtseingriffe zulassen, sollte diese Regelungstechnik nicht verwendet werden. Sie ist im Hinblick auf die Anforderungen des Demokratieprinzips (Art. 20 Abs. 2 GG) an die Transparenz der Gesetzgebung problematisch. Das Gebot der Transparenz der Entwürfe und ihrer Begründungen für das parlamentarische Gesetzgebungsgebungsverfahren und gegenüber denjenigen, die von den neu zugelassenen Grundrechtseingriffen betroffen sind, erfordert vielmehr die Beratung zusätzlicher Grundrechtseingriffe in eigenständigen Gesetzgebungsverfahren.

1. Änderung des BDBOS-Gesetzes (Artikel 8 des Entwurfs)

Die vorgeschlagenen Änderungen des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOSG) gehen erheblich über die Umsetzung der Richtlinie (EU) 2016/680 (bzw. der DSGVO) hinaus und ermöglichen zusätzliche Eingriffe in das Telekommunikationsgeheimnis (Art. 10 GG). Sie sollten daher in ein eigenständiges Gesetzgebungsverfahren ausgelagert werden (s.o., A).

Problematisch ist insbesondere die in § 19 Abs. 4 (Entwurfsfassung) vorgesehene Speicherung von Verkehrsdaten für 75 Tage. Der Digitalfunk der Sicherheitsbehörden wird von einer großen, sogar weiter steigenden Zahl von Personen genutzt. Daher umfassen die Verkehrsdaten große Mengen an personenbezogenen Kommunikationsdaten der beteiligten Mitarbeiterinnen und Mitarbeiter sowie möglicherweise in die Kommunikation eingebundener außenstehender Personen. Keiner der in § 19 Abs. 1 bis 3 der Entwurfsfassung genannten Zwecke erfordert eine undifferenzierte Speicherung sämtlicher Verkehrsdaten über einen mit 75 Tagen relativ langen Zeitraum. Daher dürfte eine so weitreichende Speicherung nicht mit

dem Zweckbindungsgrundsatz (Art. 10 GG; Art. 7 und 8 EU-Grundrechtecharta, für Polizei und Strafjustiz konkretisiert durch Art. 1 Nr. 4 b und c RL (EU) 2016/680) vereinbar sein. Alternativ sollten im Sinne des Vorrangs von *Privacy by Design*-Lösungen technische Konzepte zum Erreichen der in § 19 Ziele entwickelt werden, die mit weit weniger personenbezogenen Daten auskommen und dann im Hinblick auf den Zweckbindungsgrundsatz eher verhältnismäßig wären.

2. Änderungen des BSI-Gesetzes (Art. 13 des Entwurfs)

Auch die vorgeschlagenen Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) enthalten zusätzliche Eingriffsgrundlagen für weitreichende Grundrechtseingriffe, die über die Anpassung an das EU-Datenschutzrecht hinausgehen. Hier werden bereichsspezifische Datenerhebungs- und Datenschutzvorschriften für das IT-Sicherheitsrecht erst neu geschaffen, was grundsätzlich zu begrüßen ist.

Die Vorschrift gestattet allerdings weitreichende Formen der Datenverarbeitung für sehr unspezifisch formulierte Zwecke („Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik“). Möglichkeiten, die Zwecke präziser zu fassen und deutlich zu machen, inwiefern für Zwecke der Informationssicherheit überhaupt Daten mit Personenbezug erforderlich sind, bleiben hier ungenutzt.

Auch diese weitreichenden Änderungen sollten in ein gesondertes Gesetzgebungsverfahren verschoben und dort im Hinblick auf den Zweckbindungsgrundsatz präzisiert werden.

Empfehlung: *Der Deutsche Bundestag sollte Regelungen, die nicht im Zusammenhang mit der Anpassung bzw. Umsetzung datenschutzrechtlicher Bestimmungen im Hinblick auf das EU-Datenschutzrecht stehen, in ein eigenständiges Gesetzgebungsverfahren auslagern.*

C. Beispiele für problematische Einzelregelungen

Auch zahlreiche Einzelregelungen des vorliegenden Entwurfs sind problematisch, da teils bestehende Defizite nicht hinreichend abgestellt werden und teils neue Unklarheiten entstehen. Dies betrifft auch die in der Fachliteratur breit diskutierten Defizite der Umsetzung des EU-Datenschutz-

rechts im Bundesdatenschutzgesetz 2018. Darüber hinaus seien folgende Beispiele angeführt:

1. Bundesmeldegesetz (Art. 16 des Entwurfs)

Mit den Melderegistern verfügen bundesdeutsche Behörden über weitreichende Informationssammlungen über die Bevölkerung. Das Bundesmeldegesetz (BMG) enthält in seiner bisherigen Fassung zahlreiche, teils sehr problematische Befugnisse der Meldebehörden zur Datenübermittlung an öffentliche und nicht-öffentliche Stellen. Beispielhaft seien hier die besonders problematischen Regelungen des § 44 Abs. 3 BMG zur Übermittlung von Melderegisterdaten an Private zu Zwecken der Werbung oder des Adresshandels genannt. Diese Regelung wurde zwar geändert, aber im Kern beibehalten. Im Hinblick auf die Anforderungen des Art. 7 DSGVO an eine informierte Einwilligung wären hier zumindest konkretisierte behördliche Pflichten zur Prüfung der Voraussetzungen dieser DSGVO-Vorschrift erforderlich gewesen. Noch besser wäre ein vollständiges Verbot der Datenübermittlung an Private für Zwecke der Werbung und des Adresshandels, da kein legitimer Allgemeinwohlzweck für diese staatliche Dienstleistung an Private mit negativen Rückwirkungen auf den Grundrechtsschutz besteht.

2. Postgesetz (Art. 134 des Entwurfs)

Die Änderungen des Postgesetzes integrieren die bislang in der Postdienste-Datenschutzverordnung (PSDV) enthaltenen Vorschriften in das Postgesetz. Dies ist im Interesse der Übersichtlichkeit grundsätzlich zu begrüßen. Die Neuregelung enthält allerdings Mängel. So war bislang nach § 7 Abs. 3 PDSV ein Widerspruchsrecht für Postfachinhaber gegen die Weitergabe ihrer Daten vorgesehen. Dieses Widerspruchsrecht wurde in der Entwurfsfassung (§ 41a Abs. 2 PostG-Entwurf) gestrichen, ohne es durch eine Einwilligungserfordernis zu ersetzen.

In der Regelung zur Erhebung von Daten aus Ausweispapieren fehlt zudem der im Hinblick auf die Durchsetzung des Grundsatzes der Verhältnismäßigkeit gebotene explizite Hinweis auf die Erforderlichkeit für das Erreichen des legitimen Zwecks als Voraussetzung für die Datenerhebung (§ 41b Abs. 1 PostG-Entwurf).

D. Nach der Reform ist vor der Reform: Zukünftige „Baustellen“ für die Weiterentwicklung des Datenschutzrechts

Der umfangreiche Gesetzentwurf, der dem Deutschen Bundestag jetzt vorliegt, ist nur eine Etappe von mehreren hin zu einem modernen Datenschutzrecht.

1. E-Privacy-Verordnung

Anfang 2017 veröffentlichte die Europäische Kommission einen Verordnungsentwurf,[1] der die veraltete ePrivacy-Verordnung 2002/58/EG ablösen soll. Der Vorschlag befindet sich gegenwärtig noch im EU-Gesetzgebungsverfahren. Für die elektronische Kommunikation wird diese Verordnung die DSGVO zukünftig ergänzen und konkretisieren. Dies wird auch umfangreiche weitere Änderungen im deutschen Datenschutzrecht nach sich ziehen.

2. Evaluation der Datenverarbeitungspraxis und Nutzung von technischen Datenschutzlösungen

Der vorliegende Gesetzentwurf, der eine große Zahl von Fachgesetzen betrifft, zeigt erneut, wie ausdifferenziert das bereichsspezifische Datenschutzrecht in Deutschland ist. Die durch die DSGVO und die Richtlinie (EU) 2016/680 veranlassten Vereinheitlichungen sind indes nur ein Schritt von mehreren hin zu einem effektiven und modernen Datenschutzrecht in Deutschland. Erforderlich ist auch eine kritische Evaluation der zahlreichen Zweckänderungs- und Datenübermittlungsbefugnisse, die in den diversen Fachgesetzen vorgesehen sind. Über die praktische Nutzung dieser Befugnisse und ihre Auswirkungen auf die Betroffenen ist nur wenig bekannt. Für das zukünftige gesetzgeberische Nachsteuern und die Entwicklung technischer Datenschutzlösungen sind daher mehr empirische Informationen über die Datenverarbeitungspraxis bundesdeutscher Behörden erforderlich.

Gesamtfazit: Ich empfehle dem Deutschen Bundestag, den Entwurf nur nach gründlicher Überarbeitung zu verabschieden und die nicht mit dem EU-Datenschutzrecht zusammenhängenden „Container“-/„Omnibus“-Elemente aus dem Entwurf herauszunehmen.

Gez. Prof. Dr. Hartmut Aden

---

1 COM(2017) 10 final.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)151

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

Vorsitzende des Ausschusses
für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz, MdB
Platz der Republik 1
11011 Berlin

Nur per Mail:
innenausschuss@bundestag.de

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-5000
TELEFAX (0228) 997799-5550
E-MAIL referat11@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 26.10.2018
GESCHÄFTSZ. **11-100/044#0126**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Entwurf eines 2. Datenschutzanpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU), BT-Drs. 19/4674**

HIER Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

ANLAGEN -1-

Sehr geehrte Frau Vorsitzende,

für Ihre Beratungen zum Entwurf eines 2. Datenschutzanpassungs- und Umsetzungsgesetzes EU, BT-Drs. 19/4674 erhalten Sie im Anhang die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Ich würde mich freuen, wenn meine Vorschläge und Anregungen im weiteren Gesetzgebungsverfahren berücksichtigt würden. Für Ihre Fragen stehen Ihnen meine Mitarbeiterinnen und Mitarbeiter sowie ich selbst gern zur Verfügung. Zu den Empfehlungen des Bundesrates zu dem o. a. Gesetzentwurf werde ich gegebenenfalls gesondert Stellung nehmen.

65822/2018

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Ich bitte Sie, meine Stellungnahme den Ausschussmitgliedern zur Verfügung zu stellen.

Mit freundlichen Grüßen

Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 26. Oktober 2018

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Zweiten Datenschutzanpassungs- und Umsetzungsgesetzes-EU (2. DSAnpUG-EU), BR-Drs. 430/18, BT-Drs. 19/4674

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Vorbemerkung

Die Bundesregierung hat am 5. September 2018 den Entwurf eines Zweiten Datenschutzanpassungs- und Umsetzungsgesetzes-EU (2. DSAnpUG-EU) beschlossen. Dieser liegt dem Bundesrat (BR-Drs. 430/18) sowie dem Deutschen Bundestag (BT-Drs. 19/4674) zur Beratung vor.

Die folgende Darstellung enthält die wichtigsten Punkte, die aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im weiteren parlamentarischen Verfahren berücksichtigt werden sollten.

I. Artikel 8 (Änderung des BDBOS-Gesetzes)

1. Zu Nr. 2 – Änderung von § 19 Abs. 2 BDBOS-Gesetz

§ 19 Abs. 2 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(2) Wenn der Bundesanstalt tatsächliche Anhaltspunkte für eine rechtswidrige Inanspruchnahme des Digitalfunks BOS vorliegen, darf sie Verkehrsdaten auch verarbeiten, soweit dies erforderlich ist, um die rechtswidrige Inanspruchnahme des Digitalfunks BOS festzustellen und zu unterbinden; die tatsächlichen Anhaltspunkte sind aktenkundig zu machen und der behördliche Datenschutzbeauftragte ist über die beabsichtige Verarbeitung zu informieren.“

Vorschlag BfDI:

§ 19 Abs. 2 BDBOS-Gesetz wird gestrichen.

Begründung:

Der Regierungsentwurf enthält einen Erlaubnistatbestand zur Verarbeitung von Verkehrsdaten. Da der BOS-Funk kein öffentlich zugänglicher Telekommunikationsdienst ist, fällt dieser nicht unter die Richtlinie 2002/58/EG, sondern die DSGVO. Im Anwendungsbereich der DSGVO können die Mitgliedstaaten spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen dieser Rechtsgrundlage liegen hier nicht vor, weil die Verarbeitung nicht erforderlich, jedenfalls aber nicht verhältnismäßig ist. Eine rechtswidrige Inanspruchnahme des Digitalfunks BOS dürfte äußerst selten vorkommen, so dass es in diesen Fällen genügt, wenn die Strafverfolgungsbehörden tätig werden. Der Diebstahl und die Unterschlagung von Empfangsgeräten ist strafbewehrt (§§ 242, 246 StGB) ebenso wie das unerlaubte Abhören des BOS-Funks (§ 148 Abs. 1 Nr. 1 i.V.m. § 89 TKG). Zudem können abhandengekommene Endgeräte sowie die zugehörigen SIM-Karten aus der Ferne deaktiviert werden.

2. Zu Nr. 2 – Änderung von § 19 Abs. 4 BDBOS-Gesetz

§ 19 Abs. 4 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(4) 1Zur Sicherstellung, dass die Zwecke der Absätze 1 bis 3 erfüllt werden können, dürfen Verkehrsdaten nach ihrem Entstehen 75 Tage gespeichert werden. Nach Ablauf dieser Frist, sind die Verkehrsdaten zu löschen oder zu anonymisieren, es sei denn, ihre weitere Speicherung ist zu den in Absätzen 1 bis 3 genannten Zwecken erforderlich. 2Die weitere Speicherung ist zu begründen und zu dokumentieren. 3In Abständen von drei Monaten ist zu überprüfen, ob eine weitere Speicherung der Verkehrsdaten für die in den Absätzen 1 bis 3 genannten Zwecke erforderlich ist. 4Wird im Rahmen der Überprüfung festgestellt, dass eine weitere Speicherung der Verkehrsdaten nicht erforderlich ist, sind die Verkehrsdaten unverzüglich zu löschen oder zu anonymisieren.“

Vorschlag BfDI:

§ 19 Abs. 4 BDBOS-Gesetz wird wie folgt gefasst:

„Aus konkretem Anlass kann die Bundesanstalt einzelfallbezogen anordnen, dass Verkehrsdaten gespeichert werden, soweit dies erforderlich ist, um sicherzustellen, dass die Zwecke der Absätze 1 bis 3 erfüllt werden können. Eine solche Entscheidung ist zu begründen und zu dokumentieren. Die Erforderlichkeit der Speicherung ist in regelmäßigen Zeitabständen, spätestens alle drei Monate, zu überprüfen. Dient die Speicherung von Verkehrsdaten allein den in Absatz 1 Nummer 2 und Absatz 3 genannten Zwecken, sind die Verkehrsdaten unverzüglich zu pseudonymisieren.“

Begründung:

Der Regierungsentwurf führt für den BOS-Funk eine Vorratsdatenspeicherung ein.

Während bei der allgemeinen Vorratsdatenspeicherung nach § 113b Abs. 1 Nr. 1 TKG Verkehrsdaten zehn Wochen (= 70 Tage) lang auf Vorrat gespeichert werden, soll dies beim BOS-Funk sogar 75 Tage lang erlaubt sein. Die Erforderlichkeit einer so langen Speicherdauer kann nicht nachvollzogen werden. Der Umstand, dass zum Zeitpunkt der Speicherung der konkrete Verwendungszweck noch nicht feststeht, widerspricht dem datenschutzrechtlichen Grundsatz der Zweckbindung.

Die im TKG enthaltene anlasslose Vorratsdatenspeicherung ist derzeit Gegenstand mehrerer Gerichtsverfahren (BVerwG 6 C 12.18 und 6 C 13.18; BVerfG 1 BvR 141/16) und es bestehen erhebliche Zweifel an der Verhältnismäßigkeit einer so lan-

gen anlasslosen Speicherung. Zwar wird die Erforderlichkeit der im BDBOS-Gesetz vorgesehenen Speicherdauer umfangreich begründet. Auch unter Berücksichtigung des Erfordernisses, in einigen Fällen Daten rückwirkend auswerten zu müssen, scheint die lange Speicherung dennoch unverhältnismäßig. Eine Abwägung mit den datenschutzrechtlichen Interessen der Betroffenen findet nahezu nicht statt.

Die standardmäßig vorgegebene Speicherfrist sollte daher entfallen. Verkehrsdaten sollten grundsätzlich nur solange gespeichert werden, wie dies für den Betrieb des BOS-Funks erforderlich ist (bei den meiner Aufsicht unterliegenden Telekommunikationsanbietern wurde eine Speicherdauer zu betrieblichen Zwecken wie der Störungsbeseitigung von maximal sieben Tagen als angemessen angesehen), allerdings mit der Option einer anlassbezogenen Verlängerung eines bestimmten, näher einzugrenzenden Datenbestands im Rahmen eines sog. „Quick Freeze“, soweit dies zu den in Abs. 1 bis 3 genannten Zwecken erforderlich ist und eine entsprechende Begründung und Dokumentation erfolgt. Bei geplanten Großeinsätzen (z. B. G7-Gipfel), bei denen die Erforderlichkeit einer längeren Speicherdauer bereits vorab bekannt ist, kann eine Speicherung der benötigten Daten im Vorfeld einzelfallbezogen angeordnet werden.

Für die Zwecke des § 19 Abs. 1 Nr. 2 und Abs. 3 BDBOS-Gesetz genügen auch pseudonymisierte Daten, so dass eine weitere Speicherung von Verkehrsdaten, die allein diesen Zwecken dient, zum Schutz der Betroffenen ausschließlich in pseudonymisierter Form erfolgen sollte. Dies entspricht der Vorgabe des Art. 32 DSGVO, wonach Verantwortliche technische und organisatorische Maßnahmen wie Pseudonymisierung zu treffen haben, um ein dem Risiko angemessenes Schutzniveau herzustellen.

3. Zu Nr. 2 – Änderung von § 20 Abs. 2 BDBOS-Gesetz

§ 20 Abs. 2 BDBOS-Gesetz in der Entwurfsfassung lautet:

„(2) Um das Wiederauffinden eines abhandengekommenen Endgerätes zu unterstützen, darf auf Antrag eines Nutzers die Bundesanstalt an die für diesen Nutzer verantwortliche Zuständige Stelle für den Betrieb des Digitalfunk BOS folgende Daten übermitteln:

1. *Kennung der Basisstationen, an denen sich das Endgerät seit dem Abhandenkommen eingebucht oder einzubuchen versucht hat, und*
2. *den Zeitpunkt, zu dem die jeweilige Standortinformation erfasst wurde.*

Der Antrag ist durch den Nutzer über die für ihn verantwortliche Zuständige Stelle für den Betrieb des Digitalfunk BOS zu stellen und hat Angaben zur Identifizierung des Endgeräts zu enthalten.“

Vorschlag BfDI:

§ 20 Abs. 2 BDBOS-Gesetz ist zu streichen.

Begründung:

Der Regierungsentwurf enthält einen Erlaubnistatbestand zur Verarbeitung von Verkehrsdaten, wozu auch Standortdaten zählen, zum Zwecke des Auffindens von Endgeräten des BOS-Funks. Im Anwendungsbereich der DSGVO können die Mitgliedstaaten spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen dieser Rechtsgrundlage liegen hier nicht vor, da die Verarbeitung nicht erforderlich, jedenfalls aber nicht verhältnismäßig ist.

Die Verarbeitung ist nicht verhältnismäßig. Die Endgeräte des BOS-Funks sind wesentlich günstiger als die früheren Endgeräte beim Analogfunk. Deshalb sind die Kosten einer Suchaktion nach einem verlorenen Gerät häufig kostspieliger als die Kosten eines Neuerwerbs. Zudem können verlorene Endgeräte sowie zugehörigen SIM-Karten aus der Ferne deaktiviert werden, so dass ein Verlust zu keinen Sicherheitsrisiken führt.

II. Artikel 13 (Änderung des BSI-Gesetzes)

Zu Nr. 7 - § 6f Satz 2 BSI-Gesetz

§ 6f Satz 2 des BSI-Gesetzes (BSIG-E) in der Entwurfsfassung lautet:

„Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.“

Vorschlag BfDI:

§ 6f Satz 2 des BSI-Gesetzes in der Entwurfsfassung wird gestrichen.

Begründung:

Art. 21 Abs. 1 Satz 1 DSGVO ermöglicht es der betroffenen Person, aus Gründen, die sich aus ihrer besonderen Situation ergeben, einer an sich rechtmäßigen Verarbeitung personenbezogener Daten – bspw. durch eine Behörde – zu widersprechen. Eine Verarbeitung dieser Daten ist nach einem Widerspruch gem. Art. 21 Abs. 1 Satz 2 DSGVO nur dann erlaubt, wenn der Verantwortliche dafür zwingende schutzwürdige Gründe nachweisen kann, die die Interessen der betroffenen Person überwiegen.

§ 6f Satz 2 BSIG-E setzt an dieser Stelle an und soll es dem BSI ermöglichen, während der Prüfung der o. g. zwingenden Gründe die Verarbeitung noch fortsetzen zu dürfen. Diese Beschränkung wird auf Art. 23 DSGVO gestützt. Die dem BSI damit eingeräumte Möglichkeit, die zwingenden Gründe für die Verarbeitung ohne jede zeitliche Begrenzung zu prüfen, führt allerdings dazu, dass das Widerspruchsrecht faktisch in das Belieben des BSI gestellt und weitgehend ausgehebelt wird. Art. 23 Abs. 1 DSGVO erlaubt Beschränkungen der Betroffenenrechte nur, soweit diese eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellt. Die hierzu in der Begründung genannten Aspekte vermögen eine zeitlich unbefristete Aushebelung des Widerspruchsrechts nicht zu begründen. Der Satz ist daher zu streichen, zumindest aber mit einer zeitlich engen Frist zu versehen.

