



Wortprotokoll der 110. Sitzung

Innenausschuss

Berlin, den 27. März 2017, 10:30 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum E 400

Vorsitz: Ansgar Heveling, MdB

Öffentliche Anhörung

Einzigiger Tagesordnungspunkt

Gesetzentwurf 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)**

BT-Drucksache 18/11325

Federführend:

Innenausschuss

Mitberatend:

Ausschuss für Wahlprüfung, Immunität und
Geschäftsordnung

Ausschuss für Recht und Verbraucherschutz

Ausschuss für Ernährung und Landwirtschaft

Ausschuss für Bildung, Forschung und

Technikfolgenabschätzung

Ausschuss Digitale Agenda

Gutachtlich:

Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:

Abg. Stephan Mayer (Altötting) [CDU/CSU]

Abg. Gerold Reichenbach [SPD]

Abg. Jan Korte [DIE LINKE.]

Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]



Inhaltsverzeichnis

Seite

I. Anwesenheitslisten	4
II. Sachverständigenliste	10
III. Sprechregister der Sachverständigen und Abgeordneten	11
IV. Wortprotokoll der Öffentlichen Anhörung	12
V. Anlagen	41
Änderungsantrag der Fraktionen der CDU/CSU und SPD zu Drucksache 18/11325	18(4)842
<u>Stellungnahmen der Sachverständigen zur Öffentlichen Anhörung</u>	
Peter Schaar	18(4)824 A
Lina Ehrig	18(4)824 B
Rechtsanwalt Dr. Carlo Piltz	18(4)824 C
Rechtsanwalt Andreas Jaspers	18(4)824 D
Prof. Dr. Heinrich Amadeus Wolff	18(4)824 E
Karsten Neumann	18(4)824 F
Prof. Dr. Hartmut Aden	18(4)824 G
Andrea Voßhoff	18(4)824 H = 18(4)788

Unangeforderte Stellungnahmen

Deutscher Richterbund, Berlin	18(4)737
Deutsche Wissenschaft (gemeinsame Stellungnahme)	18(4)779 neu
Die Wirtschaftsauskunfteien e. V., Neuss	18(4)787
Institut der Wirtschaftsprüfer in Deutschland e. V., Düsseldorf	18(4)792
Bundesverband E-Commerce und Versandhandel Deutschland e. V., Berlin	18(4)812
Bundesvereinigung der Deutschen Arbeitgeberverbände, Berlin	18(4)813
Wirtschaftsprüfkammer, Berlin	18(4)814
Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e. V., Frankfurt am Main	18(4)820
Verband Forschender Arzneimittelhersteller e. V., Berlin	18(4)821
Bundesärztekammer, Berlin	18(4)826
Bundesverband Großhandel, Außenhandel, Dienstleistungen e. V., Berlin	18(4)827
Gesamtverband der Deutschen Versicherungswirtschaft e. V., Berlin	18(4)829
Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V., Eschborn	18(4)830
Deutsche Krankenhausgesellschaft e. V., Berlin	18(4)832
Deutscher Gewerkschaftsbund, Bundesvorstand, Berlin	18(4)833
Die Deutsche Kreditwirtschaft, Berlin	18(4)834
Bundessteuerberaterkammer, KdöR, Berlin	18(4)839
Handelsblatt Fachmedien GmbH, Redaktion Datenschutz-Berater, RA Dr. Philipp Kramer, Hamburg	18(4)850

Gutachterliche Stellungnahme des Parlamentarischen Beirats
für nachhaltige Entwicklung

zu Bundestags-Drucksache 18/11325	18(4)794
-----------------------------------	----------



0/f

18. Wahlperiode



Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)

Montag, 27. März 2017, 10:30 Uhr

CDU/CSU

Ordentliche Mitglieder

Unterschrift

Baumann, Günter

Binninger, Clemens

Bosbach, Wolfgang

Frieser, Michael

Hellmuth, Jörg

Heveling, Ansgar

Hoffmann (Dortmund), Thorsten

Lindholz, Andrea

Mayer (Altötting), Stephan

Ostermann Dr., Tim

Schäfer (Saalstadt), Anita

Schuster (Weil am Rhein), Armin

Veith, Oswin

Warken, Nina

Wendt, Marian

Wichtel, Peter

Woltmann, Barbara

Zertik, Heinrich

21. März 2017

Anwesenheitsliste gemäß § 14 Abs. 1 des Abgeordnetengesetzes
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32659 Fax: +49 30 227-36339

Seite 1 von 5



öf.

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 27. März 2017, 10:30 Uhr

SPD

Ordentliche Mitglieder

Castellucci Dr., Lars

Fograscher, Gabriele

Grötsch, Uli

Gunkel, Wolfgang

Hartmann, Sebastian

Lischka, Burkhard

Mittag, Susanne

Özdemir (Duisburg), Mahmut

Reichenbach, Gerold

Schmidt (Berlin), Matthias

Veit, Rüdiger

Unterschrift

Stellvertretende Mitglieder

Esken, Saskia

Fechner Dr., Johannes

Gerster, Martin

Högl Dr., Eva

Juratovic, Josip

Kolbe, Daniela

Unterschrift

21. März 2017

Anwesenheitsliste gemäß § 14 Abs. 1 des Abgeordnetengesetzes
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32659 Fax: +49 30 227-36339

Seite 3 von 5



9/

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 27. März 2017, 10:30 Uhr

DIE LINKE.

Stellvertretende Mitglieder

Pau, Petra

Unterschrift


BÜ90/GR

Ordentliche Mitglieder

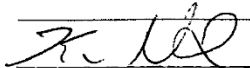
Amtsberg, Luise

Beck (Köln), Volker

Mihalic, Irene

Notz Dr., Konstantin von

Unterschrift



Stellvertretende Mitglieder

Haßelmann, Britta

Künast, Renate

Lazar, Monika

Mutlu, Özcan

Unterschrift

21. März 2017

Anwesenheitsliste gemäß § 14 Abs. 1 des Abgeordnetengesetzes
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32659 Fax: +49 30 227-36339

Seite 5 von 5



off.

Tagungsbüro



Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)

Montag, 27. März 2017, 10:30 Uhr

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

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Darenzke, Dirk	LINKE	
Alexander Lenxner	SPD	
LINKE, JÖRW	CDU/CSU	
PHILIPP VERGIN	LINKE	
Gephardt, WAW	Grüne	
Broume, Lea	Grüne	
Balzer, Sven	Grüne	

Stand: 20. Februar 2015

Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339



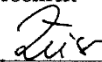
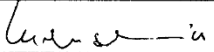
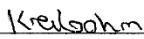
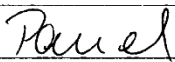


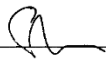
öf.

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 27. März 2017, 10:30 Uhr

Seite 3

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeichnung
Baden-Württemberg	Zeiser		RD
Bayern	Ludersch		RD
Berlin			
Brandenburg			
Bremen	Kreibohm		Hospitantin
Hamburg			
Hessen			
Mecklenburg-Vorpommern	PAUCH		
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz	Barth		
Saarland			
Sachsen	Kühne		RR'14
Sachsen-Anhalt	Stöterich		RR'14
Schleswig-Holstein			
Thüringen			

Stand: 20. Februar 2015

Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339



6/1

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 27. März 2017, 10:30 Uhr

Seite 4

Ministerium bzw. Dienststelle (bitte in Druckschrift)	Name (bitte in Druckschrift)	Unterschrift	Amts-be- zeich- nung
BfDI	Hermerschmidt		RD
ITfBI	Kraus		Ref
BMAS	Kleine		RR
BMI	Eickelpaich		RI
BMI	v. Viedtowski		RD
BMAS	Loth		
BfV	Quinich		MI
Bm	v. Knabloch		MD
BND	Kell		Ref.
BfV	Schawatz		Ref
BfV	Baier		RD
BfV	Deffner		MR
	Dr. Böhmer		MD
BfV	Kynner		RD
BK	Seedorf		RD
BfV	Oertgen		RR

Stand: 20. Februar 2015

Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339



Liste der Sachverständigen

Öffentliche Anhörung am Montag, 27. März 2017, 10.30 Uhr

Prof. Dr. Hartmut Aden

Hochschule für Wirtschaft und Recht Berlin

Lina Ehrig

Verbraucherzentrale Bundesverband e.V., Berlin

Rechtsanwalt Andreas Jaspers

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

Karsten Neumann

Landesbeauftragter für Datenschutz und
Informationsfreiheit Mecklenburg-Vorpommern a. D.
2b Advice, Bonn

Rechtsanwalt Dr. Carlo Piltz

Reusch Rechtsanwälte, Berlin

Peter Schaar

Vorsitzender der Europäischen Akademie für
Informationsfreiheit und Datenschutz e. V., Berlin

Andrea Voßhoff

Bundesbeauftragte für den Datenschutz und
die Informationsfreiheit, Bonn

Prof. Dr. Heinrich Amadeus Wolff

Universität Bayreuth



Sprechregister der Sachverständigen und Abgeordneten

<u>Sachverständige</u>	<u>Seite</u>
Prof. Dr. Hartmut Aden	14, 38
Lina Ehrig	15, 37
Rechtsanwalt Andreas Jaspers	16, 35
Karsten Neumann	17, 34
Rechtsanwalt Dr. Carlo Piltz	18, 32
Peter Schaar	20, 30
Andrea Voßhoff	21, 30
Prof. Dr. Heinrich Amadeus Wolff	23, 29
 <u>Abgeordnete</u>	
Vors. Ansgar Heveling (CDU/CSU)	12, 13, 14, 15, 16, 17, 18, 20, 21, 23, 24 26, 27, 28, 29, 30, 32, 35, 37, 38, 39
BE Abg. Stephan Mayer (Altötting) (CDU/CSU)	24
BE Abg. Gerold Reichenbach (SPD)	13, 27
Abg. Petra Pau (DIE LINKE.)	13, 26
BE Abg. Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN)	12, 28, 39



Einziger Tagesordnungspunkt

Gesetzentwurf 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)

BT-Drucksache 18/11325

Vors. **Ansgar Heveling** (CDU/CSU): Meine sehr geehrten Damen und Herren, ich würde gerne beginnen, ich bitte, Platz zunehmen.

Ich eröffne die 110. Sitzung des Innenausschusses, heute Morgen um kurz nach 10.30 Uhr. Die Sitzung findet als öffentliche Anhörung zum Datenschutz-Anpassungs- und Umsetzungsgesetz statt. Ich danke Ihnen, meine sehr geehrten Damen und Herrn Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss und ggf. aus den mitberatenden Ausschüssen zu beantworten. Die Ergebnisse dieser Anhörung dienen dazu, die Beratung zum Gesetzentwurf der Bundesregierung vorzubereiten. Ich darf auch herzlich alle anwesenden Gäste und Zuhörer begrüßen, und für die Bundesregierung Herrn Staatssekretär Dr. Ole Schröder.

Wie Sie sehen sind Kameras aufgebaut. Die Sitzung wird weltweit im Parlamentsfernsehen des Deutschen Bundestages übertragen.

Schriftliche Stellungnahme hatten wir, sehr geehrte Damen und Herren Sachverständige, trotz der Kürze der Vorbereitungszeit von Ihnen erbeten. Für die eingegangenen Stellungnahmen darf ich mich deshalb umso mehr bedanken. Sie sind an die Mitglieder des Innenausschusses und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll dieser Sitzung beigelegt. Ich gehe davon aus, dass Ihr Einverständnis zur Durchführung der Anhörung als öffentliche Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst und ernte damit keinen Widerspruch.

Von der heutigen Anhörung wird für ein Wortprotokoll eine Bandabschrift gefertigt. Das macht es auch erforderlich, dass Sie bitte wenn Sie sprechen das Mikrofon immer anstellen und auch ins Mikrofon sprechen, damit es entsprechend

aufgenommen wird. Das Protokoll wird Ihnen zur Korrektur übersandt. Im Anschreiben dazu werden Ihnen die Details zur weiteren Behandlung mitgeteilt. Die Gesamtdrucksache bestehend aus Protokoll und schriftlichen Stellungnahmen wird im Übrigen auch ins Internetangebot des Deutschen Bundestags eingestellt.

Zum zeitlichen Ablauf darf ich anmerken, dass eine Zeit bis 12.30 Uhr für die Sachverständigenanhörung vorgesehen ist. Einleitend erhalten Sie alle die Gelegenheit in einer Eingangsstellungnahme, die bitte fünf Minuten nicht überschreiten sollte, zum Beratungsgegenstand Stellung zu nehmen. Sie sehen, hier läuft keine Uhr rückwärts, sondern die Uhr des Vorsitzenden ist maßgeblich. Wenn sich die Zeit dem Ende nähert, werde ich durch dezentes Hüsteln darauf aufmerksam machen und wenn es dann noch weitergeht, behalte ich mir weitere Maßnahmen vor.

Dann würden wir mit der Beratung der Sachverständigen durch die Berichterstatterinnen und Berichterstatter sowie weitere Abgeordneter beginnen. Die Befragung wird auf Grund der einvernehmlichen Obleuteabsprache in die Themenkomplexe einerseits zur Umsetzung der Verordnung und andererseits danach zur Richtlinie unterteilt. Dies führt auch dazu, dass sowohl Herrn Prof. Dr. Aden als auch Herrn Schaar auf besonderen Fraktionswunsch hin Gelegenheit zu je dreiminütigen Eingangsstellungnahmen gegeben wird. Ich bitte auch darum, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die eine Frage gerichtet wird. Wobei ich im Interesse der Kolleginnen und Kollegen darum bitte, damit möglichst viele Fragen ermöglicht werden, Fragen knapp zu halten und limitiert zu stellen. Wenn Sie damit einverstanden sind, würden wir so verfahren.

Herr Kollege Dr. von Notz hat um das Wort gebeten, bevor wir dann zu den Eingangsstellungnahmen kommen.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ja, guten Morgen allerseits, vielen Dank, Herr Vorsitzender, meine Damen und Herren Sachverständige, auch ich danke Ihnen für Ihr Kommen. Ich möchte aber hier am Anfang einen Satz über das Verfahren verlieren, das parlamentarisch skandalös ist. Wir haben diese



Anhörung hier sowieso mit Kurzfristigkeit anberaumt, dass wir diese zwei Themen überhaupt in eine Anhörung pressen ist schon ein Vorgang für sich, der unfassbar ist. Wenn man sich das bei der EU-Datenschutzverordnung anschaut, das ist vielleicht das wichtigste Verfahren über die europäische Ebene, dass hier in den letzten fünf Jahren im Deutschen Bundestag ankommt. Das wird hier mit heißester Nadel gestrickt. Jetzt bekommen wir heute Morgen, vor einer dreiviertel Stunde, einen Änderungsantrag aus der Großen Koalition, den die Sachverständigen offensichtlich nicht kennen, und erfahren auch noch, dass das Ganze nicht etwa Ende April durch den Deutschen Bundestag gehen soll, sondern diese Woche. Das ist unfassbar. Wie soll man hier in diesem Haus seriöse Gesetze machen, wenn das so läuft? Das Ganze wird derzeit mit 70 Änderungsanträgen im Bundesrat diskutiert, wie soll das hier ernsthaft und seriös passieren? Ein Parlament, das das mitmacht, verzweifelt sich selbst und ich kann wirklich nur an die Kolleginnen und Kollegen der Großen Koalition appellieren, sich das nicht gefallen zu lassen. Das Parlament sind wir. Das ist vom Verfahren her irre. Es ist so – ich nehme das auch zur Kenntnis – wir können hier mit unserer Opposition wenig dagegen ausrichten, aber es ist parlamentarisch und diesem Haus unwürdig, deswegen protestiere ich. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege Dr. von Notz. Herr Kollege Reichenbach, bitte.

BE Abg. **Gerold Reichenbach** (SPD): Das kennen wir ja schon, wenn einem die inhaltlichen Argumente ausgehen, ruft man Skandal.

Wenn man jetzt von einem Hoppla-hopp-Verfahren spricht, mit Verlaub, dann muss man das letzte dreiviertel Jahr geschlafen haben. Die Anpassung wird seit einem dreiviertel Jahr öffentlich diskutiert. Jetzt kann man sagen, okay, das ist auch auf der Basis von Leaks erfolgt, aber alle, auch Zwischenentwurfsstände waren öffentlich und sind öffentlich diskutiert worden. Wir, beide Koalitionsparteien, haben bereits in der Einbringungsdebatte darauf hingewiesen, dass wir bei einer Reihe von Regelung noch Prüfungsbedarf sehen. Hätten wir die Anträge, die daraufhin entstanden sind, erst nach der Anhörung eingebracht, dann hätten Sie „Skandal“ gerufen, weil dann die Gutachter überhaupt keine Chance

gehabt hätten auf die Anträge einzugehen. Jetzt haben wir es, lehrend aus Ihrer letzten Monierung, genau umgekehrt gemacht, und die Änderungen wenn auch kurzfristig, so doch immerhin vorgelegt, sodass man darauf eingehen kann. Es sind ja jetzt auch nicht die weiten Bereiche, sondern die Bereiche, über die seit einem halben Jahr diskutiert wird, nämlich über die Betroffenenrechte. Dann passt es aber auch nicht. Es tut mir leid, Herr Dr. Konstantin von Notz, auch wenn ich Sie sonst sehr sympathisch finde, aber das sieht momentan sehr danach aus: Wenn man kein Haar mehr in der Suppe findet, neigt man den Kopf darüber und schüttelt ihn so lange, bis eines hineingefallen ist. Lassen Sie uns über die Inhalte diskutieren, vielleicht kommen wir da eher voran, zumal wir das Ganze ja auch gemeinsam im Bundesrat behandeln müssen. Auch da gebe ich den klugen Ratschlag: Wer auf die Bäume steigt, muss irgendwann auch wieder herunter kommen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege Reichenbach. Frau Kollegin Pau, bitte.

Abg. **Petra Pau** (DIE LINKE.): Ob das jetzt klug war, Kollege Reichenbach, so zu intervenieren, das ist natürlich Ihnen überlassen. Ich könnte noch sagen, gut, die Koalition hat sich die Kritik, die wir in der ersten Lesung hatten, zu Herzen genommen. Sie haben es in der letzten Woche nicht geschafft diesen Änderungsantrag zu übermitteln, als wir als Parlamentarier in der Sitzungswoche zusammensaßen. Ich könnte sagen, gut, dann beraten wir ihn heute noch mit, aber dann müssten sich die Koalition und die Fraktionen, die diese Koalition tragen, an eine weitere Verabredung halten. Weitere Verabredung hieß – und so ist es im Moment auch in der amtlich festgestellten Tagesordnung für diese Sitzungswoche verankert – dass wir in dieser Woche dieses Thema im Plenum des Bundestages nicht aufsetzen, sondern es erst in der nächsten Sitzungswoche abschließend behandeln. Das wäre seriös, weil, dann könnten wir uns mit Dingen, die sich heute noch ergeben, auch befassen – vielleicht Sie sogar inspirieren, noch weitere Änderungsanträge zu stellen, das halte ich nicht für ausgeschlossen.

Im Übrigen ist auch auf der bisherigen Tagesordnung des Innenausschusses für Mittwoch, den 29. März – zumindest in derjenigen, die mir heute früh in meiner Arbeitsgruppe Innenpolitik zur Verfügung stand – der Abschluss dieses



Verfahrens bisher nicht vorgesehen. Lassen Sie uns dann wenigstens zu den guten Sitten und Verabredungen zurückkehren und das in dieser Woche seriös auch nach der Anhörung behandeln und in der nächsten Sitzungswoche dann zu dem entsprechenden Schluss bringen. Ich jedenfalls werde jetzt meiner parlamentarischen Geschäftsführerin mitteilen, dass von uns aus gesehen kein Einvernehmen zur Feststellung der Erweiterung der Tagesordnung in dieser Sitzungswoche erklärt werden kann.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Kollegin Pau. Sie haben es richtigerweise schon angesprochen, das ist jetzt dann Angelegenheit der parlamentarischen Geschäftsführer was den Punkt angeht, den Sie als letztes angesprochen haben. Die Dinge, die vorher diskutiert wurden, sind ausgetauscht worden. Ich möchte nur darauf hinweisen, dass wir jetzt selbstverständlich den vorliegenden Änderungsantrag auf Ausschussdrucksache 18(4)842 auch den Sachverständigen zur Verfügung gestellt haben. Das sind die drei Seiten Änderungsantrag der CDU/CSU- und der SPD-Fraktion. Wir beginnen jetzt mit den Eingangsstellungnahmen und dazu darf ich Herrn Prof. Dr. Aden als Erstem für sein bis zu fünfminütiges Eingangsstatement das Wort geben.

SV Prof. Dr. Hartmut Aden (Hochschule für Wirtschaft und Recht Berlin): Herr Vorsitzender, meine Damen und Herren, ich danke Ihnen zunächst für die Einladung. Wie verabredet beschränkt sich meine schriftliche Stellungnahme, auf die ich verweisen möchte und für deren Verteilung ich danke, auf die Umsetzung der Richtlinie, der sogenannten Polizei- und Justizrichtlinie.

Leider ist diese Richtlinie sowohl in der Beratung auf EU-Ebene als auch jetzt in der Umsetzungsphase immer ein bisschen im Schatten der Verordnung gewesen. Wenn Sie meine Stellungnahme anschauen, werden Sie sehen, dass das sicherlich nicht gerechtfertigt ist und dass auch diese Richtlinie und ihre Umsetzung noch einer genaueren Betrachtung bedürfen.

Ich habe schon Bedenken gegen die Systematik, denn wir haben hier neuerdings ein Gesetz, in dem es zwei allgemeine Teile für die beiden großen Abschnitte geben wird. Das erscheint mir sehr

unsystematisch, bei aller Problematik die ich anerkenne: Wenn man gleichzeitig eine Verordnung und eine Richtlinie von der EU umzusetzen hat, muss man doch darauf achten, dass das Gesetz auch noch für die Anwendung geeignet ist, und zwar bis hin zur Sachbearbeiterebene in den Sicherheitsbehörden. Ich habe erhebliche Bedenken, ob das so funktionieren kann. Ich würde Ihnen raten, den allgemeinen Teil, was die Begriffsdefinition angeht, aber auch die Grundprinzipien, zusammenzuführen.

Der Umsetzungsentwurf enthält einige Problematiken, die mit diesem Gesetz sicherlich nicht abschließend gelöst werden, weil die Richtlinie für einige Bereiche schon nicht abschließend ist. Man denke etwa an die Datenverarbeitung durch die europäischen Agenturen. Dieses Thema wurde in der Richtlinie ausgeklammert. Das wird uns hier noch weiter beschäftigen. Man könnte durchaus auch jetzt schon vordenken, was das eigentlich heißt, denn da geht es auch um die Zusammenarbeit der Bundesbehörden mit den europäischen Agenturen. Das ist durchaus auch wieder ein Thema, das auf den Deutschen Bundestag zukommen wird und das man meines Erachtens auch schon jetzt mitdenken kann.

Ich habe in meiner schriftlichen Stellungnahme auch darauf hingewiesen, dass es eine Reihe von ganz konkreten Nachbesserungsmöglichkeiten gibt. Insofern könnte sich auch da die Zahl der Änderungsanträge noch erhöhen. Zunächst einmal ist mir als jemandem, der Leuten in Sicherheitsbehörden Recht beibringen muss, aufgefallen, dass es nicht sehr hilfreich ist, unnötig einfach nur den Richtlinien text in deutsche Gesetze hineinzukopieren. Man sollte sich zumindest die Mühe machen, die Bestimmungen an die deutsche Rechtssystematik und die rechtliche Terminologie anzupassen. Ich habe Ihnen ein schönes Beispiel in meiner Stellungnahme gebracht, da können Sie sich das näher anschauen. Aber es gibt eine ganze Reihe von Beispielen.

Es gibt auch inhaltliche Probleme, auf die zum Teil auch die Bundesdatenschutzbeauftragte hingewiesen hat. Man denke insbesondere an die Regelungen zu den besonders sensiblen Datenkategorien, aber auch an die Regelung zur



Zweckänderung. Wenn ich mir durchlese, was in diesem Umsetzungsgesetz vorgeschlagen ist, habe ich doch Befürchtungen, dass wir hinter die vorhandenen Rechtsschutzstandards zurückfallen werden. Da sehe ich durchaus erheblichen Präzisierungsbedarf in eine Richtung, die in ähnlicher Form auch die Bundesdatenschutzbeauftragte vorgeschlagen hat. Ich sehe im Übrigen auch Probleme mit dem deutschen Bestimmtheitsgebot, wenn man solche doch recht unbestimmten Formulierungen zu diesen sehr grundrechtssensiblen Themen in ein Bundesgesetz aufnimmt.

Schließlich gibt es auch, was die Stellung des Datenschutzes angeht, ein paar Nachbesserungsbedarfe. Mir ist aufgefallen, dass man aus dem alten Bundesdatenschutzgesetz eine Formulierung übernommen hat, nach der in den Fällen, in denen die Bundesdatenschutzbeauftragte stellvertretend Einsicht nimmt – wenn also die Behörden aus Geheimhaltungsgründen keine Auskunft erteilen – immer noch so eine Art Staatsgefahrklausel vorgesehen ist. Die halte ich für weder mit deutschen Grundrechten noch mit der Richtlinie für vereinbar. In der Richtlinie ist das schlicht und ergreifend nicht vorgesehen. Weiteres gerne auf Nachfrage. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Aden. Dann darf ich als nächstes Frau Ehrig das Wort geben.

SVe **Lina Ehrig** (Verbraucherzentrale Bundesverband e.V., Berlin): Herzlichen Dank, auch von meiner Seite für die Einladung und die Möglichkeit, hier aus Verbrauchersicht das Datenschutzanpassungsgesetz bewerten zu dürfen.

Das Thema Datenschutz beschäftigt uns schon seit Jahren. Die Verabschiedung der Datenschutzgrundverordnung war aus Verbrauchersicht ein Meilenstein. Nicht nur, weil sie die Verbraucherrechte konkretisiert und schärft und damit auch die Rechtsdurchsetzung verbessern wird, sondern auch, weil das Datenschutzrecht in Europa damit vollharmonisiert und das Marktortprinzip eingeführt wird. Das ist auch aus Unternehmenssicht ein riesiger Gewinn. Wir müssen jetzt schauen, dass wir bei der Anpassung des BDSG an die Datenschutzgrundverordnung diese Errungenschaften bewahren. Die geplanten Einschränkungen der Betroffenenrechte bspw.

könnten hier das Schutzniveau für Verbraucherinnen und Verbraucher abschwächen und damit auch hinter der Datenschutzgrundverordnung zurückfallen. Ich werde darauf gleich noch eingehen.

Vorher möchte ich ganz kurz erst einmal ein Lob für den Regierungsentwurf aussprechen, nämlich, weil die Bundesregierung sich entschieden hat, einen der größten Kritikpunkte aus dem Referentenentwurf – nämlich die Möglichkeit der Unternehmen, nachträglich die Datenverarbeitung zu anderen Zwecken durchzuführen, auch wenn diese nicht mit dem ursprünglichen Zweck vereinbar sind, und das alles auf Basis einer Interessenabwägung – nicht übernommen wurde. Das ist aus Verbrauchersicht und insgesamt mit Blick auf die Möglichkeiten, die uns die Datenschutzgrundverordnung bietet, ganz wichtig. Wir hoffen und appellieren, dass im weiteren Prozess eine entsprechende Zweckänderung nicht mehr Gegenstand des Entwurfs wird.

Das zweite, was wir begrüßen, ist die Übernahme der Regelungsinhalte zu den Scoring- und Auskunftfeiregelungen, die wir im Bundesdatenschutzgesetz bereits haben. Wichtig ist hierbei, dass es sich nicht um Datenschutzrecht, sondern um Regelungen des wirtschaftlichen Verbraucherschutzes handelt. Es werden hier Kriterien aufgestellt, wann eine Forderung als ausgefallen gilt. Dementsprechend war es auch nach einhelliger Ansicht aller Experten immer so, dass die Regelungen im BDSG praktisch an falscher Stelle verankert waren. Insofern begrüßen wir es, dass die Inhalte jetzt übernommen werden. Perspektivisch sollten sie dann aber auch in andere Gesetze überführt werden.

Ein Punkt, der uns große Kopfschmerzen bereitet, sind die Betroffenenrechte. Hier werden Einschränkungen vorgenommen, z. B. dass man Informationen bei einer Zweckänderung nicht geben muss, wenn es ein unverhältnismäßiger Aufwand ist. Hier sehen wir in der Datenschutzgrundverordnung keinerlei Spielraum, eine entsprechende Einschränkung vorzunehmen. Das Gleiche gilt für die Regelungen des Auskunfts- und des Löschrechts. Ganz konkret würde das – wenn man es auf den unverhältnismäßigen Aufwand reduziert – bedeuten, dass der kleine Laden an der Ecke, der wenige Kundendaten verarbeitet, in Zukunft seine Kunden informieren



müsste, wenn er die Daten zu einem anderen Zweck verarbeitet. Aber der große Konzern, der massenhaft Daten verarbeitet und diese dann nachträglich zu einem anderen Zweck verarbeiten will, könnte damit argumentieren, dass es sich hier um unverhältnismäßigen Aufwand handelt und die Betroffenen nicht informiert werden müssen. Wie gesagt, wir sehen hier in der Datenschutzgrundverordnung keinen Spielraum. Von daher erachten wir die Regelung als europarechtswidrig.

Die Aufsichtsbehörden haben schon angekündigt, dass sie die Regelungen in der Praxis nicht anwenden würden und sich einfach in ihrer Bewertung direkt auf die Datenschutzgrundverordnung berufen. Diese Ankündigung zeigt, dass wir hier schauen müssen, dass mit der Anpassung des BDSG an die Grundverordnung nicht massive Rechtsunsicherheit nicht nur für Verbraucher, sondern auch für Unternehmen, eintreten wird bei der Frage: Nach welchem Gesetz oder welcher Verordnung muss ich mich jetzt richten? Insofern sollten wir aus Verbrauchersicht die Anpassung des Datenschutzes an die Grundverordnung unbedingt nutzen, um die Errungenschaften zu bewahren und hier nicht durch die Anpassung größere Rechtsunsicherheit zu schaffen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Ehrig. Dann darf ich Ihnen, Herr Rechtsanwalt Jaspers, das Wort geben.

SV Rechtsanwalt Andreas Jaspers (Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn): Vielen Dank, meine Damen und Herren, ich möchte meine Stellungnahme in der Kürze der Zeit daraufhin fokussieren, welche Auswirkungen das neue BDSG insbesondere für die datenverarbeitende Wirtschaft hat und ob es zu praxisgerechten Lösungen führt.

Grundsätzlich ist anzumerken, dass es sich bei der Datenschutzgrundverordnung um eine neue Verordnungsform mit zahlreichen Öffnungen und verordnungsuntypischen vagen Formulierungen handelt. Aber gerade die sollen den nationalen Gesetzgeber die Möglichkeit geben, hier Konkretisierungen zu schaffen. Denn wenn man sich die Grundverordnung genau anschaut, finden wir auf der Ebene der Zulässigkeit aber auch der

Betroffenenrechte, eine deutliche Unterkomplexität im Verhältnis zum bisherigen BDSG, die durch das neue BDSG geschlossen werden sollte. Wenn ich mir den Verordnungsentwurf anschau und bewerte, komme ich zu dem Ergebnis, dass doch weitgehend praxisgerechte Lösungen gefunden werden. Insofern ist dieser Entwurf grundsätzlich zu unterstützen. Wichtig ist aus Sicht der datenverarbeitenden Wirtschaft natürlich, auch noch in dieser Legislaturperiode zum Abschluss zu kommen, denn Rechtssicherheit wird dringend von den datenverarbeitenden Stellen erwartet.

Ein paar Worte zum Thema Zulässigkeit und den Betroffenenrechten, die konkretisiert werden sollen. Meine beiden Vorredner haben schon einen Kernpunkt angeschnitten, der die Zulässigkeit der Datenverarbeitung anbetrifft, nämlich das Thema der Weiterverarbeitung personenbezogener Daten für Zwecke, die ursprünglich nicht festgestanden haben. Die Grundverordnung ist hier äußerst restriktiv in dem sie fordert, es muss Kompatibilität geben, die im Regelfall nicht vorliegt. Es gibt durchaus Sachverhalte, bei denen es aus organisatorischen Gründen dringend notwendig ist, Daten trotzdem weiterverarbeiten zu dürfen. Hier geht der Regierungsentwurf den Weg, dass er sagt: Es ist zulässig zur Geltendmachung, Ausübung und Verteidigung rechtlicher Ansprüche. Der Entwurf der Bundesregierung sieht nicht vor, dass es sich nur um zivilrechtliche Ansprüche handeln muss. Das ist meines Erachtens auch richtig, denn es kann durchaus auch sein, dass öffentlich-rechtliche Ansprüche auf ein Unternehmen zukommen und die muss es letztendlich auch bedienen können, ohne an der Kompatibilität zu scheitern. Stichwort wäre z. B. Förderanträge von öffentlicher Natur. Ich muss personenbezogene Daten weitergeben, um dem Förderantrag nachkommen zu können, die öffentliche Forderung zu erlangen. In diesem Fall hätte ich sonst keine Möglichkeit, d. h., ich brauche auch die öffentlich-rechtlichen Ansprüche, nicht nur die zivilrechtlichen. Ich weiß, dass die Grundverordnung hier eng ist, allerdings gibt es durchaus Möglichkeiten für diese Interpretation.

Es muss auch möglich sein, dass Ansprüche Dritter die Möglichkeit geben, die Daten weiter verarbeiten zu dürfen. Ich denke hier an Gläubigeranfragen zur Zwangsvollstreckung oder mögliche Schadensersatzansprüche von Dritten gegen eigene Arbeitnehmer: Mein Mitarbeiter fährt eine



Außenstehende an, dann möchte der Außenstehende natürlich wissen, wer das war, um Schadensersatzansprüche geltend machen zu können. Insofern müssen auch die Ansprüche Dritter bedient werden können. Das wäre im Grunde genommen nur gerecht, da wir anderweitig zu erheblichen rechtlichen Problemen kämen.

Beim Thema Beschäftigtendatenschutz ist sehr zu loben, dass die Regelung des alten § 32 in den § 26 überführt wird. Das schafft Rechtssicherheit insbesondere im Bereich des Beschäftigtendatenschutzes. Die bisherige Rechtsprechung zum Beschäftigtendatenschutz, die auch sehr arbeitnehmerfreundlich ausgestaltet ist, kann dann entsprechend fortgeführt werden. Ein paar Vorschläge haben wir gemacht, wie man das ändern könnte. Wenn z. B. für Einwilligungen die Schriftform verlangt wird, ist das ziemlich bürokratisch. Wenn der Arbeitgeber fragt, ob der Arbeitnehmer einverstanden ist, unter bestimmten Bedingungen die Privatnutzung zu erlauben, sollte man auch mit E-Mail zustimmen können und nicht zum Lohnbüro zur Unterschrift laufen müssen. Insofern: Textform statt Schriftform.

Ein weiterer Punkt, den ich ansprechen möchte, ist die Möglichkeit, investigativ tätig zu werden. Auch hier sollte dem Vorschlag des Bundesrates gefolgt werden, auch bei schweren Verfehlungen die Berechtigung zu geben, diese Daten verarbeiten zu dürfen. Ansonsten müsste der Arbeitgeber wirklich wissen, dass es sich um eine Straftat handelt. Im Grunde genommen ist das manchmal ein schwieriges Abgrenzungsproblem.

Zu den Pflichten des Verantwortlichen: Es geht um die Konkretisierung der Betroffenenrechte. Es ist wohl richtig, dass man das Auskunftsrecht dann begrenzt, wenn die Daten nur noch aufgrund von Aufbewahrungsvorschriften vorgehalten werden. Aufbewahrungspflichtige Vorschriften, die außerhalb der produktiven Systeme in Archiven gespeichert werden, zur Ausübung des Auskunftsrechts wieder einzuspielen ist doch deutlich unverhältnismäßig. Insofern sollte die alte bzw. die bestehende Rechtslage beibehalten werden.

Dasselbe betrifft den Anspruch auf Löschung. Sie müssen sich vorstellen, dass ein Löschungsanspruch nach der Grundverordnung unbedingt gewährleistet werden muss. Das hieße,

auch die in Datensicherungsbändern archivierten Daten müssten eingespielt werden, um eine Adressänderung durchzuführen. Das ist doch deutlich unverhältnismäßig. Das bisherige BDSG hat das anders gelöst und das ist sachgerecht.

Ein weiteres Thema ist die Gestaltung von Datenbanken. Hier eine Teillöschung zu verlangen – was teilweise systemtechnisch nicht geht und auch SAP-mäßig nicht funktioniert, weil die Daten aus Gründen der referenziellen Integrität verknüpft sind – ist faktisch nicht möglich. Auch hier sollte es dabei bleiben, dass eine Sperrung möglich ist.

Wenn ich noch eine Minute habe, dann möchte ich diese dazu benutzen zu sagen, dass der Vorschlag des Bundesrates für einen One-Stop-Shop in Deutschland dringend zu unterstützen ist. Wenn der europäische Gedanke ist, dass die entscheidende Aufsichtsbehörde dort ist, wo auch die Hauptniederlassung ist, dann sollte das auch in Deutschland gelten. Es kann nicht sein, dass ich mich als deutsches Konzernunternehmen mit verschiedenen Aufsichtsbehörden über ein Thema auseinandersetzen muss, das von konzernweiter Bedeutung ist. Insofern sollte der Gedanke des One-Stop-Shops transportiert werden. Der Vorschlag des Bundesrates ist in dem Punkt zu unterstützen. Danke für Ihre Aufmerksamkeit.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Jaspers, als nächster erhält Herr Neumann das Wort.

SV **Karsten Neumann** (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a. D., 2b Advice, Bonn): Vielen Dank, auch ich will mich auf einige wenige Punkte beschränken.

Herr Prof. Dr. Aden hat für den behördlichen Bereich ja schon deutlich gemacht, was für Schwierigkeiten die Komplexität der rechtlichen Materie schon für die Experten bringt und erst recht für den Sachbearbeiter, der es in der Behörde umsetzen muss, genauso sieht es für die Unternehmensjuristinnen und -juristen aus. Diese Komplexität zu reduzieren wäre sehr schön. Gleichwohl habe ich nicht den Eindruck, dass das gegenwärtig noch leistbar ist, schon gar nicht bis nächste Woche. Das wird sicherlich nicht machbar sein. Umso schöner wäre es, wenn es Ihnen im Parlament gelänge, noch an einigen Stellen zu konkretisieren und teilweise lange Streite – Herr



RA Jaspers hat das gerade angesprochen – schlicht und ergreifend einmal gesetzgeberisch zu entscheiden und zu sagen: Wir entscheiden an diesen Stellen endlich einmal und überlassen es nicht weiterhin der Rechtsprechung. Denn wenn wir uns die Kritik vorstellen, die Frau Ehrig ansprach, die von vielen Seiten kommt, dass Teile der Regelungen gegen die Datenschutzgrundverordnung verstoßen und damit ja erst nachhinein zu klären sein wird, ob dieses deutsche Umsetzungsgesetz europarechtskonform ist, das kann Jahre dauern. In diesen Jahren in der Praxis etwas umsetzen zu müssen tut dem Datenschutz nicht gut. So hehr das Ziel auch ist, es führt letztendlich dazu, dass die Umsetzungsdefizite größer werden.

Diese Umsetzungsdefizite – das hatte Herr RA Jaspers auch schon angesprochen – haben wir in der Praxis in vielen Bereichen, in denen wir schon heute gesetzliche Regelungen nach dem BDSG haben, die schlicht und ergreifend nicht umsetzbar sind und ergo auch nicht umgesetzt werden. Die spannende Frage ist, wie der Gesetzgeber eigentlich auf diesen Zustand reagiert. Natürlich muss man nicht immer das Gesetz anpassen, sondern manchmal vielleicht auch die Realität. Aber ob die Aufsichtsbehörden dazu in der Lage sind, ist dann die zweite Frage. Der Gesetzentwurf ist in der Öffentlichkeit vor allen Dingen in einem Punkt wahrgenommen worden, nämlich in der massiven Erhöhung des Bußgeldrahmens. Ob das aber angesichts der fehlenden Aufstockung von Aufsichtsbehörden und deren Kompetenz tatsächlich Angst machen muss, mag bezweifelt werden. Nur damit zu drohen hilft relativ wenig, wenn man weiß, wie oft die Aufsichtsbehörde dann überhaupt theoretisch in der Lage wäre, zu prüfen.

Diese jahrelange Rechtsunsicherheit freut natürlich alle Berater und Kommentatoren. Allein in der Praxis wird es damit sehr schwierig sein, Fortschritte zu erreichen, und das hatten wir eigentlich alle erhofft.

Ich will nur zwei Punkte herausgreifen, die aus meiner Sicht bisher zu Unrecht nicht in den Fokus geraten sind, nämlich die Abschaffung der Jedermann-Auskunftspflicht zum Verfahrensverzeichnis. Das ist ein Umstand, den ich persönlich aus unserer praktischen Erfahrung sehr bedauere. Er führt dazu, dass eines der wirksamen Transparenzmittel des bisherigen BDSG

– nämlich, dass jedermann, ohne es begründen zu müssen, also anlassunabhängig, von jedem Unternehmen verlangen kann, festzustellen, welche personenbezogenen Daten verarbeitet werden, ob er möglicherweise ein Betroffener dieser Datenverarbeitung ist – sang und klanglos verschwindet. Das finde ich bedauerlich und halte es, auch wenn es manchmal als Bürokratie gesehen wird, schon deshalb für weiterhin notwendig. Jedes Unternehmen wird ohnehin auch zukünftig gezwungen sein, ein Verfahrensverzeichnis für die Aufsichtsbehörden und den Zugriff der Aufsichtsbehörden zu erstellen. Wenn es ohnehin schon da ist, warum soll es in den Teilen, die nicht die Sicherheit der Datenverarbeitung betreffen, sondern die Transparenz der Datenverarbeitung, nicht weiterhin für jedermann zugänglich sein, ohne es separat begründen zu müssen? Er sollte nicht nur im Wege eines Auskunftsverlangens die Möglichkeit erhalten, zu den ihn betreffenden Daten Zugang zu bekommen.

Genauso ist es mit einem weiteren Punkt, der auch gerne als unliebsames Kind gehandelt wird, nämlich das Thema Verpflichtung auf das Datengeheimnis. Ich möchte Herrn RA Jaspers bei der Frage der Schriftlichkeit der Einwilligungserklärung nicht widersprechen. Bei der Verpflichtung auf das Datengeheimnis erlebe ich es schon, dass eine Unterschrift unter einem Dokument, auf dem steht: „Ich habe zur Kenntnis genommen, dass ich mich strafbar mache, wenn ich die Daten, die mir anvertraut worden sind, zweckwidrig verwende,“ sehr wohl auch weiterhin ein geeignetes Instrument ist, auch wenn es sicherlich Bürokratie erzeugt. Aber aus meiner Sicht ist diese Signalwirkung auch an die Mitarbeiterinnen und Mitarbeiter weiterhin sehr wichtig. Soweit vorweg ein paar einleitende Bemerkungen von mir.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Neumann. Dann wechseln wir jetzt auf die von mir aus gesehen linke Seite. Herr Dr. Piltz ist der Nächste.

SV Rechtsanwalt Dr. Carlo Piltz (Reusch Rechtsanwälte, Berlin): Vielen Dank, auch für die Einladung und die Möglichkeit hier vor dem Innenausschuss zu diesem wichtigen Gesetzgebungsvorhaben sprechen zu dürfen.



Ich beschränke mich in meinen einführenden Worten auf einige Eckpunkte und den Überblick zu meiner Ihnen vorliegenden Stellungnahme. Zunächst möchte ich noch einmal die Bedeutung des über alle Interessengruppen hinweg übereinstimmend bestehenden Ziels dieses Anpassungsgesetzes herausstellen. Das ist die Rechtssicherheit. Die Rechtssicherheit in der Praxis und bei der Anwendung. Mag man in der Sache auch bei konkreten Ausgestaltungen auseinanderliegen, so ist doch am Ende notwendigerweise die zu erreichende Rechtssicherheit für die Praxis entscheidend, um diesem hier vorliegenden Gesetzgebungsvorschlag zur Akzeptanz und zur Wirksamkeit zu verhelfen. Das gilt nicht nur für die Praxis, sondern natürlich auch für die von der Praxis Betroffenen und es kann auch sein, dass Widersprüche zu europäischen Vorgaben Verstöße gegen europäisches Primärrecht zur Folge haben. Deshalb sollten rechtliche Unsicherheiten zum europäischen unmittelbar anwendbaren Recht vermieden werden. Das bedeutet auch: Je mehr Sie national anpassen, konkretisieren, spezifizieren, desto mehr steigt das Risiko, solche Regelungen zu schaffen. Klar ist auch: Neben der Datenschutzgrundverordnung sind nationale Regelungen möglich und zum Teil sogar verpflichtend vorgeschrieben, sonst würden wir uns heute hier nicht treffen und diskutieren.

Der deutsche Gesetzgeber kommt mit dem vorliegenden Gesetzentwurf dieser Pflicht nach und versucht den eröffneten Gestaltungsspielraum zu nutzen. Das ist zu begrüßen, da so nämlich auch die Chance genutzt wird, das geltende Schutzniveau des BDSG beizubehalten, zumindest soweit das im Rahmen der Vorgaben der Datenschutzgrundverordnung gestattet ist. Leitlinie bei der Anpassung sollte, wie insbesondere durch die Regierung in der Vergangenheit des Öfteren betont wurde, das bestehende Schutzniveau des BDSG sein. Zu einem wichtigen Thema, das hier von den anderen Sachverständigen schon angesprochen wurde: Im Rahmen der Öffnungsklauseln der Datenschutzgrundverordnung ist der deutsche Gesetzgeber befugt, Betroffenenrechte einzuschränken. Hiervon macht er mit dem Gesetz auch Gebrauch. Das ist an sich erst einmal nicht unzulässig. Neu ist jedoch, dass eine Datenschutzgrundverordnung, also unmittelbar

anwendbares europäisches Recht, hierzu Vorgaben macht, die man auch beachten muss, wenn man einschränkend tätig sein will.

Hierzu lässt sich leider auch feststellen – daran ist jetzt nicht der deutsche Gesetzgeber schuld – dass die Datenschutzgrundverordnung selbst auch teilweise etwas unspezifisch und ungenau ist. Wichtig ist in einer solchen Situation, die Voraussetzungen für die Beschränkung genau zu beachten. Die Leitlinie sollte meines Erachtens nicht sein: Viel hilft Viel. Denn ausbaden müssen diese damit einhergehende rechtliche Unsicherheit und eventuelle Ungültigkeitserklärungen durch den EuGH am Ende die datenverarbeitenden Stellen. Das ist natürlich – darüber diskutieren wir immer – die Wirtschaft, das sind aber auch Verbände, Vereine und nicht nur die großen, sondern einfach alle Unternehmen oder alle Stellen, die personenbezogene Daten verarbeiten und schließlich auch der Betroffene, der auch wissen möchte, was er für Rechte hat und wie weit seine Rechte gehen.

Um es kurz zu machen. Teilweise gehen meines Erachtens die vorgeschlagenen Regelungen über den eröffneten Gestaltungsspielraum der DSGVO hinaus. Es besteht an einigen Stellen begründetes Risiko, dass hier gegen die DSGVO, gegen die Vorgaben, verstoßen wird. Erforderlich sind, das haben Sie meiner Stellungnahme entnommen, punktuelle Nachbesserungen. In Gänze halte ich den Gesetzentwurf der Regierung aber für gelungen und für den richtigen Weg.

Einige konkrete Anregungen möchte ich noch vorgeben, und zwar zum räumlichen Anwendungsbereich. Hier sollte entsprechend der Datenschutzgrundverordnung konkretisierend eingegriffen werden. Die Regelung zur Videoüberwachung mutet momentan wie ein exklusiver Erlaubnistatbestand an. Ob das gerade vor dem EuGH-Urteil „Breyer“ möglich ist, daran habe ich meine Zweifel. Das vorgeschlagene Verfahren zur Zusammenarbeit der Datenschutzbehörden in Deutschland und deren Vertretung im Europäischen Datenschutzausschuss sollte noch mehr an die Regelung der Datenschutzgrundverordnung angeglichen werden. Die vorgesehenen Möglichkeiten zur zweckändernden Weiterverarbeitung gehen teilweise über die Grenzen der Vorgaben aus Artikel 6 und 23 DSGVO hinaus. Jetzt habe ich aber



gesehen, dass da im Änderungsantrag etwas angepasst wurde, das muss man sich einmal genauer anschauen.

Zuletzt noch zu einer kürzlich in der Datenschutzsphäre geführten Diskussion, die sich ebenfalls auf das Ziel der Rechts- und Anwendungssicherheit dieses Gesetzes auswirkt: Nach der Rechtsprechung des europäischen Gerichtshofs dürfen deutsche Behörden nationales Recht, welches im Konflikt mit unmittelbar geltenden europäischen Normen steht, nicht anwenden. Für die Praxis – im Sinne von Unternehmen und Behörden – entsteht in solchen Situationen jedoch ein Zustand der rechtlichen Unsicherheit. Auch aus diesem Grund sollten klare Regelungen und damit einhergehende Rechtsicherheit oberstes Ziel des Anpassungsgesetzes sein. Vielen Dank für die Aufmerksamkeit. Ich freue mich auf die Diskussion.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Dr. Piltz. Dann erhält Herr Schaar als nächster das Wort.

SV **Peter Schaar** (Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz e. V., Berlin): Vielen Dank, Herr Vorsitzender. Sehr geehrte Damen und Herren Abgeordnete. Ich beschränke mich im Folgenden auf einige wenige Ausführungen zur Datenschutzgrundverordnung und verweise im Übrigen auf meine schriftliche Stellungnahme.

Mit der Datenschutzgrundverordnung verfolgt der europäische Gesetzgeber drei wesentliche Ziele. Das erste Ziel ist die Harmonisierung des Datenschutzrechts: Für alle Unternehmen die in Europa tätig sind und dabei personengezogene Daten verarbeiten, sollen dieselben Verpflichtungen geltend.

Der zweite Punkt ist die Stärkung der Betroffenenrechte. Alle Personen, deren Daten in Europa verarbeitet werden, sollen dieselben Rechte auf Information, Auskunft, Berichtigung und Löschung erhalten.

Das dritte Ziel ist eine verbesserte, eine effektive Datenschutzaufsicht.

Ich bin im Gegensatz zu einigen anderen Sachverständigen der Auffassung, dass diese Vorlage der Bundesregierung die Ziele nicht gut

erreicht. Sie ist davon getragen, soviel wie möglich vom deutschen Bundesdatenschutzgesetz zu retten. Es ist richtig, die Grundverordnung enthält einige Spielräume für den nationalen Gesetzgeber. Aber anstatt sich darauf zu konzentrieren, in den Bereichen, in denen wirklich Regelungsbedarf besteht, auch zu regeln – ich denke hier an den Beschäftigtendatenschutz, da sind die Ausführungen im Gesetzentwurf nur rudimentär, oder ich denke an den Ausgleich zwischen Informationsfreiheit und Datenschutz, auch das ist ein Thema, das sehr wichtig ist und das nicht alleine die Länder betrifft – fehlen die Ausführungen und Vorschläge gänzlich.

Stattdessen verzettelt man sich in Regelungen für die, aus meiner Sicht, kein europarechtlicher Regelungsspielraum für den nationalen Gesetzgeber besteht. Das Ergebnis ist ein sehr kompliziertes, sehr schlecht lesbares Gesetzeswerk, das man dann noch einmal neben die Datenschutzgrundverordnung legen muss. Es ist schon gesagt worden, dass da viele Rechtsunsicherheiten zu klären wären. Ob das wirklich immer gut gelingt, daran haben ich meine Zweifel. Große Unternehmen, die sich große Rechtsabteilungen leisten können, sind sicherlich dazu in der Lage, mit diesen Unterschieden umzugehen. Kleinere Unternehmen, die auf dem europäischen Markt tätig sein wollen oder sind, tun sich damit sicherlich sehr viel schwerer.

Es ist auch schon darauf hingewiesen worden, dass die Frage der Betroffenenrechte von besonderer Brisanz ist. Hier sehe ich es als besonders problematisch an, dass die Rechte auf Information und Auskunft aber auch auf Löschung in dem vorgelegten Entwurf schlechter ausfallen als in der Datenschutzgrundverordnung. Das halte ich für dringend korrekturbedürftig.

Ein weiterer Punkt, der bisher noch nicht angesprochen wurde, sind die Kontrollrechte der Datenschutzbehörden bei Berufsgeheimnisträgern. Ich verstehe, dass man im Bereich der Anwaltschaft, gerade wenn die Anwälte als Organe der Rechtspflege tätig sind, hier vielleicht etwas anders regeln würde, als das bisher im BDSG der Fall ist. Aber das, was im Gesetzentwurf steht, geht weit darüber hinaus. Sämtliche Berufsgeheimnisträger werden weitgehend von Datenschutzkontrollen ausgenommen. Das bedeutet, dass der Schutz von Gesundheitsdaten,



die in Krankenhäusern verarbeitet werden, in Zukunft nur lückenhaft gewährleistet werden kann. Das gilt auch für viele andere Bereiche. Ich halte das nicht für tragfähig. Gerade im Hinblick darauf, dass das deutsche Bundesverfassungsgericht hier sehr klar gesagt hat, dass es keine kontrollfreien Räume geben darf, aber genau das ist zu befürchten, dass das hier eintritt.

Lassen Sie mich als letztes noch einen Aspekt ansprechen, der mir besonders am Herzen liegt. Deutschland hat eine große Datenschutztradition. In Deutschland wurde das erste Datenschutzgesetz der Welt verabschiedet. Das Bundesverfassungsgericht hat wegweisende Entscheidungen zu dem Thema gefällt, die in Europa und von vielen anderen Staaten aufgegriffen wurden. Wir haben hier einen Ruf zu verlieren und ich fürchte, genau das könnte eintreten. Es werden sich auch andere Regierungen anderer Mitgliedstaaten möglicherweise von einem solchen Beispiel negativ inspirieren lassen. Dann haben wir im schlimmsten Fall wieder 28 oder vielleicht in Zukunft 27 unterschiedliche nationale Datenschutzregelungen in Europa und das Harmonisierungsziel wäre verfehlt. Das kann nicht im Interesse der Bürgerinnen und Bürger sein, das kann aber auch nicht im Interesse der Wirtschaft sein. Ich danke Ihnen.

Vors. Ansgar Heveling (CDU/CSU): Vielen Dank, Herr Schaar. Dann darf ich jetzt der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Frau Voßhoff das Wort erteilen.

SVe Andrea Voßhoff (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Herr Vorsitzender, meine Damen und Herren Abgeordnete, ich darf mich sehr herzlich für die Einladung zu Ihrer heutigen Anhörung bedanken. Vieles von dem, was ich in meiner Einleitung sagen wollte, haben meine Vorredner schon größtenteils genannt.

Ich möchte auch vorausschicken, dass es einerseits notwendig ist, die Anpassungsregelungen noch in dieser Legislatur zeitnah zu verabschieden, das ist zu begrüßen. Ob es in der Eile, wie ich es heute gehört habe, sein muss, dass darf man sicherlich hinterfragen. Gleichwohl ist es notwendig, dass wir in dieser Legislaturperiode eine Anpassungsregelung bekommen, weil wir

ansonsten Gefahr laufen, zu dem Stichtag im Mai 2018, mit Blick darauf, dass Bundestagswahlen sind und der Neukonstituierung des Bundestages, zusätzlich Zeit vergehen würde. Ich appelliere daher auch, dass wir neben diesem Anpassungsgesetz ja auch wissen, dass es weitere bereichsspezifische Anpassungsregelungen geben muss und dass auch diese möglichst zügig in Angriff genommen werden.

Wir wissen auch, das haben meine Vorredner gesagt, dass wir mit der Datenschutzgrundverordnung künftig unmittelbar anwendbares europäisches Recht haben werden. Bei unserer Datenschutztradition in Deutschland und bei unserem sehr austarierten Datenschutzrecht ist die Anpassung in besonderer Weise eine Herausforderung. Aber auch ich möchte dafür werben und appellieren, das Harmonisierungsziel der Datenschutzgrundverordnung und die Rechtssicherheit bei der Anpassung nicht aus dem Auge zu verlieren, weil die komplexen Regelungen genau das als oberstes Ziel haben sollten, um auch die Anwendbarkeit künftigen Datenschutzrechts, insbesondere auch die Rechtssicherheit für betroffene Unternehmen, nicht zu gefährden.

Der Regierungsentwurf ist sicherlich das Ergebnis intensiver Beratungen. Ich denke, es besteht sicherlich auch Einigkeit: Gegenüber den Vorentwürfen hat dieser Regierungsentwurf deutliche Verbesserungen erreicht. Gleichwohl sehe ich aber auch an einigen Stellen deutlichen Nachbesserungsbedarf. Ich werbe dafür, diesem auch nachzugeben. Lassen Sie mich auf die Schnelle vier Punkte nennen.

Zum einen, das ist hier schon durch meine Vorredner deutlich und klar geworden, besteht noch Beratungs- und Änderungsbedarf, was die Einschränkung der Betroffenenrechte betrifft. Viele Beispiele sind hier genannt worden. Ich sehe z. B. den § 33 Abs. 1 Nr. 2a) als problematisch an. Da wird darauf hingewiesen, dass allgemein anerkannte Geschäftszwecke, sofern sie beim Unternehmen gefährdet würden, die Betroffenenrechte einschränken. Ich halte dies für einen Verstoß gegen Artikel 23 DSGVO, weil dieser Privatinteressen nicht in dieser Weise nennt, sondern die dort aufgelisteten Beschränkungsmöglichkeiten und Garantien gegeben werden müssen, und diese im Kern



eigentlich öffentliche Interessen sind. Das ist ein Punkt. Die anderen habe ich auch in meiner Stellungnahme aufgeführt. Ich denke, auch die Vorredner haben hier an der einen oder anderen Stelle deutlich gemacht, dass die Betroffenenrechte oder die Beschränkungen noch bedacht werden sollten.

Ich will einen weiteren Punkt nennen, der bisher nicht angesprochen wurde, das ist die Frage der Vertretung im Europäischen Datenschutzausschuss und das Verfahren der Zusammenarbeit der Aufsichtsbehörden. Zur Vertretung im Ausschuss und zum Verfahren der Zusammenarbeit hat der Bund, wie ich finde, aus meiner Sicht eine tragfähige Regelung vorgelegt. Ich will das Thema deshalb hier ansprechen, weil ich weiß, dass der Bundesrat in seinen Änderungsanträgen hierzu eine abweichende Stellungnahme abgegeben hat. Teilweise werden diese Fragen auch aus dem politischen Raum aufgeworfen, auch in manchen der Stellungnahmen meiner Kollegen, die heute hier sind. Es geht um § 17 und § 18 des Gesetzentwurfs, in denen die Vertretung im Europäischen Datenschutzausschuss und das Verfahren der Entscheidungsfindung im Kontext der Grundverordnung zwischen den Datenschutzbeauftragten des Bundes und der Länder geregelt sind.

Meine Damen und Herren Abgeordnete, ich werbe mit Nachdruck dafür, die Grundarchitektur des Regierungsentwurfs auch beizubehalten. Nach meiner Auffassung würden die Vorschläge des Bundesrates im Ergebnis die Gewichte zu Lasten des Bundes nachhaltig verschieben und Positionen der Datenschutzaufsichtsbehörden in europäischen Angelegenheiten unnötig schwächen. Der vorgelegte Gesetzentwurf trägt dem in Artikel 23 GG verankerten Grundsatz Rechnung, dass dem Bund grundsätzlich die Aufgabe zusteht, die Interessen des Gesamtstaates in Angelegenheiten der EU zu vertreten. Nach den dort festgelegten Maßstäben wird die Außenvertretung der Bundesrepublik in der Regel vom Bund wahrgenommen. Dies ist nur dann anders, wenn die ausschließliche Gesetzgebungskompetenz der Länder in den Gebieten Bildung, Kultur und des Rundfunks betroffen sind. Der Regierungsentwurf geht zu Gunsten der Länder bereits über diesen Grundansatz hinaus, indem er den Ländervertretern entsprechende Befugnis nicht nur

in den Fällen der ausschließlichen Gesetzgebungskompetenz, sondern auch für das Verfahren von Landesbehörden einräumt. Würde dies, wie vom Bundesrat vorgeschlagen, auf alle Angelegenheiten ausgeweitet, für die die sachliche Zuständigkeit bei den Aufsichtsbehörden der Länder liegt, würde die Rolle des Bundes nach meiner Einschätzung im Ergebnis marginalisiert. Zudem ist das Abgrenzungskriterium der vom Bundesrat geforderten sachlichen Zuständigkeit auch nicht praktikabel, denn es gibt auch in Fragen der sachlichen Zuständigkeit zwischen den Aufsichtsbehörden von Bund und Ländern vielfache Überschneidungen und gemeinsame Zuständigkeiten, die dann auch klärungsbedürftig wären.

Die Entscheidungen des künftigen Europäischen Datenschutzausschusses wirken in der Regel auch über den Einzelfall hinaus. Von den Beschlüssen sind nicht nur die Aufsichtsbehörden der Länder, sondern alle deutschen Datenschutzaufsichtsbehörden betroffen. Bei der Vertretung in europäischen Angelegenheiten kommt es auf die Interessen des Gesamtstaates an. So wie in allen Fragen der europäischen Integration muss auch der Bund hierfür einstehen und die Länder im Rahmen ihrer nationalen Vollzugskompetenz verfahrensmäßig einbinden. Genau das, finde ich, hat der Regierungsentwurf auch in der gebotenen und notwendigen Art und Weise, bezogen auf die Vollzugskompetenz der Länderaufsichtsbehörden, getan.

Ich möchte kurz noch einen dritten Punkt anreißen. Die geplante Regelung des § 16 Abs. 2 des Datenschutzgesetzes neu; darin sind die Befugnisse meines Hauses im Geltungsbereich der Richtlinie für Polizei und Justiz in den Bereichen außerhalb des Geltungsbereichs des EU-Rechts geregelt. Danach soll nach dem Willen der Bundesregierung der Status quo erhalten bleiben. Das hieße, mein Haus bliebe in diesem Bereich auf Beanstandungen für den Bereich Polizei und Justiz beschränkt. Ich halte dies schlicht für europarechtswidrig. Artikel 47 der Richtlinie beinhaltet die Verpflichtung zu wirksamen Abhilfebefugnissen und gemäß Absatz 5 die Verpflichtung, Möglichkeiten einer gerichtlichen Klärung vorzusehen. Beides enthält die vorgeschlagene Regelung nicht. Das Instrument der Beanstandung ist nicht verbindlich und nicht durchsetzbar. Vertritt der Verantwortliche bzw.



dessen Aufsichtsbehörde eine andere Rechtsauffassung als die Datenschutzaufsicht, besteht keine Möglichkeit der Durchsetzung durch gerichtliche Klärung. Die BfDI kann in dieser Konstellation keine wirksame Abhilfe, wie in der Richtlinie gefordert, herbeiführen.