III. Artikel 62 (Änderung des Soldatengesetzes)

Zu Nr. 2 – Änderung von § 58c Soldatengesetz

§ 58 c Soldatengesetz lautet:

„(1) Zum Zweck der Übersendung von Informationsmaterial nach Absatz 2 Satz 1 übermitteln die Meldebehörden dem Bundesamt für das Personalmanagement der Bundeswehr jährlich bis zum 31. März folgende Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden:

1. Familienname,

2.Vornamen,

3.gegenwärtige Anschrift.

Die Datenübermittlung unterbleibt, wenn die Betroffenen ihr nach § 36 Absatz 2 des Bundesmeldegesetzes widersprochen haben.

(2) Das Bundesamt für das Personalmanagement der Bundeswehr darf die Daten nur dazu verwenden, Informationsmaterial über Tätigkeiten in den Streitkräften zu versenden.

(3) Das Bundesamt für das Personalmanagement der Bundeswehr hat die Daten zu löschen, wenn die Betroffenen dies verlangen, spätestens jedoch nach Ablauf eines Jahres nach der erstmaligen Speicherung der Daten beim Bundesamt für das Personalmanagement der Bundeswehr.“

Vorschlag BfDI:

§ 58 c Soldatengesetz wird gestrichen.

Begründung:

§ 58 c Absatz 1 Satz 2 Soldatengesetz sieht vor, dass Meldebehörden personenbezogene Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden, an das Bundesamt für Personalmanagement der Bundeswehr übermitteln dürfen, wenn die Betroffenen der Übermittlung nicht widersprochen haben.

Die Übermittlung ist eine Form der Verarbeitung (Art. 4 Nr. 2 DSGVO). Die Mitgliedstaaten können spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO liegen nicht vor. Gründe für die Übermittlung

der Daten zur Erfüllung einer rechtlichen Verpflichtung oder aus Gründen des öffentlichen Interesses werden nicht genannt.

Der Bedarf an einer bereichsspezifischen Sonderregelung für den Bereich des Bundesministeriums der Verteidigung ist daher nicht überzeugend dargelegt.

IV. Artikel 82 (Änderung des IHK-Gesetzes)
Zu Nr. 2 lit. b) – Änderung von § 9 Abs. 5 IHK-Gesetz

§ 5 Absatz 5 des IHK-Gesetzes in der Entwurfsfassung lautet:

„(5) 1Die Industrie- und Handelskammern dürfen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken die in Absatz 1 genannten Daten an nicht-öffentliche Stellen übermitteln, sofern der betroffene Kammerzugehörige der Übermittlung nicht widersprochen hat und der Empfänger der Daten sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. 2Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die Kammerzugehörigen unbeschadet der weiteren Vorgaben der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung vor der ersten Übermittlung schriftlich oder elektronisch hinzuweisen. 3Daten über Zugehörige anderer Kammern hat die Industrie- und Handelskammer nach Übermittlung an die nicht-öffentliche Stelle unverzüglich zu löschen, soweit sie nicht zur Erfüllung der ihr nach diesem Gesetz übertragenen Aufgaben erforderlich sind.“

Vorschlag BfDI:
§ 5 Absatz 5 IHK-Gesetz wird gestrichen.

Begründung:

Der Entwurf sieht vor, dass die Industrie- und Handelskammern personenbezogene Daten ihrer Kammermitglieder an nichtöffentliche Stellen übermitteln dürfen, wenn die Kammermitglieder dem nicht widersprechen. Eine solche Widerspruchslösung ist nach der DSGVO nicht zulässig.

Die Übermittlung ist eine Form der Verarbeitung (Art. 4 Nr. 2 DSGVO). Die Mitgliedstaaten können spezifischere Bestimmungen treffen, unter welchen Voraussetzungen eine Verarbeitung auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO erfolgen darf (Art. 6 Abs. 2 und 3 DSGVO). Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 Buchst. c oder e DSGVO dürften in der Mehrzahl der hier geregelten Fälle nicht vorliegen. Die Übermittlung der Daten ist nicht zur Erfüllung einer rechtli-

chen Verpflichtung erforderlich und liegt auch nicht im öffentlichen Interesse, sondern im mutmaßlichen privaten Interesse der Kammermitglieder an der Förderung von Geschäftsabschlüssen. Eine mutmaßliche Einwilligung ist nach der DSGVO allerdings nicht vorgesehen. Erforderlich sind vielmehr eindeutige bestätigende Handlungen, weshalb Stillschweigen oder Untätigkeit – hier ein Nichtwidersprechen – keine Einwilligung darstellen (Erwägungsgrund 32 Satz 3 DSGVO).

Es wurde auch kein Bedarf an einer bereichsspezifischen Sonderregelung für die Industrie- und Handelskammern dargelegt. Wenn die Übermittlungen im Interesse der Kammermitglieder sind, werden diese ihre Einwilligungen erteilen. Ein solches Verfahren stellt die Kammern nicht vor große praktische Hürden, wie das Beispiel der Wirtschaftsprüferkammer belegt, bei der ein solches Verfahren bereits praktisch etabliert ist. Im Übrigen wurden die Erlaubnistatbestände für die Übermittlung personenbezogener Daten von öffentlichen an nichtöffentliche Stellen bereits allgemein in § 25 Abs. 2 und § 23 BDSG geregelt. Dies genügt, so dass bereichsspezifische Regelungen im IHK-Gesetz nicht erforderlich sind.

V. Artikel 123 (Änderung des Fünften Buches Sozialgesetzbuch)

1. Zu Nr. 38 – Änderung von § 284 SGB V

Der Gesetzentwurf enthält keine klarstellende Regelung zur Wirkung der Einwilligung im Verhältnis des Versicherten zur gesetzlichen Krankenkasse. Obwohl in den bis zum Sommer 2018 diskutierten und im Ressortkreis konsentierten Vorentwürfen eine solche Regelung enthalten war, fehlt sie bedauerlicherweise im Regierungsentwurf.

Ich rege daher an, eine ursprünglich mit den Bundesministerien inhaltlich abgestimmte Regelung in das Gesetz aufzunehmen.

Vorschlag BfDI:

In § 284 SGB V wird folgender Absatz 5 eingefügt:

„(5) Krankenkassen dürfen Sozialdaten, sofern sie besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 sind, auf Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2016/679 in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 nur verarbeiten, sofern in diesem Buch eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Dies gilt nicht für die Übermittlung für Zwecke der wissenschaftlichen Forschung und Planung Dritter.“

Begründung:

Dem Gesetzesvorbehalt nach § 30 des Vierten Buches Sozialgesetzbuch (SGB IV) folgend knüpft § 284 SGB V die dort geregelten Datenverarbeitungsbefugnisse der Krankenkassen an die Voraussetzung, dass die zu verarbeitenden Daten für die dort abschließend aufgeführten Zwecke erforderlich sind. Um auszuschließen, dass Krankenkassen allein auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 Daten für Zwecke verarbeiten, die nicht zu ihrem gesetzlich zugewiesenen Aufgabenbereich gehören, sieht § 284 Absatz 5 SGB V auf der Grundlage der Öffnungsklausel des Artikels 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 vor, dass Krankenkassen besondere Kategorien personenbezogener Sozialdaten auf der Grundlage einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a in Verbindung mit Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 trotz Einwilligung der betroffenen Person nur dann verarbeiten dürfen, wenn im SGB V eine Verarbeitung dieser Daten mit Einwilligung ausdrücklich vorgesehen ist. Damit wird der Status quo erhalten.

Eine entsprechende Klarstellung, die die seit Jahrzehnten bestehende gemeinsame Rechtsauffassung des Bundesministeriums für Gesundheit, des Bundessozialge-

richts (siehe Urt. v. 10. Dezember 2008 – B6 KA 37/07 R -, BSGE 102, S. 134 Leitsatz 1), des Bundesversicherungsamtes und mir deutlich zum Ausdruck bringen.

Eine derartige Klarstellung ist nicht zuletzt deshalb erforderlich, da eine erhebliche Anzahl von Beschwerden von Versicherten, aber auch von Ärzten vorliegen, wonach in der Praxis diese Rechtsauffassung der Aufsichtsbehörden von Krankenkassen umgangen wird, indem Versicherte veranlasst werden, Schweigepflichtentbindungserklärungen abzugeben, um hiermit von Ärzten medizinische Daten über die Versicherten zu erheben, die ihnen gesetzlich nicht zustehen. Eine derartige Klarstellung würde zudem Erwägungsgrund 43 der DSGVO präzisieren, wonach eine Einwilligung dann keine gültige Rechtsgrundlage ist, „wenn zwischen der betroffenen Person“ (Versichertem) „und dem Verantwortlichen (gesetzliche Krankenkasse) ein klares Ungleichgewicht besteht“, … „und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“. Tatsächlich erfolgt die Forderung an den Versicherten, eine Schweigepflichtentbindungserklärung abzugeben, häufig in Fällen, in denen der Versicherte auf die Zahlung von Krankengeld angewiesen ist. Über die Probleme habe ich mehrfach berichtet (u.a. in meinem 26. [Nr. 9.2.5], 25. [Nr. 13.7.1] und 22. [Nr. 11.1.8] Tätigkeitsbericht).

2. Zur Verhängung von Geldbußen

Vorschlag BfDI:

Dem § 307 wird folgender Absatz 5 angefügt:

„(5) Abweichend von § 85a Absatz 3 des Zehnten Buches Sozialgesetzbuch kann gegen eine Krankenkasse wegen eines Verstoßes nach Artikel 83 Absatz 4, 5 oder 6 der Verordnung (EU) 2016/679, der sich auf Sozialdaten bezieht, eine Geldbuße nach Artikel 58 Absatz 2 Buchtstabe i) der Verordnung (EU) 2016/679 verhängt werden. § 17 Absatz 4 des Gesetzes über Ordnungswidrigkeiten ist anzuwenden.“

Begründung:

Der vorliegende Gesetzentwurf sieht keine Möglichkeit vor, Geldbußen bei Datenschutzverstößen durch gesetzliche Krankenversicherungen zu verhängen. Ein durchgreifender Grund, die sich verstärkt als Wirtschaftsunternehmen verstehenden gesetzlichen Krankenkassen mit einem Ausgabevolumen von zum Teil mehr als 25 Mrd. Euro gegenüber einem Handwerks- oder Industrieunternehmen zu privilegieren, ist nicht ersichtlich

Bereits mit der Einführung des geltenden § 85a des Zehnten Buches Sozialgesetzbuch (SGB X) war eine deutliche Verschlechterung des Datenschutzniveaus gegenüber der früheren, bis zum 24. Mai 2018 geltenden Regelung des § 85 SGB X a.F. eingetreten, in dem nunmehr pauschal Behörden und sonstige öffentliche Stellen, und damit auch gesetzliche Krankenkassen von der Verhängung eines Bußgeldes ausgenommen werden. So war es beispielsweise nach § 85a Absatz 1 Nr. 1a) und b) SGB X a.F. möglich, ein Bußgeld zu verhängen, falls bestimmte Versäumnisse bei der Auftragsverarbeitung nach § 80 SGB X vorlagen, nach § 85a Absatz 1 Nr. 3 SGB X a. F., wenn ein Sozialleistungsträger nicht oder nicht rechtzeitig einen internen Datenschutzbeauftragten bestellte oder nach § 85 Absatz 2 Nr. 6 SGB X a.F., wenn er eine Datenschutzverletzung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig den Rechtsaufsichts- und Datenschutzbehörden nach § 83a SGB X meldete.

Ich halte es für geboten, in das 2. DSAnpUG-EU eine Regelung aufzunehmen, die die wirtschaftliche Tätigkeit und das wirtschaftliche Auftreten der gesetzlichen Krankenkassen berücksichtigt und die es ermöglichte, in diesem Rahmen bestimmte Verstöße gegen die Datenschutz-Grundverordnung nach Art. 58 Absatz 2 Buchst. i) i.V.m. Art. 83 DSGVO mit einem Bußgeld zu sanktionieren.

Gesetzliche Krankenkassen sind einerseits öffentlich-rechtliche Körperschaften (§ 29 Absatz 1 Viertes Buch Sozialgesetzbuch – SGB IV), die gesetzliche Aufgaben zu erfüllen haben. Andererseits nehmen sie als öffentliche Unternehmen am Wettbewerb teil (§ 2 Absatz 5 BDSG). Der Wettbewerb hat in der Vergangenheit z. B. zu Fusionen geführt, die die Zahl der gesetzlichen Krankenkassen von 1.147 im Jahre 1990 auf den heutigen Stand von lediglich 110 gesetzlichen Krankenkassen reduziert hat.

Auch in der Öffentlichkeit gerieren sich die gesetzlichen Krankenkassen als öffentliche Wettbewerbsunternehmen, die mit verschiedenen Angeboten – ähnlich wie privatrechtliche Krankenversicherungsunternehmen – um ihre Kundschaft werben. So bieten etwa einige Krankenkassen in Zusammenarbeit mit privaten Anbietern ihren Kunden die Nutzung von elektronischen Gesundheitsakten an, die über eine App auf dem Smartphone oder Tablet genutzt werden sollen. Die Angebote und das Datenschutzniveau unterscheiden sich dabei deutlich und dies wird von den gesetzlichen Krankenkassen auch als Wettbewerbsvorteil gegenüber anderen Krankenkassen gesehen. Der Wettbewerb der Krankenkassen erstreckt sich u. a. zudem auf das Angebot von innovativen Versorgungsformen und (Zusatz-) Leistungen innerhalb des gesetzlich eröffneten Rahmens. Im Verhältnis zu ihren Versicherten ist das Verhalten der Krankenkassen unmittelbar am UWG zu messen, soweit dieses die Richtlinie 2005/29/EG (UGP-RL) über unlautere Geschäftspraktiken umsetzt (vgl. hierzu statt vieler BGH, Urteil vom 30. April 2014 – I ZR 170/10 –; Urteil vom 18. September 2013 – I ZR 183/12 –; EuGH, Urteil vom 03. Oktober 2013 – C-59/12 –).

Schließlich ist es einem Versicherten (bei den gesetzlichen Krankenkassen intern „Kunde“ genannt) möglich, frei von einer gesetzlichen Krankenkasse zu einer anderen zu wechseln. Dies ist bei anderen Sozialversicherungsträgern (Deutsche Rentenversicherungen, gesetzliche Unfallversicherer) nicht möglich. Die gesetzlichen Renten- und Unfallversicherungsträger stehen im Gegensatz zu den gesetzlichen Krankenkassen untereinander nicht im Wettbewerb

Es gibt daher tatsächliche Gründe, die Krankenkassen im Unterschied zu anderen Sozialversicherungsträger Wirtschaftsunternehmen gleich zu stellen.

Mit dem o. a. Vorschlag wird von der Möglichkeit einer abweichenden Regelung nach Artikel 83 Absatz 7 der Verordnung (EU) 2016/679 Gebrauch gemacht.

Geahndet werden können Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 durch die genannten Stellen bei der Verarbeitung von Sozialdaten im Zusammenhang mit ihren Aufgaben. Die Höhe des Bußgeldrahmens entspricht europarechtsgemäß dem in Artikel 83 Absatz 4 bis 6 DSGVO festgelegten Rahmen.

Zuständige Aufsichtsbehörden für die Verhängung von Geldbußen sind gemäß Artikel 58 Absatz 2 Buchstabe i in Verbindung mit Artikel 83 der Verordnung (EU) 2016/679 die jeweiligen Datenschutzaufsichtsbehörden, d. h. der oder die BfDI oder

die jeweiligen Landesdatenschutzbeauftragten. Hinsichtlich der praktischen Auswirkungen einer Bußgeldregelung weise ich darauf hin, dass die Verhängung eines Bußgeldes „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein muss(Art. 83 Absatz 1 DSGVO). Bei der Bemessung des Bußgeldes ist aber auch zu berücksichtigen, dass es sich bei den Geldern der gesetzlichen Krankenkassen um Versichertenbeiträge handelt.

VI. Artikel 135 (Änderung des Postgesetzes)

1. Zu Nr. 3 – Änderung von § 41 PostG

§ 41Postgesetz (PostG-E) in der Entwurfsfassung lautet:

„Für Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung solcher Dienste mitwirken (Diensteanbieter), werden die Vorgaben der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung durch die Regelungen der §§ 41a bis 42 ergänzt.“

Vorschlag BfDI:

§ 41 PostG wird um folgenden Satz ergänzt: *„Die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen stehen personenbezogenen Daten bei der Erbringung geschäftsmäßiger Postdienste gleich.“*

Begründung:

Das zu verfolgende Ziel im postrechtlichen Datenschutz muss sein, dass das bisherige, sich aus dem PostG und der Postdienste-Datenschutzverordnung (PDSV) ergebende Datenschutzniveau beibehalten wird und durch die Berücksichtigung der Datenschutz-Grundverordnung (DSGVO) keine Absenkung erfährt. An dem bisherigen datenschutzrechtlichen Gleichlauf bei natürlichen und juristischen Personen ist daher auch weiterhin festzuhalten. Die seinerzeitigen Erwägungen für die Schaffung eines einfachgesetzlichen, auch für juristische Personen geltenden, Postgeheimnisses durch das PostG i.V.m. der PDSV tragen nach wie vor. Die Regelungen wurden im Zuge der Privatisierung der Post und der Aufgabe des Postmonopols geschaffen. Da es sich bei Postdienstleistungen um vormals hoheitlich erbrachte Leistungen der Daseinsvorsorge handelt, die ursprünglich dem Fernmeldegeheimnis (Art. 10 GG) unterlagen, hat der Bund eine einfachgesetzliche Ausprägung des Postgeheimnisses geschaffen, damit auch bei der Leistungserbringung durch Private weiterhin vergleichbare Datenschutzstandards gelten.

Die auch zukünftig notwendige Regelung zur Gleichstellung der Einzelangaben über juristische Personen ist auch unter Berücksichtigung von Erwägungsgrund 14 der

DSGVO zulässig. Erwägungsgrund 14 stellt klar, dass sich die unmittelbare Geltung der DSGVO nicht auf juristische Personen erstreckt. Daraus ergibt sich aber im Umkehrschluss, dass der nationale Gesetzgeber Regelungen erlassen kann, die auch darin bestehen können, die DSGVO-Normen für juristische Personen anwendbar zu erklären. Die EU-weite Vollharmonisierung des Schutzes personenbezogener Daten durch die DSGVO bedeutet eine Sperrwirkung für mitgliedsstaatliche Regelungen nur bezogen auf die Verarbeitung personenbezogener Daten. Die DSGVO hindert die Mitgliedstaaten jedoch nicht daran, für Bereiche außerhalb des sachlichen Anwendungsbereichs der DSGVO diese für anwendbar zu erklären. Der nationale Gesetzgeber darf nur keine Regelungen zur Verarbeitung personenbezogener Daten natürlicher Personen treffen, soweit er keine ausdrückliche Regelungsbefugnis hat..

Die Postdienstleister erleiden durch die weiterhin bestehende Berücksichtigung der Einzelangaben juristischer Personen auch keinen Wettbewerbsnachteil dadurch, dass sie, anders als in anderen EU-Mitgliedstaaten, die Daten juristischer Personen ebenso schützen müssen wie die von natürlichen Personen. Im Gegenteil ist es gerade auch im Interesse der gesamten Wirtschaft, wenn der Schutz für die Daten juristischer Personen weiterhin bestehen bleibt.

Eine Abkehr von der Gleichstellung der Einzelangaben juristischer Personen würde die Postdienstleister auch vor schwere Herausforderungen stellen, da eine unterschiedliche Behandlung von in der Praxis gleichen Sachverhalten nicht praktikabel ist. Entgegen jeder Lebensrealität müssten die Postdienstleister jederzeit ihre Prozesse nach Geschäfts- und Privatpost trennen können. Dies ist den Postdienstleistern aus meiner Erfahrung bei datenschutzrechtlichen Kontrollen im Postbereich jedoch nicht möglich.

Es sollten daher die Vorgaben der Verordnung (EU) 2016/679, des Bundesdatenschutzgesetzes und der Regelungen der §§ 41a bis 42 PostG-E auf die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen entsprechend Anwendung finden.

2. Zu Nr. 3 – § 41b PostG

§ 41b Absatz 1 Postgesetz (PostG-E) in der Entwurfsfassung lautet:

„(1) Diensteanbieter können von am Postverkehr Beteiligten verlangen, sich über ihre Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere auszuweisen, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen.“

Vorschlag BfDI:

§ 41b PostG ist folgendermaßen zu ergänzen: *„(1) Diensteanbieter können von am Postverkehr Beteiligten verlangen, sich über ihre Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere auszuweisen, wenn dies erforderlich ist, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen.“*

Begründung:

In den Referentenentwürfen war der Erforderlichkeitsgrundsatz richtigerweise im Gesetzestext beachtet worden. Schon die Postdienste-Datenschutzverordnung (PDSV) geht in § 7 Abs. 1 von dem Erforderlichkeitsgrundsatz aus.

3. Zu Nr. 4 – Änderung von § 42 PostG

Die Überschrift zu § 42 Postgesetz lautet:

„Kontrolle und Durchsetzung von Verpflichtungen“

Vorschlag BfDI:

Die Überschrift zu § 42 PostG ist folgendermaßen zu ergänzen: *„Kontrolle, Aufsicht und Durchsetzung von Verpflichtungen“*

Begründung:

In der Überschrift zu § 42 PostG (und auch in der Inhaltsübersicht zu dieser Vorschrift) ist zusätzlich das Wort „Aufsicht“ aufzunehmen, da § 42 Abs. 3 PostG-E in Anpassung an die DSGVO und das BDSG die datenschutzrechtliche Aufsicht der BfDI behandelt. Auch die DSGVO und das BDSG sprechen von Aufsichtsbehörden bzw. Aufsicht.

VII. Nichtaufnahme einer Anpassung des TKG

Vorschlag BfDI:

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die seit dem 25. Mai 2018 anzuwendende Datenschutz-Grundverordnung erfordert eine Anpassung der datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

dem Deutschen Bundestag unverzüglich einen Gesetzentwurf vorzulegen, mit dem die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes an die Datenschutz-Grundverordnung angepasst werden.