Ein vierter Punkt ist das Stellungnahmerecht der BfDI gegenüber dem Bundestag und seinen Ausschüssen. Dieses möchte ich noch kurz erwähnen. Es betrifft die Neuregelung im Bereich des Bundesnachrichtendienstgesetzes und damit einen Bereich, der weder in der Datenschutzgrundverordnung noch in der Richtlinie vorkommt, aber gleichwohl unter Datenschutzaspekten von grundsätzlicher Bedeutung ist. Der Entwurf, so wie er im Gesetz gefasst wurde (§ 32 Abs. 1 Nr. 1b), schränkt das geltende Recht, das im BDSG(neu) grundsätzlich entsprechend fortgeschrieben wird, zu Lasten meines Hauses und des Deutschen Bundestages verfassungswidrig ein. Nach dem Gesetzesentwurf soll die Regelung, nach der ich mich proaktiv mit Stellungnahmen an den Bundestag und seine Ausschüsse wenden kann, in Bezug auf die den BND betreffenden Sachverhalte ausgeschlossen werden. Stellungnahmen soll die BfDI in diesem Bereich allein an die Bundesregierung sowie die für die Kontrolle des BND zuständigen Gremien – parlamentarisches Kontrollgremium, G 10, Vertrauensgremium – richten dürfen und auch nur, sofern der Bundesregierung zuvor Gelegenheit zur Stellungnahme gewährt worden ist.

Dies bedeutet, dass sich die BfDI – im Gegensatz zum geltenden Recht – den BND betreffend nicht mehr an den Deutschen Bundestag oder seine Ausschüsse wenden dürfte, und damit insbesondere nicht an den Innenausschuss oder einen Untersuchungsausschuss des Bundestages, der BND-relevante Sachverhalte aufklären soll. Diese Beschränkung steht nicht nur im Widerspruch zu verfassungsrechtlichen Vorgaben. Sie widerspricht nach meiner Auffassung auch der vom europäischen Gerichtshof geforderten Unabhängigkeit der Datenschutzaufsicht. Zudem beschränkt die Regelung in unzulässiger Weise das Informationsrecht des Parlaments und seiner Ausschüsse. Sie sollte daher gestrichen werden. Vielen Dank meine Damen und Herren.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Voßhoff. Nun Herr Prof. Dr. Wolff, bitte.

SV Prof. Dr. Heinrich Amadeus Wolff (Universität Bayreuth): Sehr geehrte Damen und Herren, auch ich bedanke mich ganz herzlich für die Einladung. Zusätzlich zu meiner schriftlichen Stellungnahme möchte ich hier ein paar grundsätzliche Bemerkungen machen. Erstens zu der Besonderheit des Gesetzesentwurfes, zweitens zu seiner Systematik und drittens zu ein paar übergreifenden Fragen.

Erstens, Besonderheiten: Der vorliegende Gesetzesentwurf zeichnet sich in mehrfacher Hinsicht aus. Zunächst setzt er Unionsrecht um, nicht aber eine Richtlinie, sondern eine Verordnung, die auf Grund zahlreicher Öffnungsklauseln einerseits konkretisierungsfähig und andererseits konkretisierungsbedürftig, aber an anderen Stellen wieder eng und strikt ist. Das ist nicht einfach. Weiter bildet das Datenschutzrecht eine Querschnittsmaterie, die fast die gesamte Rechtsordnung erfasst. Werden hier Fehler gemacht, kann das schlimme Folgen haben. Drittens stehen sich oft grundrechtsgeprägte Sichtweisen mit wirtschaftlich geprägten Sichtweisen unversöhnlich gegenüber. Der Entwurf macht in meinen Augen aus der vorgegebenen Situation das Beste, was möglich war.

Der Entwurf ist dabei von folgenden Eckpunkten geprägt: Das BDSG muss geändert werden. Die Vorstellung, man könnte trotz der Datenschutzgrundverordnung alles beim Alten belassen und abwarten, stünde einem juristisch unverantwortlichen Blindflug gleich. Der Entwurf lebt von folgenden Grundstrukturen: Soweit es geht, orientiert er sich an den Regelungen des alten BDSG. Er nimmt die Vorrangigkeit des Unionsrechts ernst und bildet eine aus sich heraus unvollständige Rechtsgrundlage – der Kodifikationscharakter des Datenschutzrechts ist dahin. Er macht von den Öffnungsklauseln selbstbewusst, aber nicht flächendeckend Gebrauch. Er zögert nicht, das Unionsrecht auch in den Teilen beim Wort zu nehmen, die uns bisher fremd waren.

Der Gesetzesentwurf beruht mit seinen vier Teilen auf einer klaren Struktur, die aus dogmatischer Sicht überzeugt. Ich persönlich war überrascht, dass die deutsche Ministerialbürokratie so etwas Schönes hervorbringen kann. Ich glaubte bisher immer, dass würden nur wir von den Universitäten schaffen.



Zweitens, die Systematik des BDSG: Der Verordnungsteil. Bei dem Teil der Datenschutzgrundverordnung ist es richtig, die allgemeinen Normen zu erlassen, bevor man auf dieser Basis dann bereichsspezifisches Datenschutzrecht auf seinen Änderungsbedarf durchkämmt. Die Richtlinie. Die Aufnahmen der Umsetzungsnormen der Richtlinie in das BDSG und nicht nur in die Sicherheitsgesetze, erscheint richtig, da es erstens wegen der unklaren Abgrenzung von der Verordnung zur Richtlinie einer Auffangregelung bedurfte und es zweitens sinnvoll erscheint, identische Regelungsstrukturen allgemein zusammenzufassen. Drittens, rein nationaler Raum. Am wichtigsten erscheint der Hinweis, dass es auch weiterhin zwingend einen rein nationalen Bereich geben wird. Für diesen normieren §§ 1 bis 4 und § 85 wichtige Fragen. Ungeregt bleiben aber die meisten anderen Fragen. Ich würde dringend darum bitten, trotz der gebotenen Eile zu prüfen, ob man nicht in einem § 86 BDSG(neu) einen subsidiären Verweis auf die Normen zur Umsetzung der Richtlinie einfügen kann, um den Torso-Charakter zu überwinden.

Drittens, übergreifende Fragen. Erstens, Kompetenzfragen, Vertreter im EDA. Nicht ganz einfach ist die Bestimmung der Gesetzgebungskompetenz und der Verwaltungskompetenz für die Bestimmung des Deutschen Vertreters im EDA. Die im Gesetz vorgeschlagene Regelung erscheint vernünftig. Eine Erweiterung der Kompetenz des Landesvertreters ist möglich, aber nicht zwingend. Zweitens, Kompetenzfrage Presserecht. Der gegenwärtige Entwurf enthält keine Regelung mehr zum Datenschutz im Pressewesen. Begründet wird dies mit der angeblich fehlenden Gesetzgebungskompetenz des Bundes. Hier sind sich alle einig. Einigkeit schützt nicht vor Irrtum. Einige kleine Presseverbände haben mich gebeten, die Kompetenzfrage noch einmal zu prüfen. Ich glaube, dass man es sich mit dem Verweis, der Bund dürfe das Presserecht nicht mitregeln, zu einfach macht. Der Bund muss das nicht mitregeln, er darf es aber. Zu empfehlen wäre es. Drittes, Abgrenzung zwischen Verordnung und Richtlinie. Die Begründung des Gesetzentwurfs in Verbindung mit § 45 des Entwurfs, vertreten eine klare Abgrenzungsthese zwischen Verordnung und Richtlinie. Dies ist nicht unangreifbar, aber bewundernswert. Man könnte sie dennoch klarer

fassen. Viertens, Ordnungswidrigkeitsrecht. Hier könnte die Frage, ob Verschulden nun erforderlich ist oder nicht und falls ja, wie es bei juristischen Personen zu prüfen wäre, klarer werden. Der Hinweis auf das Ordnungswidrigkeitengesetz ist zu unklar. Weiter sollten auch andere Behörden als die Aufsichtsbehörden die Datenschutzverstöße verfolgen dürfen. Fünftens, Videoüberwachung. Die Neuregelung zur Videoüberwachung bildet in meinen Augen einen klaren Verstoß gegen das Unionsrecht. Der Vorschlag aus dem früheren Referentenentwurf war systematisch viel besser, er sollte Gesetz werden. Sechstens, Bonität und Scoring. Die Regelungen zur Bonitätsauskunft und zum Scoring sind Fremdkörper. Sie überzeugen nicht. Der Hinweis auf den Verbraucherschutz ist geschummelt. Siebtens, allgemeine Verarbeitungsgrundlage. § 3 BDSG schafft eine einheitliche Rechtsgrundlage für alle Bereiche. Angelehnt an Artikel 6 Abs. 1 lit. e Grundverordnung. In der Gesetzesbegründung wird auf Artikel 6 Abs. 3 Verordnung verwiesen. Legt man dies zu Grunde, dann ist es systematisch aber eigentlich zwingend, auch die Norm von Artikel 6 Abs. 1 lit. c – zwingender Verpflichtungen – zu wiederholen. Vielen Dank, für die Aufmerksamkeit.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Wolff. Damit sind wir mit den Eingangsstellungnahmen der Damen und Herren Sachverständigen durch. Ganz herzlichen Dank für diese Stellungnahmen. Wir kämen nun zur ersten Fragerunde der Berichterstatter. Ich darf Herrn Kollegen Mayer als Erstem das Wort geben.

BE Abg. **Stephan Mayer** (Altötting) (CDU/CSU): Herzlichen Dank, Herr Vorsitzender, meine sehr verehrten Damen und Herren. Ich darf zunächst den Sachverständigen ganz herzlich für Ihre schriftlichen Stellungnahmen, aber auch für die mündlichen Ausführungen danken, die für uns sehr wichtig und instruktiv sind, insbesondere was die weitere parlamentarische Behandlung dieses Gesetzentwurfs anbelangt.

Ich persönlich bin der festen Überzeugung, dass es richtig ist, das wir dieses Anpassungs- und Umsetzungsgesetz zur Datenschutzgrundverordnung noch in der laufenden Legislaturperiode nicht nur behandeln, sondern auch verabschieden. Auch wenn die Umsetzungsfrist erst im Mai kommenden Jahres endet, denke ich, sollten wir uns hier nicht zu viel



Zeit lassen. Im Gegenteil, ich glaube, es ist richtig, dass wir noch in der laufenden Periode vor allem auch um der Wirtschaft und der Verbrauchern Willen dieses Gesetz verabschieden, um allen betroffenen Kreisen Rechtssicherheit und -klarheit zu geben. Ich bitte um Verständnis, dass meine Fragen sich aufgrund der beschränkten Zeit nur an einige Sachverständige richten können.

Ich darf zunächst an Herrn Prof. Dr. Wolff, Herrn Dr. Piltz und an Herrn RA Jaspers, Fragen richten, insbesondere was die Kritik von Herrn Schaar anbelangt, dass der Schutz der Berufsgeheimnisträger im Umsetzungsgesetz zu weit ginge. Es gibt diesbezüglich durchaus auch gegenteilige Auffassungen. Bspw. vertritt die Bundesrechtsanwaltskammer die Auffassung, dass die jetzige Regelung sogar verfassungswidrig sei, da die Rechtsanwälte als unabhängige Organe der Rechtspflege der staatlichen Datenschutzaufsicht unterzogen würden. Meine konkrete Frage ist deshalb, wie Sie diese Regelung bezüglich des Berufsgeheimnisträgerschutzes erachten und ob Sie der Auffassung sind, dass darüber hinaus eventuell noch weitergehender Änderungsbedarf gegeben ist, was eine Sonderregelung für Berufsgeheimnisträger bspw. Rechtsanwälte, anbelangt. Ich möchte hier aber auch – die sensiblen Gesundheitsdaten sind erwähnt worden – insbesondere die Ärzteschaft und die Steuerberater nennen.

Die zweite auch an die genannten Sachverständigen gerichtete Frage bezieht sich auf das Thema Fortgeltung der Einwilligungen, die unter dem jetzigen Rechtsregime rechtsgültig abgegeben worden sind. Meine konkrete Frage ist, ob es unter Bezugnahme auf den Erwägungsgrund 171 in der Datenschutzgrundverordnung aus Ihrer Sicht im jetzigen nationalen Umsetzungsgesetz einer stärkeren Konkretisierung dahingehend bedürfe, dass die jetzt schon gegebenen Einwilligungen auch weiter über den Mai 2018 hinaus fortgelten. Ich glaube, dass diese Möglichkeit der Fortgeltung für alle Betroffenenrechtskreise, sowohl für die Verbraucher aber natürlich auch für die Unternehmer, von herausragender Bedeutung ist.

Eine weitere Frage bezieht sich auf den Änderungsantrag, der schon erwähnt wurde. In diesem Änderungsantrag werden die Betroffenenrechte aus meiner Sicht richtigerweise noch einmal erweitert, konkretisiert. Meine Frage

an die drei genannten Sachverständigen ist, ob die jetzt im Änderungsantrag vorgenommenen Präzisierungen und Erweiterungen, insbesondere was die Informationspflichten der Privatwirtschaft aber auch die Löschungspflichten in den §§ 32, 33 und 35 anbelangt, aus Ihrer Sicht so unterstützenswert sind. Ich sage das auch unter Bezugnahme auf die Einlassung von Frau Ehrig, die aus meiner Sicht zu Recht darauf hingewiesen hat, dass wir hier nicht die großen Unternehmen wie Facebook und Google privilegieren wollen, also dass wir, was den unverhältnismäßigen Aufwand bei Informationspflichten oder Löschungsrechten anbelangt, nicht die großen IT-Facharbeiter privilegieren wollen, sondern durchaus auf den konkreten Umsetzungsaufwand bei kleineren, mittelständischen Unternehmen abstellen wollten. Ich persönlich bin der Überzeugung, dass mit dieser Klarstellung, dass Unternehmen nur umfasst sind, die nicht automatisierte Datenverarbeitung betreiben, wie bspw. kleinere oder mittlere Unternehmen, zu tun.

Eine weitere Frage bezieht sich auf das Thema der zuständigen Gerichtsbarkeit. Es gibt in dem Änderungsantrag auch eine Konkretisierung dahingehend, dass wenn sich die Bußgeldsumme auf einen Betrag von mehr als 100.000 Euro bezieht, nicht das Amtsgericht (AG) zuständig sein soll, sondern das Landgericht (LG). Konkrete Frage an die Sachverständigen ist, wie Sie diese Änderung der Zuständigkeit beurteilen.

Dann eine weitere Frage vor dem Hintergrund, dass wir aus meiner Sicht bei dem Umsetzungsgesetz auch tunlichst darauf achten sollten, bewährte Geschäftsmodelle, die nach dem jetzigen Bundesdatenschutzgesetz zulässig sind – bspw. im Bereich von Digitalmarketing, von Auskunftfeien, Inkassounternehmen – nicht zu unterminieren. Deswegen die konkrete Frage, ob Sie einen weiteren Umsetzungsspielraum nach der Datenschutzgrundverordnung sehen, den wir nach der jetzigen Vorlage des Umsetzungsgesetzes nicht genutzt haben. Ob es aus Ihrer Sicht hier noch offene Möglichkeiten nach der Datenschutzgrundverordnung gäbe, von denen der Gesetzgeber nach der jetzigen Fassung nicht Gebrauch macht.

Eine Frage, die sich nur an die Sachverständigen Herren Prof. Dr. Wolff und Dr. Piltz richtet, unter Bezugnahme auf die Einlassung, die Herr RA



Jaspers bereits gemacht hat, was die Schriftformerfordernisse im § 36 Abs. 2 Satz 3 des Umsetzungsgesetzes anbelangt. Ist diese Kritik von Herrn RA Jaspers berechtigt? Wenn ich sie hier noch einmal aufgreifen darf, die Kritik, dass dieses Schriftformerfordernis in dem Umsetzungsgesetz zu rigide ist und es insbesondere bei vollkommen unproblematischen aber sehr massenhaften Einwilligungen ausreichen sollte, dass nur das Textformerfordernis erfüllt wird und die Einwilligung auch in digitaler Form abgegeben werden kann.

Eine weitere Frage, die sich wiederum an alle drei Sachverständige richtet, bezieht sich auf den offenkundigen Dissens in der Datenschutzgrundverordnung zwischen dem Artikel 4 Ziffer 4 und dem Artikel 22, bezüglich des Themas Profiling. Ich habe schon erwähnt, dass es aus meiner Sicht Leitschnur sein sollte, dass wir bewährte Geschäftsmodelle nicht unterminieren. Meine Frage bezieht sich auf das Thema Direktmarketing. Sehen Sie im Lichte dieses offenkundigen Dissenses zwischen den beiden von mir genannten Artikeln einen weiteren Konkretisierungsbedarf im Umsetzungsgesetz dahingehend, dass das bewährte Geschäftsmodell des Direktmarketings auch jetzt mit dem Umsetzungsgesetz weiter betrieben werden kann?

Nachdem mich der Vorsitzende schon so durchdringend anblickt, belasse ich es jetzt mit den gestellten Fragen.

Vors. **Ansgar Heveling** (CDU/CSU): Diejenigen, an die die Fragen gestellt werden, sollen auch noch den Überblick behalten. Frau Kollegin Pau, bitte.

Abg. **Petra Pau** (DIE LINKE.): Ich würde mich gerne an die erste Frage des Kollegen Mayer anschließen, allerdings adressiere ich die Nachfrage an Herrn Neumann, Herrn Schaar und ggf. Frau Voßhoff. Mich würde zum Thema Berufsgeheimnisträger interessieren, welchen Anteil eigentlich solche Prüfverfahren bisher in der Praxis bei Ihnen eingenommen haben. In diesem Zusammenhang finde ich in der Stellungnahme von Herrn Neumann noch einmal dezidiert eine Kritik zu den jetzt vorgesehenen Regelungen. Mich würde hier Ihre Sicht darauf interessieren, wie wir im Gesetzgebungsverfahren entsprechend der Datenschutzgrundverordnung trotz allem ausgewogene aber auch sinnvolle Regelungen mit

Blick auf die Berufsgeheimnisträger umsetzen könnten.

Dann ein Thema, das hier heute noch eine Rolle spielte. Herr Neumann, Sie haben in Ihrer Stellungnahme auf das Thema Scoring Bezug genommen und waren auch bei anderer Gelegenheit hier schon einmal als Sachverständiger für uns tätig. Sie schlagen vor, die alten Regelungen zum Scoring wieder in den Gesetzestext aufzunehmen. Können Sie uns noch einmal begründen, warum das aus Ihrer Sicht notwendig ist und warum wir dann nicht in den Konflikt zur europäischen Datenschutzgrundverordnung geraten? Dann interessiert mich noch, ob wir nicht auch Regulierungen von Unternehmen, die massenhaft Social-Media-Daten für Scoring verwenden, noch darüber hinaus in diese Regelungen aufnehmen müssten.

Dann habe ich gesehen, der Verbraucherzentrale Bundesverband schlägt in seiner Stellungnahme vor, die Regelungen des § 31 des Entwurfs auch in andere zivilrechtliche Regelungsbereiche wie bspw. das Kreditrecht zu überführen. Können Sie uns dazu etwas sagen, inwieweit das aus Ihrer Sicht sinnvoll ist? Wäre es tatsächlich hilfreich, in allen fraglichen Bereichen Einzelregelungen zu treffen oder könnte man das nicht zentral in einem Gesetz regeln, so dass hier auch Wildwuchs vorgebeugt wird?

Dann ein drittes Thema, es richtet sich an Frau Voßhoff, Herrn Neumann und Herrn Schaar. Erst vor wenigen Wochen haben wir hier im Bundestag eine Änderung des Bundesdatenschutzgesetzes beschlossen. Da ging es um das Thema mehr Videoüberwachung im öffentlichen Raum und wie wir das regulieren. Mit der derzeit vorliegenden Regelung soll das in die neue Systematik überführt werden. Nun würde mich interessieren, wie Sie die vorgesehene Regelung auch hinsichtlich der zukünftigen Möglichkeit zur automatisierten Verarbeitung von Videoüberwachungsdaten, z. B. die sogenannte intelligente Videoüberwachung, einschätzen, wie Sie weiteren Regelungsbedarf, auch generell zu diesem Thema sehen. Ich könnte es auch umdrehen: Die Frage ist, wie weit Sie Ihren Aufgaben, aus Ihrer Sicht, hier in diesem Bereich überhaupt noch nachkommen können oder ob wir hier weitergehenden Regelungsbedarf haben?



Vierter und letzter Punkt, das Thema Beschäftigungsdatenschutz. Herr Neumann, Sie rufen dieses Thema in Ihrer Stellungnahme auf und halten fest, dass lediglich die Datenverarbeitung der betrieblichen Interessenvertretung mit der vorliegenden Regelung geschützt werden soll, aber nicht die von ihr zum betrieblichen Datenschutz getroffenen Vereinbarungen mit der Arbeitgeberseite. Hier interessiert mich Ihre Einschätzung, was generell im Bereich des Beschäftigtendatenschutzes in diesem aktuellen Vorhaben zu regeln wäre. Dazu kommt – das wissen wir alle, die wir seit über einem Jahrzehnt mit diesem Thema befasst sind – die nach wie vor grundsätzlich ausstehende Regelung zum Thema Beschäftigtendatenschutz. Hier würde mich noch einmal Ihre Einschätzung interessieren, welche Herausforderungen im Zeitalter der Digitalisierung ggf. auch über dieses Vorhaben hinaus bestehen. Wir werden das ja in dieser kurzen Zeit nicht umfassend regeln können, was wir zum Thema Beschäftigtendatenschutz seit dem Ende der 80er oder 90er Jahre nicht geschafft haben.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Kollegin Pau. Herr Kollege Reichenbach, bitte.

BE Abg. **Gerold Reichenbach** (SPD): Vielen Dank auch noch einmal an die Sachverständigen für die schriftlichen Gutachten und für Ihre Ausführungen.

Ich habe zunächst eine Frage an Sie, Frau Ehrig, bezogen auf das Thema Scoring. Das sind Themen, die uns auch immer wieder als Abgeordnete erreichen, wenn wir von Bürgern angeschrieben werden, dass sie Kreditverträge, Prepaid-Karten oder andere Dinge nicht bekommen, weil sie in einem bestimmten Viertel leben. Deswegen meine Frage: Sie haben gesagt, die bestehende Regelung im Bundesdatenschutzgesetz passt da eigentlich nicht hin. Warum sind Sie der Auffassung, dass die Datenschutzgrundverordnung selber nicht ausreicht, um das bestehende Verbraucherschutzniveau im Kreditscoring aufrechtzuerhalten?

Würden Sie vielleicht erläutern, warum Sie grundsätzlich der Auffassung sind, dass das eigentlich ein Rechtsrahmen ist, der gar nicht ins Datenschutzrecht hineingehört, deswegen auch hier wieder an der falschen Stelle geregelt wird

und damit auch nicht in Konflikt mit der Datenschutzgrundverordnung gerät?

Die dritte Frage ist, sind Sie der Auffassung, dass wir auf Dauer mit dieser Hilfskonstruktion leben können oder müsste man das nicht in einen anderen Rechtsrahmen überführen?

Eine weitere Frage bezieht sich auf Herrn Prof. Dr. Wolff und ist von Kollege Mayer schon an Sie, Herr Dr. Piltz, gestellt worden. Frau Ehrig, vielleicht können Sie noch einmal erläutern, wo Ihrer Ansicht nach im Gegensatz zu der Einschätzung des Sachverständigen Herrn RA Jaspers die Betroffenenrechte überproportional eingeschränkt worden sind. Frau Ehrig, noch einmal die Frage, ob nicht die Formulierung des unverhältnismäßigen Aufwandes oder der allgemein anerkannten Geschäftspraktiken dazu provozieren, Datei- und Verarbeitungsmechanismen aufzusetzen, die dann am Ende die Lösungs- und Auskunftsrechte durch unverhältnismäßige Aufwände aushebeln, so dass diese zu einem eigenen Geschäftsmodell werden könnten? Sind Sie der Auffassung, dass die von uns vorgelegten Änderungsanträge dieses Problem zu beseitigen helfen, ohne dann in eine Regelung hineinzugeraten, die auch dem kleinen Bäcker Probleme bereitet, der nur analog verarbeitet? Das ist auch für mich erst einmal etwas seltsam, wenn ich dem dann sage: Du musst die Zweckänderung ankündigen, also dem Kunden deiner Brötchendatei vorher eine Postkarte schicken, in der Du ankündigst, dass du ihm eine Werbepostkarte schicken willst.

Dann habe ich noch eine Frage zum Bereich des Beschäftigtendatenschutzes an Herrn RA Dr. Piltz. Sie haben angesprochen, dass die Verordnung in diesem Bereich eigentlich mehr spezifische Regelungen fordert und dass das, was wir im Rahmen des § 26 aus dem alten Bundesdatenschutzgesetz übernommen haben, eher allgemeinere Regelungen sind. Deswegen die Frage: Sind Sie der Auffassung – Kollegin Pau hat das auch angesprochen – dass wir am Ende solche spezifischeren Regelungen, die dann auch arbeitsrechtliche Aspekte aufgreifen müssen, eigentlich gar nicht mehr im Rahmen des Datenschutzanpassungsgesetzes regeln können, sondern dass diese ähnlich wie beim Verbraucherschutz einen eigenen Rechtsrahmen brauchen?



Was die Schriffterfordernisse betrifft, da wird in den Erwägungsgründen 155, aber auch 42 und 43 noch einmal darauf hingewiesen, dass es sich bei dem Beschäftigtenverhältnis nicht um eine Datenerhebung und um Daten bei der Verarbeitung handelt, wie sie für jeden Bürger zutrifft, weil ein gewisses Ungleichgewicht zwischen dem Arbeitgeber oder dem Verantwortlichen und demjenigen eintritt, dessen Daten erhoben und verarbeitet werden. Sind Sie nicht der Auffassung – die Frage würde ich gerne auch an Herrn Schaar richten – dass an dieser Stelle die Schriffterfordernisse, die in dem Erwägungsgrund 42 an anderer Stelle auch noch einmal angezogen werden, nicht gerade der Tatsache gerecht werden, dass wir im Beschäftigungsverhältnis eine andere Relation zwischen dem Verantwortlichen und demjenigen haben, dessen Daten erhoben werden? Ist das Schriffterfordernis nicht noch einmal eine Schranke, die – ähnlich wie im Erwägungsgrund 42 – dazu führt, dass nicht im Rahmen von anderen Rechtsgeschäften der Arbeitgeber die Zustimmung dann noch mit anderen Dingen einholt? Die Ausnahmen, die da enthalten sind, dürften nach der besonderen Form nicht ausreichen, um den Einwänden von Herrn Jaspers gerecht zu werden.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege Reichenbach. Herr Kollege Dr. von Notz, bitte.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Vielen Dank an die Damen und Herren Sachverständigen für die interessanten Einlassungen. Der Kollege Mayer hat sehr zutreffend gesagt: Das war wichtig und instruktiv. Aber ich habe das Wort „Verfassungs- oder Europarechtswidrig“ gefühlt 15 Mal vernommen, vielleicht 20 Mal. Dazu kommt der Umstand, da waren Sie noch gar nicht anwesend, Herr Mayer, dass heute Morgen ein Änderungsantrag gekommen ist, den die Sachverständigen hier gar nicht instruktiv und anders beurteilen konnten. Wenn uns eint, dass wir vor allen Dingen Rechtsunsicherheiten vermeiden wollen, dann geht das vom Verfahren her so nicht. Ich kann immer nur sagen, schlecht gemachte parlamentarische Gesetz sind auch immer schlecht für die Rechtssicherheit. Deswegen hoffe ich, dass es gelingt, hier noch mehr Zeit für ein ordentliches Verfahren hinzubekommen. Dass das diese

Legislaturperiode noch geschehen soll, das leuchtet mir völlig ein. Da sind wir auch voll dabei, aber nicht so.

Grundsätzlich finden wir die Datenschutzgrundverordnung und ihre Umsetzung sehr gut und glauben, dass tatsächlich bedeutende Innovationen für das Datenschutzrecht in dieser Verordnung stehen. Das ist zum Beispiel das Prinzip des Rechts auf Datenübertragbarkeit, Privacy by Design und by Default und auch der Umstand, dass es bei einem Vollzugsdefizit tatsächlich Sanktionen geben kann. Das ist alles sehr gut, aber es gibt auch die eine oder andere Frage mit der wir uns auseinandersetzen müssen.

Deswegen frage ich die Sachverständigen, Herr Prof. Dr. Aden, Herrn Schaar und Frau Voßhoff zu den folgenden drei Punkten, anfangend beim Scoring. Das ist meiner Ansicht nach vor allen Dingen im Hinblick auf die Betroffenheit der Menschen – das Interesse an der Anhörung ist groß, da kann man das schon ungefähr absehen – ein zentraler Punkt, wozu relativ wenig in der Verordnung steht.

Deswegen die Frage, Frau Ehrig, Sie haben es gesagt, man sollte bezüglich der Regelungen, die dann zur Anwendung kommen, vor allen Dingen auf das nationale Recht schauen. Es interessiert mich, ob Sie das für einen guten Weg halten – weil man nicht so lange warten kann – und was der Gesetzgeber mit dieser Problematik machen soll?

Das nächste betrifft tatsächlich unmittelbar die Bundesbeauftragte für den Datenschutz. Ich kann aus meinem Untersuchungsausschuss sagen, dass es im Hinblick auf den BND zehn Jahre lang eine krass rechtswidrige Praxis bei der Verwaltung von Dateien gab. Alles aufgedeckt durch kleinteilige, sehr lobenswerte und arbeitsintensive Arbeit der Datenschutzbeauftragten. Offensichtlich ist man an so einer Kontrolle nicht interessiert. Wenn das in der Großen Koalition die einhellige Meinung ist, ich kann nur sagen, dann müssen Sie Ihre Tonlage im Untersuchungsausschuss auch einmal ändern. Wenn das gewollt ist, dass hier nicht mehr parlamentarisch effizient kontrolliert wird, dann müssen Sie das so machen. Ich finde, das geht überhaupt nicht, deswegen würde mich interessieren, wie die Sachverständigen da präzise draufgucken.



Zum Schluss die Frage, wie man im Hinblick auf die Betroffenenrechte, die Frage ist schon gestellt worden, zu effizienteren Regelungen kommen kann, die tatsächlich diesen Grundsatz berücksichtigen, was in der Vorlage offenbar in der Form nicht der Fall ist. Deswegen wäre es nett, wenn die Sachverständigen darauf noch einmal Bezug nehmen könnten.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege von Notz. Dann beginnen wir diesmal in umgekehrter Reihenfolge, Herr Prof. Wolff, bitte.

SV Prof. Dr. Heinrich Amadeus Wolff (Universität Bayreuth): Die Fragen von Herrn Mayer, erstens Berufsgeheimnisträger, Änderungen der gegenwärtigen Rechtslage. Es geht um die Kontrolle eines privaten Bereiches durch staatliche Behörden. Da gibt es immer wieder Kontrollschranken, das ist nichts Ungewöhnliches. Deswegen empfinde ich die gegenwärtige Regelung, so wie sie ist, einen gut vertretbaren Weg; weder in die eine Richtung noch in die andere Richtung ist eine Änderung notwendig.

Zweitens, die Frage der Fortwirkung der bisherigen Einwilligungen. Sie dürfen sie fortwirken lassen. Das ist unionsrechtlich im Erwägungsgrund niedergelegt. Ich finde, es ist dogmatisch auch überzeugend, weil es eine alte Rechtsgrundlage war, das geht schon. Ich finde aber insgesamt, das habe ich an vielen Stellen schon geschrieben, datenschutzrechtlich hochkritisch, dass man die Einwilligungen generell begrenzt. Ich finde das unmöglich, einmal eine Einwilligung und dann unendlich gültig, außer wenn ich sie widerrufe. In gewissen Situationen müsste man die Einwilligung von Anfang an zeitlich befristen, in Wiederholung. Das aber ist ein anderes Problem, als das, was Sie angefragt haben, denn es ging um die Fortwirkung.