Begründung:

Das Telekommunikationsgesetz enthält in seinem siebten Teil (§§ 88 ff.) auch datenschutzrechtliche Bestimmungen, die nicht auf europarechtlichen Vorgaben beruhen, insbesondere nicht der Umsetzung der Richtlinie 2002/58/EG dienen, sondern nunmehr durch die DSGVO geregelt werden.

Spätestens seit Anwendbarkeit der DSGVO (25. Mai 2018) ist die Bundesrepublik verpflichtet (§ 4 Abs. 3 EUV), das TKG an diese neue Rechtslage anzupassen. Dieser „Verpflichtung aus den Verträgen“ (Art. 258 AEUV) ist Deutschland bislang nicht nachgekommen.

Dadurch, dass das TKG im bisherigen Umfang formal weiterbesteht, ist zudem nicht klar ersichtlich, welche datenschutzrechtlichen Bestimmungen – diejenigen der DSGVO oder diejenigen des TKG – auf einen bestimmten telekommunikationsrechtlichen Sachverhalt anzuwenden sind und inwieweit das TKG von dem Anwendungsvorrang der DSGVO (vgl. Art. 95 DSGVO) verdrängt wird. Dies führt bei den Betroffenen zu erheblicher Rechtsunsicherheit.

Die im TKG angelegte Zuständigkeit der Bundesnetzagentur zur Durchsetzung datenschutzrechtlicher Vorschriften sowie die Zuständigkeit derselben zur Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten (§ 149 Abs. 1 Nr. 16 bis 17d und 18 sowie 21b, 21c, 30a und 38 bis 43 TKG) widerspricht nicht nur der DSGVO, sondern auch dem europäischen Primärrecht und ist daher dringend anzupassen. Als eine der Fach- und Rechtsaufsicht unterliegende Verwaltungsbehörde ge-

nügt die Bundesnetzagentur nicht den Anforderungen, die das europäische Recht an die Unabhängigkeit und Weisungsfreiheit der Datenschutzvorschriften kontrollierenden Stellen aufstellt (Art. 8 Abs. 3 GrCh; Art. 16 Abs. 2 S. 2 AEUV). Umgekehrt ist die BfDI zwar unabhängig, verfügt jedoch nach aktueller nationaler Rechtslage über keine Durchsetzungsbefugnisse in Bezug auf Datenschutzvorschriften des TKG. Damit wird die effektive Wahrnehmung ihrer Aufgabe als unabhängige Datenschutzbehörde konterkariert.

Das BMWi hatte deshalb ursprünglich vorgesehen, im Zuge des 2. DSAnpUG-EU auch das TKG anzupassen. Ein entsprechender Referentenentwurf wird aber nicht mehr verfolgt. Die erforderlichen datenschutzrechtlichen Anpassungen finden sich auch nicht in dem Entwurf eines Vierten Gesetzes zur Änderung des Telekommunikationsgesetzes (BR-Drs. 391/18).

Andrea Voßhoff

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)176

vfa. Die forschenden Pharma-Unternehmen

Stellungnahme

zum Entwurf der Bundesregierung für ein

„Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680"

BT-Drucksache 19/4674

[Stand: 01.10.2018]

Hausvogteiplatz 13
10117 Berlin
Telefon 030 206 04-0
Telefax 030 206 04-222
www.vfa.de

Der vfa ist der Wirtschaftsverband der forschenden Pharma-Unternehmen in Deutschland. Er vertritt die Interessen von 43 weltweit führenden forschenden Pharma-Unternehmen und über 100 Tochter- und Schwesterfirmen in der Gesundheits-, Forschungs- und Wirtschaftspolitik. Die Mitglieder des vfa repräsentieren mehr als zwei Drittel des gesamten deutschen Arzneimittelmarktes und beschäftigen in Deutschland rund 80.000 Mitarbeiter. Mehr als 16.000 davon arbeiten in Forschung und Entwicklung.

Als Wirtschaftsverband der forschenden Pharmaunternehmen nimmt der vfa gerne die Gelegenheit wahr, zu pharma- und forschungsrelevanten Aspekten des Regierungsentwurfes eines *Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* (2. DSAnpUG-EU) Stellung zu nehmen.

vfa-Position

Das 2. DSAnpUG-EU soll insbesondere der Implementierung der Datenschutzgrundverordnung (EU) 2016/69 (DSGVO) vom 04.05.2016 dienen, die seit dem 25.05.2018 unmittelbar geltendes Recht ist. Da die DSGVO mit ihrem Ansatz der Harmonisierung und Schaffung eines einheitlichen Datenschutzniveaus einen Meilenstein des europäischen Datenschutzrechts darstellt, begrüßt der vfa, dass das BMI einen Referentenentwurf zur Implementierung in Deutschland vorgelegt hat, mit dem nun die notwendigen bereichsspezifischen Datenschutzregelungen des Bundes adressiert werden.

Die vorgeschlagenen Regelungen mit Bezug zur pharmazeutischen Industrie (Art. 18 und 19 im 2. DSAnpUG-EU) sind mehrheitlich sachgerecht und daher zu begrüßen. Insbesondere begrüßt der vfa, dass im Bereich der klinischen Prüfungen mit Humanarzneimitteln und mit Medizinprodukten das Schriftformerfordernis für die Einwilligung in die Datenverarbeitung im Sinne einer fortschreitenden Digitalisierung um die elektronische Form ergänzt werden soll (vgl. Art. 18 + 83 des 2. DSAnpUG-EU).

Der vfa erkennt daneben Änderungsbedarf für die Anpassung des § 40 Abs.2a AMG im Hinblick auf eine rechtliche Klarstellung zum Nichtbestehen von Lösch- und Datenportabilitätsrechten sowie für § 42b AMG im Hinblick auf die dort geregelte datenschutzrechtliche Einwilligungserklärung, die unseres Erachtens als Rechtsgrundlage praxisfern erscheint.

I. Art. 18 2.DSAnpUG-EU: § 40 Abs.2a AMG

Für § 40 Abs.2a AMG sieht das 2. DSAnpUG-EU vor, dass die betroffene Person darüber aufzuklären ist, die datenschutzrechtliche Einwilligungserklärung in die Datenverarbeitung im Rahmen der klinischen Prüfung jederzeit widerrufen zu können. In Umsetzung des Art. 28 Abs. 3 S.2 der Verordnung (EU) 536/2014, legt § 42 Abs.2a AMG schon *de lege lata* fest, dass die betroffene Person darüber aufzuklären ist, dass trotz eines möglichen Widerrufs einer Einwilligung in die Teilnahme und Datenverarbeitung in einer klinischer Prüfung die bis zum Zeitpunkt des Widerrufs gespeicherten Daten weiterhin verarbeitet werden dürfen.

In Art. 17 DSGVO ist das Betroffenenrecht auf Löschung personenbezogener Daten geregelt, in Art. 20 DSGVO das Recht auf Datenportabilität. Bei konsequentem Verständnis des Art. 28 Abs.3 S.2 der Verordnung über klinische Prüfungen mit Humanarzneimitteln (EU) 536/2014 ergeben Art. 17 und Art. 20 DSGVO im Rahmen von klinischen Prüfungen nach AMG keinen Sinn und könnten bei Geltendmachung dieser Rechte ohne einen Verstoß gegen die genannte Regelung in Art. 28 Abs. 3 S. 2 der Verordnung (EU) 536/2014 nicht erfüllt werden. Vor diesem Hintergrund schlagen wir vor, § 40 Abs. 2a S.2 AMG wie folgt zu ergänzen (Ergänzung in *kursiv*):

> „[…] 3 c) der Pflicht zur Vorlage vollständiger Zulassungsunterlagen zu genügen,
>
> *4. das Recht auf Löschung nach Art. 17 Verordnung (EU) 2016/679 und das Recht auf Datenübertragbarkeit nach Art. 20 Verordnung (EU) 2016/679 insoweit nicht bestehen,*
>
> *5.* die Daten bei den genannten Stellen für die auf Grund des § 42 Abs. 3 bestimmten Fristen gespeichert werden."

Eine Gesetzesänderung mit gleichem Regelungsgehalt hat im Übrigen der österreichische Gesetzgeber im dortigen Arzneimittelgesetz bei der Umsetzung der DSGVO im Arzneimittelrecht eingefügt (vgl. § 39 Abs.3a AMG-Österreich).

II. Art.18 2.DSAnpUG-EU: § 42b Abs.3 AMG

§ 42b Abs.3 S.4 AMG in der derzeit gültigen Fassung regelt für Berichte nach § 42b Abs.1 und 2 AMG, dass mit Ausnahme des Namens und der Anschrift des pharmazeutischen Unternehmers oder des Sponsors sowie der Angabe des Namens und der Anschrift von nach § 4a BDSG-alt einwilligender Prüfärzte die Berichte keine personenbezogenen, insbesondere patientenbezogenen Daten enthalten dürfen.

Der Änderungsvorschlag der Bundesregierung belässt als Rechtsgrundlage für die Datenverarbeitung die datenschutzrechtliche Einwilligung der Prüfärzte.

Aus Sicht des vfa ist die Vorgabe der Einwilligung als Rechtsgrundlage zur Verarbeitung des Namens und der (geschäftlichen) Anschrift der beteiligten Prüfärzte nicht praxisgerecht. Vielmehr sollten für diesen standardisierten Datenverarbeitungsprozess mit unsensiblen personenbezogenen Daten andere gesetzliche Rechtsgrundlagen zur Datenverarbeitung von den datenverarbeitenden Stellen genutzt werden dürfen, beispielsweise „*Vertragliche Zusammenarbeit*" (Art. 6 Abs.1 lit.b DSGVO) oder „*öffentliches Interesse*" (Art. 6 Abs.1 lit.e DSGVO). Neben Praktikabilitätsgesichtspunkten ist als Begründung ebenfalls heranzuziehen, dass mit Wirksamwerden der EU-Verordnung 536/2017 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG (EU-CTR) Berichte an die EMA ebenfalls keiner Einwilligung der zu benennenden Prüfärzte bedürfen und § 42b AMG in der Fassung des Vierten AMG-Änderungsgesetzes lediglich für Prüfärzte aus Drittstaaten gelten soll.

Fazit:

Verlässliche rechtliche Rahmenbedingungen sind für die forschenden Pharmaunternehmen, die unter anderem für die Entwicklung innovativer Arzneimittel, für die Gewährleistung hoher Arzneimittelsicherheit sowie für die Verbesserung der Patientenversorgung auf personenbezogene Forschungs- und Gesundheitsdaten angewiesen sind, essentiell.

Dies gilt insbesondere für die Herausforderungen der Zukunft und im Hinblick auf die digitale Transformation des Gesundheitswesens sowie z. B. den Ausbau der sogenannten Personalisierten Medizin unter Einbeziehung u.a. genetischer Biomarker. Hier bedarf es unserer Einschätzung nach weiterführenden Anpassungen sowohl im allgemeinen Datenschutzrecht als auch in bereichsspezifischen Regelungen. Dabei sollten sowohl hohe Anforderungen an den Persönlichkeitsrechtsschutz des Einzelnen gestellt als auch Zugang zu qualitativ hochwertigen Datensätzen für Forscher und Akteure des Gesundheitswesens gewährt werden. Der insoweit erforderliche gesetzliche Anpassungsbedarf sollte in dieser Legislatur geprüft werden. In die dazu erforderliche Diskussion bringt sich der vfa gerne mit ein und steht für entsprechende Gespräche zur Verfügung.

(Stand: 14. November 2018)

WIRTSCHAFTSPRÜFERKAMMER
Körperschaft des öffentlichen Rechts

WIRTSCHAFTSPRÜFERKAMMER · Postfach 30 18 82 · 10746 Berlin

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Wirtschaftsprüferhaus
Rauchstraße 26
10787 Berlin
Telefon +49 30 726161-0
Telefax +49 30 726161-212
E-Mail kontakt@wpk.de

Rue des Deux Églises 35
1000 Bruxelles
E-Mail bruessel@wpk.de
Internet www.wpk.de

1. Oktober 2018
Ass. jur. Robert Kamm
Durchwahl: **-147**

GG 32/2018/239/904
- bitte stets angeben -

Vorab per E-Mail: innenausschuss@bundestag.de

Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (BR-Drs. 430/18)
Stellungnahme der Wirtschaftsprüferkammer

Sehr geehrte Frau Vorsitzende Lindholz,

anbei dürfen wir Ihnen die Stellungnahme der Wirtschaftsprüferkammer zu o. g. Gesetzentwurf übermitteln (**Anlage**).

Wir bitten höflich um Weiterleitung der Stellungnahme an die Mitglieder Ihres Ausschusses und würden uns wünschen, dass unsere Anregungen in den Ausschussberatungen aufgegriffen werden.

Für Fragen stehen wir Ihnen sehr gern zur Verfügung.

Mit freundlichen Grüßen

Dr. Reiner J. Veidt

RA Dr. Eberhard Richter

Anlage

Geschäftsführer Dr. Reiner J. Veidt Telefon +49 30 726161-100 Telefax +49 30 726161-107 E-Mail reiner.veidt@wpk.de
stellv. Geschäftsführer Dr. Eberhard Richter Telefon +49 30 726161-200 Telefax +49 30 726161-104 E-Mail eberhard.richter@wpk.de

WIRTSCHAFTSPRÜFERKAMMER
Körperschaft des öffentlichen Rechts

Stellungnahme der Wirtschaftsprüferkammer

zum Gesetzesentwurf der Bundesregierung

eines Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU

(BR-Drs. 430/18)

Berlin, den 1. Oktober 2018
GG 32/2018

Ansprechpartner: Ass. jur. Robert Kamm
Wirtschaftsprüferkammer
Postfach 30 18 82, 10746 Berlin
Rauchstraße 26, 10787 Berlin
Telefon 030 726161-147
Telefax 030 726161-287
E-Mail Berufsrecht@wpk.de
www.wpk.de

Die Wirtschaftsprüferkammer ist eine Körperschaft des öffentlichen Rechts, deren Mitglieder alle Wirtschaftsprüfer, vereidigten Buchprüfer, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften in Deutschland sind. Die Wirtschaftsprüferkammer hat ihren Sitz in Berlin und ist für ihre über 21.000 Mitglieder bundesweit zuständig. Ihre gesetzlich definierten Aufgaben sind unter www.wpk.de ausführlich beschrieben. Die Wirtschaftsprüferkammer ist im Transparenzregister der Europäischen Kommission unter der Nummer 025461722574-14 eingetragen.

– – –

Der Entwurf eines Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU) soll das bereichsspezifische Datenschutzrecht an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) anpassen. Zugleich soll die Richtlinie (EU) 2016/680 umgesetzt werden.

Neben im Wesentlichen redaktionellen Änderungen an der Wirtschaftsprüferordnung (WPO, Art. 79 des Referentenentwurfs) enthält der Entwurf in Art. 82 Änderungen am Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHKG), die die Weitergabe von Daten an Dritte (nicht-öffentliche Stellen) und zu Zwecken der Wahlwerbung auf eine sichere Rechtsgrundlage stellen. Die Weitergabe soll auf Grundlage einer Widerspruchslösung erfolgen.

Das neue Datenschutzrecht macht für die Weitergabe von Daten durch die Wirtschaftsprüferkammer an nicht-öffentliche Stellen auch Änderungen an der WPO erforderlich. Vor diesem Hintergrund **empfiehlt es sich, einige der geplanten Änderungen am IHKG auch auf die WPO zu übertragen.**

Konkret regen wir an, **§ 36a WPO um folgende Absätze zu ergänzen:**

> *(6) [1]Die Wirtschaftsprüferkammer darf zur Erfüllung der ihr nach diesem Gesetz übertragenen Aufgaben Daten nach §§ 37, 40a an nicht-öffentliche Stellen übermitteln, sofern das betroffene Mitglied nicht widersprochen hat und der Empfänger der Daten sich gegenüber der Wirtschaftsprüferkammer verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. [2]Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die Mitglieder unbeschadet der weiteren Vorgaben 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 (Daten-*

schutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung vor der ersten Übermittlung schriftlich oder elektronisch hinzuweisen.

(7) [1]An Bewerber und Kandidaten für die Wahl der Beiratsmitglieder nach § 59 dürfen zum Zweck der Wahlbewerbung durch die Bewerber und der Wahlwerbung durch die Kandidaten Name, Firma, Anschrift und E-Mail-Adresse über Wahlberechtigte aus ihrer jeweiligen Gruppe übermittelt werden, sofern der Empfänger der Daten sich gegenüber der Wirtschaftsprüferkammer verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. [2]Bewerber und Kandidaten haben die übermittelten Daten nach der Durchführung der Wahl unverzüglich zu löschen."

Die Absätze entsprechen § 9 Abs. 5 und 6 IHKG-E.

– – –

Wir würden uns freuen, wenn unsere Anregung in den Ausschussberatungen berücksichtigt wird. Inhaltlich haben wir unsere Ausführungen auf Fragestellungen beschränkt, die die Stellung und Funktion der Wirtschaftsprüferkammer und ihrer Mitglieder betreffen.

– – –

An:

Deutscher Bundestag – Innenausschuss

Zur Kenntnisnahme:

Bundesministerium des Innern, für Bau und Heimat

Bundesministerium für Wirtschaft und Energie – Referat Freie Berufe (VII B 3)

Bundesrechtsanwaltskammer

Bundessteuerberaterkammer

Bundesnotarkammer

Patentanwaltskammer

Bundesverband der Freien Berufe

Institut der Wirtschaftsprüfer in Deutschland e. V.

Deutscher Buchprüferverband e. V.

wp.net e. V. Verband für die mittelständische Wirtschaftsprüfung

Deutscher Wirtschaftsprüferverein e. V.

Deutscher Genossenschafts- und Raiffeisenverband e. V.

Deutscher Sparkassen- und Giroverband e. V. (Prüfungsstellen)

Deutscher Steuerberaterverband e. V.

Deutscher Anwaltverein e. V.

Deutscher Notarverein e. V.

Deutscher Richterbund e. V.

European Federation of Accountants and Auditors for SMEs

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)186

Stellungnahme der Bundesärztekammer

zum Regierungsentwurf 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. DSAnpUG-EU)

vom 01.10.2018

Berlin, 05.12.2018

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

A. Vorbemerkung

Mit dem Regierungsentwurf ist eine weitere Anpassung des auf der Bundesebene einschlägigen Datenschutzrechts an die europäische Rechtsentwicklung beabsichtigt. Im Zuge der Anpassung und Umsetzung der Regelungsmöglichkeiten der EU-Datenschutzgrundverordnung 2016/679 (nachfolgend: DSGVO) hatte der Bundesgesetzgeber bereits ein neues Bundesdatenschutzgesetz (nachfolgend: BDSG) verabschiedet, das ebenfalls seit dem 25.05.2018 gilt. Die Bundesärztekammer hatte hierzu im Gesetzgebungsverfahren Stellungnahmen abgegeben.[1]

Weiterer gesetzlicher Anpassungsbedarf ergab sich hinsichtlich der bereichsspezifischen Datenschutzregelungen des Bundes, was nunmehr Gegenstand des Regierungsentwurfs eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (nachfolgend: 2. DSAnpUG-EU) vom 01.10.2018 ist. Der Entwurf umfasst 154 Gesetze. Die vorliegende Stellungnahme würdigt vornehmlich die Gesetze und Vorschriften, die für die Datenverarbeitung im Gesundheitswesen von Bedeutung sind und an welcher Ärzte[2] beteiligt sind. Sie beschränkt sich im Rahmen einer grundlegenden Würdigung des Gesetzesvorhabens auf die wesentlichen Aspekte und unterbreitet konkrete Änderungsvorschläge. Ferner wird auf weiteren Regelungsbedarf im Zusammenhang mit der DSGVO hingewiesen. Soweit gegenüber dem Referentenwurf im Regierungsentwurf keine Änderungen vorgenommen worden sind und unverändert Bedarf zur Bewertung bestimmter Fragen besteht, wird ergänzend und wegen der Einzelheiten auf die Stellungnahme der Bundesärztekammer zum Referentenentwurf eines 2. DSAnpUG-EU Bezug genommen, die als **Anlage** beigefügt wird.[3]

Zugleich erfolgt mit dem Gesetzesentwurf eine Umsetzung der Richtlinie (EU) 2016/680. Dazu erfolgt keine Stellungnahme.

---

1 Stellungnahme der Bundesärztekammer zum Referentenentwurf des Bundesministeriums des Innern zu dem Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 23.11.2016 und Stellungnahme der Bundesärztekammer zum Gesetzesentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU) vom 01.02.2017.

2 Berufs-, Funktions- und Personenbezeichnungen wurden unter dem Aspekt der Verständlichkeit dieses Textes verwendet. Eine geschlechtsspezifische Differenzierung ist nicht beabsichtigt.

3 Stellungnahme der Bundesärztekammer zum Referentenentwurf 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. DSAnpUG-EU) vom 21.06.2018.

B. Stellungnahme der Bundesärztekammer

I. Notwendige Anpassung des Gesundheitsdatenschutzrechts an die EU-Datenschutzgrundverordnung

Am 25.05.2018 ist bereits ein neues Bundesdatenschutzgesetz in Kraft getreten, das auch wesentliche Bestimmungen für die Datenverarbeitung im Gesundheitswesen enthält (§§ 22, 24 BDSG). Hinsichtlich der bestehenden **bereichsspezifischen Datenschutzregelungen** des Bundes ergibt sich gleichwohl ein weiterer gesetzlicher **Anpassungsbedarf**, auf den der Gesetzesentwurf abzielt (vgl. RegE, Seite 1 f.). Die verfolgte Anpassung der bereichsspezifischen Datenschutzgesetze an die DSGVO ist konsequent und im Interesse der Rechtsanwendungssicherheit im Grundsatz erforderlich. Soweit die **elektronische Erklärungsform** neben der schriftlichen Einwilligung in viele Vorschriften übernommen wird, trägt dies der sog. Digitalisierung im Gesundheitswesen angemessen Rechnung.[4] Viele Änderungen beziehen sich darüber hinaus auf **redaktionelle und begriffliche Anpassungen** der vorfindlichen Rechtslage an die DSGVO. Dies ist teilweise notwendig, hat jedoch keine Verbesserungen im Hinblick auf die überaus komplexe Regelungslage im Gesundheitswesen zur Folge.

II. Vereinfachung der Regelungslage im Gesundheitsdatenschutzrecht anstreben

Eine befriedigende Regelungslage für den Gesundheitsdatenschutz kann mit dem Gesetzesentwurf nicht erzeugt werden. Über redaktionelle Anpassungen hinaus wäre auch die Aufrechterhaltung einiger Regelungen zu hinterfragen gewesen, denn der Zustand des stark fragmentierten Gesundheitsdatenschutzrechts bleibt problematisch. Der Gesetzesentwurf erkennt zwar insgesamt das Problem des „stark ausdifferenzierten deutschen Datenschutzrechts“ (vgl. RegE, Seite 2), vermag aber – wie schon das 1. DSAnpUG-EU – dieses Defizit nicht zu beheben. Erstrebenswert wären aber eine Verschlankung der Rechtsmaterie und eine Beseitigung der unübersichtlichen Regelungslage im Bereich des Gesundheitsdatenschutzes.

Ein Ansatzpunkt wäre die **Reduzierung des Umfanges der vielen bereichsspezifischen,** gegenüber dem BDSG vorrangigen[5] **Regelungen**, welche denselben Verarbeitungsvorgang betreffen und bereits durch allgemeine Normen des Gesundheitsdatenschutzes legitimiert werden könnten. So bietet § 22 BDSG bereits hinreichende Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten im Bereich der Gesundheitsvorsorge, medizinischen Diagnostik, ärztlichen Behandlung einschließlich des Austausches von Daten zwischen mehreren Behandlern, ferner zur Qualitätssicherung sowie zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Arzneimitteln und Medizinprodukten. Es wäre vorzugswürdig, auf diese allgemeine Regelung zum Schutz von Gesundheitsdaten zu verweisen, anstatt dieselben Lebenssachverhalte – gleichsam doppelt – vielen Spezialregelungen zu unterwerfen und das undurchsichtige Normenwirrwarr mit den damit verbunden Unsicherheiten bei der Rechtsanwendung aufrechtzuerhalten. Lediglich im Hinblick auf spezifische Aufgabenbeschreibungen und besondere Anforderungen müssten ausdifferenzierte Regelungen dann noch entsprechenden Fachgesetzen vorbehalten bleiben.[6]

---

4 Zum Hinweis auf weitere Erklärungsformen siehe die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter C., VI., 2., Seiten 12 f.

5 § 1 Abs. 2 S. 1 und 2 BDSG.

6 Siehe zum Folgenden und zu den Einzelheiten die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3), Seiten 3 ff., 11 ff.

Zu hinterfragen sind beispielsweise Vorschriften im SGB V, die für Vertragsärzte Sonderregelungen für die Datenverarbeitung in routinemäßigen Behandlungssituationen mit einem unerlässlichen Informationsaustausch zwischen Haus- und Fachärzten zum Zwecke der Dokumentation und der weiteren Behandlung (z. B. § 73 Abs. 1b SGB V), bei der Weiterbehandlung nach einem Krankenhausaufenthalt (§ 39 Abs. 1a S. 11 SGB V) oder für die Qualitätssicherung (§ 299 Abs. 1 SGB V) mit zum Teil abweichenden Anforderungen enthalten. Es ist nicht nachvollziehbar, warum für Ärzte ein spezifisches Datenschutzrecht innerhalb des SGB notwendig ist, wenn der Bundesgesetzgeber im BDSG für gleichgelagerte Verarbeitungszwecke ausreichende Befugnisse zur Verarbeitung von Gesundheitsdaten geschaffen hat. Vereinfachungen der Rechtslage wären in jedem Fall zu begrüßen.

Oftmals wird in den vorgenannten vertragsärztlichen Regelungen auf die **Einwilligung** des Versicherten als Legitimationsgrundlage für die Datenverarbeitung abgestellt. Dieses Instrument ist in Behandlungskontexten aber **meist ungeeignet, weil allenfalls der Schein informationeller Selbstbestimmung erzeugt wird**. Die besondere Situation, in welcher sich Patienten anlässlich einer ärztlichen Behandlung befinden, sowie die unerlässliche Notwendigkeit eines Informationsaustauschs im Rahmen von z. B. besonderen Versorgungsformen lässt die Freiwilligkeit einer Entscheidung des Patienten für die Weitergabe von Daten in Frage stehen. Eine echte Wahl oder ein vordringliches Interesse des Patienten an einer informationellen Selbstbestimmung besteht in diesen Situationen zumeist nicht. Die Zustimmung zur Datenverarbeitung kraft Einwilligung steht damit lediglich auf dem Papier.

Das z. B. in § 73 Abs. 1b SGB V statuierte **Einwilligungserfordernis** steht zudem nicht nur im Widerspruch zu der in § 22 Abs. 1 Nr. 1 BDSG vollzogenen allgemeinen Wertung, eine Verarbeitung von Gesundheitsdaten in typischen Behandlungssituationen aufgrund eines klaren Gesetzes zuzulassen, sondern schafft darüber hinaus einen für die ärztliche Praxis **schwer zu bewältigenden bürokratischen Aufwand**. **Für die angestrebte Digitalisierung** im Gesundheitswesen erscheint dies **kontraproduktiv**. Im Interesse einer praxisgerechten Umsetzung des Datenschutzes im Arzt-Patienten-Verhältnis sowie zur Vereinfachung des Informationsaustausches zwischen mit- und nacheinander behandelnden Ärzten wäre anstelle einer Einwilligung eine klare gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten vorzugswürdig.

Insofern ist der Gesetzgeber dazu berufen, die Entscheidung für eine Datenverarbeitung zu treffen, wie er dies bereits im Rahmen von § 22 BDSG getan hat. Wie dargelegt, erscheint diese Regelung ausreichend, um eine **Datenverarbeitung im Gesundheitswesen auf eine rechtsichere Grundlage zu stellen**. Die Bundesärztekammer empfiehlt daher, insbesondere in den vorgenannten Regelungen, folgenden Verweis auf § 22 BDSG aufzunehmen:

> *„Die Verarbeitung personenbezogener Daten erfolgt gemäß § 22 Absatz 1 Nummer 1 BDSG“.*

III. Bürokratie abbauen und insbesondere datenschutzrechtliche Informationspflichten für Ärzte praxisgerecht regeln

Von erheblicher Bedeutung sind eine Vereinfachung und Praktikabilität des Datenschutzes sowie ein Abbau einer damit verbundenen ausufernden Bürokratie. Insbesondere bedarf es praxisgerechter Ausnahmen hinsichtlich der weitreichenden Informationspflichten, denen Ärzte in der Praxis begegnen. Der Datenschutz sollte das Verhältnis zwischen Arzt und Patient nicht belasten und nicht von den wichtigen Aufgaben der Patientenversorgung abhalten. In einigen Situationen, wie z. B. im Rahmen der telefonischen Terminvereinbarung mit anschließender Datenerhebung oder bei einer zulässigen Fernbehandlung, können Informationspflichten nicht ohne Weiteres umgesetzt werden. Die Erfüllung von Transparenzpflichten bei Datenverarbeitung sollte vor diesem Hintergrund in einem angemessenen Verhältnis zu dem

dazu erforderlichen Aufwand stehen. Sinnvoll und im Interesse der Verhältnismäßigkeit geboten wäre es, die **Erfüllung der Informationspflichten einzuschränken**, was gem. Art. 23 Abs. 1 Buchst. e und i DSGVO im Interesse der Aufrechterhaltung einer wirksamen und effektiven Gesundheitsversorgung als ein wichtiges Gemeinwohlinteresse möglich ist (näher siehe Anlage[7]). Die Bundesärztekammer schlägt eine Regelung vor, die in § 32 Abs. 1 BDSG aufgenommen werden sollte:

> *„Die Pflicht zur Information gemäß Artikel 13 und Artikel 14 der Verordnung (EU) 679/2016 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn die Informationserteilung die ordnungsgemäße Erfüllung der im öffentlichen Interesse liegenden ärztlichen Aufgaben beeinträchtigen würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss."*

IV. Abstimmung des datenschutzrechtlichen Auskunftsrechts mit dem Recht auf Einsichtnahme in die Patientenakte gemäß § 630g BGB

Mehrfach hat die Bundesärztekammer auf den Abstimmungsbedarf datenschutzrechtlicher Regelungen mit anderen Regelungen aus dem Medizinrecht hingewiesen.[8] Mit Blick auf das Recht des Patienten auf Einsichtnahme in seine Patientenakte gem. § 630g BGB ergeben sich Abgrenzungsprobleme zum Auskunftsrecht gem. Art. 15 DSGVO, die der gesetzgeberischen Klarstellung bedürfen. Beide Rechte des Patienten verfolgen dieselbe Zielrichtung und stehen in Konkurrenz. § 630g BGB stellt eine Spezialregelung gem. Art. 23 Abs. 1 Buchst. i DSGVO bzw. Art. 9 Abs. 4 DSGVO dar.

Es sollte klargestellt werden, dass Ärzte die datenschutzrechtliche Auskunftspflicht durch die Gewährung der Einsichtnahme in die Patientenakte oder durch Aushändigung einer Kopie gem. § 630g BGB erfüllen können (näher siehe Anlage[9]). In das BDSG sollte daher entsprechend Art. 17 Nr. 2 (§ 68a Personenstandgesetz) des 2. DSAnpUG-EU folgende Regelung aufgenommen werden:

> „*Das Auskunftsrecht nach Artikel 15 Absatz 1 und das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) werden dadurch gewährleistet, dass der betroffenen Person unter den Voraussetzungen von § 630g Absatz 1 und 2 des Bürgerlichen Gesetzbuches Einsicht in die sie betreffende Patientenakte zu gewähren ist.*"

V. Notwendige Abstimmung von Löschpflichten und Verjährungsfristen

Im Interesse eines rechtssicheren Handelns im ärztlichen Alltag wäre eine klare Regelung zur zulässigen Dauer der Aufbewahrung von Patientendaten unter Berücksichtigung von zivilrechtlichen Verjährungsfristen notwendig. Zwar stellen Art. 17 Abs. 3 Buchst. b DSGVO und § 35 Abs. 3 BDSG für den wichtigen Fall der gesetzlichen, satzungsgemäßen oder vertraglichen Aufbewahrungspflicht sicher, dass Patientendaten nicht zu löschen sind. Nach Abschluss der Behandlung ist in der Regel eine 10-jährige Aufbewahrungsdauer für Patientenunterlagen zu

---

7 Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter D., I., Seite 19.

8 Stellungnahme der Bundesärztekammer zum RegE zum DSAnpUG-EU (Fn. 1), Seiten 4, 21 und Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter D., II., Seite 20.

9 Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter D., II., Seite 20.

beachten (§ 630f Abs. 3 BGB, vgl. § 10 Abs. 3 MBO-Ä), soweit nicht nach besonderen Vorschriften längere Aufbewahrungsfristen zu beachten sind. Die Patienten wären nach Ablauf dieser Frist zu löschen; sie sind für die Behandlung nicht mehr erforderlich (Art. 5 Abs. 1 Buchst. e und Art. 17 Abs. 1 Buchst. a DSGVO). Allerdings könnte die Patientendokumentation unter Umständen noch zur späteren Verteidigung von Rechtsansprüchen in potentiellen Behandlungsfehlerprozessen relevant werden, wobei etwaige Ansprüche erst nach 30 Jahren verjähren (§ 199 Abs. 2 BGB). Dem Arzt würden in diesem Fall nach Ablauf der 10-jährigen Aufbewahrungsfrist wichtige Beweismittel in einem möglichen Prozess und Gedächtnisstützen zu dem Behandlungsfall genommen. Er könnte sich nicht mehr sachangemessen verteidigen und seine justiziellen Rechte wären beschränkt. Dass es nach Ablauf der 10-jährigen Aufbewahrungsfrist nicht mehr zu Beweiserleichterungen zugunsten des Patienten kommen soll,[10] ändert nichts daran, dass die Notwendigkeit besteht, sich zur Durchsetzung der eigenen rechtlichen Interessen überhaupt zu dem Behandlungsfall kundig machen zu können, was unmöglich wäre, wenn die Dokumentation unwiederbringlich gelöscht wurde. Art. 17 Abs. 3 Buchst. e DSGVO, der eine Ausnahme von der Löschpflicht bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen statuiert, dürfte dabei erst zur Anwendung gelangen, wenn es hinreichende Anhaltspunkte für eine entsprechende rechtliche Auseinandersetzung gibt. Potentielle Rechtsstreitigkeiten erfasst die Regelung nicht, weil die bloß abstrakte Möglichkeit rechtlicher Auseinandersetzungen nicht genügt.[11]

Die Vernichtung von Patientenunterlagen nach Ablauf der Aufbewahrungszeit z. B. gemäß der Berufsordnung ist vor diesem Hintergrund problematisch und § 35 Abs. 3 BDSG ist als Ausnahmeregelung unzureichend. Sinnvoll wäre es, wenn es gesetzlich klargestellt werden würde, dass die Verarbeitung der Patientendaten nach Ablauf der 10-jährigen Aufbewahrungsfrist zu bis zum Ablauf gesetzlicher Verjährungsfristen beschränkt werden kann. § 35 Abs. 3 BDSG könnte folgender Satz 2 angefügt werden:

> *„Absatz 1 kommt entsprechend zur Anwendung, soweit der Löschung gesetzliche Verjährungsfristen entgegenstehen.*

Damit würden auch die „schutzwürdigen Interessen" des Verantwortlichen berücksichtigt. Eine gesetzliche Ausnahmeregelung ließe sich auf Art. 23 Abs. 1 Buchst. i oder j DSGVO stützen.

VI. Keine Pflicht zur Benennung eines Datenschutzbeauftragten in Arztpraxen

Die Pflicht zur Benennung eines Datenschutzbeauftragten ist in kleineren Einrichtungen der Gesundheitsversorgung organisatorisch sowie mit Blick auf die anfallenden Kosten unverhältnismäßig. Eine Entlastung für diese Unternehmen wäre sinnvoll. Mit der Regelung des § 38 BDSG stellt der Bundesgesetzgeber aber sogar geringere Anforderungen als Art. 37 Abs. 1 Buchst. b DSGVO auf, sodass häufiger ein Datenschutzbeauftragter benannt werden muss. Wie der Ausschuss für Innere Angelegenheiten des Bundesrates zutreffend festgestellt hat und von vielen Wirtschaftsverbänden bestätigt wird, werden insbesondere die **kleinen und mittleren Unternehmen sowie Freiberufler, übermäßig, vor allem finanziell, von der Pflicht belastet**.[12] Das gilt insbesondere, weil immer mehr Geschäftsprozesse digitalisiert werden und demnach viele kleinere Unternehmen bereits einen Datenschutzbeauftragten zu benennen hätten, ohne dass es – wie von der DSGVO vorausgesetzt – auf das erhöhte Risiko für die Rechte des Betroffenen ankommt. Es sollten Erleichterungen gesetzlich geregelt werden für Unternehmen, bei welchen die Datenverarbeitung nicht schwerpunktmäßig zur Kerntätigkeit ihres geschäftlichen Wirkens zählt.

---

10 Vgl. OLG Hamm, Urt. v. 29.01.2003 – 3 U 91/02.
11 Vgl. *Herbst*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 17, Rn. 83.
12 BR-Drs. 430/1/18, Seite 3 ff.

Die Bundesärztekammer befürwortet daher die folgenden Vorschläge des Innenausschusses des Bundesrates, nach denen § 38 S. 1 BDSG wie folgt gefasst werden soll:

> *„Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen und die Verarbeitung gewerblichen Zwecken dient."*

Hilfsweise ist § 38 S. 1 BDSG wie folgt zu fassen:

> *„Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 50 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen."*

Darüber hinaus ist die **europarechtswidrige Vorschrift des § 38 S. 2 BDSG zu streichen**, weil sie die Anforderungen an die Benennungspflicht gegenüber Art. 37 Abs. 1 Buchst. c DSGVO unzulässig modifiziert und letztlich eine wichtige Voraussetzung umgeht. Das zusätzliche Merkmal der „Kerntätigkeit" muss wegen des Verweises auf die Voraussetzungen der Pflicht zur Durchführung einer Datenschutzfolgenabschätzung (Art. 35 Abs. 3 Buchst. b DSGVO) – anders als im Rahmen von Art. 37 Abs. 1 Buchst. c DSGVO – nicht erfüllt sein. Ein Datenschutzbeauftragter muss also unabhängig von der Frage der Kerntätigkeit schon dann bestellt werden, wenn nur eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt und deswegen eine Datenschutzfolgenabschätzung durchzuführen ist. Die Vorschrift steht damit nicht im Einklang mit der DSGVO (siehe Anlage[13]).

VII. Patientengeheimnisschutz auch bei Tätigkeiten externer Datenschutzbeauftragter sicherstellen

Zudem sollten auch externe Datenschutzbeauftragte der strafbewehrten Schweigepflicht unterstellt werden, da diese aus Anlass ihrer Tätigkeit für Ärzte mit Patientengeheimnissen in Berührung kommen können. Patientengeheimnisse müssen in deren Sphäre ebenfalls geschützt werden. **Die bestehende Schutzlücke ist zu schließen**. § 203 Abs. 4 S. 1 StGB ist mit Blick auf Art. 37 Abs. 6 DSGVO entsprechend anzupassen, indem im zweiten Satzteil die Worte „*bei den*" durch die Worte „*für die*" ersetzt werden. Der Satzteil lautet dann:

> *„[…] oder als <u>für die</u> in den Absätzen 1 und 2 genannten Personen tätiger Datenschutzbeauftragter bekannt geworden ist."*[14]

VIII. Keine Abmahnungen wegen Verstößen gegen datenschutzrechtliche Informationspflichten

Abmahnungen von Datenschutzverstößen stellen keine tauglichen Mittel dar, um einen besseren Datenschutz zu erreichen. Die Einhaltung des Datenschutzes kann besser und wirksam durch die zuständigen Aufsichtsbehörden für den Datenschutz überwacht und durchgesetzt werden. Für die Durchsetzung des Datenschutzrechts sieht die DSGVO zudem empfindliche Sanktionen vor, sodass der Datenschutz auf diesem Wege sichergestellt werden kann.

---

13 Siehe zu den Einzelheiten die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter C., I., 2., Seite 7.

14 Siehe zu den Einzelheiten die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter C., IV., Seiten 9 f.

Vor allem mit Blick auf das abschließende Sanktionssystem der DSGVO sind **Datenschutzverstöße** nach der vorzugswürdigen Auffassung in der Rechtsprechung und juristischen Literatur **nicht nach dem UWG abmahnfähig**. Weil diese Frage zur Zeit aber sehr kontrovers beurteilt wird,[15] regt die Bundesärztekammer eine gesetzliche Klarstellung im UWG an, um Rechtssicherheit zu erzeugen. In Anlehnung an den Vorschlag aus dem Land Bayern für einen „Entwurf eines Gesetzes zur Anpassung zivilrechtlicher Vorschriften an die Datenschutz-Grundverordnung" (BR-Drs. 304/18) sollte an § 3a UWG folgender Satz angefügt werden:

> *„Die Datenschutzvorschriften stellen keine Marktverhaltensregelungen im Sinne von Satz 1 dar"*

Jedenfalls sollten aber bloße **Verstöße gegen datenschutzrechtliche Informationspflichten** oder marginale Fehler bei der Erstellung nicht abmahnfähig sein oder zivilrechtliche Drittansprüche auslösen. Das gilt insbesondere in Ansehung der komplexen Rechtslage im Gesundheitsdatenschutzrecht, die es schwierig werden lässt, stets die jeweilige Rechtsgrundlage für alle in Betracht kommenden Datenverarbeitungsschritte zutreffend anzugeben. An § 3a UWG daher folgender Satz angefügt werden:

> *„Die Datenschutzvorschriften nach Artikel 13 und 14 der Verordnung (EU) 2016/679 stellen keine Marktverhaltensregelungen im Sinne von Satz 1 dar"*

Ferner sollten missbräuchliche Abmahnungen durch Unternehmen, die damit eigene Geschäftszwecke verfolgen, eingedämmt werden, wie dies mit dem Gesetz zur Stärkung des fairen Wettbewerbs geplant ist.

IX. Keine Übertragung datenschutzrechtlicher Pflichten der Unfallversicherungsträger auf Ärzte

Die mit Art. 128 Nr. 9 Buchst. b) des 2. DSAnpUG-EU beabsichtigte Änderung von § 201 Abs. 1 S. 3 SGB VII-E, infolgedessen die originär den Unfallversicherungsträgern obliegenden datenschutzrechtlichen Pflichten zur Auskunftserteilung auf Ärzte übertragen werden, ist unzulässig und abzulehnen. Die Formulierung „*Für die Unterrichtung des Versicherten aufgrund seines Auskunftsrechts nach Artikel 15 [DSGVO] gilt § 25 Absatz 2 des Zehnten Buches entsprechend*" ist jedenfalls missverständlich, als sie das Auskunftsrecht durch den Verweis auf § 25 Abs. 2 SGB X auf den Arzt zu übertragen scheint. Die beabsichtigte **Neuregelung widerspricht damit dem Prinzip der Verantwortlichkeit nach der DSGVO**, denn datenschutzrechtliche Pflichten können nicht vom Verantwortlichen ohne Weiteres auf andere verlagert werden (siehe auch Anlage[16]). § 201 Abs. 1 S. 3 SGB VII-E ist europarechtswidrig und aus diesem Grund wie folgt zu ändern:

> *„Soweit der Versicherte sein Auskunftsrecht nach Artikel 15 der Verordnung (EU) 2016/679 über die von den Ärzten und den Psychotherapeuten übermittelten Angaben zu seinen gesundheitlichen Verhältnissen gegenüber dem Unfallversicherungsträger geltend macht, gilt § 25 Absatz 2 des Zehnten Buches entsprechend."*

Auch die mit Art. 128 Nr. 5 und Nr. 11 des 2. DSAnpUG-EU beabsichtigten Änderungen zu § 188 S. 3 SGB VII-E und § 203 Abs. 2 SGB VII-E zur Übertragung datenschutzrechtlicher Pflichten der Leistungsträger auf Ärzte sind – wie § 201 Abs. 1 S. 3 SGB VII-E – nicht mit der DSGVO zu vereinbaren und daher im vorstehenden Sinne zu ändern.