Die Frage mit den Informationsrechten. Ich habe jetzt den Änderungsantrag noch nicht voll im Blick. Sie gehen bei den Informationsrechten durchaus keinen Weg, bei dem die Konformität im Unionsrecht auf den ersten Blick zu 100 Prozent zu ersehen ist. Insbesondere, wenn es um unverhältnismäßige Verarbeitung geht, wenn man dafür die Information einschränken darf. Das ist jetzt wohl ein bisschen relativiert. Ich finde, die Wahrscheinlichkeit, dass wir unionsrechtlich etwas auf die Mütze bekommen nicht sehr hoch, aber sie ist nicht völlig auszuschließen. Deswegen

würde ich sagen, ich verstehe das Ziel, dass man den kleinen schützen soll und ich finde, durch den Hinweis auf die Unverhältnismäßigkeit schützt man ihn. Man geht aber ein gewisses Risiko ein. Politisch müssen Sie das übertragen.

Änderungen vom AG zum LG bei Ordnungswidrigkeiten, weiß der Teufel, das leuchtet mir ein, aber es ginge auch anders.

Viertens, bewährte Geschäftsmodelle. Haben Sie Umsetzungsspielräume die Sie nicht wahrnehmen? Sie haben wenige Umsetzungsspielräume, weil diese bewährten Geschäftsmodelle Interessensabwägungen sind, wo wir nun einmal nationalrechtlich nicht mehr hineindürfen. Das ist eindeutig, Artikel 1 Abs. 1 lit. f) ist unionsrechtlich dem EuGH zugewiesen und nicht dem Deutschen Bundestag. Deswegen haben Sie wenig Spielraum. Ich finde, es gibt einen Spielraum, den Sie früher im Referentenentwurf genutzt haben, den Sie jetzt nicht mehr nutzen. Das ist die Frage, inwiefern Sie in bestimmten Bereichen Privaten öffentliche Aufträge zuweisen. Das wäre die Möglichkeit, einem Privaten ohne ihn zu verpflichten, bei Verpflichtung wäre es lit. e), ermöglichen bzw. ihn über öffentliche Aufträge berechtigen. Das haben Sie nicht mehr genutzt, das wäre aber für die Geschäftsmodelle, von denen Sie sprechen, keine echte Hilfe, denn die Geschäftsmodelle bewegen sich im Bereich, den Sie schwer zum öffentlichen Auftrag machen können. Vielleicht übersehe ich etwas, aber da sehe ich eine systematische weitere Tätigkeit für Sie.

Schriftform oder Textform? Ich finde Textform würde mir beim Beschäftigungsmodell einleuchten. Artikel 4 Abs. 4 im Verhältnis zu Artikel 23 – Profiling – direkt managen – nein, das geht nicht mehr, das können Sie nationalrechtlich nicht mehr regeln. Ich fürchte, da würden Sie mit offenem Visier in die Lanze laufen.

Dann die Frage von Herrn Reichenbach mit den betroffenen Rechten. Da ist das Bild das gleiche. Sie haben mich nicht zum Scoring gefragt. Ich tue jetzt aber so, als hätten Sie mich gefragt. Ich glaube, dass es deswegen geschummelt ist, weil der Hinweis auf die Verbraucherrichtlinien nicht trägt, denn die Datenschutzgrundverordnung sagt, wo sie die Richtlinie kennt, in Artikel 95, da ist sie nicht aufgeführt, d. h. all das andere Unionsrecht muss sich an Artikel 6 orientieren. Da gibt es die



Möglichkeit entweder zwingende Vorschriften zu machen oder öffentliche Aufgaben zu öffentlichen Aufträgen, unionsrechtlich oder nationalrechtlich, zu formulieren. Wenn das Unionsrecht es selbst nicht zur Pflicht macht, müssen wir es zur Pflicht machen oder dürfen es nicht. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Wolff. Frau Voßhoff, bitte.

SVe **Andrea Voßhoff** (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Ich antworte zunächst auf die Frage der Abgeordneten Pau, da geht es noch einmal um das Thema Berufsgeheimnisträger § 29 Abs. 3. Was den Bereich der Anwalts- und Ärzteschaft anbetrifft fällt es nicht in die Zuständigkeit der Bundesbeauftragten. So gesehen habe ich da keine Erfahrung die ich hier mitteilen kann. Aber ich denke, dass die Auswirkung dieser Regelung, das sehe ich genauso, das Risiko von kontrollfreien Räumen z. B. im Gesundheitswesen nicht unbeachtlich ist. Da hat auch die BfDI teilweise Prüfkompetenzen, wenn wir z. B. beim Krankenhausfallmanagement die datenschutzrechtlichen Vorgaben prüfen, es sind besonders sensible Daten, dann könnte – und so gesehen ist diese Regelung unpräzise – uns entgegengehalten werden, dass damit Betriebs- und Geschäftsgeheimnisse verletzt werden und deshalb das auch entsprechend verwehrt wird. Deshalb habe ich in meiner Stellungnahme auch den Versuch unterbreitet, in Kenntnis der Problematik die damit geregelt werden soll, vielleicht auch eine Kompromissvariante zu finden, die diese Kontrolllücke dann verhindert.

Zum Thema, Änderung Videoverbesserungsgesetz. Wir haben es in der Ressortabstimmung, aber jetzt auch in der Stellungnahme zumindest noch kurz erwähnt: Ich bin schon der Auffassung, dass diese individuelle rechtliche Regelung jetzt in dem Anpassungsgesetz europarechtlich mehr als fragwürdig ist. Zumal wir auch sehen, dass der Regelungsspielraum für den nichtöffentlichen Bereich durchaus begrenzt ist und deshalb auch dort in dieser Ausgestaltung nicht geregelt werden darf. Es ist dann halt in der Folge Artikel 6, das ist unmittelbares Recht. Das ist dann auch ein Entwicklungsprozess in der Anwendung und deshalb ergibt sich der Regelungsbedarf aus der künftigen Regelung zusammen in Artikel 6. Und das würde ich auch, nicht nur bei der

automatisierten, sondern auch bei der Weiterentwicklung der intelligenten Videoüberwachung so sehen.

Dann die Frage von Herrn Dr. von Notz zum Thema Scoring. Dazu ist hier schon viel gesagt worden. Auch da sehen wir grundsätzlich bei aller Berechtigung, weil es auch ein nachhaltiges Anliegen aus unserer Sicht ist, hier Bürger und Verbraucher zu schützen. Die Übernahme in diesem Gesetzgebungsvorhaben nach § 28a und § 28b unseres bisherigen geltenden Rechts; auch hier ist die Frage, ob das der Gesetzgeber so ausgestalten darf und das ist sicherlich auch europarechtswidrig oder mit Fragezeichen zu versehen. Auch da würde dann wieder gelten, künftig Artikel 6, wenn man allerdings das Thema und dafür spricht sicherlich auch einiges, von grundsätzlicher Bedeutung auch mit Blick auf Verbraucherschutz sieht, dann muss man nationale Möglichkeiten dazu entsprechend nutzen.

Zum Thema BND, Herr Dr. von Notz, Sie haben das kommentiert, ich glaube, ich brauche das hier an der Stelle nicht weiter ausführen. Ich denke, ich habe dazu auch in meinem Vortrag und auch in der Stellungnahme hinreichend gerade den § 16 Abs. 2 thematisiert, halte daran fest und halte das für europarechtswidrig, weil es den Vorgaben der Richtlinie nicht entspricht.

Was die Betroffenenrechte anbetrifft, effizientere Regelungen. Wie kann man dazu kommen? Auch da, ohne dass ich jetzt alle Details aus meiner Stellungnahme wiederhole. Ich habe hier auch versucht, das, was der Gesetzgeber an Vorgaben dargelegt hat, in den gravierenden Punkten mit entsprechenden Vorschlägen zu entschärfen. Ich würde mich freuen, wenn diese noch Berücksichtigung finden könnten.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Voßhoff. Herr Schaar, bitte.

SV **Peter Schaar** (Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz e. V., Berlin): Vielen Dank, Herr Vorsitzender. Zum Thema Berufsgeheimnisträger und der Frage, welche Bedeutung diese Bereiche in der Prüfpraxis der Datenschutzbehörden hatten und haben: In meiner Zeit als Bundesbeauftragter für den Datenschutz hatten wir etliche Prüfungen im Bereich der Sozialversicherungsträger und der von diesen betriebenen Krankenhäuser, bspw.



Reha-Kliniken. Da wird sehr viel mit sehr sensiblen personenbezogenen Daten gearbeitet. Eine wirksame Prüfung dieser Einrichtungen setzte voraus und setzt meines Erachtens auch in Zukunft voraus, dass die entsprechenden Daten nicht von der Prüfkompetenz der Aufsichtsbehörden ausgenommen werden.

Wenn ich den Zusammenhang noch einmal zu der strafrechtlichen Regelung des § 203 StGB herstellen darf, dann heißt das auch, dass eine Offenbarung nur dann einen Verstoß gegen Berufsgeheimnisse darstellt, wenn diese Offenbarung unbefugter Weise erfolgt. Deshalb enthält das jetzige Bundesdatenschutzgesetz die Regelung, dass solche besonderen Geheimhaltungspflichten nicht den Datenschutzaufsichtsbehörden entgegengehalten werden können, d. h., die Offenbarung erfolgt befugt. Wenn aber diese Regelung in Zukunft nicht mehr besteht, ist damit eine Prüfung dieser Daten nicht mehr möglich, weil eine ausdrückliche Befugnis zur Offenbarung nicht mehr vorliegt. Die soll nach dem Vorschlag der Bundesregierung gestrichen werden. Das bedeutet, dass in sehr vielen Bereichen, wo sehr hochsensible Daten verarbeitet werden, ich denke hier an die Telematikinfrastruktur des Gesundheitswesens, wo eine Prüfkompetenz der Bundesbeauftragten besteht, aber auch eine sehr umfangreiche Prüftätigkeit der Landesdatenschutzbehörden stattfindet, das in Zukunft ausgeschlossen ist.

Um auf die Anwaltschaft zurückzukommen. Da gab es verhältnismäßig wenige Prüfungen. Allerdings ist es richtig, dass es hier besonders konfliktreich war, während das im Gesundheitswesen bisher nicht der Fall war, das im Grunde genommen jetzt auch entsprechend ausgenommen wird. Auch bei der Anwaltschaft denke ich, dass es hier differenzierter Regelungsansätze bedarf. Soweit die Anwaltschaft als Organ der Rechtspflege tätig ist, könnte ich mir vorstellen, dass man das ausnimmt, aber eine generelle Ausnahme für alle Berufsgeheimnisträger daraus zu machen, halte ich für schlecht.

Im Übrigen auch noch zum Thema staatliche Eingriffsmöglichkeiten: Die Aufsichtsbehörden sind jetzt unabhängig. Ursprünglich konnte ich die Anwaltschaft sogar noch besser verstehen, als wir die Aufsichtsbehörden im Zuständigkeitsbereich der Innenministerien hatten, so dass dort von der Anwaltschaft auch befürchtet wurde, dass der

Staat, also die Ministerien, auf die entsprechenden Informationen zugreifen könnten, über die Aufsichtsbehörden. Das ist heute aus meiner Sicht völlig ausgeschlossen durch die Unabhängigkeit der Aufsichtsbehörden, das hat es früher im Übrigen auch nicht gegeben.

Thema Videoüberwachung, dazu hat Frau Voßhoff schon einiges gesagt. Ich denke, dass diese Regelungen zu weit führen. Sie haben diese Bestimmungen auch schon in einem anderen Zusammenhang beschlossen. Gerade im Hinblick auf intelligente Videosysteme besteht das Problem, dass hier für diese Zwecke auch eine Verarbeitung durch private Stellen stattfindet. Damit kommen wir dann im Grunde genommen sehr schnell in einen Problembereich, wo wir dann ein Profiling durch Private rechtfertigen durch diese Änderungen. Ich halte das auch im Hinblick auf die Vorgaben der Verordnung nicht für richtig. Hier wird, finde ich, zu Unrecht diese ausbalancierte Abwägung, die wir bisher im Bundesdatenschutzgesetz haben oder hatten, aufgegeben. Das sehe ich kritisch.

Herr Reichenbach, Sie haben nach der Schriftformerfordernis im Bereich der Arbeitsverträge gefragt. Schriftform, um das noch einmal in Erinnerung zu bringen, umfasst ja auch die elektronische Form. Insofern gibt es durchaus auch zeitgemäße Möglichkeiten diese Schriftformerfordernisse zu erfüllen. Wenn das bisher noch nicht so gegriffen hat, dann müsste man da vielleicht dran arbeiten und nicht daran, diese Formerfordernisse abzusenken. Das Schriftformerfordernis hat im Grunde zwei zentrale Aspekte. Der eine ist die sogenannte Warnfunktion. Der Betroffene soll wirklich gewarnt sein, da ist etwas Wichtiges in das er einwilligt. Das ist im Arbeitsleben schon der Fall. Das zweite ist die Beweisfunktion. Das ist mit der Beweisfunktion im Hinblick auf die Textform schon so eine Sache: Textform, da reicht irgendeine E-Mail, die meinen Absender trägt, aus. Wir wissen, wie problematisch das ist; wie leicht das entsprechend auch geändert werden kann. Insofern halte ich es für richtig, jedenfalls für sehr gut nachvollziehbar, dass der Gesetzgeber hier anders als in anderen Bereichen, die weniger gravierend sind, an diesen erhöhten Anforderungen festhält.



Herr Dr. von Notz, Sie haben das Thema Scoring-Regelung aufgerufen. Ich teile hier vollständig die Auffassung von Frau Voßhoff, auch wenn es wünschenswert ist, die Substanz dieser Regelung zu behalten, und dass es zumindest ein gefährlicher Weg ist, das im Bundesdatenschutzgesetz zu machen. Zu den Inhalten haben Sie mich jetzt nicht gefragt, aber da könnte ich mir auch noch einige Verbesserungen vorstellen.

Letzter Punkt, wie kann man denn die Betroffenenrechte sinnvoller gestalten? Ganz einfach, indem man auf die Sonderregelung Datenschutzanpassungsgesetz verzichtet. Dann gelten die Regelungen der Datenschutzgrundverordnung. Die reichen meines Erachtens völlig aus.

Vors. **Ansgar Heveling** (CDU/CSU): Dankeschön, Herr Schaar. Herr Dr. Piltz, bitte.

SV Rechtsanwalt Dr. Carlo Piltz (Reusch Rechtsanwälte, Berlin): Ich beginne mit den Fragen von Herrn Mayer zu den Berufsgeheimnisträgern. Ob die Regelung jetzt so in Ordnung ist bzw. was man da noch machen könnte. Diese Regelung beruht auf dem Artikel 90 der Datenschutzgrundverordnung der im Endeffekt vorgibt, was der nationale Staat machen darf in Bezug auf Berufsgeheimnisträger. Teilweise klingt das so, als ob jetzt hier die Rechtsanwälte oder andere Berufsgeheimnisträger komplett herausgenommen werden. So verstehe ich den Artikel 90 nicht. Da wird spezifisch auf zwei Untersuchungsbefugnisse der Datenschutzbehörden rekuriert, dass die nicht in den Betrieb hineindürfen. Ansonsten Artikel 58 die Befugnisse der Aufsichtsbehörden sind weiterhin auch auf Berufsgeheimnisträger anwendbar, die übrigen. Deswegen finde ich den jetzt vorliegenden Vorschlag, wie Professor Wolff auch gesagt hat, eigentlich so in Ordnung.

Die zweite Frage, Fortgeltung der Einwilligung. Da habe ich Sie so verstanden, dass Sie vielleicht überlegen, nochmal im jetzt vorliegenden Entwurf eine Anpassung vorzunehmen, dass man Alteinwilligungen noch einmal klarstellt und hinzufügt, dass die in Zukunft fortgelten, wenn sie jetzt wirksam sind. Sie haben auch schon den Erwägungsgrund 171 erwähnt, der leider auch teilweise nicht ganz klar ist, und deswegen auch

schon in der Literatur umstritten ist, was das jetzt genau bedeutet. Die Landesdatenschutzbehörden wie auch die Bundesdatenschutzbeauftragte hatten sich dazu geäußert, was mit Alteinwilligungen geschieht. Grundsätzlich sind die weiterhin gültig, müssen nicht neu eingeholt werden, wenn sie der Art nach die Bedingungen der Datenschutzgrundverordnung erfüllen, d. h. in Zukunft, ab dem 25. Mai 2018, müssen diese Einwilligungen die Bedingungen der Datenschutzgrundverordnung erfüllen. Das steht auch in dem Erwägungsgrund drin. Ob sie das jetzt noch einmal ins BDSG klarstellend hineinschreiben möchten, dass würde ich jetzt sagen, ist Ihnen überlassen. Ich halte es nicht für unbedingt erforderlich, dass Sie das noch einmal hineinschreiben.

Die dritte Frage betraf die neuen Änderungsanträge, die hier vor uns liegen. Da bitte ich um Verständnis, dass ich jetzt nicht alles in der Kürze der Zeit durchschauen konnte. Was mir aufgefallen ist, die zweite Änderung, also rechtlich durch das Wort zivilrechtlich ersetzen, das hatte ich auch in meiner Stellungnahme angemerkt, das halte ich durchaus für sinnvoll, weil es auch so in der Datenschutzgrundverordnung steht.

Bei der Änderung unter I Buchstabe d) zu § 32 Abs. 1 Nr. 1, das ist, wenn Sie meine Stellungnahme gesehen haben ein Bereich, wo ich schon ein Risiko sehe. Ich verstehe, dass das jetzt hier angepasst und das mit dem unverhältnismäßigen Aufwand hier herausgenommen wird. Das finde ich richtig. Die Frage, die sich ganz allgemein bei einer Beschränkung auf dieser Ebene bei einer Direkterhebung bei der betroffenen Person und der Weiterverarbeitung stellt, ist: Können wir das so einschränken wie wir das wollen? Denn mit diesen Unverhältnismäßigen, das war im Artikel 14 DSGVO, wenn die Daten nicht beim Betroffenen erhoben wurden. So etwas gibt es nicht im Artikel 13. Grundsätzlich wäre das zu begrüßen, ich bin aber noch nicht 100 Prozent sicher, ob das dann so mit den Vorgaben des Artikels 13 konform wäre.

Die vierte Frage von Ihnen war, Landgericht ab einem Bußgeld von 100.000 Euro. Da bin ich, glaube ich, leidenschaftslos. Ich würde es auch nicht unbedingt am Geld festmachen. Ein Bußgeldbescheid über 100.000 Euro oder mehr kann bei relativ einfachen Fragen des Datenschutzrechts beim Bußgeld z. B.



ausgesprochen werden, wenn es einfach ein massenhafter Verstoß ist. Es kann genauso gut sein, dass Sie einen Bußgeldbescheid über weit weniger hohe Beträge haben, der aber rechtlich interessante, schwierige Fragestellungen beinhaltet, wo man sagen würde, naja, das wäre nicht schlecht, wenn das in die Kammer am LG geht, wo jetzt nicht nur ein Amtsrichter sitzt. Aus meiner Erfahrung heraus, rein subjektiv, kann ich sagen – das ist natürlich im Ordnungswidrigkeitenrecht nicht zu machen –, dass daneben natürlich auch die Verwaltungsgerichtsbarkeit in dem Thema relativ gut drin ist, teilweise sogar besser als die Zivilrechtsprechung. Wie gesagt, jetzt sind wir hier im OWiG-Bereich. Am Geld, am Betrag würde ich es nicht festmachen. Deswegen habe ich da auch nicht eine konkrete Größe für Sie, wann man da ans LG geht.

Weiterhin haben Sie zur Schriftform gefragt. § 26 Abs. 2 BDSG dem Beschäftigtendatenschutz. Da haben schon die Vorredner auch etwas zu gesagt, wie das ist. Ob man das regeln kann? Ob man das regeln sollte? Grundsätzlich haben wir auch hier ein Problem der Datenschutzgrundverordnung, nämlich das die sagt, wir können im Beschäftigtendatenschutz Spezifizierungen vornehmen. Jetzt weiß niemand, was das genau bedeutet. Was sind diese Spezifizierungen? Meint Spezifizierung, das Schutzniveau auf jeden Fall gleich zu belassen, wenn nicht sogar in diesem Bereich anzuheben; das ergibt sich zum Beispiel daraus, wenn Sie schauen worauf der Artikel 88 in der DSGVO rekurriert, da steht dann nämlich „zur Gewährleistung des Schutzes der Rechte und Freiheiten“. Ich hätte in jedem Fall ein Problem damit, wenn Sie sagen, wir gehen jetzt hier vom Schutzniveau hinunter. Dem Wortlaut nach, Gewährleistung des Schutzes spricht mindestens für eine Gleichbehandlung zur DSGVO wenn nicht sogar eine Erhöhung. Die Frage ist, sollte man es regeln? Da bin ich so ein bisschen bei Herrn Schaar. Selbst wenn Sie sagen, wir wissen nicht genau ob wir Schriftformerfordernis einführen möchten, dem Schutzniveau würde es sicherlich dienen und im Zweifel wird sich das sowieso in der Praxis, wie es jetzt meistens ist, etablieren, um dieser Nachweispflicht nachzukommen, weil ich ein Problem als datenverarbeitende Stelle habe, wenn ich es nur in elektronischer Form habe. Das könnte dann aus Versehen gelöscht werden, wenn ich es nur in Textform hätte, gut man kann sagen,

Papier kann auch verschwinden, wie auch immer. Deswegen kann man das durchaus mit der Schriftform regeln. Ich gebe nur zu bedenken, meines Erachtens dürfen Sie es bei der Schriftform nicht so ausgestalten, dass dann erst die Einwilligung wirksam ist. Der Erlaubnistatbestand der Einwilligung der ist in der Datenschutzgrundverordnung definiert. Was Sie meines Erachtens aber machen können, ist die Schriftform als zusätzliches Erfordernis zu nehmen und zu sagen: „Es liegt eine Einwilligung im Arbeitsverhältnis vor und wir fordern dich dazu auf, dass diese in Schriftform abgegeben wird.“ Die Einwilligung muss aber wirksam vorliegen.

Ihr letzte Frage richtete sich auf das Profiling, Artikel 4 Ziffer 4 und Artikel 22. Kann man Direktmarketing im neuen BDGS regeln, da bin ich auch beim Professor Wolff und würde sagen, nein, das geht nicht. Das können Sie z. B. meines Erachtens auch daraus ablesen, dass direkte Werbung – Marketing ist schon in der Datenschutzgrundverordnung genannt, explizit in den Erwägungsgründen im Rahmen der Interessenabwägung – ein berechtigtes Interesse darstellen kann. Der Unionsgesetzgeber hat sich gedacht, Regelungen des Profiling müssen jetzt nicht Direktmarketing betreffen, sondern es gibt auch Direktmarketing einfach nur aufgrund berechtigter Interessen, das nicht in dieses pauschale Verbot des Artikels 22 hineinfällt. Deswegen würde ich nein sagen, es gibt keine Möglichkeit mehr das zu regeln.

Zu den Fragen von Herrn Reichenbach. Sie hatten die Betroffenenrechte zuerst angesprochen und die Einschätzung ob da jetzt noch zu viel eingeschränkt wurde. Ich habe, glaube ich, meine Antwort jetzt schon gegeben, bei diesem Vorschlag des § 32 Abs. 1 Nr. 1, wie gesagt, da bin ich mir nicht sicher, ob da nicht bei Direkterhebung und Nichtsituation der Direkterhebung die Einschränkung durcheinander gehen. Wenn die Direkterhebung im Artikel 13 vorliegt, ist nur wenig Möglichkeit, da die Betroffenenrechte und die Informationspflicht einzuschränken.

Die zweite Frage bezog sich auf den Beschäftigtendatenschutz und die Frage, was ist denn nun spezifisch, könne wir das in Zukunft regeln, bzw. müssen wir es in einem anderen Gesetz regeln und gar nicht in einem eigenen BDSG. Sie haben natürlich Recht, dass das



teilweise ein Graubereich ist vom Datenschutzrecht und Arbeitsrecht, dass das ineinander überschwappt. Solange wir jetzt bei diesen Regelungen bleiben, die wir jetzt vorgesehen haben, würde ich sagen, klar, da geht es um die Verarbeitung personenbezogener Daten. Da können wir spezifischere Vorschriften vorsehen. Grundsätzlich würde ich aber nicht ausschließen, dass man irgendwann einmal sagt, das ist so ein besonderer Bereich, da müssen wir einmal ein eigenes Gesetz in Angriff nehmen, weil auch die Ausgangssituation, in der wir uns befinden, so besonders ist. Wie Sie es gesagt haben, die Datenschutzgrundverordnung geht auch davon aus: besondere Situationen, Ungleichgewicht. Ich erinnere übrigens daran, dass auch die Europäische Kommission dieses Schlagwort Arbeitnehmerdatenschutz vor Jahren schon einmal in einer Mitteilung erwähnt hat und dazu schon einmal, glaube ich, eine Befragung der nationalen Mitgliedstaaten eingeleitet hat. Also, so komplett neu ist auch das Thema auf europäischer Ebene nicht. Damit bin ich durch, vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Dr. Piltz. Dann dürfen Sie nun, Herr Neumann.

SV Karsten Neumann (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a. D., 2b Advice, Bonn): Vielen Dank für die Nachfragen. Ich glaube, sie zeigen wie komplex das Thema ist und dass wir zu wenig Zeit dafür haben. Deshalb will ich es aus meiner Sicht auch kurz abhandeln.

Das Thema Berufsgeheimnisträger und Relevanz der vorgesehenen Regelung. Ich arbeite inzwischen als externer Datenschutzbeauftragter und war vorher als Aufsichtsbehörde tätig. Sie bekommen eine Beschwerde, dass Ihr behandelnder Arzt die Daten auf Dropbox hoch lädt. Was tun Sie? Was tut die Aufsichtsbehörde? Die Aufsichtsbehörde fragt, tust du das wirklich und der Arzt sagt, das verstößt gegen die ärztliche Schweigepflicht. Weil schon die Information darüber, ob der Anfragende mein Patient ist der ärztlichen Schweigepflicht unterliegt. Wer entscheidet jetzt, wie in § 29 Abs. 3 DSAnpUG-EU vorgesehen, ob die Inanspruchnahme der Befugnisse der Aufsichtsbehörde zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Wer soll das bitteschön entscheiden? Was

kann die Aufsichtsbehörde machen? Die Aufsichtsbehörde kann sagen, okay, der Arzt antwortet mir nicht, also mache ich einen Bescheid, verhängt ein Bußgeld, vielleicht sogar ein Zwangsgeld, das finde ich immer eine schöne Variante. Dann trifft man sich vor Gericht und vor Gericht sagt der Arzt, sorry, das ist gar nicht mein Patient, es war ein anderer. Das kann auch nicht gewollt sein. Oder unter den neuen Bedingungen, ich habe mir das gerade überlegt, wäre die Aufsichtsbehörde in der Lage, den betrieblichen Datenschutzbeauftragten des Krankenhauses als Anlaufstelle der Aufsichtsbehörde mit der Prüfung zu beauftragen, der dürfte dann nämlich prüfen, ist das nicht absurd, weil der unter den Schutzbereich fällt. D. h. aus meiner Sicht führt das wirklich zu einer Unklarheit, Herr Schaar hat es gesagt. Ganz einfach, lassen Sie den zweiten Satz stehen, nehmen den ersten weg und wir hätten die Situation geklärt und klargestellt für den der sie braucht, dass natürlich auch bei einer aufsichtsbehördlichen Prüfung die Aufsichtsbehörde dann den selben Verschwiegenheitspflichten unterliegt wie der Arzt, Anwalt, Steuerberater oder die Schwangerschaftskonfliktberatungsstelle. Ich glaube, das ist schon heute für die Aufsichtsbehörden selbstverständlich und kann hier dann entsprechend mit einer kurzen Änderung, denke ich, klargestellt werden.

Die weiteren Fragen zum Thema Scoring und Beschäftigtendatenschutzgesetz und Videoüberwachung kann man eigentlich mit einem Punkt zusammenfassen. Herr Professor Wolff hat es schon kurz, vielleicht nicht deutlich genug, gesagt, der Deutsche Bundestag hat die Gesetzgebungskompetenz verloren, und zwar in immer mehr Bereichen. Ich weiß nicht ob deshalb die Reaktion von Frau Ehrig war, zu sagen, lasst uns das lieber im fachspezifischen Bereich regeln, weil es da genauer passt als im Datenschutzrecht. Datenschutz ist eben Querschnittsrecht. Am Ende der datenschutzrechtlichen Frage hängt immer eine fachpolitische Frage. Ob es nun ärztliche Schweigepflicht, Versicherungsvertragsrecht, Verbraucherkreditwesen ist etc. pp. wir haben es immer mit solchen Querschnittsfragen zu tun. D. h. der Konflikt, glaube ich, wird hier an diesem Beispiel sehr schön deutlich: Wenn man die Gesetzgebungsbefugnis für einen solchen Querschnittsbereich Europa überträgt, bleibt die



spannende Frage, was bleibt übrig? Und der am anderen Ende, in dem Fall wir, ist bemüht, in den Fachgesetzen so viel wie möglich zu regeln. Aus meiner Sicht, und das sage ich aus meiner dritten ehemalige Funktion als Parlamentarier, ist das auch richtig, weil genau diese Debatten gehören eigentlich in die Fachausschüsse, wo es um Kreditwesen, Geschäftsmodelle geht und nicht in ein solches Querschnittsthema. Bisher haben wir, aus welchen Gründen auch immer, Teilbereiche allerdings im Datenschutz geregelt, da wäre es aus meiner Sicht, und deshalb auch meine Vorschläge dazu, angebracht, diesen bisher erreichten Konsens, hier in den Ausschüssen, Anhörungen, Gesetzgebungsverfahren, z. B. zum Thema Scoring, zu retten, wenn es zu retten ist. Aus meiner Sicht spricht jedenfalls nichts dagegen. Ich wüsste nicht, was europarechtlich dagegen sprechen sollte, das bei den Themen zu machen.

Das Gleiche gilt für die Herausforderung durch intelligente Videoüberwachung. Ob das tatsächlich intelligent ist, ist eine andere Frage. Aber das, was dieser Begriff bezeichnet führt natürlich zu einer Situation, die das Bundesverfassungsgericht 1983 sehr klar beantwortet hat, nämlich: Die Gefahr durch eine unkontrollierte Verarbeitung personenbezogener Daten kann ich am besten beseitigen, wenn ich das Gerät beseitige. Wenn das Gerät einmal da ist, kann ich die Kontrolle dahinter ob nun diese Videokamera schon seit zwei Monaten kaputt ist, ob sie von Anfang an eine Attrappe war – übrigens der Großteil von Videoüberwachungsanlagen sind Attrappen – oder ob ein intelligentes System dahinter ist, dass die Daten mit Facebook, Social Media und Co verknüpft, um gleichzeitig meinem Steuerberater mitzuteilen, dass ich heute in Berlin war, das können wir nicht einschätzen. Das können die Aufsichtsbehörden von außen nicht einschätzen und auch die Betroffenen nicht d. h., diese Fragestellungen sind sehr schwer und komplex. Herr Jaspers hat mich gerade daran erinnert, vor zehn Jahren saßen wir einmal hier zum Thema Modernisierung des Datennutzrechtes. Sie haben sich, glaube ich, fünf Jahre in einer Enquete-Kommission die Köpfe auf der Suche nach Lösungswegen zerbrochen, die haben wir mit der Datennutzgrundverordnung weder gefunden noch kodifiziert. Diese Aufgabe wird bleiben. Da bleibe ich dann Egoist und sage, dann lieber in den Fachausschüssen hier im Deutschen Bundestag als

auf europäischer Ebene, wo in den nächsten 20 Jahren zum Thema Datenschutz sicherlich einiges passieren wird, aber nicht in diesen Fragen, befürchte ich.