---

[15] Siehe einerseits Landgericht Bochum, Urt. v. 7.8.2018 – I-12 O 85/18; Landgericht Wiesbaden, Urt. v. 5.11.2018 – 5 O 214/18; andererseits aber andere Ansicht Landgericht Würzburg, Beschl. v. 13.9.2018 – 11 O 1741/18 UWG).

[16] Siehe zu den Einzelheiten die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter C., VII., 1., Seiten 16 ff.; siehe zu Art. 128 Nr. 5 (§ 188 S. 3 SGB VII-E) und Nr. 11 (§ 203 Abs. 2 SGB VII-E) des 2. DSAnpUG-EU ebd., Seite 18.

X. Ausnahmeregelungen für ärztliche Berufsgeheimnisträger im BKA-Gesetz aufnehmen

Ein weiteres bereichsspezifisches Datenschutzgesetz ist das BKA-Gesetz. Bezogen auf Berufsgeheimnisträger bedarf es dringend der Anpassung an die verfassungsrechtlichen Anforderungen. Unter Berücksichtigung der von Verfassungs wegen besonders geschützten Vertraulichkeit im Arzt-Patienten-Verhältnis besteht ein gesteigerter Schutzbedarf für die Berufsgruppe der Ärzte. Der Schutz des Kernbereichs privater Lebensgestaltung muss hinreichend geschützt werden. In diesem Sinne **muss die Arzt-Patienten-Beziehung absolut vor Überwachungsmaßnahmen gem. dem BKA-Gesetz geschützt werden** und nicht nur einer Abwägungsentscheidung im Einzelfall überlassen sein. Ärzte sind daher in den Kreis besonders geschützter Personengruppen und in die Ausnahmeregelung des § 62 BKAG aufzunehmen (siehe Anlage[17]).

C. Synopse zu weiteren Anmerkungen

RegE	***RefE***	***Inhalt***	***Stellungnahme der Bundesärztekammer zum RefE***
Art. 16 Nr. 1) b) bb) aaa) (§ 40 AMG)	Art. 18 Nr. 1) b) bb) aaa) (§ 40 AMG)	Zusätzliche (wiederholte) Informationspflicht über Widrrufbarkeit der Einwilligung	Zur Kritik der BÄK s. C., II., 1. (Seite 8 f.)
Art. 21 Nr. 1 (§ 8 Abs. 1 GenDG)	Art. 23 Nr. 1 (§ 8 Abs. 1 GenDG)	Klarstellung zur Einwilligung	Zur Zustimmung der BÄK s. C., III., 1 (Seite 9)
Art. 21 Nr. 3 (§ 26 GenDG)	Art. 23 Nr. 4 (§ 26 GenDG)	Bereinigung des Bußgeldtatbestandes	Zur Zustimmung der BÄK s. C., III., 2 (Seite 9)
Art. 120 Nr. 6 c) (§ 39 SGB V)	Art. 123 Nr. 6 c) (§ 39 SGB V)	Schriftform der Informationserteilung	Zur Kritik der BÄK s. C., VI., 2 (Seite 13)

[17] Siehe ausführlich die Stellungnahme der Bundesärztekammer zum RefE zum 2. DSAnpUG-EU (Fn. 3) unter D., III., Seiten 21 f.

Anlage

Stellungnahme der Bundesärztekammer

zum Referentenentwurf 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. DSAnpUG-EU)

vom 21.06.2018

Berlin, 16.07.2018

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

A. Vorbemerkung

Mit dem Referentenentwurf ist eine weitere Anpassung des auf der Bundesebene einschlägigen Datenschutzrechts an die europäische Rechtsentwicklung beabsichtigt. Seit dem 25.05.2018 gilt die EU-Datenschutzgrundverordnung 2016/679 (nachfolgend: DSGVO) allgemein und unmittelbar in allen Mitgliedstaaten der Europäischen Union. Sie dient der Angleichung des Datenschutzrechts in Europa. Die DSGVO räumt dem nationalen Gesetzgeber jedoch insbesondere für den Bereich der Verarbeitung von Gesundheitsdaten Regelungsmöglichkeiten durch zahlreiche Ausgestaltungs-, Konkretisierungs- und Ergänzungsklauseln sowie Regelungsaufträge und -optionen für Ausnahmen ein. Im Zuge der Anpassung und Umsetzung der Regelungsmöglichkeiten der DSGVO hatte der Bundesgesetzgeber bereits ein neues Bundesdatenschutzgesetz (nachfolgend: BDSG) verabschiedet, das ebenfalls seit dem 25.05.2018 gilt. Die Bundesärztekammer hatte hierzu im Gesetzgebungsverfahren Stellungnahmen abgegeben.[1]

Weiterer gesetzlicher Anpassungsbedarf ergab sich hinsichtlich der bereichsspezifischen Datenschutzregelungen des Bundes, was nunmehr Gegenstand des am 21.06.2018 bekannt gewordenen Referentenentwurfs des Bundesministeriums des Innern, für Bau und Heimat eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (nachfolgend: „2. DSAnpUG-EU") ist. Der Referentenentwurf umfasst 152 Gesetze. Die vorliegende Stellungnahme würdigt vornehmlich die Gesetze und Vorschriften, die für die Datenverarbeitung im Gesundheitswesen von Bedeutung sind, an welcher Ärzte[2] beteiligt sind.

Zugleich erfolgt mit dem Referentenentwurf eine Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (nachfolgend: JI-Richtlinie). Zur Umsetzung der der Richtlinie (EU) 2016/680 erfolgt keine Stellungnahme.

Im Rahmen der vorliegenden Stellungnahme erfolgt zunächst eine grundlegende Bewertung des Gesetzesvorhabens und eine Zusammenfassung der gesamten Stellungnahme (s. dazu B.) bevor auf einzelne Aspekte der im Referentenentwurf bearbeiteten Gesetze eingegangen wird und zum Teil konkrete Änderungshinweise oder Regelungsvorschläge unterbreitet werden (s. dazu C.). Abschließend wird ergänzend auf einen bislang außer Acht gelassen, aber notwenigen Regelungsbedarf im Zusammenhang mit der DSGVO hingewiesen (s. dazu D.).

---

1 Stellungnahme der Bundesärztekammer zum Referentenentwurf des Bundesministeriums des Innern zu dem Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 23.11.2016 und Stellungnahme der Bundesärztekammer zum Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU) vom 01.02.2017.

2 Berufs-, Funktions- und Personenbezeichnungen wurden unter dem Aspekt der Verständlichkeit dieses Textes verwendet. Eine geschlechtsspezifische Differenzierung ist nicht beabsichtigt.

B. Grundlegende Bewertung und Zusammenfassung

Notwendige Anpassung des Gesundheitsdatenschutzrechts an die EU-Datenschutzgrundverordnung

Am 25.05.2018 ist bereits ein neues Bundesdatenschutzgesetz in Kraft getreten, das auch wesentliche Bestimmungen für die Datenverarbeitung im Gesundheitswesen enthält (§§ 22, 24 BDSG). Hinsichtlich der bestehenden **bereichsspezifischen Datenschutzregelungen** des Bundes ergibt sich gleichwohl ein weiterer gesetzlicher **Anpassungsbedarf**, auf den der Referentenentwurf abzielt (vgl. RefE, S. 1). Es ist erforderlich, das bereichsspezifische Datenschutzrecht im Gesundheitswesen im Hinblick auf seine Vereinbarkeit mit der DSGVO zu überprüfen und, soweit erforderlich, Vorschriften anzupassen oder aufzuheben.

Insoweit ist jedenfalls die verfolgte Anpassung der bereichsspezifischen Datenschutzgesetze konsequent und im Interesse der Rechtsanwendungssicherheit im Grundsatz erforderlich. Viele Änderungen beziehen sich auf die Anpassungen an neue Begriffe der DSGVO. Beispielsweise wird anstelle der die Phasen der Datenverarbeitung präzise beschreibenden Begriffe des „Erhebens", „Verarbeitens", „Nutzens" (vgl. § 3 Abs. 3 bis 5 BDSG a. F.) der einheitliche Begriff der „Verarbeitung" (Art. 4 Nr. 2 DSGVO) verwendet. Es erfolgen damit **redaktionelle und begriffliche Anpassungen** der vorfindlichen Rechtslage an die DSGVO. Dies ist teilweise notwendig, hat jedoch keine Verbesserungen im Hinblick auf die komplexe Regelungslage im Gesundheitswesen zur Folge.

Vereinfachung der Regelungslage im Gesundheitsdatenschutzrecht anstreben

Ein widerspruchsfreies Regelungswerk für den Gesundheitsdatenschutz kann mit dem vorliegenden Referentenentwurf nicht erzeugt werden. Über redaktionelle Anpassungen hinaus wäre auch die Aufrechterhaltung einiger Regelungen zu hinterfragen gewesen, denn der Zustand des stark fragmentierten Gesundheitsdatenschutzrechts bleibt problematisch. Der Referentenentwurf erkennt zwar insgesamt das Problem des „stark ausdifferenzierten deutschen Datenschutzrechts" (vgl. RefE, S. 1), vermag aber – wie schon das 1. DSAnpUG-EU – dieses Defizit nicht zu beheben. Erstrebenswert wäre eine Verschlankung der Rechtsmaterie und eine Beseitigung der unübersichtlichen Regelungslage.

Im Hinblick auf die Verarbeitung von Gesundheitsdaten i. S. v. Art. 9 Abs. 1 DSGVO ist die DSGVO keineswegs abschließend. Die zahlreichen Öffnungsklauseln in Art. 9 Abs. 2 DSGVO lassen ein weitergehendes gesetzgeberisches Handeln zu. Die Bundesärztekammer hatte dementsprechend schon anlässlich des Regierungsentwurfes zum 1. DSAnpUG-EU vorgeschlagen, ein **konsistentes Gesundheitsdatenschutzgesetz** zu schaffen,[3] das die wesentlichen Grundsätze für die Datenverarbeitung im Gesundheitswesen enthält und nur im Hinblick auf spezifische Aufgabenbeschreibungen und besondere Anforderungen den entsprechenden Fachgesetzen Regelungen vorbehält. Damit wäre eine Reduzierung des Umfanges der vielen bereichsspezifischen Regelungen für den Gesundheitsdatenschutz möglich. Zwar bleiben die zahlreichen Regelungen zum Gesundheitsdatenschutz im Kompetenzbereich der Bundesländer davon unberührt. Auch die Länder müssen ihre spezifischen Datenschutzvorschriften (ggf. Landeskrankenhausgesetze und Heilberufe- und Kammergesetze) an die DSGVO anpassen. Sie könnten aus diesem Anlass ebenfalls den Weg wählen, auf ein allgemeines Gesundheitsdatenschutzgesetz zu verweisen, anstatt dieselben Lebenssachverhalte einer eigenen Regelung zu unterwerfen.

[3] Vgl. Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 3, 13.

Jedenfalls auf der Bundesebene könnte aber eine Vereinfachung der Regelungslage erreicht werden. Es stellt sich hierzu die Frage, inwieweit es bestimmter Spezialregelungen in Fachgesetzen noch bedarf. Es ist eine Prüfung erforderlich, welche Einzelregelungen aufgehoben werden könnten, weil die von ihnen betroffenen Sachverhalte bereits unter die allgemeinen Vorschriften des § 22 BDSG subsumiert werden könnten. Einige Gesetze regeln spezifische Sachverhalte, die ebenso von § 22 Abs. 1 Nr. 1 BDSG erfasst werden. In Kenntnis des § 1 Abs. 2 S. 1 und 2 BDSG hat die Bundesärztekammer auf solche Friktionen anlässlich der Gesetzgebung zu einem neuen Bundesdatenschutzgesetz bereits hingewiesen.[4] Wegen der vom Bundesgesetzgeber vorgezogenen weiten Tatbestände in § 22 Abs. 1 Nr. 1 BDSG sind einige bereichsspezifische Regelungen nun aber augenscheinlich nicht mehr erforderlich. Jedenfalls sollten Auslegungs- sowie Abgrenzungsprobleme vermieden und Unsicherheiten bei der Rechtsanwendung vorgebeugt werden.

Im Rahmen des gewählten Vorgehens des Bundesgesetzgebers, mit dem BDSG ein Auffanggesetz mit allgemeinen Generalklauseln zu schaffen,[5] bietet es sich als Alternative zu einer Gesamtkodifikation für den Gesundheitsdatenschutz jedenfalls an, auf die allgemeinen Regelungen im BDSG Bezug zu nehmen. Möglich wäre eine **Referenz auf § 22 BDSG**, der z. B. die Gesundheitsvorsorge, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheitsbereich oder die Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten als zulässigen Verarbeitungszweck aufführt. Anstelle einer Spezialregelung kann also ein vermehrter Rückgriff bzw. Verweis auf die allgemeinen Tatbestände des BDSG erfolgen. Das wäre auch in anderen Bereichen möglich, wo der Verarbeitungszweck nicht über die in § 22 BDSG aufgeführten Zwecke hinausgeht. Zu hinterfragen sind damit viele Vorschriften im SGB V, die für Vertragsärzte Sonderregelungen für die Datenverarbeitung in Behandlungssituationen (z. B. § 73 Abs. 1b SGB V) oder für die Qualitätssicherung (§ 299 Abs. 1 SGB V) enthalten. Im Interesse einer praxisnahen Umsetzung des Datenschutzes im Arzt-Patienten-Verhältnis sowie zur Erleichterung des Informationsaustausches zwischen Ärzten wäre **anstelle einer Einwilligung eine klare gesetzliche Grundlage** für die Verarbeitung von Gesundheitsdaten vorzugswürdig (s. näher unter C., VI.). Eine solche ist mit § 22 BDSG gegeben. Es ist daher zu prüfen, inwieweit bereichsspezifische Regelungen in einigen Bereichen noch erforderlich sind.

Schaffung von Rechtsgrundlagen für die Datenverarbeitung einschließlich des Informationsaustausches zur Erfüllung gesetzlicher Aufgaben

Überdies bedarf es der Schaffung von Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten und den Informationsaustausch für Bereiche, in denen bislang keine hinreichenden Rechtsgrundlagen für die Erfüllung von Aufgaben bestehen (s. dazu insbesondere unter C., II., 2.).

Ferner sollte der Anwendungsbereich von Rechtsgrundlagen mit unbestimmten Rechtsbegriffen jedenfalls in der Gesetzesbegründung näher umschrieben werden, damit bei deren Anwendung im Gesundheitsbereich hinreichende Rechtssicherheit besteht (s. dazu insbesondere unter C., I., 1).

---

[4] Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 8 und 9 f.

[5] S. dazu schon die Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 7 f. und passim.

Keine Übertragung datenschutzrechtlicher Pflichten von Leistungsträgern auf Ärzte

Die mit den beabsichtigten Änderungen im SGB VII verbundene Übertragung der den Unfallversicherungsträgern originär obliegenden datenschutzrechtlichen Pflichten auf Ärzte ist abzulehnen. Dies sollte in zutreffender Weise in den entsprechenden Regelungen abgebildet werden (s. dazu näher unter C., VII., 1.).

Bürokratie abbauen und insbesondere datenschutzrechtliche Informationspflichten für Ärzte praxisgerecht regeln

Von erheblicher Bedeutung ist eine Vereinfachung und Praktikabilität des Datenschutzes sowie ein Abbau einer damit verbundenen Bürokratie. Das z. B. in § 73 Abs. 1b SGB V statuierte Einwilligungserfordernis steht nicht nur im Widerspruch zu der in § 22 Abs. 1 Nr. 1 BDSG vollzogenen Wertung, eine Verarbeitung von Gesundheitsdaten in typischen Behandlungssituationen aufgrund eines Gesetzes zuzulassen, sondern schafft darüber hinaus einen für die ärztliche Praxis schwer zu bewältigenden bürokratischen Aufwand (s. dazu C., VI., 1.). Insgesamt sollte der Datenschutz das Vertrauensverhältnis zwischen Arzt und Patient nicht belasten und von den Aufgaben der Patientenversorgung abhalten. Aus ähnlichen Gründen bedarf es praxisgerechter Ausnahmen hinsichtlich der weitreichenden Informationspflichten, die Ärzte in der Praxis treffen (s. dazu auch unter D., I.).

Abstimmung des datenschutzrechtlichen Auskunftsrechts mit dem Recht auf Einsichtnahme in die Patientenakte gemäß § 630g BGB

Bereits in der Stellungnahme zum 1. DSAnpUG-EU hatte die Bundesärztekammer auf den Abstimmungsbedarf mit anderen Regelungen aus dem Medizinrecht hingewiesen.[6] Mit Blick auf das Recht des Patienten auf Einsichtnahme in seine Patientenakte gem. § 630g BGB ergeben sich Abgrenzungsprobleme zum Auskunftsrecht gem. Art. 15 DSGVO, die der gesetzgeberischen Klarstellung bedürfen. Beide Rechte des Patienten verfolgen dieselbe Zielrichtung und stehen in Konkurrenz. Es sollte klargestellt werden, dass Ärzte ihr datenschutzrechtliches Auskunftsrecht durch die Gewährung der Einsichtnahme in die Patientenakte oder durch Aushändigung einer Kopie gem. § 630g BGB erfüllen können (s. D., II.).

Ausnahmeregelungen für ärztliche Berufsgeheimnisträger im BKA-Gesetz aufnehmen

Unter Berücksichtigung der von Verfassungs wegen besonders geschützten Vertraulichkeit im Arzt-Patienten-Verhältnis besteht ein gesteigerter Schutzbedarf für die Berufsgruppe der Ärzte. Daher muss die Arzt-Patienten-Beziehung absolut vor Überwachungsmaßnahmen gem. dem BKA-Gesetz geschützt werden und nicht nur einer Abwägungsentscheidung im Einzelfall überlassen sein. Ärzte sind daher in den Kreis besonders geschützter Personengruppen und in die Ausnahmeregelung des § 62 BKAG aufzunehmen (s. dazu unter D., III.).

[6] Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 4, 21.

Eindämmung missbräuchlicher Abmahnungen wegen Verstößen gegen datenschutzrechtliche Informationspflichten

Bloße Verstöße gegen datenschutzrechtliche Informationspflichten sollten keine zivilrechtlichen Ansprüche Dritter begründen können und missbräuchliche Abmahnungen durch Unternehmen zu eigenen Geschäftszwecken sollten eingedämmt werden. Die Einhaltung des Datenschutzes kann wirksam durch die zuständigen Aufsichtsbehörden für den Datenschutz überwacht und durchgesetzt werden (s. dazu D., IV.).

C. Stellungnahme im Einzelnen

I. Artikel 10 (Bundesdatenschutzgesetz)

1. Zu Nummer 5 (§ 22 Abs. 1 S. 1 Nr. 1 lit. d BDSG-E)

a. Beabsichtigte Neuregelung

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO soll nunmehr auch für nichtöffentliche Stellen im Interesse eines „erheblichen öffentlichen Interesses" zulässig sein. Dazu wird § 22 Abs. 1 S. 1 Nr. 1 um den Buchstaben d ergänzt.

Die Änderung ermöglicht ausweislich der Begründung im Referentenentwurf den auch im öffentlichen Interesse tätigen privaten Trägern, sensible Daten zu verarbeiten und ihrem Beratungsauftrag nachzukommen. Nichtöffentliche Stellen, die solche Daten geschäftsmäßig im Rahmen eigener gewerblicher Geschäftsmodelle verarbeiten, sollen ihre Datenverarbeitung hingegen nicht auf die neue Befugnisnorm stützen können, da das von der Norm geforderte zwingende Erfordernis eines erheblichen öffentlichen Interesses in diesen Fällen bereits tatbestandlich nicht vorliegt. Insgesamt schaffe die Vorschrift Rechtssicherheit für die nichtöffentlichen Stellen, die sensible Daten mit Sicherheitsrelevanz verarbeiten. Weil die Verarbeitung gem. Art. 9 Abs. 2 lit. g DSGVO in einem angemessenem Verhältnis zu dem verfolgten Ziel stehen muss, wird § 22 Abs. 1 S. 1, Nr. 1 lit. d BDSG-E in die Interessenabwägung i. S. v. § 22 Abs. 1 S. 1 BDSG-E mit einbezogen (vgl. RefE, S. 242).

b. Stellungnahme der Bundesärztekammer

Die Regelung ermöglicht vom Wortsinn her auch Arztpraxen oder anderen nichtöffentlichen Stellen die Verarbeitung von Gesundheitsdaten aus Gründen eines „erheblichen öffentlichen Interesses". Inwieweit von diesem unbestimmten Rechtsbegriff auch ärztliche Tätigkeiten erfasst werden, ist mangels aufschlussreicher Gesetzesbegründung nicht klar.[7] Zwar werden Ärzte die Daten ihrer Patienten regelmäßig *auch* geschäftsmäßig im Rahmen ihrer Gewinnerzielung bzw. eigener geschäftlicher Zwecke verarbeiten. Zugleich werden sie dabei aber häufig im öffentlichen Interesse tätig. Im öffentlichen Interesse liegen grundsätzlich alle Belange, die für die Gemeinschaft und Bevölkerung von Bedeutung sind. Sie sind erheblich, soweit sie dabei von besonderem Gewicht sind. Wichtige Gründe des öffentlichen Interesses sind nach Erwägungsgrund 46 der DSGVO beispielsweise „die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren

[7] Zur Kritik s. bereits die Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 11.

Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen". Erwägungsgrund 52 führt darüber hinaus als „öffentliche Interessen" u. a. die „Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren" an. In der Begründung zu Art. 10 Nr. 5 des 2. DSAnpUG-EU sollte daher deutlicher klargestellt werden, dass auch weitere „erhebliche öffentlichen Interessen" bei der Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO in Betracht kommen und es sollten exemplarisch auch solche aus dem Gesundheitsbereich aufgeführt werden.

c. Änderungshinweise der Bundesärztekammer

In der Begründung sollte deutlicher klargestellt werden, welche „erheblichen öffentlichen Interessen" bei der Verarbeitung besonderer Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO in Betracht kommen. Anstelle einer Beschränkung auf den bislang hervorgehobenen „Sicherheitsbereich" sollten Anwendungsfälle für den Gesundheitsbereich in der Begründung aufgenommen werden (z. B. die Datenverarbeitung im Rahmen der Subsitutionsbehandlung, des Infektionsschutzes, der Bekämpfung von Pandemien oder im Rahmen des Katastrophenschutzes).

2. Weitere notwenige Änderungen des Bundesdatenschutzgesetzes

a. Bestehende Regelung des § 38 S. 2 BDSG

§ 38 S. 2 BDSG regelt in Abweichung von Art. 37 Abs. 1 DSGVO und gestützt auf Art. 37 Abs. 4 DSGVO die Pflicht zur Benennung eines Datenschutzbeauftragten. Verantwortliche haben danach unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen, wenn sie Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen.

b. Stellungnahme der Bundesärztekammer

Art. 35 Abs. 3 lit. b DSGVO nimmt tatbestandlich lediglich eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten" in Bezug. Der Inhaber einer Arztpraxis müsste demnach bereits eine Datenschutz-Folgenabschätzung durchführen und einen Datenschutzbeauftragten schon dann benennen, wenn eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt, ohne dass es auf die Frage der „Kerntätigkeit" ankommt. Das Merkmal der „Kerntätigkeit" ist jedoch für die Benennung eines Datenschutzbeauftragten gem. Art. 37 Abs. 1 lit. c DSGVO zusätzlich von Bedeutung. Weil § 38 S. 2 BDSG insoweit die Voraussetzungen der Benennungspflicht gegenüber Art. 37 Abs. 1 lit. c DSGVO modifiziert, indem das zusätzliche Merkmal der „Kerntätigkeit" nicht mehr erfüllt sein muss, steht die Vorschrift nicht im Einklang mit der DSGVO. Die Regelungsmöglichkeit von Art. 37 Abs. 4 DSGVO dient nicht dazu, Regelungen der DSGVO abzuändern, sondern darf sich nach dem eindeutigen Wortsinn nur auf „andere" als die in Art. 37 Abs. 1 DSGVO „genannten Fälle" beziehen.

c. Änderungsvorschlag der Bundesärztekammer

Die europarechtswidrige Vorschrift des § 38 S. 2 BDSG ist zu streichen.

II. Artikel 16 (Arzneimittelgesetz)

1. Zu Nummer 1) b) bb) und cc) (§ 40 AMG)

a. Beabsichtigte Neuregelung

Mit der Anpassung wird die gem. Art. 7 Abs. 3 S. 1 DSGVO vorgesehene Widerruflichkeit der Einwilligung in die spezifische Informationspflicht gem. § 40 Abs. 2a AMG einbezogen. Ferner erfolgen redaktionelle (Folge-)Änderungen.

b. Stellungnahme der Bundesärztekammer

Aus der Begründung zum Referentenentwurf lässt sich eine Grundlage für die Regelung einer zusätzlichen und spezifischen Informationspflicht neben Art. 13 und 14 DSGVO nicht entnehmen. Die Information über die Widerruflichkeit der Einwilligung hat bereits gem. Art. 13 Abs. 2 lit. c bzw. Art. 14 Abs. 2 lit. d DSGVO zu erfolgen. Es besteht daher die Problematik der im Europarecht grundsätzlich verbotenen Normwiederholung.

Mit den Anpassungen wird ungeachtet dessen zutreffend der DSGVO Rechnung getragen, wonach die Einwilligung widerruflich ist (Art. 7 Abs. 3 S. 1 DSGVO). Die bisher enthaltene Unwiderruflichkeit wird damit richtigerweise aufgehoben. Es bleibt der Widerruf aber ohne Folgen für die bereits erhobenen Daten, die weiterverwendet werden dürfen (§ 40 Abs. 2a Nr. 3 und S. 3 AMG-E). Dies ist sachgerecht und steht im Einklang mit der Regelung des Art. 7 Abs. 3 S. 2 DSGVO, wonach durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird. Das trägt den Vorhaben der klinischen Prüfungen Rechnung, bereits erhobene Daten nicht löschen zu müssen.

c. Änderungshinweise der Bundesärztekammer

Es wäre zu prüfen, welche Informationspflichten bereits durch Art. 13 und Art. 14 DSGVO erfüllt werden. Das liegt z. B. für § 40 Abs. 2a Nr. 1b-d, Nr. 2 und ggf. Nr. 3 AMG wegen Art. 13 Abs.1 lit. c und e, Abs. 2 lit. c bzw. Art. 14 Abs.1 lit. c und e, Abs. 2 lit. d DSGVO nahe.

2. Weiterer Regelungsbedarf im AMG

a. Schaffung einer Rechtsgrundlage für den Informationsaustausch zur Aufgabenerfüllung der Ethikkommissionen gem. § 40 Abs. 5 AMG n. F.

Mit der voraussichtlich im Jahre 2020 erfolgenden Anwendung der Verordnung (EU) Nr. 536/2014 über klinische Prüfungen mit Humanarzneimitteln wird die zuständige Ethik-Kommission nach dem Geschäftsverteilungsplan gem. § 41b Abs. 2 AMG ermittelt. Somit entfällt die lokale Zuständigkeit der Ethik-Kommissionen bei der Bewertung von Anträgen auf Durchführung von klinischen Prüfungen mit Humanarzneimitteln.

Insbesondere bei der durch die zuständige Ethik-Kommission vorzunehmenden Bewertung der Qualifikation der Prüfer und Geeignetheit der Prüfstellen gem. § 40 Abs. 5 AMG n. F. (in der Fassung des Vierten Gesetzes zur Änderung arzneimittelrechtlicher und anderer Vorschriften vom 20.12.2016, BGBl. I S. 3048), ist im Bedarfsfall für eine ordnungsgemäße Erfüllung der Aufgaben ein Informationsaustausch mit den lokalen Ethik-Kommissionen, aber auch mit weiteren für den Vollzug des Arzneimittelgesetzes zuständigen Behörden, Stellen und Kommissionen unerlässlich. Um eine zügige und einheitliche Durchführung des Verfahrens unter den neuen rechtlichen Rahmenbedingungen zu sichern, bedarf es einer entsprechenden Erlaubnisnorm für den notwendigen Datenaustausch.

b. Regelungsvorschlag der Bundesärztekammer

Nach § 41 Abs. 2 AMG n. F. (in der Fassung des Vierten Gesetzes zur Änderung arzneimittelrechtlicher und anderer Vorschriften vom 20.12.2016, BGBl. I S. 3048) sollte der folgende neue Abs. 2a eingefügt werden:

„Soweit es zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist, kann die Ethik-Kommission mit anderen registrierten Ethik-Kommissionen und mit den für den Vollzug des Arzneimittelgesetzes zuständigen Behörden und Stellen personenbezogene Daten austauschen."

III. Artikel 21 (Gendiagnostikgesetz)

1. Zu Nummer 1 (§ 8 Abs. 1 GenDG)

a. Beabsichtigte Neuregelung

In § 8 Abs. 1 wird nach Satz 2 folgender Satz 3 eingefügt: *„Die Einwilligung nach Satz 1 umfasst auch die Einwilligung in die Verarbeitung genetischer Daten."*

b. Stellungnahme der Bundesärztekammer

Es handelt sich durch Aufnahme des § 8 Abs. 1 S. 3 GenDG-E um eine Klarstellung in § 8 Abs. 1 GenDG, dass die Einwilligung auch die Verarbeitung genetischer Daten umfasst und damit eine Rechtsgrundlage für die Verarbeitung von genetischen Daten i. S. v. Art. 9 Abs. 1 i. V. m. Art. 4 Nr. 13 DSGVO besteht (vgl. auch RefE, S. 268). Diese Klarstellung ist nicht zu beanstanden. Bislang musste aus der Zustimmung zur Vornahme diagnostischer Maßnahmen der Schluss gezogen werden, der Patient willige in die Datenverarbeitung durch den Arzt ein. Die neue Regelung schafft damit mehr Rechtsklarheit.

2. Zu Nummer 3 (§ 26 GenDG)

a. Beabsichtigte Neuregelung

Die neue Regelung des § 26 GenDG-E enthält Bußgeldtatbestände, die nicht von der DSGVO erfasst sind. Es handelt sich um Verstöße, die nicht „rein datenschutzrechtlich" sind (RefE, S. 270).

b. Stellungnahme der Bundesärztekammer

Die Bereinigung ist sachgerecht. Insbesondere bleibt der Arztvorbehalt durch § 26 Abs. 1 Nr. 1 GenDG-E weiterhin sanktionsbewehrt.

IV. Artikel 60 (Strafgesetzbuch)

Zu Nummer 1 (§ 203 Abs. 4 S. 1 StGB)

a. Stellungnahme der Bundesärztekammer

Die Regelung des § 203 Abs. 4 S. 1 StGB bezieht bislang nur die *„bei den"* Berufsgeheimnisträgern tätigen Beauftragten für den Datenschutz ein. Art. 37 Abs. 6 DSGVO lässt indes auch die Beauftragung *externer* Datenschutzbeauftragter aufgrund eines Dienstleistungsvertrages zu. Der dem Vertrauensverhältnis zwischen Arzt und Patient dienende Schutz des Patientengeheimnisses muss – wie noch gem.

§ 203 Abs. 2a StGB a. F. – in diesen Fällen ebenfalls strafrechtlich abgesichert sein. Daher ist es erforderlich, auch solche Datenschutzbeauftragte mit einer hinreichenden Bestimmtheit (Art. 103 Abs. 2 GG) der Strafbarkeit zu unterwerfen, die als externe Dienstleister (z. B. für Arztpraxen) tätig werden.

Ausweislich der Begründung zum Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen sollte mit der Änderung und Streichung der vorherigen Regelung des § 203 Abs. 2a StGB a. F. zwar eine inhaltliche Änderung nicht verbunden sein (BT-Drs. 18/11936, S. 28). § 203 Abs. 2a StGB a. F. differenzierte indes nicht zwischen *„bei den"* Berufsgeheimnisträgern tätigen und externen Datenschutzbeauftragten. Die möglicherweise versehentlich herbeigeführte materielle Änderung sollte im Interesse der Rechtsklarheit für die Normadressaten korrigiert werden.

b. Änderungsvorschlag der Bundesärztekammer

§ 203 Abs. 4 S. 1 StGB ist mit Blick auf Art. 37 Abs. 6 DSGVO entsprechend anzupassen, indem im zweiten Satzteil die Worte *„bei den"* durch die Worte *„für die"* ersetzt werden. Der Satzteil lautet dann:

„[…] oder als für die in den Absätzen 1 und 2 genannten Personen tätiger Datenschutzbeauftragter bekannt geworden ist."

V. Artikel 119 (Strahlenschutzgesetz)

Zu Nummer 5 (§ 170 Abs. 6-8 StrlSchG-E)

a. Beabsichtigte Neuregelung

§ 170 Abs. 6 StrlSchG wird gem. Art. 119 Nr. 5 lit. a) des 2. DSAnpUG-EU aufgehoben, weil sich eine entsprechende Informationspflicht direkt aus Art. 14 DSGVO und ein entsprechendes Auskunftsrecht direkt aus Art. 15 DSGVO folgt.

In § 170 StrlSchG wird gem. Art. 119 Nr. 5 lit. b) des 2. DSAnpUG-EU ein neuer Absatz 6 eingefügt, der im Kontext der Verarbeitung „personenbezogener Daten" zu „Zwecken der wissenschaftlichen Forschung" unter anderem folgende Regelung enthält: *„Soweit die betroffenen Personen nicht in die Veröffentlichung der sie betreffenden Daten eingewilligt haben, dürfen Forschungsergebnisse nur anonymisiert veröffentlicht werden."*

Zudem enthält § 170 Abs. 8 S. 3 StrlSchG-E gem. Art. 119 Nr. 5 lit. d), cc) des 2. DSAnpUG-EU eine Zweckbindungs- und Zweckänderungsregelung für die Verarbeitung von z. B. Gesundheitsdaten zu Forschungszwecken.

b. Stellungnahme der Bundesärztekammer

Die Aufhebung des bisherigen Absatzes 6 ist sachgerecht, weil sich die Informationspflicht direkt aus Art. 14 DSGVO ergibt und ein entsprechendes Auskunftsrecht aus Art. 15 DSGVO folgt (s. RefE, S. 410).

Im Rahmen der Änderung gem. Art. 119 Nr. 5 lit. b) des 2. DSAnpUG-EU zum neuen Absatz 6 wird präzisiert, dass bei fehlender Einwilligung der betroffenen Personen die Forschungsergebnisse nur anonymisiert veröffentlicht werden dürfen. Dies erscheint sachgerecht, wenngleich offen bleibt unter welchen Voraussetzungen anonymisierte Daten nach der jüngsten Rechtsprechung des EuGH und des BGH (EuGH, Urt. v. 19.10.2016 – Rs. C-582/14; Beschl. v. 06.12.2016 – Rs. C-582/14 REC und BGH,

Urt. v. 16.05.2017 – VI ZR 135/13) weiter als personenbezogene Daten behandelt werden müssen.

Unklar bleibt ferner, ob sich die eingeräumten Befugnisse in Absatz 6 auch auf die Verarbeitung von Gesundheitsdaten beziehen. Dies ergibt sich allenfalls implizit aus § 170 Abs. 7 S. 4 und Abs. 8 S. 3 StrlSchG-E.

Die Weiterverarbeitung von Gesundheitsdaten nach § 170 Abs. 8 S. 3 StrlSchG-E infolge der Änderung gem. Art. 119 Nr. 5 lit. d) cc) des 2. DSAnpUG-EU dürfte im Einklang mit Art. 89 Abs. 1 DSGVO und Art. 9 Abs. 4 DSGVO stehen.

VI. Artikel 120 (SGB V)

1. Allgemeine Bemerkungen

Die Änderungen beziehen sich dem ersten Anschein nach im Wesentlichen auf redaktionelle Anpassungen an die DSGVO. Es wird z. B. der einheitliche Begriff der „Verarbeitung" oder des „Verantwortlichen" verwendet. Inhaltliche Änderungen sind damit in den meisten Fällen nicht verbunden.

Anlässlich der Gesetzgebung stellt sich jedoch die Frage, inwieweit eine **Vereinfachung des bislang sehr fragmentierten Gesundheitsdatenschutzrechts** hergestellt werden könnte (zur Kritik am sehr komplexen Gesundheitsdatenschutzrecht s. nur *Kingreen/Kühling*, in: Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 440 ff.). Im Rahmen des gewählten Vorgehens des Bundesgesetzgebers, mit dem BDSG ein Auffanggesetz mit allgemeinen Generalklauseln zu schaffen,[8] bietet es sich an, einige Spezialregelungen aufzuheben oder jedenfalls auf die allgemeinen Regelungen im BDSG Bezug zu nehmen. Im letzteren Fall wäre eine Referenz auf § 22 BDSG möglich, der auf Art. 9 Abs. 2 lit. h DSGVO zurückzuführen ist und z. B. die Versorgung oder Behandlung im Gesundheitsbereich als zulässigen Verarbeitungszweck aufführt. Auch den vertragsärztlichen Vorschriften im SGB V, die zwar zugleich auf Art. 9 Abs. 4 DSGVO gestützt werden können, liegt dieser Verarbeitungszweck regelmäßig zu Grunde, sodass es spezifischer Regelungen nicht bedarf. Eine Referenz auf das BDSG wäre in Bereichen möglich, wo der Verarbeitungszweck nicht über die Gesundheitsvorsorge, medizinische Diagnostik, Versorgung oder Behandlung hinausgeht. Entsprechend ist hinsichtlich der anderen Tatbestände von § 22 Abs. 1 Nr. 1 BDSG zu prüfen, inwieweit bereichsspezifische Regelungen in einigen Bereichen noch erforderlich sind oder Verarbeitungszwecke bereits von dieser Norm abgedeckt sind.

Die bislang im SGB V enthaltenden Regelungen mit Einwilligungsvorbehalten sind zu hinterfragen. Zu bedenken ist, dass die **Einwilligung in Behandlungskontexten** nach verbreiteter Auffassung ein **ungeeignetes Instrument** ist, weil es die Beziehung zwischen Arzt und Patienten belasten kann. Fraglich ist neben den bürokratischen Folgen bei der praktischen Umsetzung vor allem, ob stets von einer informierten und vor allem freiwilligen Einwilligung die Rede sein kann, wenn Patienten vordringlich an der Gesundheitsversorgung interessiert sind (statt vieler schon *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 4a, Rn. 3 ff.; vgl. zusammenfassend zuletzt *Veil*, NVwZ 2018, 686, 688). Die informationelle Selbstbestimmung kraft Einwilligung steht damit zumeist lediglich auf dem Papier. Daher ist es vorzugswürdig, den **Austausch von Gesundheitsdaten auf eine rechtssichere gesetzliche Grundlage zu stellen**.

[8] S. dazu schon die Stellungnahme der Bundesärztekammer vom 21.03.2017 RegE der BReg: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 u.a. vom 01.02.2017, S. 7 f. und passim.

Soweit – entgegen praktischer Bedürfnisse – an dem Einwilligungserfordernis im vertragsärztlichen Bereich festgehalten werden soll, sind die dort statuierten **Formanforderungen problematisch**. Im Hinblick auf die Einwilligung soll an zahlreichen Stellen im SGB V neben der Schriftform auch die elektronische Form zugelassen werden. Diese Änderung vollzieht zwar nach, das im Einklang mit der DSGVO neben der Schriftform auch eine elektronische Form der Erklärung in Betracht kommt. Die Schriftform und die elektronische Form sind aber keineswegs die abschließend von der DSGVO zugelassenen Formen einer Einwilligungserklärung. Übersehen wird, dass die ausdrückliche Einwilligung nach Erwägungsgrund 32 DSGVO auch mit einer mündlichen Erklärung erfolgen kann. Im Rahmen der Kommunikation über Telefon oder mittels Videotelefonie (z. B. bei zulässigen Fernbehandlungen) ist diese Möglichkeit von praktischer Bedeutung. Bei der Verarbeitung von Gesundheitsdaten unzulässig sind allein konkludente Einwilligungen (vgl. Art. 9 Abs. 2 lit. a DSGVO, Erwägungsgrund 51). Die DSGVO stellt darüber hinaus lediglich die Anforderung auf, dass der Verantwortliche die Einwilligung nachweisen kann (Art. 7 Abs. 1 DSGVO). Im Fall der mündlich erklärten Einwilligung kann dies etwa durch eine Dokumentation der Einwilligung erfolgen.

Zwar wären davon abweichend strengere Formanforderungen als zusätzliche Bedingungen oder Einschränkungen für die Verarbeitung von Gesundheitsdaten von der Öffnungsklausel des Art. 9 Abs. 4 DSGVO gedeckt (so auch RefE, S. 413). Eine Begründung für die strengeren Anforderungen und eine Auseinandersetzung mit der Umsetzbarkeit in der Praxis unterbleiben im Referentenentwurf jedoch. Vielmehr wird insinuiert, es müsse eine Anpassung an § 67b Abs. 2 S. 1 SGB X erfolgen (RefE, S. 420 f.), was aus systematischen Gründen nicht überzeugt, weil Ärzte keine Leistungsträger sind, die Sozialdaten verarbeiten (s. dazu unten bei C., VI., 3., b.). Die Schriftform bzw. elektronische Form sagen zudem nichts darüber aus, ob die Einwilligung tatsächlich informiert erfolgt und sich der Betroffene aufgrund dessen der Tragweite seines Handelns bewusst wird (*Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 7, Rn. 22). Im Falle einer mündlich erteilten Einwilligung kann demnach ebenso eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung" (Art. 4 Nr. 11 DSGVO) vorliegen.

Soweit die „elektronische" Form eingeführt wird, stellt sich zudem die Frage, welche Anforderungen an diese zu stellen sind und wie das Verhältnis zu anderen nationalen Rechtsvorschriften zu bestimmen ist. Die Auslegung nach der DSGVO ergibt, dass eine elektronische Erklärung etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen kann, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert (Erwägungsgrund 32). Demgegenüber gilt gem. § 126a Abs. 1 BGB für die elektronische Form, welche die Schriftform ersetzt, dass das elektronische Dokument u. a. mit einer qualifizierten elektronischen Signatur versehen werden muss (vgl. für Leistungsträger im Bereich des Sozialdatenschutzrechts § 36a Abs. 2 SGB X). Die Möglichkeit, die Einwilligung mittels einfacher E-Mail zu erklären, würde Patienten demnach entzogen werden, weil der Gesetzgeber auf § 67b Abs. 2 SGB X verweist, der seinerseits im Regelungszusammenhang zu § 36a Abs. 2 SGB X zu betrachten wäre. Der Einsatz einer qualifizierten elektronischen Signatur i. S. v. § 126a Abs. 1 BGB ist unrealistisch, da diese Patienten gegenwärtig selten zur Verfügung steht. Die von der DSGVO zugelassene elektronische Form würde unter diesem Gesichtspunkt praktisch keine Anwendung finden. Wegen der Divergenzen bei der Auslegung des Begriffs der „elektronischen Erklärung" sollte eine Regelung von Formvorgaben im SGB V unterbleiben. Da die DSGVO keine bestimmte Form der Einwilligung vorsieht und sich die Formanforderungen für die Einwilligung bei der Verarbeitung von Gesundheitsdaten

unmittelbar aus Art. 7 DSVGO ergeben, genügt es, an den jeweiligen Stellen (z. B. in § 73 Abs. 1b S.1-3 SGB V), das Wort „schriftlich" zu streichen.