Die Regelung zum Thema Beschäftigtendaten, das halte ich einfach für ein redaktionelles Versehen. Ich habe es selber nicht geglaubt, als ich es gelesen habe. Dass die Formulierung des Gesetzesvorschlages darauf hinausläuft, dass die Datenverarbeitung durch die Interessenvertretung, also durch den Betriebsrat, auf Basis einer Betriebsvereinbarung weiterhin erlaubt sein soll, aber nicht eine Datenverarbeitung auf Grund einer Betriebsvereinbarung, z. B. zum Thema Reisedaten, Reisekosten, Renten oder sonst irgendwas. Ich lese die Formulierung jedenfalls so, dass sie sich nur auf die Datenverarbeitung durch den Betriebsrat oder Personalrat bezieht – wenn das zutrifft, das halte ich hoffentlich nur für ein redaktionelles Versehen. Wenn es das nicht ist, dann ist es ein riesen Problem für die Praxis. Denn natürlich basieren eine ganze Reihe, auch eine ganze Fülle von Interessenabwägungen auf betrieblicher Ebene zwischen den berechtigten Interessen der Beschäftigten und den Unternehmensinteressen auf Betriebsvereinbarungen. Dafür sind sie auch da und diese Möglichkeit sollte auch erhalten bleiben. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Dankeschön, Herr Neumann. Herr Jaspers, bitte.

SV Rechtsanwalt Andreas Jaspers (Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn): Vielen Dank. Ich möchte auf die Fragen des Abgeordneten Mayer antworten. Als erstes auf das punktuelle Spannungsverhältnis zwischen Datenschutzaufsichtsbehörde auf der einen Seite und den Berufsgeheimnisträgern. Wenn man sich die Praxis anschaut, Herr Neumann, hat es schon angedeutet, dann liegen die Probleme bei den Berufsgeheimnisträgern manchmal nicht konkret in der Datenverarbeitung einer einzelnen Person, sondern in der Ermangelung einer Datenschutzorganisation. Dann liegen die Akten herum, sind nicht gesichert, die Verträge sind im Grunde genommen nicht sauber ausgestaltet. Für alle diese Fälle bleibt es dabei, dass die Aufsichtsbehörde sich anschauen kann, wie die Organisation beim Berufsgeheimnisträger vor Ort aussieht. Ich brauche gar nicht im Einzelfall zu kontrollieren, wie die personenbezogene



Datenverarbeitung eines Mandanten aussieht. Wenn dann die Anfrage kommt und ich beschwere mich bei einer Aufsichtsbehörde, kann ich doch der Aufsichtsbehörde auch die Einwilligung geben, „Ja, du darfst in meine Akte hineinschauen“. Dann habe ich dafür eine Rechtsgrundlage. Ich möchte aber einräumen, dass der Vorschlag von Herrn Neumann einen gewissen Charme hat, die Aufsichtsbehörden wie auch die betrieblichen Datenschutzbeauftragten einer entsprechenden Verschwiegenheitsverpflichtung zu unterziehen. Dann käme man möglicherweise aus der Nummer heraus. Ich habe das zwar nicht geprüft, aber da spricht einiges für. In der Sache selber meine ich, dass die Vorschrift so erhalten bleiben kann, weil die Aufsichtsbehörden hinreichende Möglichkeiten haben, Mängel in der Datenschutzorganisation zu beanstanden, auch bei Berufsgeheimnisträgern.

Thema Fortgeltung der Einwilligung. Hier ist schon einiges zum Thema gesagt worden. Die deutschen Aufsichtsbehörden im Düsseldorfer Kreis haben gesagt, Alteinwilligungen können weiter gelten. Der Kernpunkt ist, ob in Alteinwilligungen auf die Widerruflichkeit für die Zukunft hingewiesen worden ist oder nicht. Das ist der entscheidende Punkt. Denn nach der Rechtslage heute muss ich das nicht machen. Die Frage ist, muss ich wegen dieses Mangels alles nachholen? Die deutschen Aufsichtsbehörden sagen wegen Erwägungsgrund Nr. 171, das musst du nicht machen. Das ist im Grunde genommen dadurch abgedeckt. Es gibt keine Notwendigkeit, neue Einwilligungen einzuholen.

An dem Punkt muss man vielleicht doch einmal den Finger in die Wunde legen. Das sagen die deutschen Aufsichtsbehörden. Das hat noch nicht der Europäische Datenschutzausschuss gesagt. Da müssen wir in der Tat hinschauen. Wir sind im Verhältnis zur Datenschutzgrundverordnung zum Europäischen Datenschutzausschuss. Ich muss mir anschauen in welche Richtung er tendiert. Ja, es gibt ihn noch nicht, den Datenschutzausschuss, wohl aber bereits eine Gruppe, die Fablab-Gruppe, die bereits Auslegungen der Grundverordnungen vornimmt. Da dann die Vertreter der Artikel 29-Gruppe und des Datenschutzausschusses wahrscheinlich personenidentisch sind, werden auch die Entscheidungen des Datenschutzausschusses wohl so aussehen, wie die ersten Workingpapers. D. h., in dem Fall haben wir

in vielen Bereichen eine Deutungshoheit des Datenschutzausschusses. Vor diesem Hintergrund ist es richtig und wichtig, dass der deutsche Gesetzgeber in dem Rahmen, der ihm zur Verfügung steht, auch gesetzgeberisch tätig wird, dann haben wir mehr Rechtssicherheit und ich möchte behaupten, dass die demokratische Legitimität des deutschen Gesetzgebers höher ist, als die der Aufsichtsbehörden, die nur eine aufsichtsbehördliche Sicht auf das Thema haben. Das ist das Petitum am Rande. Ich glaube aber, in diesem Fall gibt es keine Möglichkeit des deutschen Gesetzgebers tätig zu werden. Ich sehe keine Eröffnungsklausel, d. h. wir müssen hoffen, dass der Europäische Datenschutzausschuss so entscheidet und die Dinge so sieht, wie die deutschen Aufsichtsbehörden im Düsseldorfer Kreis.

Zum Thema Betroffenenrechte: Auch hier will ich nicht gegen den Datenschutz reden. Nur der ursprüngliche Entwurf des BMI sagt, ich muss dann, wenn ich bereits Daten beim Betroffenen erhoben habe und sie für andere Zwecke weiterverarbeite, nicht informieren, wenn das einen unverhältnismäßigen Aufwand betrifft. Natürlich muss ich darüber informieren, was ich mit den Daten machen möchte. Darin sehe ich kein Problem. Das Problem ist nur, dass damit auch andere Informationspflichten verbunden sind. Ich muss wieder sagen, das ist eine Aufsichtsbehörde, du hast die und die Recht, die man standardmäßig hat, d. h., es kommt zu einer langen, langen Litanei von Informationspflichten, die standardmäßig vorgegeben sind. Das wirkt am Ende des Tages äußerst unpraktisch. Deswegen hatte ich im ursprünglichen Vorschlag der Bundesregierung den Charme gesehen, nicht immer mit Litaneien das Ganze zu verbinden. Ich sehe allerdings wie Dr. Piltz die Problematik, dass das möglicherweise europarechtswidrig sein kann. Von daher ist jedenfalls die Einschränkung, die jetzt im Änderungsantrag vorliegt, wahrscheinlich die Richtung zu mehr Rechtssicherheit; ob das praktisch sinnvoll ist, ist eine andere Frage.

Zur Frage der Gerichtsbarkeit LG oder AG. Wenn man sich die Bußgeldregelungen anschaut und auch die Bewertungsmaßstäbe, wo es heißt, wirksam, verhältnismäßig abschreckend, dann sind auch mit Blick auf den 4-Prozent-Wert des weltweiten Konzernumsatzes Summen im Raum,



die möglicherweise sehr schnell die 100.000 Euro erreichen können. Dann den Amtsrichter mit diesen Themen zu belasten – ich würde einmal sagen, eine Kammerentscheidung ist wahrscheinlich der Weg, wo mal mehrere Köpfe darüber nachdenken. Im Übrigen sehe ich doch in vielen Fällen eine lange gerichtliche Auseinandersetzung, denn Unternehmen, die mit solchen Bußgeldern konfrontiert werden. Diese werden sich auch entsprechend anwaltlich munitionieren und am Ende entscheidet der Europäische Datenschutzausschuss. Von daher erst einmal das LG heranzulassen ist wahrscheinlich ein brauchbarer und denkbarer Weg.

Zum Thema Ausnutzung des Umsetzungsspielraums in hinreichendem Maße: Stichwort Inkassounternehmen. Ich glaube, hier gibt es keine Möglichkeit, das auch noch im Detail zu regeln. Die Frage, ob künftig Unternehmen berechtigt sind, Inkassounternehmen zu beauftragen, entscheidet der Europäische Datenschutzausschuss. Das muss man dann entsprechend abwarten. Die Möglichkeiten des bundesdeutschen Gesetzgebers hier etwas zu konkretisieren, sehe ich nicht.

Dann noch zum Thema, was Sie angeschnitten haben: Beißen sich die Regelungen zum Profiling mit den anerkannten Methoden der Direktwerbung? Ich sehe das rechtlich nicht so, denn, wenn das Profiling nicht die Konsequenz hat, rechtliche Folgen unmittelbarer Art nach sich zu ziehen, sondern nur die vorbereitende Datenauswertung für eine werbliche Maßnahme ist, werden diese Profilingregelungen aus der Grundverordnung gar nicht erst greifen. Im Übrigen hat das auch der Ordnungsgeber erkannt, indem er gesagt hat: Wenn du das nicht willst, weder Werbung noch Profiling, kannst du sagen, mach das nicht: Dann ist das Thema vom Tisch. Insofern sehe ich keine Widersprüche und deswegen können anerkannte Methoden des CRM im Grundsatz auch nach Geltung der Grundverordnung entsprechend weiter gehen. Das waren eigentlich die Punkte zu denen ich etwas sagen sollte.

Letzter Punkt, dann sage ich unaufgefordert etwas: Betriebsrat und Datenverarbeitung. Es ist sinnvoll, dass der Bundesgesetzgeber nunmehr dem Betriebsrat erlaubt, Datenverarbeitung für eigene Zwecke zu betreiben. Das liegt daran, dass nach

dem Betriebsverfassungsgesetz es nur ganz bestimmte punktuelle Datenverarbeitungsrechte gibt. Es musste das Bundesarbeitsgericht z. B. über die Frage entscheiden, ob der Betriebsrat einen Anspruch hat, diejenigen Mitarbeiter zu erfahren, die einen betrieblichen Einwilligungsmangementanspruch haben. Das macht der Bundesgesetzgeber jetzt klar und sagt: Ja, für konkrete Aufgaben des Betriebsrates ist auch die Datenverarbeitungslegitimation gegeben – insofern eine sinnvolle Lösung. Davon meines Erachtens ungeachtet bleibt es dabei, dass selbstverständlich Betriebsvereinbarungen vorrangige Rechtsnormen sind. Das regelt auch Artikel 88. Insofern, Herr Neumann, glaube ich, können wir uns auf den Standpunkt stellen, dass wir weiterhin die Rechtsgrundlage haben, entsprechend auch tätig werden zu können und der Betriebsrat die Kompetenzen behält. Ich hoffe, Ihre Fragen beantwortet zu haben.

Vors. **Ansgar Heveling** (CDU/CSU): Danke schön, Herr Jaspers. Frau Ehrig, bitte.

Sve **Lina Ehrig** (Verbraucherzentrale Bundesverband e.V., Berlin): Vielen Dank für die Nachfragen. Zunächst zum Scoring. Die Datenschutzgrundverordnung hat den Artikel 22 der definiert, dass Verbraucher nur unter bestimmten Bedingungen einer automatisierten Einzelfallentscheidung unterliegen müssen. In dem Artikel 22 sind keinerlei Einmeldekriterien definiert, die wir in den bisherigen Regelungen zum Scoring und den Auskunfteien im BDSG haben und die nun von ihrem Inhalt her in den § 31 überführt wurden. Wenn wir nur den Artikel 22 hätten, dann würde zukünftig allein vermutlich erstmal auf Basis einer Interessenabwägung entschieden werden müssen, welche Forderung und welche Information einfließen können, um einen Scorewert zu regeln. Das würde einfach enorme Rechtsunsicherheit bergen. Wir haben die Regelung im BDSG seit 2009/2010 um klar zu definieren, welche Forderung überhaupt erfasst werden dürfen, also Einmeldekriterien, so dass nicht nur ausschließlich auf Basis der Anschrift ein Scorewert gebildet werden kann. Insofern haben wir hier eine sehr viel stärkere Konkretisierung, die dem Verbraucherschutz dient.

Von daher möchte ich gleich zur zweiten Fragen überleiten. Warum sind es keine



Datenschutzregeln? Die Regelungsinhalte regeln nicht, wer wie mit welchen personenbezogenen Daten umgeht sondern die Regelungsinhalte regeln, unter welchen Bedingungen ein Scorewert im Wirtschaftsverkehr verwendet werden darf. Von daher ist es so, dass sie ursprünglich im BDSG angesiedelt werden, weil hier bei Auskunfteien es zu einem Anwendungsfall kommt. Aber es ist eigentlich keine Datenschutzregelung, deswegen sehen wir hier keine Europarechtswidrigkeit.

Im Hinblick auf den Einwand von Prof. Dr. Wolff möchte ich noch einmal sagen, es geht hier nicht um Regelungen der Verbraucherrechterichtlinie, es geht hier ausschließlich um nationale Regelungen des BDSG, die wir vom Inhalt her überführt haben möchten. Sie hatten noch gesagt, wir wollen perspektivisch die Regelung gerne außerhalb des neuen BDSG haben. Das ist aber in der jetzigen Legislatur einfach aufgrund der knappen Zeit nicht möglich. Insofern wäre es sinnvoll, die Regelungsinhalte zukünftig in zivilrechtliche Regelungen z. B. zu überführen und da natürlich auch noch einmal die Regelungsinhalte insgesamt zu diskutieren. Also, brauchen wir vielleicht eine Verschärfung oder einfach eine Konkretisierung?

Vielleicht noch einmal ganz kurz zu den Betroffenenrechten, unverhältnismäßiger Aufwand, Gefährdung des Geschäftszwecks. Das sind einfach Formulierungen, die interpretationsfähig sind, gerade beim unverhältnismäßigen Aufwand muss man sagen, könnten Unternehmen bzw. verantwortliche Stellen schon geneigt sein, dann ihre Systeme genau so zu etablieren und zu programmieren, dass es einen unverhältnismäßigen Aufwand darstellt, um ggf. unter diese Ausnahmeregelung, die wir jetzt in § 32 haben, zu fallen. Eigentlich muss es genau umgekehrt sein. Die Systeme müssen so gestaltet sein, dass es gerade keinen unverhältnismäßigen Aufwand darstellt, sondern Stichwort Privacy by Design datenschutzfreundlich und datenschutzarm. Insofern sind wir der Meinung, dass das natürlich provozieren kann. Die Vorschläge jetzt im Änderungsantrag sind sehr viel enger gefasst und eine Verbesserung im Vergleich zu dem jetzigen § 32. Ich kann nicht abschließend beurteilen, im Hinblick auf die Europarechtskonformität, ob die Vorschrift haltbar wäre. Ich habe nur eine Anregung: Herr Mayer, Sie hatten es in Ihrer Eingangsfrage gesagt, dass es sich praktisch auf

Situationen bezieht, wo ausschließlich in nicht digitaler Form die Daten erhoben wurden, aber im Text heißt es „ausschließlich oder überwiegend“. Von daher, um es noch konkreter zu fassen, würde ich „oder überwiegend“ streichen, weil dann haben wir wirklich ganz enge Sachverhalte, die hier einer Ausnahmesituation unterworfen werden können, die ggf. – wie gesagt, ich kann es nicht abschließend beurteilen – vereinbar wären mit Artikel 13 der Datenschutzgrundverordnung.

Ich glaube, das war es. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Ehrig. Nun noch Herr Prof. Dr. Aden.

SV Prof. Dr. Hartmut Aden (Hochschule für Wirtschaft und Recht Berlin): Vielen Dank. Ich möchte anknüpfend an die Fragen von Herrn Dr. von Notz gerne noch auf Artikel 2 bis 4 des Gesetzentwurfs zu sprechen kommen, die hier bisher nur am Rand behandelt wurden, und zwar unter zwei Gesichtspunkten.

Zunächst einmal an die Betroffenenrechte anknüpfend. Wir müssen sehen, dass wir im Sicherheitsbereich einen anderen Ausgangspunkt bei den Betroffenenrechten als im Verbraucherschutz haben. Im Verbraucherschutz haben wir zumindest noch die Möglichkeit, dass Verbraucherinnen und Verbraucher etwa ungewünschte Werbung bekommen und deswegen auf diese Problematik überhaupt aufmerksam werden. Diese Ausgangsvoraussetzung haben wir im Sicherheitsbereich leider nicht, weil in der Regel die Betroffenen gerade nichts davon wissen werden, dass über sie Daten vorhanden sind. Deswegen brauchen wir gerade da die Kompensations- und Kontrollinstrumentarien, die Frau Voßhoff hier auch noch einmal ganz berechtigt angemahnt hat.

In dem Zusammenhang stellt sich die Frage, wenn wir uns die Artikel 2 bis 4 des vorliegenden Gesetzentwurfs anschauen, was für eine Art von Accountability hier eigentlich gewollt ist. Wir haben eine starke Tendenz gerade bei den Nachrichtendiensten, dass es eine Zersplitterung gibt mit neuen Gremien, die jeweils für einen bestimmten Ausschnitt von Kontrolle zuständig sind – das halte ich für sehr problematisch. Da muss man in einem nächsten Schritt meines Erachtens zu einem ganz anderen Modell kommen, das sehr viel stärker auf die parlamentarische



Kontrolle fokussiert ist, welche dann in einem zweiten Schritt ermöglicht, dass sich die verschiedenen Aufsichtsinstitutionen untereinander abstimmen und koordinieren, auch ihre Erkenntnisse austauschen können und das Ganze dann an das Parlament zurückspiegeln. Das sind Argumente, die dazu führen, dass man in einem Gesetz wie diesem keine Departementalisierung fördern sollte, indem man für die Bundesbeauftragte hier die Kontrollrechte einschränkt. Da besteht nach meiner Einschätzung ganz konkreter Handlungsbedarf. Das gilt auch, gerade für die Artikel 2 bis 4 bezüglich der Dienste, wo wir auch noch einige interessante Fragen im Raum haben, nämlich bis zu welchem Punkt dort das EU-Recht überhaupt gilt.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Aden. Dann sind wir am Ende der Zeit angekommen. Ich danke den Damen und Herren Sachverständigen für ihre Statements und die Beantwortung der Fragen und gebe jetzt noch einmal dem Kollegen Dr. von Notz das Wort.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Da der Gesetzentwurf am Donnerstag wohl im Plenum sein wird, bräuchten wir morgen das Protokoll, damit wir das irgendwie berücksichtigen können. Ich weiß, es tut mir leid, das ist eine Zumutung, aber es ist für alle eine Zumutung.

Vors. **Ansgar Heveling** (CDU/CSU): We do our very best. Ganz herzlichen Dank. Ich schließe die Sitzung.

Schluss der Sitzung: 12:39 Uhr

Ansgar Heveling, MdB

Vorsitzender



STEPHAN MAYER
MITGLIED DES DEUTSCHEN BUNDESTAGES
INNENPOLITISCHER SPRECHER



CDU/CSU

Fraktion im
Deutschen Bundestag

BURKHARD LISCHKA
MITGLIED DES DEUTSCHEN BUNDESTAGES
INNENPOLITISCHER SPRECHER



SPD
BUNDESTAGS
FRAKTION

An den Vorsitzenden des Innenausschusses
Herrn Ansgar Heveling MdB

Per E-Mail: INNENAUSSCHUSS@BUNDESTAG.DE

Berlin, den 27. März 2017

Sehr geehrter Herr Vorsitzender,

zu dem Entwurf des Datenschutz-Anpassungs- und Umsetzungsgesetzes (Drucksache 18/11325)
stellen wir für die Fraktionen der CDU/CSU und SPD den beigefügten Änderungsantrag.

Mit freundlichen Grüßen

Stephan Mayer MdB

Burkhard Lischka MdB

POSTANSCHRIFT PLATZ DER REPUBLIK 1 11011 BERLIN WWW.CDU/CSU.DE
BÜROANSCHRIFT WILHELMSTRASSE 60 10117 BERLIN
TELEFON (030) 227-74932 TELEFAX (030) 227-76781 E-MAIL STEPHAN.MAYER@BUNDESTAG.DE

POSTANSCHRIFT PLATZ DER REPUBLIK 1 11011 BERLIN WWW.SPDFRAKTION.DE
BÜROANSCHRIFT JAKOB-KAISER-HAUS 10117 BERLIN
TELEFON (030) 227-71908 TELEFAX (030) 227-76908 E-MAIL BURKHARD.LISCHKA@BUNDESTAG.DE

Innenausschuss	
Eingang mit	Anl. am 27.3.2017
1. Vors. m.d.B. um <u>Kenntnisnahme/Rücksprache</u>	
2. Mehrfertigungen mit/ohne Anschreiben an Abg. BE, Obl. Sekr.	
an <u>Adm</u>	
3. Wv	
4. z.d.A. (alphab.-Gesetz- BMI)	

Änderungsantrag

der Fraktionen der CDU/CSU und der SPD

zu dem Gesetzentwurf der Bundesregierung

– Drucksache 18/11325 –

Entwurf eines Gesetzes zur Anpassung des Datenschutzes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzanpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU)

Der Bundestag wolle beschließen,
den Gesetzentwurf auf Drucksache 18/11325 mit folgenden Maßnahmen, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:
 - a) § 23 Absatz 1 wird wie folgt geändert:
 - aa) Nummer 3 wird gestrichen.
 - bb) Die bisherigen Nummern 4 bis 7 werden die Nummern 3 bis 6.
 - b) In § 24 Absatz 1 Nummer 2 ist das Wort „rechtlicher“ durch das Wort „zivilrechtlicher“ zu ersetzen.
 - c) § 31 Absatz 2 wird wie folgt geändert:
 - aa) Nummer 4 Buchstabe c wird wie folgt gefasst:

„c) der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, darüber unterrichtet wurde, dass eine Berücksichtigung durch eine Auskunft möglich ist und“.
 - bb) Nummer 5 wird wie folgt gefasst:

„5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor darüber unterrichtet wurde, dass eine Berücksichtigung durch eine Auskunft möglich ist.“
 - d) § 32 Absatz 1 Nummer 1 wird wie folgt gefasst:

„1. eine Weiterverarbeitung betrifft, deren Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person ausschließlich oder überwiegend nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf

den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,“.

- e) § 33 Absatz 1 Nummer 2 Buchstabe a wird wie folgt gefasst:
 - „a) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Datenverarbeitung der Schadensverhütung dient, sofern nicht das berechnigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder“.
- f) § 34 Absatz 1 Nummer 1 wird wie folgt gefasst:
 - „1. die betroffene Person nach § 33 Absatz 1 Nummer 1, Nummer 2 Buchstabe b oder Absatz 3 nicht zu informieren ist, oder“.
- g) In § 35 Absatz 1 Satz 1 werden nach den Wörtern „Ist eine Löschung“ die Wörter „im Falle nicht automatisierter Datenverarbeitung“ eingefügt.
- h) Dem § 41 Absatz 1 wird folgender Satz angefügt:
 - „§ 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn die festgesetzte Geldbuße die Summe von hunderttausend Euro übersteigt.“

Begründung

Zu Nummer 1 (Artikel 1 – Bundesdatenschutzgesetz)

Zu Buchstabe a (§ 23 Absatz 1 BDSG)

Zu Doppelbuchstabe aa (§ 23 Absatz 1 Nummer 3 BDSG)

Die bislang für öffentliche Stellen vorgesehene Möglichkeit der Verarbeitung allgemein zugänglicher Daten oder solcher, die der Verantwortliche veröffentlichen dürfte, zu anderen Zwecken, wird gestrichen. Allgemein zugängliche Daten können in der Regel auch neu erhoben werden, einer Weiterverarbeitungsbefugnis bedarf es insofern nicht.

Zu Doppelbuchstabe bb (§ 23 Absatz 1 Nummer 4 bis 7 BDSG)

Es handelt sich um eine redaktionelle Folgeänderung zu Doppelbuchstabe aa.

Zu Buchstabe b (§ 24 Absatz 1 Nummer 2 BDSG)

Die Änderung greift einen Vorschlag des Bundesrates auf. Die Möglichkeit der Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen wird auf zivilrechtliche Ansprüche begrenzt. Der neue Wortlaut übernimmt insoweit den Wortlaut des Artikels 23 Absatz 1 Buchstabe j der Verordnung (EU) 2016/679.

Zu Buchstabe c (§ 31 Absatz 2 Nummer 4 Buchstabe c und Nummer 5 BDSG)

Die Änderungen dienen der Klarstellung, dass die Unterrichtungspflichten gegenüber dem Schuldner nicht zwingend durch den Gläubiger selbst zu erfüllen sind, sondern auch von Dritten vorgenommen werden können, die die Forderung im Namen des Gläubigers geltend machen.

Zu Buchstabe d (§ 32 Absatz 1 Nummer 1 BDSG)

Die Neufassung enthält eine Ausnahme von der Informationspflicht nach Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 für mit dem ursprünglichen Erhebungszweck vereinbare Weiterverarbeitungen personenbezogener Daten. Voraussetzung ist ferner, dass die Kommunikation mit der betroffenen Person ausschließlich oder überwiegend nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls als gering anzusehen ist.

Durch die Einschränkung der Informationspflicht sollen insbesondere kleine und mittlere Unternehmen der analogen Wirtschaft von der Informationspflicht ausgenommen werden, deren Kommunikationswege ausschließlich oder überwiegend in nicht digitaler Form erfolgen. Auf die Unverhältnismäßigkeit des mit der Erfüllung der Informationspflicht verbundenen Aufwands kommt es nicht mehr an. Hierdurch wird ein Vorschlag des Bundesrates aufgegriffen.

Für die Ermittlung, ob die beabsichtigte Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Erhebungszweck vereinbar ist, sind die Kriterien des Artikels 6 Absatz 4 der Verordnung (EU) 2016/679 heranzuziehen. Hierbei sind gemäß Erwägungsgrund 50 die vernünftigen Erwartungen der betroffenen Personen einzubeziehen. Dieser Rechtsgedanke wird in § 32 Absatz 1 Nummer 1 aufgegriffen, so dass auch bei kompatiblen Verarbeitungszwecken im Einzelfall zu prüfen ist, ob das Interesse der betroffenen Person an der Informationserteilung, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist.

Zu Buchstabe e (§ 33 Absatz 1 Nummer 2 Buchstabe a BDSG)

Mit der Neufassung wird die Einschränkung der Informationspflicht gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 für nicht-öffentliche Stellen konkretisiert. Eine Informationspflicht besteht nicht, wenn die Information der betroffenen Person die Durchsetzung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Datenverarbeitung der Schadensverhütung (z.B. Betrugspräventionsdateien der Wirtschaft) dient. Die Einschränkung greift in beiden Fallgruppen jedoch nicht, sofern das berechnigte Interesse der betroffenen Person an der Informationserteilung überwiegt.

Zu Buchstabe f (§ 34 Absatz 1 Nummer 1 BDSG)

Die Neufassung nimmt § 33 Absatz 1 Nummer 2 Buchstabe a BDSG von der Beschränkung des Auskunftsrechts aus. Auch wenn die betroffene Person nach § 33 Absatz 1 Nummer 2 Buchstabe a BDSG nicht durch den Verantwortlichen zu informieren ist, wenn die Information der betroffenen Person die Durchsetzung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Datenverarbeitung der Schadensverhütung (z.B. Betrugspräventionsdateien der Wirtschaft) dient, ist der betroffenen Person dennoch auf deren Verlangen Auskunft zu erteilen. Dies trägt der besonderen Bedeutung des Auskunftsrechts für die Transparenz der von der Datenverarbeitung betroffenen Personen Rechnung.

Zu Buchstabe g (§ 35 Absatz 1 Satz 1 BDSG)

Der Anwendungsbereich des § 35 Absatz 1 BDSG wird auf Fälle nicht automatisierter Datenverarbeitung beschränkt. Die Einschränkung dient der Konkretisierung des Tatbestandsmerkmals der „besonderen Art der Speicherung“. Eine Löschung personenbezogener Daten kommt nicht in Betracht, wenn die Löschung im Falle nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Erfasst werden von der Vorschrift vor allem Archivierungen in Papierform oder die Nutzung früher gebräuchlicher analoger Speichermedien, etwa Mikrofiche, bei denen es nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, einzelne Informationen selektiv zu entfernen.

Zu Buchstabe h (§ 41 Absatz 1 Satz 3 BDSG)

Die Verordnung (EU) 2016/679 sieht bei Verstößen Geldbußen von bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes vor. Angesichts dessen ist die Zuständigkeit des Landgerichts sachgerecht, wenn die Geldbuße die Summe von hunderttausend Euro übersteigt. Die streitwertabhängige Zuständigkeit des Landesgerichts folgt aus dem Rechtsgedanken des § 23 Nummer 1 des Gerichtsverfassungsgesetzes.



Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
Euroean Academy for Freedom of Information and Data Protection

EAD

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)824 A

Berlin, den 22. Februar 2017

Stellungnahme zum Entwurf der Bundesregierung v. 1. Februar 2017 für ein Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) - Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

Die Anpassung des deutschen Rechts sollte der von der Datenschutzgrundverordnung (Datenschutz-GVO) und der Richtlinie für Polizei und Justiz verfolgten Maxime folgen, das Grundrecht zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gem. Art. 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Art. 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zu verwirklichen (vgl. DS-GVO, EG 1) zu verwirklichen und dabei ein einheitliches Datenschutzniveau in der EU zu gewährleisten. Der Entwurf der Bundesregierung verfehlt diese Ziele. Zu befürchten ist, dass der deutsche Datenschutz teils unter dem in der übrigen EU vorgesehenen Niveau bleibt und auch darüber hinaus Sonderwege beschreitet, die weder im Sinne der Bürgerinnen und Bürger noch der Unternehmen sein können.

Zu befürchten ist auch, dass andere Mitgliedstaaten sich an der deutschen Gesetzgebung orientieren und ebenfalls eigene Wege gehen könnten. Im Ergebnis wäre schlimmstenfalls ein weiterhin zersplittertes Datenschutzrecht in der EU.

Angesichts des Umfangs des Entwurfs beschränkt sich die nachfolgende Stellungnahme auf diejenigen Punkte, in denen Änderungen im Hinblick auf europa- und verfassungsrechtliche Anforderungen in besonderem Maße geboten erscheinen:

- Rechte der betroffenen Person (§§ 4 Abs. 2, 32-37)
- Verarbeitung personenbezogener Daten zu anderen Zwecken (§ 23-25),
- Aufsichtsbehördliche Befugnisse und Betroffenenrechte im Fall von Geheimhaltungspflichten (§ 29).



Europäische Akademie für Informationsfreiheit und Datenschutz e.V.
Vorstand: Heide Schaar * Dr. Alexander Urb * Kirsten Neumann * Prof. Dr. Alfred Bielebach * Dr. Dennis-Kunjakpikier
Geschäftsstelle: Bismarckallee 46/48 * D-14193 Berlin * Telefon: +49 151-62914576
E-Mail: gf@ead-berlin.de * www.ead-berlin.de
Vereinsregister-Nr. VR 21680 B Amtsgericht Charlottenburg * Steuer-Nr. 27/664/52926
IBAN DE84 1005 0000 0190 3076 92 * BIC BELADE33XXX * Berliner Sparkasse

1. Rechte der betroffenen Person (§§ 4 Abs. 2, 32-37)

- 1.1. Die Rechte der betroffenen Person auf Information, Auskunft, Berichtigung und Löschung der sie betreffenden Daten gehören zu den zentralen Voraussetzungen für einen **effektiven Schutz des Grundrechts auf informationelle Selbstbestimmung** i.S.v. Art. 2 Abs 1 i.V.m. Art. 1 Abs.1 GG. Die Rechte auf Auskunft und Berichtigung werden ebenfalls durch das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 der EU-Grundrechtecharta gewährleistet. Einschränkungen sind nur im überwiegenden Allgemeininteresse zulässig. Das Auskunftsrecht trägt auch dem Grundsatz der Gewährung eines effektiven Rechtsschutzes Rechnung. Wäre der Bürger gehindert, Kenntnis davon zu erlangen, wer wo über welche seiner personenbezogenen Daten in welcher Weise und zu welchen Zwecken verfügt, so wäre sein Rechtsschutz verfassungsrechtlich unzureichend.