2. Zu Nummer 6 (§ 39 SGB V)

a. Beabsichtigte Neuregelung

§ 39 Abs. 1a S. 11 SGB V regelt bislang, dass das Entlassmanagement und eine dazu erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur mit Einwilligung und nach vorheriger Information des Versicherten erfolgen dürfen. Neben den redaktionellen Anpassungen an den umfassenden Verarbeitungsbegriff nach Art. 120 Nr. 6 a) des 2. DSAnpUG-EU soll § 39 Abs. 1a SGB V nach Art. 120 Nr. 6 c) des 2. DSAnpUG-EU einen neuen Satz 12 erhalten, wonach die Information sowie die Einwilligung „schriftlich oder elektronisch" erfolgen müssen. Insoweit hat künftig nicht nur die Einwilligung, sondern auch die Vermittlung der Informationen zum Entlassmanagement und der darauf bezogenen Datenverarbeitung schriftlich oder elektronisch zu erfolgen. Bislang ließ § 39 Abs. 1a S. 11 SGB V aber offen, in welcher Form die Information erfolgt. Ausweislich der Begründung erfolgt die Änderung, um einen Gleichklang mit dem Formerfordernis der Einwilligung herzustellen (RefE, S. 417).

b. Stellungnahme der Bundesärztekammer

Beim Übergang in die Versorgung nach einer Krankenhausbehandlung ist zum Zweck der Gesundheitsversorgung eine Übermittlung von Gesundheitsdaten erforderlich. § 39 Abs. 1a S. 11 SGB V schreibt vor, dass das Entlassmanagement und eine dazu erforderliche Verarbeitung personenbezogener Daten nur mit Einwilligung und nach vorheriger Information des Versicherten erfolgen dürfen. Wegen der vom Bundesgesetzgeber vorgezogenen weiten Regelung des § 22 Abs. 1 Nr. 1 lit. b BDSG sollte geprüft werden, inwieweit die bereichsspezifische Regelung mit einem Einwilligungsvorbehalt in § 39 Abs. 1a S. 11 SGB V noch erforderlich ist. Eine Verarbeitung von Gesundheitsdaten zum Zweck u. a. der Fortsetzung der Behandlung kann ohne weiteres über die Regelung des BDSG legitimiert werden. Für darüber hinausgehende Verarbeitungen von Gesundheitsdaten sähe Art. 9 Abs. 2 lit. a DSGVO bereits eine Einwilligungsmöglichkeit vor. Wegen der weiteren Argumentation wird auf die Ausführungen zu § 73 Abs. 1b SGB V (s. bei C., VI., 3., b.) verwiesen. In Satz 11 bedarf es der Einwilligung daher nur noch, soweit die Regelung die Teilnahme am Entlassmanagement betrifft.

Problematisch ist zudem die gem. Art. 120 Nr. 6 c) des 2. DSAnpUG-EU vorgesehene Änderung, nach der die Information des Patienten „schriftlich oder elektronisch" erfolgen soll. Das lässt die Formen außer Acht, die Art. 12 Abs. 1 DSGVO zur Erfüllung der Informationspflichten überdies vorsieht. Die Übermittlung der Informationen soll nach Art. 12 Abs. 1 S. 2 DSGVO schriftlich oder in anderer Form, gegebenenfalls auch elektronisch erfolgen. Falls von der betroffenen Person verlangt, kann die Information nach Art. 12 Abs. 1 S. 3 DSGVO aber auch mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. Ob diese Begrenzung der zulässigen Formen bei der Erfüllung von Betroffenenrechten auf Art. 23 Abs. 1 lit. e DSGVO gestützt werden kann, ist zweifelhaft, weil es sich nicht um Beschränkungen des Betroffenenrechts handelt, sondern um eine formalistische Verschärfung der Anforderungen zur Erfüllung der Informationspflichten, die von den Öffnungsklauseln der DSGVO nicht gedeckt sein dürfte.

Wegen der Formerfordernisse für die Einwilligung wird auf die vorstehenden Ausführungen verwiesen (C., VI., 1.).

c. Änderungsvorschlag der Bundesärztekammer

Wegen der vom Bundesgesetzgeber vorgezogenen weiten Regelung des § 22 Abs. 1 Nr. 1 lit. b BDSG sollte geprüft werden, inwieweit die bereichsspezifische Regelung mit einem Einwilligungsvorbehalt in § 39 Abs. 1a S. 11 SGB V noch erforderlich ist. Aus hiesiger Sicht kann die Regelung gestrichen werden. Alternativ kann eine klarstellende Bezugnahme auf § 22 Abs. 1 Nr. 1 lit. b BDSG erfolgen.

In § 39a Abs. 1a S. 11 werden die Wörter *„und eine dazu erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten dürfen"* durch das Wort *„darf"* ersetzt.

Alternativ kann zusätzlich ein neuer Satz 12 mit folgender Formulierung angefügt werden: *„Die Verarbeitung personenbezogener Daten erfolgt auf der Grundlage von § 22 Abs. 1 Nr. 1 lit. b BDSG".*

Soweit der datenschutzrechtliche Einwilligungsvorbehalt in § 39 Abs. 1a S. 11 SGB V. entgegen dem vorgenannten Vorschlag, aufrechterhalten bleiben sollte, muss § 39 Abs. 1a S. 12 SGB V-E gem. dem Vorschlag des Referentenentwurfes in Art. 120, Nr. 6, lit. c) des 2. DSAnpUG-EU gestrichen werden.

3. Zu Nummer 13 (§ 73 Abs. 1 b SGB V)

a. Beabsichtigte Neuregelung

Beabsichtigt sind mit Art. 120 Nr. 13 a)-d) des 2. DSAnpUG-EU im Wesentlichen begriffliche und redaktionelle Anpassungen.

b. Stellungnahme der Bundesärztekammer

Soweit ausweislich der Begründung eine Anpassung an § 67b Abs. 2 SGB X erfolgt (RefE, S. 420), überzeugt das nicht, denn Leistungserbringer verarbeiten keine Sozialdaten. Die vielkritisierte Rechtsprechung des BSG (Urt. v. 2008 – B 6 KA 37/07 R; zur Krit. statt vieler *Kircher*, in: Kingreen/Kühling, Gesundheitsdatenschutzrecht, S. 186, 237 ff. jew. m. w. Nw.) verkannte die systematischen Zusammenhänge und qualifizierte solche Daten unzutreffend als Sozialdaten, wenn Gesundheitsdaten aufgrund einer Regelung im SGB V durch Ärzte verarbeitet werden. Sozialdaten sind jedoch gem. § 67 Abs. 2 SGB X personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB verarbeitet werden. § 35 SGB I verpflichtet nur Leistungsträger als solche Stellen, nicht hingegen sog. Leistungserbringer. Für Ärzte stellen die Regelungen im SGB V also bereichsspezifische Regelungen des Gesundheitsdatenschutzrechts jenseits des Sozialdatenschutzrechts dar, die gem. § 1 Abs. 2 S. 1 und 2 BDSG als „andere Rechtsvorschriften des Bundes über den Datenschutz" den Vorschriften des BDSG vorgehen. Einer Anpassung an die Vorschriften des § 67b SGB X bedarf es daher nicht (so aber RefE, S. 420).

Nicht zuletzt wegen dieser vorstehend angedeuteten Missverständnisse und dem weitreichenden „Regelungswirrwarr" im Gesundheitsdatenschutzrecht (s. z. B. *Mand*, MedR 2003, 393, 395) stellt sich die Frage, inwieweit für Ärzte ein spezifisches Datenschutzrecht innerhalb des SGB aufrechterhalten bleiben muss, wenn der Bundesgesetzgeber an anderer Stelle im BDSG umfassende Befugnisse zur Verarbeitung in Kontexten der Gesundheitsversorgung geschaffen hat. Vereinfachungen der Rechtslage wären zu begrüßen.

Es überzeugt z. B. nicht, für den nach § 73 Abs. 1b SGB V vorgesehenen Informationsaustausch zwischen Haus- und Fachärzten zum Zwecke der Dokumentation und der weiteren Behandlung im vertragsärztlichen Bereich eine schriftliche oder

elektronische Einwilligung des Patienten zu fordern. Aufrechterhalten bleiben kann zwar die Verpflichtung gem. § 73 Abs. 1b S. 2 Hs. 1 und S. 5 Hs. 1 SGB V, wonach Patientendaten zum Zwecke der Dokumentation und der weiteren Behandlung zu übermitteln sind. Darüber hinaus bedarf es aber keiner Ermächtigung zur Datenverarbeitung (bisher § gem. § 73 Abs. 1b S. 1, S. 2 Hs. 2 und S. 3 sowie S. 5 Hs. 2 SGB V), weil sich diese zum Zweck der Behandlung bereits aus § 22 Abs. 1 Nr. 1 lit. b BDSG ergibt. **Vorzugswürdig und ausreichend wäre allenfalls eine klarstellende Bezugnahme auf § 22 Abs. 1 Nr. 1 lit. b BDSG**, der die Versorgung oder Behandlung im Gesundheitsbereich als zulässigen Verarbeitungszweck aufführt und damit dieselbe Situation wie § 73 Abs. 1b SGB V beschreibt.

Bezweifelt werden muss, ob der Einwilligungsvorbehalt in § 73 Abs. 1b SGB V sachgerecht ist. Es besteht ein Wertungswiderspruch zu Art. 9 Abs. 2 lit. h DSGVO und zur Regelung des § 22 Abs. 1 Nr. 1 lit. b BDSG, die die Datenverarbeitung zum Zweck u. a. der Behandlung auf eine gesetzliche Grundlage stützen. Das umfasst auch den Austausch von Gesundheitsdaten zum Zweck der Weiterbehandlung. In üblichen Versorgungssituationen ist eine Einwilligung entbehrlich, weil der Patient mit der Weitergabe seiner Daten rechnet, wenn er im Anschluss an den Hausarztbesuch aufgrund einer Überweisung einen Facharzt aufsucht und dieser die Untersuchungsergebnisse an den die Untersuchung veranlassenden Hausarzt rückmeldet. Das entspricht im Übrigen der Regelungslage zur ärztlichen Schweigepflicht im Berufsrecht (vgl. § 9 Abs. 4 MBO-Ä). Anders ist dies nur zu bewerten, wenn eine Einbeziehung von anderen Stellen, z. B. von Krankenkassen, erfolgt. Hier wäre die Einwilligung des Patienten erforderlich. Für über den Anwendungsbereich von § 22 Abs. 1 Nr. 1 BDSG hinausgehende Verarbeitungen von Gesundheitsdaten sieht Art. 9 Abs. 2 lit. a DSGVO aber bereits eine Einwilligungsmöglichkeit vor.

Der Informationsaustausch zwischen nacheinander behandelnden Ärzten ist ein Massenvorgang, der mit der Einwilligung praktischen Umsetzungsproblemen ausgesetzt ist (s. o. bei C., VI., 1.). Wenig hilfreich sind auch die bisher unterbreiteten Vorschläge zur Interpretation von § 73 Abs. 1 b SGB V. So hat der frühere Bundesbeauftragte für Datenschutz – ausweislich eines der Bundesärztekammer vorliegenden Schreibens aus dem Jahr 2012 –, entgegen dem Wortlaut der Norm, bislang vertreten, dass für den in § 73 Abs. 1b SGB V geregelten Fall eine konkludente Einwilligung anzunehmen und die Schriftform nicht zu wahren sei. Die Einwilligung erzeugt bei einer solchen Handhabung lediglich noch den blassen Schein einer Legitimation. Die Auffassung ist auch nicht mehr mit Art. 9 Abs. 2 lit. a DSGVO vereinbar, wonach die Einwilligung ausdrücklich zu erfolgen hat (vgl. schon § 4a Abs. 3 BDSG a. F.). Zur Beseitigung der bisher unklaren Rechtslage im Interesse einer praxisnahen Umsetzung des Datenschutzes im Arzt-Patienten-Verhältnis sowie zur praxisgerechten Erleichterung des Informationsaustausches zwischen Ärzten ist eine klare gesetzliche Grundlage erforderlich.

Soweit – entgegen praktischer Bedürfnisse in der ärztlichen Versorgung – an dem spezialgesetzlich normierten Einwilligungserfordernis im vertragsärztlichen Bereich festgehalten werden soll, ist darauf hinzuweisen, dass die DSGVO keine bestimmte Form der Einwilligung vorsieht und sich die Anforderungen für die Einwilligung bei der Verarbeitung von Gesundheitsdaten unmittelbar aus Art. 7 DSVGO ergeben. Die Einführung der elektronischen Erklärung neben der Schriftform lässt mündliche Erklärungen außer Acht und steht in einem Spannungsverhältnis zu Regelungen, welche für die elektronischen Erklärung eine qualitfizierte elektronische Signatur vorsehen (vgl. oben C., VI., 1.). In § 73 Abs. 1b S.1-3 SGB V ist das Wort „schriftlicher" insoweit zu streichen.

c. Änderungsvorschlag der Bundesärztekammer

Wegen der vom Bundesgesetzgeber vorgezogenen weiten Regelung des § 22 Abs. 1 Nr. 1 lit. b BDSG sollte geprüft werden, inwieweit die bereichsspezifische Regelung mit einem Einwilligungsvorbehalt in § 73 Abs. 1b SGB V noch erforderlich ist. Aus hiesiger Sicht kann die Regelung gestrichen werden. Alternativ kann eine klarstellende Bezugnahme auf § 22 Abs. 1 Nr. 1 lit. b BDSG erfolgen.

Sollte an dem spezialgesetzlich normierten Einwilligungserfordernis festgehalten werden, sind in § 73 Abs. 1b S. 1-3 das Wort *„schriftlicher"* bzw. in Art. 120 Nr. 13 lit. a)-c) des Entwurfstextes zum 2. DSAnpUG-EU die Worte *„schriftlicher oder elektronischer"* zu streichen.

4. Nummer 46 (§ 299 SGB V)

a. Beabsichtigte Neuregelung

Beabsichtigt sind mit Art. 120 Nr. 46 a)-f) im Wesentlichen begriffliche und redaktionelle Anpassungen.

b. Stellungnahme der Bundesärztekammer

Die Übermittlung von Daten zum Zwecke der Qualitätssicherung wäre auch aufgrund § 22 Abs. 1 Nr. 1 lit. c BDSG zulässig. Es ist daher fraglich und zu überprüfen, ob es der Spezialregelung des § 299 Abs. 1 SGB V bedarf.

c. Änderungsvorschlag der Bundesärztekammer

Wegen der vom Bundesgesetzgeber vorgezogenen weiten Regelung des § 22 Abs. 1 Nr. 1 lit. c BDSG sollte geprüft werden, inwieweit die bereichsspezifische Regelung in § 299 Abs. 1 S. 1 SGB V noch erforderlich ist. Aus hiesiger Sicht kann die Regelung gestrichen werden. Alternativ kann eine klarstellende Bezugnahme auf § 22 Abs. 1 Nr. 1 lit. c BDSG erfolgen.

VII. Artikel 125 (SGB VII)

1. Zu Nummer 10 lit. b) (§ 201 Abs. 1 S. 3 SGB VII-E)

a. Beabsichtigte Neuregelung

Die bisherigen Sätze 3 bis 5 in § 201 SGB VII, welcher die Erhebung, Speicherung und Übermittlung von Gesundheitsdaten durch Ärzte im Zusammenhang mit einer Heilbehandlung nach einem Versicherungsfall regelt, sollen durch eine Bestimmung ersetzt werden, nach der das Auskunftsrecht des Betroffenen (Versicherten) gegenüber dem Unfallversicherungsträger durch den die Daten übermittelnden Arzt erfüllt wird. Die Regelung lautet: *„Für die Unterrichtung des Versicherten aufgrund seines Auskunftsrechts nach Artikel 15 der Verordnung (EU) 2016/679 über die von den Ärzten und den Psychotherapeuten übermittelten Angaben zu seinen gesundheitlichen Verhältnissen gilt § 25 Absatz 2 des Zehnten Buches entsprechend."* § 25 Abs. 2 SGB X enthält folgende Regelung: *„Soweit die Akten Angaben über gesundheitliche Verhältnisse eines Beteiligten enthalten, kann die Behörde statt dessen den Inhalt der Akten dem Beteiligten durch einen Arzt vermitteln lassen. Sie soll den Inhalt der Akten durch einen Arzt vermitteln lassen, soweit zu befürchten ist, dass die Akteneinsicht dem Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde. Soweit die Akten Angaben enthalten, die die Entwicklung und Entfaltung*

der Persönlichkeit des Beteiligten beeinträchtigen können, gelten die Sätze 1 und 2 mit der Maßgabe entsprechend, dass der Inhalt der Akten auch durch einen Bediensteten der Behörde vermittelt werden kann, der durch Vorbildung sowie Lebens- und Berufserfahrung dazu geeignet und befähigt ist. Das Recht nach Absatz 1 wird nicht beschränkt."

b. Stellungnahme der Bundesärztekammer

Der Regelungsvorschlag für § 201 Abs. 1 S. 3 SGB VII-E ist abzulehnen, denn eine Übertragung des originär dem Verantwortlichen obliegenden Auskunftsrechts gem. Art. 15 DSGVO auf einen Dritten ist europarechtswidrig. Die beabsichtigte Neuregelung widerspricht dem Prinzip der Verantwortlichkeit für die Datenverarbeitung nach der DSGVO.

Bisher kann der Versicherte gem. § 201 Abs. 1 S. 3 SGB VII vom Unfallversicherungsträger verlangen, über die von den Ärzten und den Psychotherapeuten übermittelten Daten unterrichtet zu werden. Gem. § 201 Abs. 1 S. 4 SGB VII i. V. m. § 25 Abs. 2 SGB X kann die Behörde dabei *den Inhalt von Akten*, die Angaben über gesundheitliche Verhältnisse eines Beteiligten enthalten, durch einen Arzt *vermitteln lassen* (S. 1). Die Behörde soll den *Inhalt der Akten* durch einen Arzt *vermitteln lassen*, soweit zu befürchten ist, dass die Akteneinsicht dem Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde (S. 2).

Zweck der Regelung in § 25 Abs. 2 SGB X ist indes nicht die Übertragung des dem Unfallversicherungsträger originär obliegenden datenschutzrechtlichen Auskunftsrechts gem. Art. 15 DSGVO oder der Informationspflicht gem. Art. 14 DSGVO auf Ärzte, sondern eine zum Schutz des Betroffenen erfolgende fachlich korrekte Vermittlung von Inhalten einer Akte, über welche dem Versicherten Auskunft von Seiten der Behörde zu erteilen ist. „Vermitteln" ist hierbei im Sinne von „Erklären" und nicht „Auskunfterteilen" im datenschutzrechtlichen Sinne gemeint.

Die mit dem Referentenentwurf beabsichtigte Übertragung des Auskunftsrechts auf Ärzte widerspricht dem Prinzip der Verantwortlichkeit nach dem Datenschutzrecht in der DSGVO. „Verantwortlicher" ist gem. Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Fall der Unfallversicherung entscheidet der Unfallversicherungsträger über die Zwecke und Mittel der Verarbeitung von Gesundheitsdaten, indem er die Überprüfung der Leistungsvoraussetzungen und Abrechnung der Leistungen vornimmt. Zu diesem Zweck sind Ärzte verpflichtet, Daten über die Behandlung und den Zustand des Versicherten sowie andere personenbezogene Daten an den Unfallversicherungsträger zu übermitteln.

Dementsprechend hat der Unfallversicherungsträger als derjenige dem Betroffenen Auskunft über seine personenbezogenen Daten zu erteilen, der für die Verarbeitung verantwortlich ist. Art. 15 DSGVO verpflichtet vom Wortsinn her eindeutig den Verantwortlichen und eröffnet nicht die Möglichkeit, sich dieser Verpflichtung durch einen Verweis auf Dritte zu entziehen. Art. 23 Abs. 1 lit. i i. V. m. Abs. 2 lit. c DSGVO vermag eine Abweichung von dem Grundprinzip der DSGVO, entgegen der Auffassung im Referentenentwurf (RefE, S. 460), nicht zu decken.

Da sich der Auskunftsanspruch des Versicherten gegenüber dem Unfallversicherungsträger direkt aus Art. 15 DSGVO ergibt, bedarf es der Regelung des § 201 Abs. 1 S. 3 SGB VII nicht mehr. Ebenso verhält es sich mit der dem Unfallversicherungsträger obliegenden Informationspflicht im Fall der Dritterhebung gem. Art. 14 Abs. 1 lit. c DSGVO. Dabei ist gem. Art. 14 Abs. 2 lit. f DSGVO auch über die Quelle zu unterrichten, aus der personenbezogenen Daten stammen. Eine Normierung

der Informationspflicht im nationalen Recht ist entbehrlich, weil sich der Anspruch direkt aus der DSGVO ergibt (so auch RefE, S. 460).

Entbehrlich ist auch die Regelung des bisherigen § 201 Abs. 1 S. 5 SGB VII, der eine Unterrichtungspflicht des Arztes vorsieht, die sich für Ärzte, welche Daten an den Unfallversicherungsträger übermitteln, nunmehr direkt aus Art. 13 DSGVO ergibt. Sie haben danach den Patienten unter anderem über die Kategorien von Empfängern der personenbezogenen Daten (Abs. 1 lit. e) oder über das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen (Abs. 2 lit. b) zu informieren. Im Hinblick auf diese Pflichten bedarf es keiner Regelung im nationalen Recht. Diese Informationspflicht ersetzt aber auch nicht das Auskunftsrecht des Unfallversicherungsträgers, wie es die Begründung des Referentenentwurfs nahezulegen scheint (RefE. S. 460).