Der Gesetzentwurf **schränkt die Betroffenenrechte über die ohnehin in der DS-GVO vorgesehenen Ausnahmen weiter ein**, ohne dass hierfür überzeugende Gründe erkennbar sind. Auf diese Einschränkungen sollte im Hinblick auf den hohen Stellenwert der Betroffenenrechte für die Grundrechtsgewährleistung und wegen der zumindest teilweisen Europarechtswidrigkeit der Einschränkungen verzichtet werden.

- 1.2. Die gebotene **Information auf eine Videoüberwachung** soll nach § 4 Abs. 2 des Entwurfs „zum frühestmöglichen Zeitpunkt“ gegeben werden. Das lässt dem Verantwortlichen einen zu großen zeitlichen Spielraum, wann er über eine Videoüberwachung informieren will. Es muss – wie nach geltendem Recht – dabei bleiben, dass eine Videoüberwachung nur stattfinden darf, wenn spätestens mit der Aktivschaltung von Kameras auch über sie und die dafür verantwortliche Stelle informiert wird, so dass betroffene Personen entscheiden können, ob sie einen optisch-elektronisch überwachten Bereich betreten wollen. Eine Einschränkung von Art. 13 der DS-GVO ist auch in diesem Punkt nicht gerechtfertigt.
- 1.3. Auch die in § 32 des Entwurfs vorgesehene **Einschränkung der Informationspflicht bei einer Datenerhebung bei der betroffenen Person** genügt den verfassungsrechtlichen Vorgaben nur unzureichend. Zugleich entspricht § 32 nicht den Anforderungen der DS-GVO, denn er vermengt in unzulässiger Weise Interessen der verantwortlichen Stelle (unverhältnismäßiger Aufwand) mit dem Schutz der betroffenen Person und der Rechte Dritter. Art. 13 DS-GVO sieht bewusst keine Ausnahme von der Informationspflicht bei unverhältnismäßigem Aufwand vor, auch Art. 23 DS-GVO tut dies nicht.
- 1.4. § 33 Abs. 1 Nr. 1 lit. a schränkt die Informationspflicht öffentlicher Stellen nach Art. 14 DS-GVO schon dann ein, wenn die Information die **ordnungsgemäße Erfüllung der in der Zuständigkeit der jeweiligen Stelle liegenden Aufgabe gefährden** würde. Die Verordnung sieht eine solche Beschränkungsmöglichkeit nicht vor, anders bei Gefährdung der öffentlichen Sicherheit (dazu § 33 Abs. 1 Nr. 1 lit. b, der allerdings entgegen dem Unionsrecht auch eine Gefährdung der öffentlichen Ordnung nennt). Aus diesem Grund geht auch die Beschränkung des Auskunftsrechts in § 34 Abs. 1 Nr. 1 des Entwurfs, soweit er auf § 33 Abs. 1 verweist, zu weit.

- 1.5. Ein möglicher **unverhältnismäßiger Aufwand für die Auskunftserteilung**, der diese nach § 34 Abs. 1 Nr. 2 entbehrlich machen soll, ist nach der Grundverordnung (im Gegensatz zu § 19 Abs. 1 Satz 3 BDSG-alt) kein zulässiger Grund für die Auskunftsverweigerung. Das gilt auch für das Auskunftsrecht nach Art. 14 der Richtlinie 680/16 (dennoch will § 57 Abs. 2 des Entwurfs in solchen Fällen die Auskunftspflicht entfallen lassen).
- 1.6. § 35 Abs. 1 des Entwurfs schränkt das Recht der betroffenen Person auf **Löschung der sie betreffenden Daten** in einer mit dem Unionsrecht unvereinbaren Weise ein. Eine Löschung soll stets dann nicht verlangt werden können, wenn diese „wegen der besonderen Art der Speicherung“ nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Darauf könnten sich die Hersteller und Anbieter von Hard- oder Software und deren Anwender berufen, sofern die Produkte eine Löschung nicht zulassen. Ziel der Grundverordnung ist es aber gerade, durch Technikgestaltung die Verarbeitung von personenbezogenen Daten auch in zeitlicher Hinsicht auf das erforderliche Maß zu beschränken. Art. 23 Abs. 1 lit. i DS-GVO ist deshalb nicht so zu verstehen, dass die Verwender von nicht datenschutzgerechter Hard- und Software (die eine Löschung nicht ermöglicht) von Betroffenenrechten freigestellt werden können.
- 1.7. § 37 Abs. 1 Nr. 2 erlaubt - zusätzlich zu den in Art. 22 DS-GVO vorgesehenen Fällen - **automatisierte Einzelentscheidungen** unter Verwendung von sensiblen Gesundheitsdaten bei der Abwicklung von Versicherungsverträgen auch in Fällen, in denen einem Antrag eines Versicherten nicht stattgegeben wird. Die zur Kompensation vorgesehenen Maßnahmen greifen lediglich rückwirkend und setzen jeweils voraus, dass der Betroffene die automatisiert getroffene Entscheidung anfechtet. Eine solche Privilegierung der Versicherungswirtschaft - gem. § 37 Abs. 2 auch im Bereich der besonders schützenswerten Gesundheitsdaten (Art. 4 Nr. 15 und Art. 9 DS-GVO) - ist sinnwidrig. In solchen Fällen das Widerspruchsrecht des Betroffenen nach Art. 21 generell auszuschließen, ist mit dem Unionsrecht nicht zu vereinbaren.

2. Verarbeitung zu anderen Zwecken (§§ 23-25)

- 2.1. Nach Art. 5 Abs. 1 Lit. b DS-GVO gilt bei der Verarbeitung personenbezogener Daten der **Grundsatz der Zweckbindung**. Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Allerdings enthält die Verordnung eine Reihe von Bestimmungen, die eine Bearbeitung zu anderen Zwecken ausnahmsweise rechtfertigen. Die im Regierungsentwurf vorgesehenen Änderungen zur Verarbeitung für andere Zwecke sollen zusätzlich zu dem ohnehin in der Verordnung vorgesehenen Zweckänderungsklauseln gelten. Im Hinblick auf die besondere Problematik von Zweckänderungen sollten entsprechende Vorschriften im nationalen Recht auf das unabdingbare Maß begrenzt werden. Demgegenüber enthält der Entwurf sehr weitgehende zusätzliche Zweckänderungsregelungen, die teilweise sogar über das jetzige BDSG hinausgehen.
- 2.2. Den vorgesehenen Bestimmungen **mangelt es generell an Transparenz**. Aus dem verfassungsrechtlich verankerten Recht auf informationelle Selbstbestimmung ergeben sich die Anforderungen an die Kenntnis über und die Mitwirkung der Betroffenen Personen bei der Zweckänderung. Dieser grundsätzliche Mitwirkungserfordernis wird in den §§ 23-25 nicht Rechnung getragen. Generell fehlen auch Regelungen über besondere Vorkehrungen zum Schutz der artiger Daten nach erfolgter Zweckänderung.

- 2.3. § 23 enthält eine **generalklauselartige Ermächtigungsnorm für Zweckänderungen** bei der Verarbeitung durch öffentliche Stellen. Eine Konkretisierung ist sowohl nach europäischem Recht als auch nach deutschem Verfassungsrecht geboten. Dies gilt insb. für die unpräzisen Formulierungen in § 23 Abs. 1 („Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen *im Rahmen ihrer Aufgabenerfüllung* ist zulässig...“) im Vergleich zum geltenden § 14 Abs. 1 S. 1 BDSG („Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es *zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich* ist ...“). Auch die in § 23 Abs. 1 Nrn. 2, 3 und 4 vorgesehenen Aufgabenbeschreibungen erfüllen nicht die nach europäischem und deutschem Recht erforderlichen Anforderungen an die Konkretheit und Klarheit einer grundrechtsbeschränkenden Befugnisnorm.
- 2.4. In den meisten der in § 23 Abs. 1 vorgesehenen Zweckänderungsbefugnissen fehlt eine **Abwägung mit entgegenstehenden berechtigten Interessen der betroffenen Person**. Insofern sollte die in Nr. 7 vorgesehene Abwägungsklausel („... soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen“) generell für die in Abs. 1 vorgesehenen Zweckänderungen gelten.
- 2.5. Die in § 24 Abs. 1 Nr. 1 genannte Aufgabe („Abwehr von **Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten**“) obliegt grundsätzlich den dafür zuständigen öffentlichen Stellen. Deshalb ist die vorgesehene generelle Befugnis zur zweckändernden Verarbeitung personenbezogener Daten zur Erfüllung dieser Aufgabe durch nicht-öffentliche Stellen abzulehnen.
- 2.6. Für § 25 (Datenübermittlung durch öffentliche Stellen) gelten die Anmerkungen zu § 23 entsprechend.

3. Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten (§ 29)

- 3.1. § 29 Abs. 1 Sätze 1, 2 und 3 enthalten gleichlautend eine **Ausnahme von der Informationspflicht** des Verantwortlichen gegenüber der betroffenen Person nach Art. 14 DS-GVO, **von der Auskunftspflicht** nach Art. 15 DS-GVO und **von der Benachrichtigungspflicht** bei Datenpannen nach Art. 34 DS-GVO, soweit dadurch „Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen“.
- Diese Einschränkungen widersprechen in ihrer Allgemeinheit dem Unionsrecht, das (insbesondere in der DS-GVO) keine Informationen kennt, die „ihrem Wesen nach“ geheim gehalten werden müssen. Die Worte „ihrem Wesen nach, insbesondere“ sind deshalb zu streichen.
- 3.2. § 29 Abs. 1 Sätze 1 und 2 sehen **Ausnahmen von der Informations- und Auskunftspflicht** „insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten“ vor. Damit will die Bundesregierung von der Befugnis des Art. 23 Abs. 1 lit. i DS-GVO Gebrauch machen, versäumt es aber, die notwendigen kompensatorischen Ausgleichsregelungen, die Art. 23 Abs. 2 DS-GVO vorschreibt, im

DSAnpUG selbst zu treffen. Insbesondere wird auf jede Abwägung mit den schutzwürdigen Interessen der betroffenen Person verzichtet. Der Verweis auf „Rechtsvorschriften“ in § 29 Abs. 1 Satz 2 reicht dafür nicht aus. Auch diese Ausnahmetatbestände widersprechen deshalb dem Unionsrecht und sind entweder zu streichen oder durch eine Abwägungsklausel ähnlich dem § 29 Abs. 1 Satz 4 zu ergänzen.

- 3.3. § 29 Abs. 2 beruht entweder auf einem unzutreffenden Verständnis des Art. 13 Abs. 3 DS-GVO oder ist jedenfalls ungeeignet, um das angestrebte Ziel einer Ausnahme von der **Informationspflicht im Verhältnis zu Berufsgeheimnisträgern** zu erreichen. Art. 13 Abs. 3 DS-GVO betrifft nur die Informationspflicht bei Zweckänderungen. Nicht in allen Fällen, in denen ein Verantwortlicher im Anwendungsbereich der Grundverordnung einem Berufsgeheimnisträger Daten über Dritte übermittelt, liegt aber eine Zweckänderung vor. Die Ausnahme von der Informationspflicht muss sich daher auch auf Art. 13 Abs. 1 und 2 DS-GVO beziehen.
- 3.4. § 29 Abs. 3 sieht eine völlig inakzeptable **Beschränkung der Befugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern** und ihren Auftragnehmern vor. Art. 90 Abs. 1 DS-GVO gestattet den Mitgliedstaaten nur, die Rechte der Aufsichtsbehörden auf Zugang zu den Daten und Geschäftsräumen insoweit zu beschränken, als dies notwendig und verhältnismäßig ist, um die Geheimhaltungspflicht des Berufsgeheimnisträgers mit dem Datenschutz in Einklang zu bringen. Durch die vorgesehene Bestimmung würden die Aufsichtsbehörden an jeglicher **effektiver Prüfung der Verarbeitung personenbezogener Daten** bei den durch § 203 Abs. 1 StGB genannten Bereichen gehindert. So wäre es ihnen nicht mehr möglich, Prüfungen der Datenverarbeitung bei Krankenhäusern, privaten Krankenversicherungen, Apotheken, Anwaltskanzleien, Steuerberatern usw. durchzuführen - eine unabhängige datenschutzrechtliche Kontrolle der gerade in diesen Bereichen in großem Umfang anfallenden hochsensiblen Daten müsste unterbleiben.
- Damit würde die bisherige Rechtslage auf den Kopf gestellt, wonach sich die Kontrollbefugnisse der bzw. des Bundesbeauftragten für den Datenschutz und der Aufsichtsbehörden auch auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (§ 24 Abs. 2 S. 1 Nr. 2 i.V.m. § 24 Abs. 6 BDSG).
- 3.5. Das Bundesverfassungsgericht hat in seinem in der Gesetzesbegründung zitierten Beschluss vom 12. April 2005 (2 BvR 1027/02) die Beschlagnahme des vollständigen Aktenbestandes einer Anwaltskanzlei gerügt und betont, dass ein Mandatsverhältnis nicht wegen der **Gefahr eines unbeschränkten Datenzugriffs** von Anfang an mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet werden darf (Rn. 94). Diese Gefahr besteht aber angesichts der Beschränkung des Art. 58 Abs. 1 lit. e DS-GVO nicht, wo es heißt, dass Aufsichtsbehörden nur den Zugang zu allen personenbezogenen Daten und Informationen, **die zur Erfüllung ihrer Aufgaben notwendig sind**, verlangen können. § 29 Abs. 3 ist deshalb zu streichen.

KEINE ABSENKUNG DES DATEN- SCHUTZNIVEAUS BEI DER ANPAS- SUNG DES RECHTSRAHMENS AN DIE DSGVO

Angepasste Stellungnahme des Verbraucherzentrale
Bundesverbands e.V. zum Regierungsentwurf eines
Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU –
DSAnpUG-EU

13. Februar 2017

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Markgrafenstraße 66
10969 Berlin

digitales@vzbv.de

INHALT

I. EINLEITUNG	3
II. DIE KERNFORDERUNGEN IM ÜBERBLICK	4
III. DIE EINZELNEN REGELUNGEN	5
1. § 24 - Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen	5
2. § 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften	5
3. Einschränkung der Betroffenenrechte.....	7
3.1 § 27 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und statistischen Zwecken.....	7
3.2 Kapitel 2 – Rechte der betroffenen Person	7
3.3 § 32 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	7
3.4 § 33 – Informationspflicht, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden	8
3.5 § 34 – Auskunftsrechte der betroffenen Person	8
3.6 § 35 – Recht auf Löschung	9
3.7 § 37 – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	9

I. EINLEITUNG

Am 14. April 2016 wurde die europäische Datenschutz-Grundverordnung¹ (DSGVO) durch das Europäische Parlament beschlossen und trat am 24. Mai 2016 in Kraft. Ihre unmittelbare Anwendung in den Mitgliedstaaten beginnt ab dem 25. Mai 2018. In der Zwischenzeit muss der nationale Rechtsrahmen an die Regelungen der Datenschutz-Grundverordnung angepasst werden. Zu diesem Zweck hat die Bundesregierung am 01. Februar 2017 den 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)“ – im Folgenden BDSG-neu – veröffentlicht.

Der Verbraucherzentrale Bundesverband e. V. (vzbv) möchte die Gelegenheit ergreifen, zum vorliegenden Regierungsentwurf Stellung zu beziehen. Aufgrund der Eile des Gesetzgebungsprozesses und des Umfangs des Entwurfs können dabei an dieser Stelle jedoch nur einzelne und besonders drängende Aspekte des Gesetzesentwurfs thematisiert werden. Dies sind insbesondere die Regelungen zur Zweckänderung, die Regelung zu automatisierten Einzelfallentscheidungen sowie die Einschränkungen der Betroffenenrechte. Bedauerlicherweise muss aufgrund des knappen Zeitrahmens an dieser Stelle Kritik an vielen weiteren Regelungen, wie beispielsweise zur Videoüberwachung, zur Vertretung im Europäischen Datenschutzausschuss oder zu den Kontrollbefugnissen der Aufsichtsbehörden unterbleiben. Der vzbv behält sich daher vor, diese kritischen Punkte im weiteren Verlauf des Gesetzgebungsverfahrens zu adressieren.

Auch wenn der vorliegende Regierungsentwurf im Vergleich zu vorherigen Referentenentwürfen deutlichen Verbesserungen unterzogen wurde, bedauert der vzbv, dass viele der vorgeschlagenen Bestimmungen hinter das Schutzniveau der DSGVO zurückfallen. Insbesondere die weitreichenden Vorschläge für Einschränkungen der Betroffenenrechte sind inakzeptabel und nach Einschätzung des vzbv europarechtswidrig. Sollten die vorgeschlagenen Regelungen in ihrer derzeitigen Form beschlossen werden, würde dies zu einer massiven Verschlechterung der Verbraucherrechte führen. Deutsche Verbraucherinnen und Verbraucher² wären künftig datenschutzrechtlich deutlich schlechter gestellt, als die Verbraucher in anderen EU-Mitgliedsstaaten. Und auch für in Deutschland ansässige Unternehmen dürfte die absehbare jahrelange Rechtsunsicherheit höchst unbefriedigend sein.

Daher plädiert der vzbv dafür, die vorgeschlagenen Regelungen zu überarbeiten und die Rechte der Verbraucher und Bürger konsequent ins Zentrum der Anpassung des deutschen Rechtsrahmens an die DSGVO zu stellen.

¹ 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. Alle Artikel und Erwägungsgründe ohne Gesetzesangaben beziehen sich auf die DSGVO.

² Die gewählte männliche Form bezieht sich stets auf weibliche und männliche Personen. Wir bitten um Verständnis für den weiteren Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

II. DIE KERNFORDERUNGEN IM ÜBERBLICK

1. REGELUNGEN ZUR ZWECKÄNDERUNG

Bei der Zweckbindung handelt es sich um eines der Grundprinzipien des Datenschutzes, das in der DSGVO sowie in der Europäischen Grundrechtecharta verankert ist.

Der vzbv begrüßt ausdrücklich, dass die Bundesregierung davon abgesehen hat, eine Änderung des Verarbeitungszwecks durch eine nicht-öffentliche Stelle im Nachhinein auf Basis einer Interessenabwägung zu ermöglichen.

2. SCHUTZ DES WIRTSCHAFTSVERKEHRS BEI SCORING UND BONITÄTSAUSKUNFTEN

Bei den bisherigen Vorschriften zur Datenübermittlung an Auskunftsteile und zum Scoring handelt es sich nicht um Datenschutzbestimmungen, sondern um Regelungen des wirtschaftlichen Verbraucherschutzes.

Der vzbv begrüßt daher, dass die entsprechenden Vorschriften als zivilrechtliche Regelungen fortgeführt werden sollen. Es muss jedoch klargestellt werden, dass die Voraussetzungen des § 31 Abs. 1 BDSG-neu für die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten eines Betroffenen kumulativ erfüllt sein müssen. Außerdem müssen die Regelungen des § 31 BDSG-neu in die Bußgeldvorschriften des § 43 BDSG-neu aufgenommen werden.

3. EINSCHRÄNKUNG DER BETROFFENENRECHTE

Die vorgeschlagenen Einschränkungen der Betroffenenrechte gehen zu weit und sind aus Sicht des vzbv europarechtswidrig. Die DSGVO sieht keine Einschränkungen der Informations-, Auskunfts- oder Löschrechte vor, wenn diese einen unverhältnismäßigen Aufwand für die Verantwortlichen darstellen könnten oder weil ein Geschäftszweck gefährdet werden könnte. Inhaltlich ist unverständlich, warum Verbraucher in Deutschland künftig schlechter gestellt werden sollten, als Verbraucher in anderen EU-Mitgliedsstaaten.

Entsprechende Beschränkungen der Betroffenenrechte sind daher zu streichen.

4. AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL EINSCHLIEßLICH PROFILING

§ 37 BDSG-neu weitet die Regelungsspielräume der DSGVO unzulässig aus und eröffnet den Verantwortlichen gleichzeitig Formen der Datenverarbeitung, die über die Möglichkeiten des BDSG-alt hinausgehen. Es ist nicht nachvollziehbar, warum auf Kosten der Rechte der Betroffenen eine Sonderregelung zum Schutz künftiger Geschäftsmodelle eines einzelnen Wirtschaftszweigs geschaffen wird.

Daher ist § 37 BDSG-neu zu streichen.

III. DIE EINZELNEN REGELUNGEN

1. § 24 - VERARBEITUNG ZU ANDEREN ZWECKEN DURCH NICHT-ÖFFENTLICHE STELLEN

Art. 6 Abs. 4 eröffnet den Mitgliedsstaaten die Möglichkeit, Regelungen zur Zweckänderung zu erlassen, wenn diese eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 genannten Ziele darstellen. Diese Ziele müssen im öffentlichen Interesse des Mitgliedsstaates liegen oder in Ausübung öffentlicher Gewalt erfolgen. Dabei ist der Begriff des öffentlichen Interesses eng auszulegen. Art. 6 Abs. 4 i.V.m. in Art. 23 enthält keine Befugnis für die Mitgliedsstaaten, umfassende Regelungen zur Zweckänderung im nicht-öffentlichen Bereich zu erlassen.

Vor diesem Hintergrund begrüßt der vzbv, dass die Bundesregierung davon abgesehen hat, eine Änderung des Verarbeitungszwecks durch eine nicht-öffentliche Stelle im Nachhinein auf Basis einer Interessenabwägung zu ermöglichen.

Bei der Zweckbindung handelt es sich um eines der Grundprinzipien des Datenschutzes, das nicht nur in der DSGVO, sondern auch in der Europäischen Grundrechtecharta verankert ist. Darüber hinaus wurde in den Verhandlungen zur DSGVO der Vorschlag abgelehnt, eine Änderung des Verarbeitungszwecks im Nachhinein auf Basis einer Interessenabwägung zu ermöglichen. Eine solche Regelung im nationalen Recht wäre daher inakzeptabel gewesen.

Allerdings bleibt § 24 Abs. 1 Nr. 2 BDSG-neu hinter den Vorgaben des Art. 23 Abs. 1 lit. j) zurück, da Art. 23 Abs. 1 lit. j) lediglich auf die Durchsetzung zivilrechtlicher Ansprüche beschränkt ist und nicht die Geltendmachung, Ausübung oder Verteidigung jeglicher rechtlicher Ansprüche erlaubt.

§ 24 Abs. 1 Nr. 2 BDSG-neu muss daher auf die Durchsetzung zivilrechtlicher Ansprüche beschränkt werden.

2. § 31 SCHUTZ DES WIRTSCHAFTSVERKEHRS BEI SCORING UND BONITÄTSAUSKÜNFTE

Der vzbv begrüßt ausdrücklich, dass mit § 31 BDSG-neu die in § 28a BDSG-alt sowie in § 28b BDSG-alt enthaltenen Vorschriften fortgeführt werden sollen. Die Erhaltung der Vorschriften stärkt die Verbraucherrechte und erhöht die Rechtssicherheit der Unternehmen.

Bei den genannten Regeln handelt es sich um Bestimmungen des wirtschaftlichen Verbraucherschutzes. Denn finden bestrittene beziehungsweise bestreitbare Forderungen unrichtigerweise Eingang in den Datenbestand von Auskunftsteilen, könnte als Folge drohen, dass beispielsweise Zahlungskarten und Versorgungsverträge gesperrt werden oder die Anschlussfinanzierung für das Eigenheim scheitert. § 28a BDSG-alt wurde daher im Jahr 2010 unter anderem eingeführt, um zu verhindern, dass Verbraucher nur

aus Angst vor den genannten Auswirkungen eines negativen Kreditscores gegenüber Forderungsgebern einlenken und auch unberechtigte Forderungen akzeptieren. Somit würde sich Anbietern ein Weg eröffnen, vorschnell und ungeprüft auch fragwürdige Forderungen durchzusetzen, statt auf den Rechtsweg angewiesen zu sein. § 28b BDSG-alt hingegen soll Verbraucher vor Diskriminierung und damit verbundenen wirtschaftlichen Beeinträchtigungen schützen. Beispielsweise kann Scoring, das auf Basis von Adressdaten durchgeführt wird, zu einer strukturellen Ausgrenzung bestimmter Personengruppen führen. Die Bewohner ganzer Straßenzüge könnten durch solche Praktiken Nachteile erleiden.

Daher begrüßt der vzbv, dass mit § 31 BDSG-neu, die bisherigen Regelungen der § 28a BDSG-alt sowie in § 28b BDSG-alt als zivilrechtliche Regelungen fortgeführt werden sollen. Es muss jedoch klar gestellt werden, dass die Voraussetzungen des § 31 Abs. 1 BDSG-neu für die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person kumulativ erfüllt sein müssen.

Damit die Vorschriften jedoch auch tatsächlich eine Wirkung entfalten können, müssen Verstöße außerdem bußgeldbewehrt sein.

Dementsprechend müssen die Regelungen des § 31 BDSG-neu in die Bußgeldvorschriften des § 43 BDSG-neu aufgenommen werden.

Es sollte außerdem dringend in Erwägung gezogen werden, die Regelungen des § 31 BDSG-neu künftig in andere zivilrechtliche Regelungsbereiche und Gesetze außerhalb des Datenschutzes zu überführen. Ungeachtet ihrer bisherigen Verortung im Datenschutzrecht handelt es sich um Regelungen, die ihre Bedeutung auch im Kreditrecht haben. Hierdurch werden Anforderungen, die an die Bewertung der Kreditwürdigkeit von Verbrauchern zu stellen sind, aufgestellt. Als verbraucherschützende kreditbezogene Regelungen müssten sie Eingang in die zivilrechtlichen und aufsichtsrechtlichen Vorschriften zu Kreditverträgen finden. Da die Bonitätsbewertung auch Auswirkungen auf den Bereich von Krediten außerhalb des Kreditwesengesetzes entfalten können, etwa in Bezug auf den Onlinehandel und den Zugang zum Angebot und zum Zahlungsweg, wäre eine generelle zivilrechtliche Vorgabe aus Verbrauchersicht wünschenswert. Wichtig sind Vorgaben zur Sicherung der Datenqualität jedoch mindestens im Kreditbereich. Denn hierzu gibt es auch konkrete mit den Vorgaben der Verbraucherdarlehensrichtlinie II und der Wohnimmobilienkreditrichtlinie zu erreichende Ziele. Nur bestimmte Daten haben eine kausale bonitätsrelevante Aussage und sollten für dieses Scoring verwendet werden dürfen. Hierbei handelt es sich um Qualitätsmaßstäbe, die sicherstellen sollten, dass die Entscheidungen auf einer hinreichend fundierten und nicht lediglich auf korrelativen Annahmen beruht. Die Voraussetzungen hierzu sollten auch die bisherigen Erfahrungen aus der Evaluation der am 01. April 2010 in Kraft getretenen Änderungen einbeziehen.

3. EINSCHRÄNKUNG DER BETROFFENENRECHTE

3.1 § 27 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und statistischen Zwecken

§ 27 Abs. 2 Satz 2 BDSG-neu schränkt die Rechte der Betroffenen in unzulässiger Weise ein. Weder Art. 23 noch Art. 89 Abs. 2 sehen eine Einschränkung des Rechts auf Auskunft vor, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand für den Verantwortlichen darstellen könnte.

| Daher ist § 27 Abs. 2 Satz 2 BDSG-neu zu streichen.

3.2 Kapitel 2 – Rechte der betroffenen Person

Die Überschriften des Kapitels und der §§ 32 bis 36 BDSG-neu sind fehlerhaft, da es sich bei den Bestimmungen nicht um Regelungen über die Rechte der betroffenen Person handelt, sondern diese im Gegenteil die durch die DSGVO eingeräumten Rechte einschränken.

Darüber hinaus wurden die Betroffenenrechte in der DSGVO hinsichtlich Datenverarbeitungen im nicht-öffentlichen Bereich abschließend geregelt. Die DSGVO sieht in diesem Bereich eine Vollharmonisierung vor. Eine Einschränkung der Verbraucherrechte über das BDSG-neu ist in diesem Bereich nur in sehr engen Ausnahmen möglich. Betroffenenrechte dürfen nur eingeschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die die Ziele des Art. 23 Abs. 1 sicherstellen soll. Art. 23 Abs. 1 erlaubt es den Mitgliedsstaaten zwar, Vorschriften zu erlassen, die im öffentlichen Interesse liegen. Allerdings ist der Begriff des öffentlichen Interesses eng auszulegen. Außerdem müssen die Gesetzgebungsmaßnahmen spezifische Vorschriften gemäß Art. 23 Abs. 2 enthalten. Diese Anforderungen erfüllen viele der Bestimmungen des Kapitels 2 BDSG-neu nicht. So wird innerhalb Kapitel 2 BDSG-neu insbesondere Art. 23 Abs. 1 lit. i) fehlerhaft ausgelegt. Von dieser Vorschrift wird nicht der für die Datenverarbeitung Verantwortliche eingeschlossen. Diese Regelung bezieht sich in erster Linie auf natürliche Personen und ihre Persönlichkeitsrechte.

Inhaltlich entbehrt es jeglicher Grundlage, warum Verbraucher in Deutschland künftig schlechter gestellt werden sollten als Verbraucher in anderen EU-Mitgliedsstaaten. Eine aus Sicht des vzbv europarechtswidrige Absenkung des Schutzniveaus für deutsche Verbraucher ist daher nicht akzeptabel.

3.3 § 32 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

§ 32 Abs. 1 Nr. 1 BDSG-neu bleibt hinter dem BDSG-alt zurück, das keine so weitreichenden Einschränkungen der Informationspflichten vorsieht. Eine Einschränkung der Informationspflicht wegen eines unverhältnismäßigen Aufwands ist im BDSG-alt nicht generell, sondern nur in bestimmten Fällen vorgesehen.

Auch sieht Art. 13 – im Gegensatz zu Art. 14 – solche Ausnahmen nicht vor. Daher muss davon ausgegangen werden, dass diese Ausnahmen vom europäischen Gesetzgeber auch im Falle von Zweckänderungen nicht gewollt sind. Die Informationspflichten sind im Gegenteil gerade im Falle von Zweckänderungen für die Betroffenen von besonderer Bedeutung. Darüber hinaus ist es nicht Zweck des Art. 23, den Mitgliedsstaaten die Möglichkeit zu eröffnen, vermeintliche Lücken der DSGVO zu schließen.

Durch eine solche Bestimmung würden insbesondere solche Datenverarbeitungen bevorzugt werden, bei denen besonders viele Daten von besonders vielen Betroffenen in einer Art und Weise verarbeitet werden, dass eine Information der Betroffenen als unverhältnismäßig erachtet werden würde. Damit setzt diese Bestimmung falsche Anreize und steht dem Grundsatz der Datenvermeidung entgegen.

Darüber hinaus ist nicht nachvollziehbar, warum die Rechte und Freiheiten anderer Personen aufgrund eines erhöhten Aufwands des Verantwortlichen beeinträchtigt werden sollten.

■ Daher ist § 32 Abs. 1 Nr. 1 BDSG-neu zu streichen.

Darüber hinaus bleibt § 32 Abs. 1 Nr. 4 BDSG-neu hinter den Vorgaben des Art. 23 Abs. 1 lit. j) zurück, da Art. 23 Abs. 1 lit. j) lediglich auf die Durchsetzung zivilrechtlicher Ansprüche beschränkt ist und nicht die Geltendmachung, Ausübung oder Verteidigung jeglicher rechtlicher Ansprüche erlaubt.

■ § 32 Abs. 1 Nr. 4 BDSG-neu muss auf die Durchsetzung zivilrechtlicher Ansprüche beschränkt werden.

3.4 § 33 – Informationspflicht, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden

§ 33 Abs. 1 Nr. 2 lit. a) BDSG-neu ist nicht vereinbar mit Art 23 Abs. 1, da der Schutz „allgemein anerkannter Geschäftszwecke“ kein in Art 23 Abs. 1 genanntes Ziel darstellt. Vielmehr stellt eine solch weite Ausnahme ein großes Missbrauchspotential dar, dem auch durch die in Abs. 2 genannten Transparenzmaßnahmen nicht ausreichend begegnet wird.

■ Daher ist § 33 Abs. 1 Nr. 2 lit. a) BDSG-neu zu streichen.

3.5 § 34 – Auskunftsrechte der betroffenen Person

§ 34 Abs. 1 BDSG-neu ist nicht vereinbar mit Art 23 Abs. 1. Weder der Schutz „allgemein anerkannter Geschäftszwecke“ (§ 34 Abs. 1 Nr. 1 BDSG-neu) noch ein möglicher unverhältnismäßiger Aufwand (§ 34 Abs. 1 Nr. 2 BDSG-neu) sind gemäß der DSGVO zulässige Gründe für eine Auskunftsverweigerung. Vielmehr muss der Verantwortliche technische und organisatorische Maßnahmen treffen, um die Anforderungen der DSGVO zu erfüllen.

Auskunftsverweigerungen zum Schutz von Geschäftszwecken sowie wegen eines unverhältnismäßigen Aufwands sind nicht mit der DSGVO vereinbar und daher zu streichen.

3.6 § 35 – Recht auf Löschung

Auch § 35 Abs. 1 BDSG-neu ist nicht vereinbar mit Art 23 Abs. 1. Ein möglicher unverhältnismäßiger Aufwand für den Verantwortlichen ist gemäß der DSGVO kein zulässiger Grund, einen Löschanspruch des Betroffenen zu verweigern. Die Datenverarbeitungssysteme sollten vielmehr dahingehend von vornherein rechtskonform gestaltet werden, dass Daten selektiv oder vollständig sowie regelmäßig gelöscht werden können. Alles andere würde einen Anreiz bieten, die Systeme bewusst so zu gestalten, dass eine Löschung einen unverhältnismäßigen Aufwand bedeuten würde.

Daher ist § 35 Abs. 1 BDSG-neu zu streichen.

3.7 § 37 – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

§ 37 BDSG-neu weitet die Regelungsspielräume der DSGVO unzulässig aus und eröffnet den Verantwortlichen gleichzeitig Formen der Datenverarbeitung, die über die Möglichkeiten hinausgehen, die das BDSG-alt vorsieht.

Denn während sich Art. 22 (und damit auch die Öffnungsklausel in Art. 22 Abs. 2 lit. b) sowie § 6a Abs. 2 Nr. 1 BDSG-alt lediglich auf Zwei-Personenverhältnisse - im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses - beziehen, sollen durch die neuen Regelungen entsprechend der Gesetzesbegründung ausdrücklich auch Mehr-Personenverhältnisse erfasst werden, bei denen der Betroffene in keinem direkten Verhältnis zum Verantwortlichen steht.

Darüber hinaus wird durch § 37 Abs. 1 Nr. 2 BDSG-neu der Schutzstandard im Vergleich zur derzeit geltenden Rechtslage massiv abgesenkt. Denn bisher gilt, dass bei Anträgen, denen nicht vollumfänglich stattgegeben wird, eine menschliche Überprüfung und Entscheidung erfolgen muss. Dieser Automatismus wird durch § 37 Abs. 1 Nr. 2 BDSG-neu ausgehebelt. Zwar müssen die Verantwortlichen auch in Zukunft Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person treffen, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung zählt. Jedoch sind zum einen diese Schutzmaßnahmen zu unbestimmt, zum anderen sollen die Betroffenen in Zukunft lediglich auf diese Rechte hingewiesen werden. Zur Wahrung ihrer Interessen müssen die Betroffenen jedoch selbst tätig werden. Damit wird eine Hürde für eine Intervention des Verbrauchers aufgestellt.

Kritisch ist außerdem, dass § 37 Abs. 2 BDSG-neu den Verantwortlichen berechtigt, automatisierte Entscheidungen im Rahmen der Leistungserbringung nach einem Versicherungsvertrag auf der Basis von Gesundheitsdaten durchzuführen. Dies geht über die bisherigen Möglichkeiten hinaus, da bisher automatisierte Entscheidungen im Einzelfall auf der Basis von Gesundheitsdaten nicht auf § 6a BDSG-alt gestützt werden konnten. Bisher regelt § 28 Abs. 6 bis Abs. 8 BDSG-alt abschließend die Verarbeitung von personenbezogenen Daten besonderer Art (einschließlich Gesundheitsdaten). Demnach ist eine solche Verarbeitung für eigene Geschäftszwecke ohne Einwilligung

des Betroffenen nur in engen Grenzen zulässig. Mit der nun vorgeschlagenen Regelung in § 37 BDSG-neu wird somit das bisherige Einwilligungserfordernis umgangen.

Sollen darüber hinaus im Rahmen der Leistungserbringung von Versicherungen automatisierte Entscheidungen im Einzelfall für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sein, ist dies bereits auf Basis des Art. 22 Abs. 2 lit a) möglich.

Insgesamt ist nicht nachvollziehbar, warum hier – auf Kosten der Rechte der Betroffenen – eine Sonderregelung geschaffen wird, um künftige Geschäftsmodelle eines einzelnen Wirtschaftszweigs zu schützen.

■ Daher ist § 37 BDSG-neu vollständig zu streichen.

Stellungnahme

**anlässlich der öffentlichen Anhörung des Innenausschusses des
Deutschen Bundestages am 27. März 2017**

zum

**Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts
an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtli-
nie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungs-
gesetz EU – DSAnpUG-EU)**

BT-Drucksache 18/11325

begrenzt auf ausgewählte Regelungen der §§ 1 – 85 BDSG-E

von

**Dr. Carlo Piltz, Rechtsanwalt
Reusch Rechtsanwälte, Berlin**

Inhaltsverzeichnis

A. Zusammenfassung der Ergebnisse	4
B. Allgemein – Einordnung des BDSG-E und Vorgaben für den Gesetzgeber	6
I. Anwendungsvorrang von EU-Recht	6
II. Möglicher Verstoß gegen den EU-Vertrag durch Schaffung rechtlicher Unsicherheit	8
III. Handlungsmöglichkeiten der Mitgliedstaaten im Rahmen von Öffnungsklauseln	8
IV. Dürfen die deutschen Aufsichtsbehörden das BDSG unangewendet lassen?	10
C. Rechtliche Würdigung ausgewählter Vorschriften des BDSG-E mit Bezug zur DSGVO (§§ 1 – 44 BDSG-E)	13
I. § 1 Abs. 4 – Räumlicher Anwendungsbereich	13
II. § 3 – Verarbeitung personenbezogener Daten durch öffentliche Stellen	15
III. § 4 – Videoüberwachung öffentlich zugänglicher Räume	15
IV. § 17 – Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle	17
V. § 18 – Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder	19
VI. § 19 – Zuständigkeiten	21
VII. § 21 – Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission	21
VIII. § 22 – Verarbeitung besonderer Kategorien personenbezogener Daten	23
IX. § 24 – Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen	24
X. § 26 – Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses	26
XI. § 29 – Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten	28
XII. § 32 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	28
XIII. § 35 – Recht auf Löschung	30
XIV. Einwilligung Minderjähriger	30
D. Rechtliche Würdigung einzelner Aspekte der Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680	31
I. Mindestharmonisierung durch die JI-RL	32
II. § 46 Nr. 17 – Einwilligung	32
III. § 49 – Verarbeitung zu anderen Zwecken	33
IV. § 57 – Auskunftsrecht	33
V. § 65 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten	34
VI. § 83 – Schadensersatz und Entschädigung	34



A. Zusammenfassung der Ergebnisse

Zur Anpassung an die EU Datenschutz-Grundverordnung (DSGVO):

- Auch neben der DSGVO sind nationale Regelungen möglich und zum Teil sogar verpflichtend vorgeschrieben. Der deutsche Gesetzgeber kommt mit dem vorliegenden Gesetzentwurf dieser Pflicht nach und versucht den eröffneten Gestaltungsrahmen zu nutzen. Dies ist zu begrüßen.
- Leitprinzip des nationalen Anpassungsgesetzes sollte die Schaffung von Rechtssicherheit und -klarheit sein. Widersprüche zu europäischen Vorgaben müssen vermieden werden. Andernfalls besteht das Risiko eines Verstoßes gegen das europäische Primärrecht (Art. 4 Abs. 3 des Vertrags über die Europäische Union).
- Im Rahmen der „Öffnungsklauseln“ der DSGVO ist der deutsche Gesetzgeber ausdrücklich befugt, Betroffenenrechte einzuschränken. Jedoch müssen in diesen Fällen die Voraussetzungen für Beschränkungen genau beachtet werden. Teilweise gehen die vorgeschlagenen Regelungen über die eröffneten Gestaltungsspielräume hinaus und sollten daher punktuell angepasst werden.
- Nach der Rechtsprechung des Europäischen Gerichtshofs dürfen deutsche Behörden nationales Recht, welches im Konflikt mit unmittelbar geltenden europäischen Normen steht, nicht anwenden. Für die Praxis entsteht in solchen Situationen jedoch ein Zustand rechtlicher Unsicherheit, da die Kriterien, wann eine nationale Norm nicht anzuwenden ist, umstritten sind.
- Die Vorgaben zum räumlichen Anwendungsbereich des BDSG-E sollten konkretisiert und Art. 3 Abs. 1 DSGVO angepasst werden.
- Die Regelung zur Videoüberwachung mutet wie ein exklusiver Erlaubnistatbestand an. Sie sollte angepasst werden, um klarzustellen, dass die Erlaubnistatbestände der DSGVO nicht ausgeschlossen sind.
- Das vorgeschlagene Verfahren der Zusammenarbeit der nationalen Aufsichtsbehörden und deren Vertretung im Europäischen Datenschutzausschuss sollte noch mehr an die Regelungen der DSGVO angeglichen werden. Zudem bestehen offene Fragen zur Zusammenarbeit zwischen Vertreter und Stellvertreter.
- Die vorgesehenen Möglichkeiten zur zweckändernden Weiterverarbeitung gehen derzeit teilweise über die Grenzen der Art. 6 Abs. 4, 23 Abs. 1 DSGVO hinaus und sollten daher angepasst werden.
- Die angedachten „Spezifizierungen“ im Bereich des Beschäftigtendatenschutzes bleiben zum Teil hinter den Erfordernissen des Art. 88 Abs. 1 DSGVO zurück, gehen andererseits aber darüber hinaus. Auch hier sollte der deutsche Gesetzgeber entsprechende Angleichungen vornehmen.

- Die Beschränkung der Untersuchungsbefugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern ist zweckmäßig und sollte beibehalten werden.
- Im Rahmen der Beschränkung der Informationspflicht werden im Gesetzesentwurf zum Teil Verarbeitungssituationen und darauf bezogene Einschränkungsmöglichkeiten entgegen den Vorgaben der DSGVO vermengt. § 32 Abs. 1 BDSG-E sollte diesbezüglich überarbeitet werden.

Zur Anpassung an die Richtlinie 2016/680 (JI-RL):

- Die Einführung der Definition der Einwilligung ist zu begrüßen und sollte beibehalten werden.
- Die Einschränkung des Auskunftsrechts sollte mit Blick auf die Erreichung eines in § 15 Abs. 1 JI-RL bestimmten Zieles konkretisiert werden.
- Für Schadensersatzansprüche sollten, wie vom Gesetzgeber vorgesehen, keine Haftungshöchstgrenzen festgelegt werden. Anderenfalls besteht das Risiko, das Ziel zur Schaffung eines „wirksamen Schadenersatzes“ zu verfehlen.

B. Allgemein – Einordnung des BDSG-E und Vorgaben für den Gesetzgeber

Das Ziel der EU Datenschutz-Grundverordnung (DSGVO) ist die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU).¹ Die oft zitierte Zielvorgabe „One continent, one law“ wird jedoch mit der DSGVO nicht in Gänze erreicht. Zwar wird ab dem 25. Mai 2018 ein unmittelbar anwendbares „Datenschutzgesetz“ in der EU existieren. Jedoch erlaubt es die DSGVO den Mitgliedstaaten an vielen Stellen weiterhin nationale Regelungen vorzusehen. Die DSGVO ähnelt in Teilen daher eher einer europäischen Richtlinie, deren Regelungen nicht unmittelbar anwendbar sind, sondern erst nationalstaatlich umgesetzt werden müssen.² Über diese Öffnungsklauseln, die zum Teil einen obligatorischen Regelungsauftrag erteilen, zum Teil fakultative Handlungsmöglichkeiten eröffnen, wird das Datenschutzrecht in Zukunft in Europa also auch von einer Gemengelage aus europäischem und nationalem Recht geprägt sein. Ab dem 25. Mai 2018 werden datenverarbeitende Stellen, betroffene Personen, Aufsichtsbehörden und auch Gerichte bei ihrer Anwendung der Vorschriften mit dieser Mischung aus europäischen und nationalen Vorgaben (nicht nur jenen in Deutschland) umgehen müssen. Ob dies im Ergebnis zu mehr oder weniger Rechtssicherheit in der Praxis führen wird, dürfte auch maßgeblich davon abhängen, wie die Regelungen der nationalen Datenschutzgesetze ausgestaltet sind und wie sich diese in das Gesamtregelungskonzept der DSGVO einfügen. Wichtig ist daher bereits hier darauf hinzuweisen, dass das vorgeschlagene deutsche Gesetz das Ziel haben sollte, harmonische, verständliche und praxistaugliche Regelungen zu schaffen, um Rechtsanwender und Betroffene nicht mit noch mehr Rechtsunsicherheit (die bereits allein mit Blick auf die Anwendung der DSGVO besteht) zu belasten.

I. Anwendungsvorrang von EU-Recht

Für eine adäquate Bewertung des vorgeschlagenen BDSG (BDSG-E) und auch der aus meiner Sicht noch vorzunehmenden Ergänzungen am Gesetzentwurf im Hinblick auf sein Verhältnis zur DSGVO (vgl. unter C.) ist es unerlässlich, die Grenzen zu kennen, in denen sich der deutsche Gesetzgeber bewegt, wenn er die Öffnungsklauseln der DSGVO mit Leben füllen möchte.

Treffen in der Praxis nationale und europäische Regelungen aufeinander, gilt ein Anwendungsvorrang des europäischen vor nationalem Recht.³ Bei einem Widerspruch der nationalen Norm gegenüber der unmittelbar anwendbaren europäischen Regelung genießt letztere Anwendungsvorrang.

¹ ErwG 10 DSGVO.

² *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016 S. 1.

³ Grundlegend hierzu: EuGH, Urt. v. 15.07.1964, C-6/64 - Costa / E.N.E.L.; vgl. auch *Terhechte*, JuS 2008, 403.

Nationales Recht ist nicht nichtig, aber nationale Stellen (sowohl Behörden und auch Gerichte) müssen im Fall einer Kollision nationales Recht unangewendet lassen.⁴

Für den deutschen Gesetzgeber wird sich beim Entwurf des BDSG-E daher stets die Frage stellen, ob bei den vorgeschlagenen Regelungen eine solche Kollision vorliegt und damit das BDSG-E nicht anwendbar wäre. Es dürfte klar sein, dass es das Ziel sein sollte, diese Situation zu vermeiden.

Dieser Konflikt europäischen Rechts mit nationalem Recht und der damit einhergehende Anwendungsvorrang des EU-Rechts entsteht dann, wenn eine direkte oder auch indirekte Kollision gesetzlicher Regelungen vorliegt.⁵ Damit eine solche Kollision vorliegt, muss die europäische Norm unmittelbar anwendbar sein, was bei der DSGVO nach Art. 288 Abs. 2 AEUV der Fall ist. Zudem muss aber auch die Regelung selbst (im Sinne des konkreten Artikels und seines Wortlauts) derart gestaltet sein, dass sie im Mitgliedstaat unmittelbar angewendet werden kann. Hierzu ist erforderlich, dass die Norm hinreichend bestimmt und unbedingt formuliert ist. Für einige der Öffnungsklauseln der DSGVO trifft dieses Merkmal nicht zu, da dem nationalen Gesetzgeber, etwa hinsichtlich bestimmter Verarbeitungssituationen, nur der Rahmen an die Hand gegeben wird, den er bei der Schaffung nationaler Regelungen zu beachten hat. Innerhalb dieses Rahmens können und müssen aber nationale Datenschutzregelungen geschaffen werden, die zur Konkretisierung und Spezifizierung neben der DSGVO zur Anwendung kommen. Solange eine europäische Norm einen Sachverhalt nicht abschließend regelt, können auch nationale Regelungen bestehen bleiben und insbesondere auch eigene Vorgaben vorsehen. Ein Konflikt mit europäischem Recht existiert dann also nicht, wenn die EU-Norm einen Sachverhalt gar nicht selbst regelt bzw. aufgrund mangelnder Gesetzgebungskompetenz auf europäischen Ebene nicht selbst regeln darf. Kein Konflikt besteht auch dann, wenn kein Widerspruch zwischen nationaler und europäischer Norm existiert.

Zudem muss bei der Frage, ob ein Konflikt von europäischem und nationalem Recht besteht, stets der Anwendungsbereich der DSGVO beachtet werden. Ein Konflikt mit Ihren Regelungen ist nur möglich, soweit sich eine nationale Norm innerhalb des sachlichen Anwendungsbereich der DSGVO bewegt, der sich konkret aus Art. 2 DSGVO ergibt.

⁴ Hierzu näher unter B. IV.

⁵ Umfassend zur Situation vor dem Hintergrund der DSGVO: *Roßnagel*, in: *Roßnagel*, Europäische Datenschutz-Grundverordnung, 2017, S. 69 ff.; *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 3 ff.

Es bleibt mithin festzuhalten, dass unter Geltung der DSGVO weiterhin nationale Regelungen möglich sind, ja teilweise sogar verpflichtend vorgeschrieben werden. Soweit diese nationalen Regelungen die Gestaltungsspielräume der DSGVO (und die dort jeweils aufgestellten Voraussetzungen, etwa in Art. 6 Abs. 3 und Abs. 4 oder Art. 23 Abs. 1 DSGVO) erfüllen und nicht im Widerspruch zu den Zielvorgaben der DSGVO stehen, können sie angewendet werden.⁶

Die nachfolgende Stellungnahme zu den Regelungen des BDSG-E wird sich daher insbesondere auf Situationen konzentrieren, in denen ein solcher Widerspruch möglicherweise vorliegt und/oder die bindenden Vorgaben der DSGVO zum nationalen Gestaltungsspielraum nicht (in Gänze) eingehalten werden. Aufgrund des Umfangs des Gesetzesentwurfs und der für die Erarbeitung dieser Stellungnahme knapp bemessenen Bearbeitungszeit, beschränke ich meine Ausführungen auf ausgewählte Regelungsbereiche des BDSG-E.

II. Möglicher Verstoß gegen den EU-Vertrag durch Schaffung rechtlicher Unsicherheit

Aus dem Anwendungsvorrang des unmittelbar anwendbaren europäischen Rechts ergibt sich für den deutschen Gesetzgeber eine im Rahmen des hier vorliegenden Gesetzesentwurfs besonders zu beachtendes Risiko. Nach der Rechtsprechung des EuGH ergeben *„sich aus der Einführung oder unveränderten Beibehaltung einer gegen eine Vorschrift des Gemeinschaftsrechts verstoßenden Bestimmung in den Rechtsvorschriften eines Mitgliedstaats, selbst wenn diese Gemeinschaftsvorschrift in der Rechtsordnung der Mitgliedstaaten unmittelbar gilt, Unklarheiten tatsächlicher Art, weil die betroffenen Normadressaten bezüglich der ihnen eröffneten Möglichkeiten, sich auf das Gemeinschaftsrecht zu berufen, in einem Zustand der Ungewissheit gelassen werden. Eine solche Beibehaltung stellt deshalb eine Verletzung der Verpflichtungen des genannten Mitgliedstaats aus dem EWG-Vertrag dar“*.⁷ Nach Art. 4 Abs. 3 des Vertrags über die Europäische Union (EUV) sind die Mitgliedstaaten verpflichtet, die Union bei der Erfüllung ihrer Aufgabe zu unterstützen und müssen alle Maßnahmen unterlassen, die die Verwirklichung der Ziele der Union gefährden könnten. Eine solche Gefährdung kann sich aus gegen DSGVO verstoßende Normen im neuen BDSG ergeben, sollten diese im Widerspruch zur Verordnung stehen.⁸

III. Handlungsmöglichkeiten der Mitgliedstaaten im Rahmen von Öffnungsklauseln

⁶ Roßnagel, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, S. 73.

⁷ EuGH, Urt. v. 26.04.1988 – C-74/86, Rn. 10 (Kommission ./ Bundesrepublik Deutschland).

⁸ So auch: Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 3.

Das hier zu bewertende DSAnpUG-EU dient mit seinem Vorschlag für ein neues BDSG in Artikel 1 der Umsetzung der fakultativen und obligatorischen Regelungsaufträge der DSGVO und auch der Richtlinie 2016/680 (zu dieser unter D.). Die Öffnungsklauseln der DSGVO stellen sich in verschiedenen Varianten dar. Sie erlauben die Konkretisierung, die Ergänzung und auch die Modifikation der Vorgaben der DSGVO.

Im Rahmen dieser Öffnungsklauseln ist es den nationalen Gesetzgebern jedoch nicht gestattet, Spezifizierungen in der Art vorzunehmen, dass ein höheres Schutzniveau als jenes der DSGVO geschaffen wird. Dies zumindest soweit, wie eine Erhöhung des Schutzniveaus nicht durch die Vorgaben der DSGVO selbst vorgesehen ist.⁹ Dies ergibt sich zum einen aus den Arbeitsdokumenten des Rates zur DSGVO.¹⁰ Insbesondere Art. 6 Abs. 2 und 3 DSGVO erlauben es den Mitgliedstaaten nicht, ein gegenüber der DSGVO höheres Schutzniveau zu schaffen.¹¹ Die Europäische Kommission weist zum anderen in ihrer Mitteilung zum Standpunkt des Rates darauf hin, dass die Einigung den Mitgliedstaaten Spielraum für eine Spezifizierung der Datenschutzvorschriften für den öffentlichen Sektor lässt.¹² Ein höheres Schutzniveau, insbesondere durch strengere Regelungen als sie in der DSGVO existieren, ist damit vor allem für Verarbeitungen im öffentlichen Sektor nicht gestattet. Diese Schlussfolgerungen lassen sich auch mit Blick auf den Sinn und Zweck der DSGVO und insbesondere ihren Verordnungscharakter begründen. Die Verordnung soll gerade ein einheitliches Schutzniveau schaffen, von dem nicht jeder Mitgliedstaat beliebig, sondern nur in ausdrücklich gesetzlich geregelten Fällen nach unten¹³ abweichen darf. Andernfalls hätte es des Instruments der Verordnung nicht bedurft. Selbst für EU-Richtlinien hat der Europäische Gerichtshof anerkannt, dass bei einer intendierten Vollharmonisierung strengere Vorschriften nicht angewendet werden dürfen.¹⁴ Schutzbereich und –niveau nationaler Umsetzungsregelungen müssen in diesem Fall identisch oder

⁹ Vgl. etwa Art. 9 Abs. 4 DSGVO, mit dem Mitgliedstaaten gestattet wird, zusätzliche Beschränkungen bei der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten einzuführen.

¹⁰ In Ratsdokument 14732/12, 24.10.2014 wurde eine sog. Minimumharmonisierungsklausel (Art. 1 Abs. 2a) vorgeschlagen, in der es den Mitgliedstaaten ausdrücklich gestattet werden sollte, „strengere“ nationale Regelungen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen vorzusehen. Dieser Vorschlag wurde nicht in den finalen Text übernommen. In Ratsdokument 9398/1/13 REV 1 ADD 1, 27.05.2013, S. 48 dort Fn. 47 forderten die deutsche und die dänische Delegation, dass Mitgliedstaaten nicht nur die Möglichkeit haben sollten, spezifischere sondern umfassendere Regelungen vorzusehen. Auch dieser Vorschlag wurde nicht übernommen.

¹¹ Ratsdokument 15389/14, 13.11.2014, S. 5 f.

¹² Mitteilung der Kommission an das Europäische Parlament betreffend den Standpunkt des Rates im Hinblick auf den Erlass einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr (Datenschutz-Grundverordnung) und zur Aufhebung der Richtlinie 95/46/EG, COM(2016) 214 final, 11.04.2016, S. 4.

¹³ Eine solche gesetzliche Erlaubnis zur Abweichung vom aufgestellten Schutzniveau findet sich insbesondere in Art. 23 (Beschränkungen); vgl. hierzu: Stellungnahme des Juristischen Dienstes des Rates, Ratsdokument 15712/14, 18.11.2014.

¹⁴ EuGH, Urt. v. 08.04.2003 – C-44/01, Rn. 44 (Pippig Augenoptik).

zumindest gleichwertig sein.¹⁵ Ähnlich stellt sich die Situation unter der DSGVO dar, die dem Grunde nach eine verbindliche Verordnung ist, jedoch an eine Richtlinie erinnernde Umsetzungsmöglichkeiten für Mitgliedstaaten eröffnet.¹⁶ Der Harmonisierungscharakter der DSGVO kann aber nur mit jenem der Vollharmonisierung einer Richtlinie verglichen werden, in deren Grenzen und nicht darüber hinausgehend, nationale Spezifizierungen möglich sind.

In der öffentlichen Diskussion um den vorliegenden Gesetzesentwurf wurde oft kritisiert, dass die Bundesregierung das Datenschutzniveau der DSGVO absenken möchte und dass dies nicht zulässig sei. Man muss es noch einmal klar sagen: die Absenkung des Schutzniveaus (so man überhaupt von einer „Absenkung“ sprechen kann, wenn nationale Vorschriften den durch die DSGVO eröffneten Regelungsrahmen ausfüllen) bei der Verarbeitung personenbezogener Daten nach unten, insbesondere durch die Einschränkung der Betroffenenrechte (Art. 23 DSGVO), ist vom europäischen Gesetzgeber, auch im Bereich der Datenverarbeitung durch private Stellen, vorgesehen, gewollt und nicht unzulässig, solange die Vorgaben der DSGVO eingehalten werden. Der juristische Dienst des Rates der Europäischen Union stellt hierzu fest:¹⁷

*„...the Commission has accepted that there will be different levels of data protection in the draft regulation as it has proposed, and this has been accepted, that Member States could be allowed to derogate from the harmonised level of protection **by providing a lower protection** in certain cases“.*
(Hervorhebung durch den Autor)

Mit den Vorschlägen der Beschränkung von Betroffenenrechten im BDSG-E wird also per se nicht gegen die DSGVO verstoßen. Dem nationalen Gesetzgeber sind beschränkende Maßnahmen nach Art. 23 DSGVO ausdrücklich gestattet. Die Frage ist freilich, ob die Beschränkungen die in der DSGVO hierfür aufgestellten Anforderungen erfüllen.

IV. Dürfen die deutschen Aufsichtsbehörden das BDSG unangewendet lassen?

Aus dem vorstehend beschriebenen Anwendungsvorrang des europäischen Rechts im Konfliktfall kann sich für deutsche Datenschutzbehörde das Problem ergeben, mit, zumindest ihrer Meinung nach, europarechtswidrigen Regelungen des BDSG-E konfrontiert zu sein, die sie, aufgrund ihrer Bindung an die Gesetze (Art. 20 Abs. 3 GG), eigentlich anwenden müssten. Die Vorsitzende der Datenschutzkonferenz von Bund und Ländern, Barbara Thiel, hat hierzu kürzlich festgestellt, dass

¹⁵ *Nils Wahl*, Schlussanträge v. 15.05.2013 – C-184/12, Rz. 42.

¹⁶ *Kühling/Martini*, EuZW 2016, 448, 449.

¹⁷ Ratsdokument 15712/14, 18.11.2014, S. 10.

für die Aufsichtsbehörden das Europarecht in jedem Fall bindend ist und die Aufsichtsbehörden sich in ihren Auslegungsprinzipien deshalb an der Datenschutz-Grundverordnung zu orientieren haben.¹⁸

Diese Problematik der (Nicht)Anwendung von möglicherweise europarechtswidrigen Normen durch nationale Behörden ist nicht neu. Wichtig ist jedoch zunächst hervorzuheben, dass es nicht um die Frage geht, ob eine Behörde eine nationale Norm als ungültig erklären darf, also etwa in einem Verwaltungsakt, sondern um die Frage der Nichtanwendung nationaler Regelungen, die ihrer Ansicht nach gegen europäisches Recht verstoßen.

Es geht mithin um die Frage, ob und gegebenenfalls unter welchen Voraussetzungen einer nationalen Behörde prinzipiell die Befugnis zusteht, Vorschriften nationalen Rechts im Falle der von ihr so beurteilten Gemeinschaftswidrigkeit außer Anwendung zu lassen.¹⁹

Der EuGH hat sich in der Vergangenheit oft mit dieser Frage befasst. In seiner Entscheidung vom 22.06.1989 ist er, im Fall einer EU-Richtlinie und einer damit nicht in Einklang stehenden nationalen Regelung, zu dem Ergebnis gelangt, dass eine Nichtanwendungspflicht jedenfalls dann besteht, wenn sich der Einzelne auf die gemeinschaftsrechtliche Bestimmung berufen kann.²⁰ Im Fall der hier vorliegenden DSGVO kann sich jeder Adressat bereits ipso iure auf ihre Regelungen berufen. Der Vorrang des Gemeinschaftsrechts bedeutet im Fall der Normenkollision eine Verpflichtung zur Nichtanwendung des nationalen Rechts und auch die öffentlichen Verwaltung ist verpflichtet, nationale Regelungen, die mit den europäischen unvereinbar sind, nicht anzuwenden.²¹

In einem weiteren Verfahren vor dem EuGH ging es um die italienische Wettbewerbsbehörde, die nationale Regelungen zum gesetzlichen Zündholzsystem Italiens auf deren Vereinbarkeit mit den Vorgaben des EU-Rechts prüfte, und die italienischen Regelungen, dies ist besonders hervorzuheben, vor jeder gerichtlichen Feststellung eines italienischen Gerichts als gemeinschaftswidrig einstufte.²² Der EuGH entschied in diesem Fall, dass „die Pflicht, eine dem Gemeinschaftsrecht entgegenstehende nationale Rechtsvorschrift unangewendet zu lassen, nicht nur den nationalen Gerichten obliege, sondern allen staatlichen Organen einschließlich der Verwaltungsbehörden“.²³

¹⁸ Heise online vom 17.03.2017, Datenschutzaufsicht: Entwurf zum Bundesdatenschutzgesetz teilweise europarechtswidrig, abrufbar unter: <https://www.heise.de/newsticker/meldung/Datenschutz-aufsicht-Entwurf-zum-Bundesdatenschutzgesetz-teilweise-europarechtswidrig-3657607.html>.

¹⁹ Vgl. hierzu etwa: OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06; OVG Lüneburg, Urt. v. 28.11.2016 – 9 LC 335/14.

²⁰ EuGH, Urt. v. 22.06.1989 – C-103/88, Rn. 28 ff. (Fratelli Costanzo).

²¹ *Dámaso Ruiz-Jarabo Colomer*, Schlussanträge v. 25.06.2009 – C-205/08, Rn. 51.

²² EuGH, Urt. v. 09.09.2003 – C-198/01 (CIF).

²³ EuGH, Urt. v. 09.09.2003 – C-198/01, Rn. 49 (CIF).