Dagegen kann eine ärztlich unterstützte Vermittlung der Inhalte einer Akte, über die der Versicherte gem. Art. 15 DSGVO gegenüber dem Unfallversicherungsträger Auskunft erlangt, in bestimmten Fällen gleichwohl erforderlich sein, sodass der Verweis auf § 25 Abs. 2 SGB X erhalten bleiben sollte. Die bisher gefundene Formulierung *„Für die Unterrichtung des Versicherten aufgrund seines Auskunftsrechts nach Artikel 15 [DSGVO] gilt § 25 Absatz 2 des Zehnten Buches entsprechend"* ist jedenfalls missverständlich, als sie das Auskunftsrecht durch den Verweis auf § 25 Abs. 2 SGB X auf den Arzt zu übertragen scheint. Es bedarf daher einer anderen Formulierung.

c. Änderungsvorschlag der Bundesärztekammer

Die mit Art. 125 Nr. 10 lit. b) des 2. DSAnpUG-EU vorgeschlagene Regelung des § 201 Abs. 1 S. 3 SGB VII-E, das dem Wortsinn nach das Auskunftsrecht des Unfallversicherungsträgers auf den Arzt überträgt, ist unzulässig, jedenfalls aber missverständlich und daher wie folgt zu ändern:

„Soweit der Versicherte sein Auskunftsrecht nach Artikel 15 der Verordnung (EU) 2016/679 über die von den Ärzten und den Psychotherapeuten übermittelten Angaben zu seinen gesundheitlichen Verhältnissen gegenüber dem Unfallversicherungsträger geltend macht, gilt § 25 Absatz 2 des Zehnten Buches entsprechend."

2. Zu Nummer Nr. 6 (§ 188 S. 3 SGB VII-E) und Nummer 12 (§ 203 Abs. 2 SGB VII-E)

Hinsichtlich der beabsichtigten Änderungen zu § 188 S. 3 SGB VII-E und § 203 Abs. 2 SGB VII-E, ist unzutreffend, dass das bisherige Recht beibehalten wird (so aber RefE. S. 458, 460). Die Regelungsvorschläge, welche datenschutzrechtliche Pflichten der Leistungsträger auf Ärzte übertragen, sind – wie § 201 Abs. 1 S. 3 SGB VII-E – nicht mit der DSGVO zu vereinbaren. Insoweit wird auf die vorstehenden Ausführungen verwiesen (s. C., VII., 1.).

D. Ergänzender Änderungsbedarf

I. Praktikable Regelung der datenschutzrechtlichen Informationspflichten

Ferner von erheblicher Bedeutung sind eine Vereinfachung und Praktikabilität des Datenschutzes und ein Abbau einer damit verbundenen Bürokratie. Insbesondere bedarf es praxisgerechter Ausnahmen hinsichtlich der weitreichenden Informationspflichten, die Ärzte in der Praxis treffen.

Im Bundesgesetz über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzte in Österreich ist für den ärztlichen Bereich in § 3b Abs. 2 Ärztegesetz eine bemerkenswerte Ausnahme vorgesehen: *„Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 sind die Rechte und Pflichten gemäß Art. 13, 14, 18 und 21 Datenschutz-Grundverordnung ausgeschlossen."* Diese Ausnahme von der Erfüllung bestimmter Betroffenenrechte wird aufgrund Art. 23 DSGVO insbesondere zum „Schutz der öffentlichen Gesundheit" und in Ansehung des „beträchtlichen und unverhältnismäßigen Aufwandes" statuiert.

Die der Transparenz der Datenverarbeitung dienenden Pflichten zur Information der Betroffenen gem. Art. 13 und 14 DSGVO stoßen auch in der ärztlichen Praxis deutscher Ärzte auf erhebliche Probleme und die Erfüllung dieser Pflichten sollte in einem angemessenen Verhältnis zu dem dazu erforderlichen Aufwand stehen. Zwar können die Pflichten in den meisten Fällen durch Aushändigung oder Aushang entsprechender Informationsblätter in der Arztpraxis erfüllt werden. In einigen Situationen, wie z. B. im Rahmen der telefonischen Terminvereinbarung oder einer zulässigen Fernbehandlung, welche eine Erhebung von Daten in der Arztpraxis zur Folge haben, kann deren Umsetzung jedoch nicht ohne Weiteres erfolgen, ohne dass der Praxisbetrieb nachteilig beeinflusst und Behandlungsmaßnahmen unnötig hinausgezögert werden. So kann am Telefon die Information weder schriftlich (Art. 12 Abs. 1 S. 2 DSGVO) noch „zum Zeitpunkt der Erhebung" (Art. 12 Abs. 1 DSGVO) erfolgen, weil die personellen Voraussetzungen in Arztpraxen dies in der Regel nicht zulassen und Patienten vordringlicher an der Terminvereinbarung interessiert sein werden als an einer umfangreichen datenschutzrechtlichen Information über alle in Art. 13 Abs. 1 und 2 DSGVO aufgeführten Inhalte.

Sinnvoll und im Interesse der Verhältnismäßigkeit geboten wäre es daher, die Erfüllung der Informationspflichten einzuschränken. Ausnahmen wären zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zum Schutz der betroffenen Person gem. Art. 23 Abs. 1 lit. e und i DSGVO möglich. Die Aufrechterhaltung einer wirksamen und effektiven Gesundheitsversorgung stellt ein wichtiges Gemeinwohlinteresse dar, das nicht zuletzt dem Patienten zu dienen bestimmt ist. Eine Nachholung der Informationspflicht anlässlich des auf die Terminvereinbarung folgenden Praxisbesuchs erscheint sachgerecht und verhältnismäßig. Eine Regelung, die in § 32 Abs. 1 DSGVO aufgenommen werden sollte, könnte wie folgt lauten:

> *„Die Pflicht zur Information gemäß Artikel 13 und Artikel 14 der Verordnung (EU) 679/2016 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn die Informationserteilung die ordnungsgemäße Erfüllung der im öffentlichen Interesse liegenden ärztlichen Aufgaben beeinträchtigen würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss."*

II. Abstimmung des Datenschutzrechts mit § 630g BGB

Ferner ist eine Abstimmung des datenschutzrechtlichen Auskunftsrechts gem. Art. 15 DSGVO mit dem auf dasselbe Interesse gerichtete Einsichtsrecht des Patienten gem. § 630g BGB vorzunehmen. Aus datenschutzrechtlicher Sicht ist Art. 15 DSGVO anzuwenden, wenn der Patient Auskunft über die zu seiner Person gespeicherten (Gesundheits-)Daten begehrt. Aus vertragsrechtlicher Sicht (Behandlungsvertrag) hat der Patient gem. § 630g BGB grundsätzlich das Recht, auf Verlangen unverzüglich Einsicht in seine vollständige Patientenakte oder das Recht eine Kopie zu erhalten. Wie der Gesetzesbegründung zu § 630g BGB zu entnehmen ist, dient die Regelung insbesondere der Umsetzung des Rechts des Patienten auf informationelle Selbstbestimmung, denn der Patient habe ein schutzwürdiges Interesse zu wissen, wie mit seiner Gesundheit umgegangen wurde, welche Daten sich dabei ergeben haben und wie die weitere Entwicklung eingeschätzt wird (BT-Drs. 17/10488, S. 26). Auf dasselbe Interesse ist Art. 15 DSGVO gerichtet, der das in Art. 8 Abs. 2 S. 2 EU-Grundrechtecharta verbürgte Recht der Person konkretisiert, Auskunft über die sie betreffenden erhobenen Daten zu erhalten. Insoweit besteht Deckungsgleichheit als in der Regel nach lebensnaher Betrachtung beide Rechte zusammen geltend gemacht werden und die Ansprüche inhaltlich auf dieselben Informationen gerichtet sind.

Da § 630g BGB die Rechtsprechung des Bundesverfassungsgerichts aus dem Jahre 2006 (BVerfG NJW 2006, 1116) aufgreift und wichtige Ausnahmen vom Einsichtsrecht vorsieht, stellt die Regelung eine auf den Gesundheitsbereich spezifisch zugeschnittene Vorschrift dar, die beibehalten bleiben muss. Insbesondere die in der Norm benannten Verweigerungsgründe (therapeutische Gründe, entgegenstehende Rechte Dritter) dienen dem „Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen" i. S. v. Art. 23 Abs. 1 lit. i DSGVO. Teilweise wird diesen entgegenstehenden Interessen auch in der DSGVO Rechnung getragen. So darf das Recht auf Erhalt einer Kopie gem. Art. 15 Abs. 3 DSGVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (vgl. Art. 15 Abs. 4 DSGVO). Für die bedeutsamen „therapeutischen Gründe" finden sich indes keine Entsprechungen in der DSGVO.

Aus diesen Gründen bedarf es einer Klarstellung, welche der Normen Anwendung finden soll. Schon das OLG Hamm hatte zum Verhältnis von § 630g BGB zum BDSG a. F. die Auffassung vertreten, dass die Vorschriften des BDSG nicht neben der Spezialregelung aus dem BGB anwendbar seien (OLG Hamm, Urt. v. 02.01.2017 – 3 W 43/16). Diese Frage muss für das Verhältnis zur DSGVO nunmehr wegen des grundsätzlichen Anwendungsvorrangs der DSGVO und der lex posterior-Regel vom Gesetzgeber neu bewertet und entschieden werden.

Vorzugswürdig ist die Klarstellung, dass das datenschutzrechtliche Auskunftsrecht durch Ausübung des durch § 630g BGB gewährleisteten Einsichtsrechts realisiert werden kann. Entsprechend der Änderung in Art. 15 (Änderung des Personenstandsgesetzes, zu § 68a) des Referentenentwurfs zum 2. DSAnpUG-EU sollte folgende Regelung in das BDSG aufgenommen werden:

> *„Das Auskunftsrecht nach Artikel 15 Absatz 1 und das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) werden dadurch gewährleistet, dass der betroffenen Person unter den Voraussetzungen von § 630g Absatz 1 und 2 des Bürgerlichen Gesetzbuches Einsicht in die sie betreffende Patientenakte zu gewähren ist."*

III. Ausnahmeregelungen für ärztliche Berufsgeheimnisträger im BKA-Gesetz

Keine Berücksichtigung im Referentenentwurf hat das seit dem 25.05.2018 geltende Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG) gefunden, obgleich dieses dringend der Überarbeitung bedarf. Ärzten ist der gleiche strikte verfassungsrechtliche Schutz als Berufsgeheimnisträger gegenüber Ausspähung und Überwachung durch staatliche Dienste einzuräumen wie z. B. Rechtsanwälten.

Mit Schreiben vom 19.04.2017 hatte sich bereits der Präsident der Bundesärztekammer an den Bundesminister des Innern gewendet und darauf hingewiesen, dass von den im BKA-Gesetz vorgesehenen Maßnahmen zur Abwehr terroristischer Bedrohungen auch Ärzte mitbetroffen sein können, wenn es zu einer Überwachung einer ihrer Patienten kommen sollte. Insbesondere verdeckte Eingriffe in informationstechnische Systeme einer Praxis oder eines Krankenhauses, Durchsuchungen von Praxisräumen oder andere eingriffsintensive Überwachungsmaßnahmen werden zu einer Beeinträchtigung der Geheimhaltungsinteressen von Patienten führen. Betroffen sind nicht nur Zielpersonen, sondern sämtliche in medizinischen Einrichtungen versorgte Patienten, wenn z. B. auf informationstechnische Systeme zugegriffen wird, die Informationen aller dort behandelten Patienten speichern. Zugleich stellt diese Verletzung des Patientengeheimnisses eine erhebliche Belastung für das vertrauensvolle Arzt-Patienten-Verhältnis dar und beeinträchtigt damit die ärztliche Berufsausübung.

Das Bundesverfassungsgericht hatte dem Gesetzgeber in seinem Urteil vom 20.04.2016 – 1 BvR 966/09 aufgegeben, im BKA-Gesetz besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie einen Schutz von Berufsgeheimnisträgern vorzusehen. Das BKA-Gesetz soll ausweislich seiner Begründung „umfangreiche Änderungen der Voraussetzungen [...] zum Schutz des Kernbereichs privater Lebensgestaltung [und] zum Schutz von Berufsgeheimnisträgern" einführen (BT-Drs. 18/11163, S. 77). Nach § 62 BKAG sind aber nur bestimmte Berufsgruppen von den Maßnahmen des BKAG ausgenommen. Ärzte zählen nicht dazu, weil sich gem. § 62 Abs. 1 S. 7 sowie Abs. 2 S. 3 BKAG die Ausnahmeregelung lediglich auf „Rechtsanwälte oder Kammerrechtsbeistände" erstreckt. Diese Differenzierung ist nicht sachgerecht, denn sie ignoriert und beeinträchtigt fundamental das Vertrauensverhältnis zwischen den im medizinischen Bereich tätigen Berufsgeheimnisträgern und Patienten, die um deren ärztliche Hilfe ersuchen müssen. Vertrauen ist aber konstitutiv für dieses Verhältnis. Nur Patienten, die sich sicher sein können, dass Angaben über ihre Krankheit und weitere höchst sensible Informationen nicht zur Kenntnis Dritter gelangen, werden die für ihre medizinische Versorgung erforderlichen Angaben machen. Diese hoch sensiblen Informationen sind zugleich Grundvoraussetzung dafür, dass Ärzte eine qualifizierte Versorgung gewährleisten können; ein vertrauensvolles Verhältnis ist die Basis für eine funktionsfähige ärztliche Gesundheitsversorgung insgesamt. Darüber hinaus kann die Vertrauensbedürftigkeit der Kommunikationsbeziehung essentiell für die von Art. 12 Abs. 1 GG geschützte Berufsausübung sein, worauf auch das Bundesverfassungsgericht in der genannten Entscheidung hinwies (Rn. 258).

Die Vertrauensbeziehung zwischen Arzt und Patient betrifft bisweilen sogar den absolut geschützten Kernbereich der privaten Lebensgestaltung. Gerade Ärzte erlangen im Rahmen des Gesprächs mit ihren Patienten nicht selten intimste Informationen aus der inneren Persönlichkeitssphäre. Das betrifft nicht nur ärztlich-psychotherapeutische Gespräche, die insoweit mindestens gleichermaßen zu schützen sind, wie etwa das Gespräch eines Strafverteidigers mit seinem Mandanten aus Anlass eines begangenen Sachbeschädigungsdelikts. Ferner hatte das Bundesverfassungsgericht in der genannten Entscheidung bereits darauf hingewiesen, dass neben Familienangehörigen, Geistlichen und Verteidigern auch

Ärzte als Personen des höchstpersönlichen Vertrauens an der geschützten nichtöffentlichen Kommunikation des Einzelnen teilnehmen, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden (Rn. 121). Daher muss auch die Arzt-Patienten-Beziehung absolut vor Überwachungsmaßnahmen geschützt werden und nicht nur einer Abwägungsentscheidung im Einzelfall überlassen sein.

Auch im Rahmen einer gemeinsamen Resolution mit anderen Berufsverbänden hatte die Bundesärztekammer im April 2017 den Bundesgesetzgeber dementsprechend aufgefordert, alle in § 53 Abs. 1 S. 1 Nr. 3 StPO genannten Berufe gleichermaßen absolut vor Überwachungsmaßnahmen zu schützen und den Schutz nicht auf einzelne Berufe zu beschränken. § 62 Abs. 1 S. 7, in Abs. 2 S. 1 der Verweis auf § 53 Abs. 1 S. 1 Nr. 3 der StPO, Abs. 2 S. 3 BKAG und § 41 Abs. 3 S. 6 BKAG sollten gestrichen werden.

Der Bundesgesetzgeber kam dieser Forderung nicht nach. Der 120. Deutsche Ärztetag 2017 lehnte im Leitantrag Ia-01 daraufhin die vom Bundestag beschlossene Novelle des sogenannten BKA-Gesetzes ab: *„Der Gesetzgeber hat es trotz heftiger Proteste der Ärzteschaft versäumt, bei Überwachungsmaßnahmen auch Ärztinnen und Ärzte in den Kreis besonders geschützter Personengruppen aufzunehmen. Dabei hatte das Bundesverfassungsgericht in seinem Urteil vom 20.04.2016 darauf hingewiesen, dass neben Familienangehörigen, Geistlichen und Verteidigern auch Ärzte als Personen des höchstpersönlichen Vertrauens an der geschützten nichtöffentlichen Kommunikation des Einzelnen teilnehmen, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden. Das Gesetz verstößt gegen die Intention des Gerichtes. Verdeckte Eingriffe in die Systeme einer Praxis oder eines Krankenhauses beeinträchtigen das Geheimhaltungsinteresse der Patientinnen und Patienten, zumal nicht sichergestellt werden kann, dass bei solchen Maßnahmen nicht auch die Daten anderer Patienten offengelegt werden. Patienten sind eine besonders geschützte Personengruppe und deshalb muss bei Ärzten der gleiche Vertrauensschutz gewährleistet werden wie bei Strafverteidigern und Abgeordneten."*

Auch die Entschließung Ia-04 des 120. Deutschen Ärztetages betont, dass das Vertrauensverhältnis zwischen Ärzten und Patienten zu schützen ist und das BKA-Gesetz daher überarbeitet werden muss. Das Gesetz sei dahingehend zu novellieren, dass Ärztinnen und Ärzten sowie Psychologischen Psychotherapeuten der gleiche strikte verfassungsrechtliche Schutz als Berufsgeheimnisträger gegenüber Ausspähung und Überwachung durch staatliche Dienste eingeräumt wird wie Geistlichen, Bundestagsabgeordneten und Rechtsanwälten. Zur Begründung wird Folgendes angeführt: *„Ein geschütztes Vertrauensverhältnis zwischen Arzt und Patient ist die Grundlage jeglicher ärztlicher Tätigkeit. Dieses gehört selbstverständlich zum Kernbereich privater Lebensführung, dessen Schutz das Bundesverfassungsgericht 2016 in seiner Entscheidung gegen das bisherige BKA-Gesetz gefordert hat. Ohne den Schutz der ärztlichen Schweigepflicht vor Ausspähung und Überwachung durch staatliche Institutionen wird darüber hinaus ein ärztlicher oder psychotherapeutischer Beitrag zur Gefahrenabwehr z. B. durch psychisch kranke Gewalttäter kaum noch möglich sein, da diese sich dann eher gar nicht mehr in Behandlung begeben werden. Die kürzlich erfolgte Novelle des Gesetzes entspricht nicht den Anforderungen des Bundesverfassungsgerichtes in seiner Entscheidung vom April 2016, in der es einen besseren Schutz der Berufsgeheimnisträger gefordert hatte. Die Wahrung der ärztlichen Schweigepflicht ist unabdingbar; sie kann nicht Gegenstand einer Abwägungsentscheidung sein."*

Unter Berücksichtigung dieser Forderungen und der von Verfassung wegen besonders geschützten Vertraulichkeit im Arzt-Patienten-Verhältnis besteht ein gesteigerter Schutzbedarf auch für die Berufsgruppe der Ärzte. Daher sollte der Gesetzgeber den ihm eingeräumten Gestaltungsspielraum ausüben und Ärzte von der Ausnahmeregelung des § 62 BKAG erfassen. Aus den genannten Gründen sollten § 62 Abs. 1 S. 7 und Abs. 2 S. 3 BKAG gestrichen oder jedenfalls vor dem Wort „Rechtsanwälte" um den Zusatz „Ärzte,"

ergänzt werden. Ferner bedarf es aus den genannten Gründen einer entsprechenden Änderung in § 41 Abs. 3 S. 6 BKAG betreffend des dort geregelten Auskunftsverweigerungsrechts: Dort sollte Abs. 3 S. 6 BKAG gestrichen oder jedenfalls vor dem Wort „Rechtsanwälte" um den Zusatz „Ärzte," ergänzt werden.

IV. Anpassung weiterer zivilrechtlicher Vorschriften an die DSGVO zur Eindämmung missbräuchlicher Abmahnungen

Das Land Bayern hat mit Datum vom 26.06.2018 einen „Entwurf eines Gesetzes zur Anpassung zivilrechtlicher Vorschriften an die Datenschutz-Grundverordnung" im Bundesrat eingebracht (BR-Drs. 304/18). Damit soll unter anderem einem Abmahnmissbrauch dadurch begegnet werden, dass bloße Verstöße gegen datenschutzrechtliche Unterrichtungs- und Mitteilungspflichten keine zivilrechtlichen Drittansprüche nach dem UKlaG begründen können und klargestellt werden, dass Datenschutzvorschriften keine Marktverhaltensregelungen i. S. .d. § 3a UWG darstellen. Dieses Vorhaben entspricht der Auffassung der Bundesregierung, einen Missbrauch des Abmahnrechts im Zusammenhang mit dem Datenschutz zu verhindern.[9]

Die Bundesärztekammer begrüßt das Vorhaben insoweit, als damit zu eigenen Geschäftszwecken in größerem Umfang erfolgende missbräuchliche Abmahnungen eingedämmt werden sollen. Es sollten insbesondere bloße Verstöße gegen datenschutzrechtliche Informationspflichten keine zivilrechtlichen Ansprüche Dritter begründen können (vgl. BR-Drs. 304/18, S. 2). Die Kontrolle der Einhaltung des Datenschutzes und eine darauf bezogene Aufsicht kann effektiv und kompetent durch die zuständigen Aufsichtsbehörden für den Datenschutz durchgeführt werden. Für die Durchsetzung des Datenschutzrechts sieht die DSGVO empfindliche Sanktionen vor, sodass eine Durchsetzung des Datenschutzes auf diesem Wege bereits in wirksamer Weise erreicht werden kann.

[9] S. die Antwort der Bundesregierung auf die kleine Anfrage der BT-Drs. 19/2811 zu Auswirkungen der Datenschutz-Grundverordnung im Gesundheits- und Pflegebereich, BT-Drs. 19/3194, S. 6 unter Hinweis auf den Koalitionsvertrag, Rz. 5819).