Aus der Formulierung „alle Verwaltungsbehörden“ folgt, dass die genannte Nichtanwendungspflicht sich an alle zuständigen staatlichen Träger richtet.²⁴ Gehen also etwa in Zukunft die deutschen Datenschutzbehörden von der Europarechtswidrigkeit einer Norm des BDSG-E aus, so ist es ihnen gestattet, die nationale Regelung unangewendet zu lassen.²⁵ Jedoch ist darauf hinzuweisen, dass eine solche Situation und Vorgehensweise wohl insbesondere für datenverarbeitende Unternehmen ein erhebliches rechtliches Risiko darstellt und der effektiven Umsetzung des neuen Datenschutzrechts in Deutschland einen Bärendienst erweisen würde. Zudem besteht aus Sicht der Behörde das Risiko, eine nationale Norm unangewendet zu lassen, die im Ergebnis, etwa in einem anschließenden Verwaltungsgerichtsprozess mit Vorlage an den EuGH, als europarechtskonform eingestuft wird.

Im Übrigen geht auch das Bundesverwaltungsgericht davon aus, dass der Anwendungsvorrang von EU-Recht es für die Zeit des „Widerspruchs“ zwischen nationalen und europäischen Recht verbietet, die entgegenstehenden Bestimmungen des nationalen Rechts einer behördlichen oder gerichtlichen Entscheidung zugrunde zu legen.²⁶

Aus Art. 20 Abs. 3 GG lässt sich nicht herleiten, dass eine Verwaltungsbehörde unmittelbar geltendes Gemeinschaftsrecht unangewendet lassen muss, um entgegenstehendem nationalem Recht den Vorrang zu verschaffen.²⁷ Bindung an Recht und Gesetz bedeutet im Falle des Anwendungsvorrangs von unmittelbar geltendem Gemeinschaftsrecht eine Bindung (auch) an das europäische Recht. Wie beschrieben, sind alle nationalen Behörden an unmittelbar geltendes EU-Recht gebunden. Hieraus folgt auch, dass das Gewaltenteilungsprinzip des Art. 20 GG nicht verletzt sein kann.²⁸

Natürlich lässt sich diese Rechtsprechung des EuGH auch kritisieren, da es, mit Blick auf die fehlende Möglichkeit von Behörden im Vergleich zu den Gerichten, ein Vorabentscheidungsersuchen an den EuGH zu stellen, zweifelhaft erscheinen kann, warum sie dennoch verpflichtet sind, inländische Bestimmungen nicht anzuwenden.²⁹ Die Exekutive ist nicht befugt, gesetzliche Regelungen für ungültig zu erklären. Dies obliegt der Legislative. Es wird daher vermittelnd vorgeschlagen, nationalen Behörden die Nichtanwendung nationaler Normen dann zu gestatten, wenn die Gemeinschaftsrechtswidrigkeit evident ist.³⁰ Dennoch ist festzuhalten, dass die Rechtsprechung des EuGH in die-

²⁴ OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06.

²⁵ So auch für deutsche Behörden in anderen Fällen: OVG Lüneburg, Urt. v. 28.11.2016 – 9 LC 335/14; OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06.

²⁶ BVerwG, Urt. v. 29.11.1990 – 3 C 77/87.

²⁷ OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.

²⁸ OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.

²⁹ *Dámaso Ruiz-Jarabo Colomer*, Schlussanträge v. 25.06.2009 – C-205/08, Rn. 51; *Ruffert*, in: *Calliess/Ruffert/Ruffert*, EUV/AEUV, 5. Aufl. 2016, AEUV Art. 288 Rn. 73.

³⁰ *Ruffert*, in: *Calliess/Ruffert/Ruffert*, EUV/AEUV, 5. Aufl. 2016, AEUV Art. 288 Rn. 73 f. mwN.

ser Frage zur Nichtanwendung nationaler Normen gefestigt erscheint. Ich tendiere für derartige Situationen, in denen eine deutsche Datenschutzbehörde in Zukunft möglicherweise Bestimmungen des BDSG-E nicht anwenden möchte, zu der eben zitierten vermittelnden Ansicht. Möchte eine Datenschutzbehörde nationale Normen nicht anwenden, sollte in jedem Fall eine Überzeugungsgewissheit über den Verstoß nationaler Bestimmungen gegen vorrangiges Gemeinschaftsrecht als erforderlich, wohl aber auch als ausreichend erachtet werden. Nicht ausreichend wäre eine bloße Vermutung der Gemeinschaftswidrigkeit.³¹

C. Rechtliche Würdigung ausgewählter Vorschriften des BDSG-E mit Bezug zur DSGVO (§§ 1 – 44 BDSG-E)

Nachfolgend werden ausgewählte Regelungen des Gesetzentwurfs vor dem Hintergrund des Anwendungsvorrangs der DSGVO insbesondere auf ihre Vereinbarkeit und Widerspruchsfreiheit mit deren Vorgaben der DSGVO untersucht. Ziel des BDSG-E muss es, wie bereits erwähnt, sein, mit der DSGVO konsistente und ihr nicht widersprechende nationale Normen zu schaffen. Nur so kann Rechtssicherheit für die datenverarbeitende Praxis (Behörden als auch private Stellen) und Betroffene hergestellt und die Gefahr einer Verletzung des EUV vermieden werden.

I. § 1 Abs. 4 – Räumlicher Anwendungsbereich

Zwar macht die DSGVO selbst keine Vorgaben dazu, wann welches nationale Datenschutzrecht, welches in Ausübung der eröffneten Spielräume der diversen (obligatorischen als auch fakultativen) Öffnungsklauseln entsteht, Anwendung findet. Bereits dieses Fehlen einer europarechtlich einheitlichen Vorgabe in der DSGVO ist zu kritisieren, aber nicht dem Bundesgesetzgeber anzulasten. Jedoch sind die Vorgaben zum räumlichen Anwendungsbereich des BDSG-E auch selbst nicht in Gänze mit der Regelung des Art. 3 DSGVO kongruent.

In Abweichung zu den Regelungen des Art. 3 Abs. 1 DSGVO bestimmt § 1 Abs. 4 S. 2 BDSG-E, dass die Vorschriften dieses Gesetzes bereits dann Anwendung finden, sofern der Verantwortliche oder Auftragsverarbeiter personenbezogenen Daten im Inland verarbeitet. Nach Art. 3 Abs. 1 DSGVO findet die DSGVO Anwendung „auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet“.

³¹ OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.

In § 1 Abs. 4 S. 2 Nr. 1 BDSG-E fehlt der Bezug zu einer Niederlassung. Auf die Verarbeitung im Rahmen der Tätigkeiten einer inländischen Niederlassung wird zwar in § 1 Abs. 4 S. 2 Nr. 2 BDSG-E Bezug genommen, der jedoch alternativ neben den anderen Varianten des § 1 Abs. 4 S. 2 BDSG-E. Anders als in Art. 3 Abs. 1 DSGVO, fehlt in § 1 Abs. 4 S. 2 Nr. 2 BDSG-E (in dem die Niederlassung angesprochen wird) aber der Zusatz, dass es irrelevant ist, ob die Datenverarbeitung technisch in der Union bzw. hier im Gebiet der Bundesrepublik Deutschland stattfindet. Es ließe sich also der Schluss ziehen, dass der deutsche Gesetzgeber es durchaus für die Frage der Anwendbarkeit des Gesetzes für relevant hält, wo personenbezogene Daten technisch verarbeitet werden, da der Hinweis „unabhängig davon, ob die Verarbeitung in der Union stattfindet“ fehlt.

Hierfür spricht die Regelung in § 1 Abs. 4 S. 2 Nr. 1 BDSG-E, wonach das Gesetz Anwendung findet, sofern der Verantwortliche oder Auftragsverarbeiter personenbezogen Daten im Inland verarbeiten. Der Regelungsbereich dieser Norm scheint sich gerade allein auf den physischen Ort der Datenverarbeitung zu beziehen, denn ansonsten (wenn es also um eine Niederlassung gehen würde) wäre er deckungsgleich mit der Vorgabe des § 1 Abs. 4 S. 2 Nr. 2 BDSG-E.

Verwirrend ist zudem die Erläuterung hierzu in der Gesetzesbegründung (S. 80). Dort wird davon gesprochen, dass die Vorschriften des BDSG-E bereits bei einer Datenverarbeitung im Inland zur Anwendung kommen, unabhängig davon, ob eine Niederlassung im Inland existiert. Der räumliche Anwendungsbereich des BDSG-E ist damit also, bei einer entsprechenden Interpretation, weiter als jener der DSGVO nach Art. 3 Abs. 1 DSGVO, da dort in jedem Fall Bezug auf eine Niederlassung genommen wird.

Inkongruent mit den Vorgaben des Art. 3 Abs. 1 DSGVO ist, zumindest wenn man sich die Gesetzesbegründung hierzu betrachtet, die Regelung des § 1 Abs. 4 S. 2 Nr. 2 BDSG-E. Laut der Gesetzesbegründung (S. 80) kommt das BDSG-E zur Anwendung, wenn eine Datenverarbeitung durch eine in Deutschland ansässige Niederlassung vorliegt. Diese Umschreibung des Anwendungsbereichs weicht jedoch entscheidend von den Vorgaben des Art. 3 Abs. 1 DSGVO bzw. § 1 Abs. 4 S. 2 Nr. 2 BDSG-E ab, wo es darauf ankommt, dass eine Datenverarbeitungen im Rahmen der Tätigkeiten einer Niederlassung vorgenommen wird. Mit Blick auf Rechtsprechung des Europäischen Gerichtshofs zu dem Merkmal „im Rahmen der Tätigkeiten“ lässt sich feststellen, dass es hierbei eben gerade nicht, wie in der Gesetzesbegründung angeführt, darum geht, dass eine Datenverarbeitung „durch“ eine Niederlassung (also faktisch von ihr selbst) vorgenommen werden muss.³² Die Datenverarbeitung muss nur im Rahmen ihrer Tätigkeiten erfolgen und damit im Zusammenhang stehen.

³² EuGH, Urt. v. 13.05.2014 – C-131/12, Rn. 52 (Google Spain); EuGH, Urt. v. 01.10.2015 – C-230/14, Rn. 35 (Weltimmo); *Piltz*, K&R 2014, 566, 567.

II. § 3 – Verarbeitung personenbezogener Daten durch öffentliche Stellen

Nach § 3 BDSG-E ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Mit § 3 BDSG-E möchte der Gesetzgeber eine Rechtsgrundlage entsprechend den Vorgaben der Art. 6 Abs. 3 S. 1, Art. 6 Abs. 1 lit. e) DSGVO schaffen. Nach Art. 6 Abs. 3 S. 2 DSGVO muss der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt oder hinsichtlich einer Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich sein. Diese Voraussetzungen sind in § 3 BDSG-E nicht in Gänze erfüllt. Denn eine Verarbeitung soll danach bereits zulässig sein, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Kein Bezug wird auf die „öffentlichen Interessen“ genommen. Grundsätzlich wäre mithin eine Verarbeitung durch eine Behörde also auch dann zulässig, wenn damit eine Aufgabe wahrgenommen wird, die nicht im öffentlichen Interesse liegt.

Nicht teilen kann ich die Kritik des Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV),³³ dass § 3 BDSG-E den datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt aufheben würde. Denn auch nach § 3 BDSG-E ist die Datenverarbeitung dem Grunde nach verboten und nur zulässig, wenn bestimmte Voraussetzungen erfüllt sind. Im Übrigen sieht die DSGVO, wie oben erwähnt, einen solchen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten in Art. 6 Abs. 1 lit. e) DSGVO gerade vor.

III. § 4 – Videoüberwachung öffentlich zugänglicher Räume

Dem Wortlaut nach mutet § 4 Abs. 1 S. 1 BDSG-E wie ein exklusiver Erlaubnistatbestand an („ist nur zulässig“). Die Schaffung eigener Erlaubnistatbestände ist dem nationalen Gesetzgeber jedoch nur im Rahmen des Art. 6 Abs. 3 DSGVO gestattet, wenn es um Verarbeitungen für die in Art. 6 Abs. 1 lit. c) oder e) DSGVO bezeichneten Zwecke geht. § 4 Abs. 1 S. 1 Nr. 3 BDSG-E deckt aber auch die Datenverarbeitung durch optisch-elektronische Geräte ab, welche auf der Grundlage einer Interessenabwägung erfolgt. Für den Erlaubnistatbestand der Interessenabwägung in Art. 6 Abs. 1 lit. f) DSGVO sieht jedoch Art. 6 Abs. 3 DSGVO nicht die Möglichkeit vor, nationale Erlaubnistatbestände zu schaffen. Auch ist es dem deutschen Gesetzgeber nicht möglich, eine Legitimation der Datenver-

³³ Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 1.

arbeitung im Rahmen der Videoüberwachung über andere in der DSGVO vorgesehene Erlaubnistatbestände (etwa die Einwilligung) auszuschließen. Dem Wortlaut nach wird mit § 4 Abs. 1 BDSG-E aber gerade ein solcher Ausschluss bezweckt. Ich empfehle daher, das Wort „nur“ zu streichen und durch „insbesondere“ zu ersetzen. So wird deutlich, dass auch andere Erlaubnistatbestände eingreifen können, um die Datenverarbeitung zu legitimieren.

Der Gesetzgeber möchte in § 4 Abs. 1 S. 2 BDSG-E konkrete Vorgaben für die zu treffende Abwägungsentscheidung im Rahmen der Interessenabwägung machen. Bei der Abwägungsentscheidung sollen der Schutz von Leben, Gesundheit oder Freiheit von Personen als ein besonders wichtiges Interesse gelten. Die vorzunehmende Interessenabwägung wird damit zumindest in eine Richtung gelenkt bzw. möchte der Gesetzgeber die bei der Interessenabwägung gedanklich zum Einsatz kommende Waage bereits einseitig vorbeladen. In seinem Urteil in Sachen „Breyer“ hat der Europäische Gerichtshof festgestellt, dass die Mitgliedstaaten in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten keine anderen als die in Art. 7 der geltenden EU-Richtlinie (RL 95/46/EG) (jetzt Art. 6 DSGVO) aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Erlaubnistatbestände verändern dürfen.³⁴ Ein Mitgliedstaat kann daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt. Vorliegend dürfte man gut vertretbar argumentieren können, dass die Vorgabe in § 4 Abs. 1 Nr. 2 S. 2 BDSG-E noch nicht die Schwelle zur Unzulässigkeit einer Einschränkung der vorzunehmenden Interessenabwägung überschreitet. Denn ein Ergebnis wird nicht vorgegeben. Jedoch kann man durchaus darüber diskutieren, inwiefern mit einer solchen gesetzlichen Vorgabe noch eine unvoreingenommene und freie Interessenabwägung möglich ist.

Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind nach § 4 Abs. 2 BDSG-E durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Nach Art. 13 Abs. 1 DSGVO müssen Informationen bereits zum Zeitpunkt der Erhebung der Daten mitgeteilt werden. Der „frühestmögliche“ Zeitpunkt nach dem BDSG-E muss freilich in der Praxis nicht immer der Zeitpunkt der Erhebung selbst sein. Die Information des Betroffenen könnte nach § 4 Abs. 2 BDSG-E also, abweichend von Art. 13 Abs. 1 DSGVO, später erfolgen. Im Ergebnis wird hierdurch das Recht der Betroffenen auf Informationserteilung aus Art. 13 Abs. 1 DSGVO beschränkt. Man könnte überlegen, diese Beschränkung der Betroffenenrechte unter die entsprechende Gestattung zur Beschränkung nach Art. 23 Abs. 1 DSGVO zu fassen. Jedoch müsste dann

³⁴ EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 57 (Breyer).

geprüft werden, welche dort abschließend aufgezählten Ziele der nationalen Beschränkungsmaßnahme hier mit § 4 Abs. 2 BDSG verfolgt werden. Der Schutz von Leben, Gesundheit oder Freiheit von Personen wird in Art. 23 BDSG-E nicht genannt. Jedoch wird in Art. 23 Abs. 1 lit. i) DSGVO das Ziel des Schutzes der betroffenen Person genannt. Diesem Ziel dient wohl § 4 Abs. 1 BDSG-E. Ob jedoch auch § 4 Abs. 2 BDSG-E diesem Ziel dient, darüber lässt sich diskutieren. Denn die Information Betroffener bereits bei der Erhebung der Daten verpflichtend vorzusehen, dürfte dem intendierten Zweck des Gesetzgebers, die Videoüberwachung und damit verbundene Datenverarbeitung zu legitimieren, nicht entgegenstehen. Man sollte daher überlegen, § 4 Abs. 2 BDSG-E entsprechend anzupassen.³⁵

IV. § 17 – Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

§ 17 BDSG-E regelt die Vertretung der deutschen Aufsichtsbehörden (sowohl jene des Bundes also auch der Länder) im neu zu gründenden Europäischen Datenschutzausschuss. Diese Regelungen zur Vertretung im Europäischen Datenschutzausschuss sind insbesondere deshalb relevant, weil dieser Ausschuss in Zukunft mit einer eigenen Rechtspersönlichkeit ausgestattet sein wird und die Befugnis besitzt, bindende Beschlüsse zu erlassen (vgl. 65 DSGVO).

Nach Art. 51 Abs. 3 DSGVO bestimmt ein Mitgliedstaat, in dem mehr als eine Aufsichtsbehörde existiert (also wie in Deutschland), „*die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt*“. Dem Wortlaut nach („die Aufsichtsbehörde“) kann also nur eine Aufsichtsbehörde als gemeinsamer Vertreter im Europäischen Datenschutzausschuss bestimmt werden.

Des Weiteren sieht ErwG 119 DSGVO vor, dass ein Mitgliedstaat, in dem mehrere Aufsichtsbehörden vorhanden sind, mittels Rechtsvorschriften sicherstellen soll, „*dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Ausschuss und der Kommission gewährleistet*“.

Nach § 17 Abs. 1 S. 1 BDSG-E soll die BfDI sowohl gemeinsamer Vertreter im Ausschuss (Art. 51 Abs. 3 DSGVO) als auch zentrale Anlaufstelle für die anderen nationalen Aufsichtsbehörden (ErwG 119 DSGVO) werden. Die Vertretung erfolgt für alle deutschen Behörden also durch eine Behörde:

³⁵ So auch: Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 2.

die BfDI. § 17 Abs. 1 S. 2 BDSG-E sieht jedoch zusätzlich vor, dass ein Stellvertreter des gemeinsamen Vertreters durch den Bundesrat gewählt werden muss. Dieser Stellvertreter ist gleichzeitig Leiter einer Landesaufsichtsbehörde.

Mit Blick auf diese Regelungen wird man durchaus diskutieren können, ob, entsprechend den Vorgaben der DSGVO, tatsächlich allein eine einzige Aufsichtsbehörde bestimmt wird, die die anderen Behörden im Ausschuss vertritt. Diese Problematik muss aber insbesondere auch mit Blick auf die Vorgaben des § 17 Abs. 2 BDSG-E gesehen werden, der regelt, wann der gemeinsame Vertreter (also die BfDI) die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss an den Stellvertreter übertragen muss.

§ 17 Abs. 2 BDSG-E bestimmt, dass der gemeinsame Vertreter in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss überträgt.

Grundsätzlich stellt sich mit Blick auf die Vorgaben des Abs. 2 die Frage, ob es einen Anspruch des Stellvertreters auf Übertragung der Verhandlungsführung gibt. Was geschieht etwa, wenn es zum Streit zwischen dem gemeinsamen Vertreter und seinem Stellvertreter kommt? Dem Wortlaut der Regelung nach ist die Verhandlungsführung und das Stimmrecht allein dann zu übertragen, wenn der Stellvertreter dies verlangt. Was geschieht aber etwa in Fällen, in denen die Kompetenz der Länder betroffen ist, unter Stellvertreter die Übertragung nicht verlangt? Kann in einem solchen Fall der gemeinsame Vertreter im Namen der Aufsichtsbehörden der Länder sprechen? Kann der Stellvertreter, etwa durch die Landesbehörden verpflichtet werden, die Übertragung der Verhandlungsführung zu verlangen?

Die Regelung des § 17 Abs. 2 BDSG-E macht die Übertragung des Stimmrechts und der Verhandlungsführung zudem zum einen davon abhängig, dass eine Aufgabe betroffen ist, für welche die Länder alleine das Recht zur Gesetzgebung haben oder aber alternativ dann, wenn es sich um eine Aufgabe handelt, welche die Einrichtung oder das Verfahren von Landesbehörden betreffen. Diese letzte Alternative scheint aber nicht im Sinne einer Exklusivität für das Vorhandensein der Landeskompetenz zu sprechen. Was geschieht also etwa in Fällen, wenn im Ausschuss eine Aufgabe bzw. Materie verhandelt wird, die sowohl die Einrichtung oder das Verfahren von Landes- als auch Bundesbehörden betreffen?

Insgesamt sollte das Verfahren zwischen gemeinsamen Vertreter und Stellvertreter entweder genauer ausgestaltet und die Übertragungsvoraussetzungen für die Verhandlungsführung genauer festgeschrieben werden oder aber es sollte allein tatsächlich ein gemeinsamer Vertreter aus den Reihen der BfDI und der Landesdatenschutzbehörden festgelegt werden.

V. § 18 – Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

Nach § 18 Abs. 1 S. 1 BDSG-E arbeiten die oder der Bundesbeauftragte und die Aufsichtsbehörden der Länder (Aufsichtsbehörden des Bundes und der Länder) in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammen. Dies entspricht der Vorgabe des Art. 51 Abs. 3 DSGVO nach der, wenn in einem Mitgliedstaat mehrere Aufsichtsbehörden vorhanden sind, *„sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten“*. Danach arbeiten die Aufsichtsbehörden im Rahmen des in Abschnitt 2 (ab Art. 63 DSGVO) beschriebenen Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.

Nach § 18 Abs. 1 S. 2 BDSG-E müssen sich die Aufsichtsbehörden des Bundes und der Länder vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Kommission oder den Europäischen Datenschutzausschuss, *„frühzeitig Gelegenheit zur Stellungnahme“* geben. Fraglich ist jedoch, was konkret mit „frühzeitig“ gemeint ist. Hierzu fehlt es an genauen Vorgaben. Diesbezüglich ist insbesondere zu beachten, dass in den Art. 63 ff. DSGVO teilweise bestimmte Fristen für Stellungnahmen des Europäischen Datenschutzausschuss vorgesehen sind. So etwa in Art. 64 Abs. 3 DSGVO. Insbesondere ist auch auf die Frist von 4 Wochen in Art. 60 Abs. 4 DSGVO hinzuweisen, innerhalb derer eine betroffene Aufsichtsbehörde Einspruch gegen einen Beschlussentwurf der federführenden Behörde einlegen kann. Diese in der DSGVO vorgesehenen Fristen werden leider nicht auf das Abstimmungsverfahren zwischen den deutschen Aufsichtsbehörden übertragen. So verständlich das Absehen von der Vorgabe für konkrete Fristen gegenüber den deutschen Datenschutzbehörden ist, lässt die Offenheit der Begrifflichkeiten jedoch Interpretationsspielräume, die in der Praxis zu Unsicherheiten führen können.

§ 18 Abs. 2 S. 1 BDSG-E sieht für zwischen den Aufsichtsbehörden des Bundes und der Länder streitige Fälle vor, dass, soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vorlegt. Im Grunde wird in diesem § 18 Abs. 2 BDSG-E das Verfahren der Zusammenarbeit zwischen federführender Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden des Art. 60 DSGVO kopiert. Dieser Ansatz ist durchaus auch begrüßenswert und richtig.

Jedoch fehlt in § 18 Abs. 1 und 2 BDSG-E eine dem Art. 60 Abs. 3 S. 2 DSGVO entsprechende Regelung. Danach ist die federführende Aufsichtsbehörde dazu verpflichtet, den anderen betroffenen Aufsichtsbehörden „*unverzüglich einen Beschlussentwurf zur Stellungnahme*“ vorzulegen und zusätzlich ihren „*Standpunkten gebührend Rechnung*“ zu tragen. Die Vorlage des Beschlussentwurfs ist im § 18 Abs. 1 S. 2 und Abs. 2 S. 1 BDSG-E enthalten, wenn auch das Merkmal „unverzüglich“ fehlt. Gänzlich fehlt jedoch die Pflicht, den Standpunkten der anderen betroffenen Aufsichtsbehörden (im hiesigen Fall also anderen Landesdatenschutzbehörden) gebührend Rechnung zu tragen.

§ 18 Abs. 2 S. 2 und 3 BDSG-E sehen vor, dass für den Fall, dass sich der gemeinsame Vertreter und sein Stellvertreter „*nicht auf einen Vorschlag für einen gemeinsamen Standpunkt*“ einigen, entweder der gemeinsame Vertreter oder der Stellvertreter (wenn Landesangelegenheiten betroffen sind) einen Vorschlag festlegt.

Auch bei dieser Regelung ist jedoch unklar, welche konkreten Situationen umfasst sind, wenn davon gesprochen wird, dass Aufgaben betroffen sind, „*welche die Einrichtung oder das Verfahren von Landesbehörden betreffen*“. Soll dies bedeuten, dass es um Aufgaben geht, die allein und ausschließlich die Einrichtungen betreffen oder sollen auch solche Aufgaben umfasst sein, die die Einrichtung oder das Verfahren von Landesbehörden „auch betreffen“? Falls die zweitgenannte Alternative umfasst ist, stellt sich die Frage, warum in einem solchen Fall der Stellvertreter (also der vom Bundesrat gewählte Leiter einer Landesaufsichtsbehörde) die Letztentscheidungsbefugnis haben soll, wenn eventuell auch die Einrichtung oder das Verfahren von Bundesbehörden betroffen sind.

§ 18 Abs. 2 S. 4 BDSG-E sieht vor, dass grundsätzlich der nach den Sätzen 1-3 vorgeschlagene Standpunkt den Verhandlungen im Europäischen Datenschutzausschuss zu Grunde zu legen ist, „*wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen*“. Hinsichtlich dieser Regelung stellt sich die Frage, warum der deutsche Gesetzgeber nicht im Sinne eines Stufenverhältnisses, wie dies im Rahmen der Streitbeilegung durch den Europäischen Datenschutzausschuss in Art. 65 Abs. 2 DSGVO vorgesehen ist, zunächst eine Zweidrittelmehrheit bei der Stimmenabgabe der Aufsichtsbehörden verlangt. Dem Grunde nach handelt es sich ja bei dem in § 18 Abs. 2 BDSG-E geregelten Verfahren um nichts anderes, als das Streitbeilegungsverfahren auf europäischer Ebene im Europäischen Datenschutzausschuss nach Art. 65 DSGVO. Dort wird aber, wie beschrieben, zunächst eine Zweidrittelmehrheit verlangt, um streitige Angelegenheiten zwischen Aufsichtsbehörden zu klären und erst in einem zweiten Schritt, wenn eine Zweidrittelmehrheit nicht erreichbar ist, eine Abstimmung mit einfacher Mehrheit für aus-

reichend erachtet (vgl. Art. 65 Abs. 3 DSGVO). Vorteil dieser Regelung wäre, dass einem gemeinsamen Standpunkt mit Zweidrittelmehrheit (insbesondere nach Außen) ein deutlich robusteres Unterstützungsbild zugrunde liegen würde.

VI. § 19 – Zuständigkeiten

§ 19 BDSG-E trifft Regelungen zur innerstaatlichen Zuständigkeit der Aufsichtsbehörden des Bundes und der Länder im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII DSGVO.

Nach § 19 Abs. 1 S. 3 BDSG-E findet im Falle des Streits über die Frage, welche nationale Aufsichtsbehörde als federführende Aufsichtsbehörde agiert, *„für die Festlegung der federführenden Aufsichtsbehörde...§ 18 Absatz 2 entsprechende Anwendung“*. Diese Regelung ist in der Tat erforderlich, da die DSGVO nicht die Frage der innerstaatlichen Bestimmung der federführenden Aufsichtsbehörde im Fall des Bestehens mehrerer Aufsichtsbehörden regelt. Nach der Gesetzesbegründung (S. 92) wird auf den in § 18 Abs. 2 BDSG-E vorgesehenen Mechanismus der Mehrheitsentscheidung aller Aufsichtsbehörden verwiesen.

Ein ähnlicher Mechanismus existiert auch innerhalb des Europäischen Datenschutzausschusses (Art. 65 Abs. 1 lit. b) DSGVO). Jedoch weicht das BDSG-E hier von der DSGVO in der Weise ab, dass der entsprechende Mechanismus in der DSGVO zu der Frage, wie ein Streit über die federführende Aufsichtsbehörde entschieden werden soll, von einer Abstimmung und einer Entscheidungsfindung durch Zweidrittelmehrheit abhängig gemacht wird (vgl. Art. 65 Abs. 2 S. 1 DSGVO). Hiervon weicht die Regelung des § 19 Abs. 1 S. 3 BDSG-E ab, indem sie allein die einfache Mehrheit ausreichen lässt. In der Konsequenz bedeutet dies, dass bereits eine Stimme den Ausschlag darüber gibt, welche Behörde innerhalb Deutschlands als federführende Aufsichtsbehörde gilt. Für mehr Sicherheit in der Praxis und um nach einer Wahl weitere Zwistigkeiten zwischen den Behörden möglichst zu begegnen, würde es sich anbieten, wenn man eine Zweidrittelmehrheit festschreiben würde. Freilich kann dies auch bedeuten, dass die Entscheidungsfindung schwieriger wird.

VII. § 21 – Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission

§ 21 BDSG-E ist Folge des EuGH-Urteils zur Ungültigkeit der Safe Harbor-Entscheidung der Europäischen Kommission.³⁶ Dort hatte der Gerichtshof geurteilt, dass der nationale Gesetzgeber

³⁶ EuGH, Urt. v. 06.10.2015 – C-362/14 (Schrems).

Rechtsbehelfe vorsehen muss, die es nationalen Kontrollstellen ermöglichen, die von ihnen als begründet erachteten Rügen gegen Angemessenheitsentscheidung der Kommission (wie etwa derzeit das EU-US Datenschutzschild) vor den nationalen Gerichten geltend zu machen. § 21 BDSG-E beruht dem Grunde nach auf einem Antrag des Landes Hamburg im Bundesrat.³⁷ Der damals vorgeschlagene Gesetzesentwurf enthielt noch einige kritische Regelungen.³⁸ Diese wurden in dem nun vorliegenden Entwurf verbessert.

Grundsätzlich zu beachten ist bei einer solchen Regelung zu einem Rechtsbehelf gegen Angemessenheitsbeschlüsse der Europäischen Kommission (dabei handelt es sich um für die Behörden bindende Beschlüsse), dass die Feststellung der Ungültigkeit eines solchen Unionsrechtsaktes allein durch den EuGH erfolgen darf.³⁹ Aus diesem Grund wird in § 21 BDSG-E auch nicht die Möglichkeit vorgesehen, dass das Bundesverwaltungsgericht die Ungültigkeit eines Angemessenheitsbeschlusses feststellen kann. Nach § 21 Abs. 6 S. 3 BDSG-E ist das Bundesverwaltungsgericht bei vorhandenen Zweifeln über die Gültigkeit eines Angemessenheitsbeschlusses dazu verpflichtet, die Frage der Gültigkeit im Wege des Vorabentscheidungsersuchen (Art. 267 AEUV) dem Europäischen Gerichtshof vorzulegen. Zu der in § 21 BDSG-E vorgesehenen Prüfung der Gültigkeit eines Angemessenheitsbeschlusses der Europäischen Kommission sind die nationalen Gerichte befugt.⁴⁰ Jedoch dürfte weder das Bundesverwaltungsgericht noch eine Datenschutzaufsichtsbehörde die Ungültigkeit eines Angemessenheitsbeschlusses feststellen.⁴¹ Die vorgesehene Möglichkeit für das Bundesverwaltungsgericht, die Gültigkeit des Angemessenheitsbeschlusses der Europäischen Kommission selbst festzustellen, ist rechtlich jedoch nicht zu beanstanden und wurde so vom EuGH auch schon bestätigt.⁴² Mit einer Entscheidung, dass der europäische Rechtsakt in vollem Umfang gültig ist, stellt ein nationales Gericht nämlich die Existenz des Gemeinschaftsrechtsakts nicht infrage.

Nicht völlig deutlich wird jedoch, welche verwaltungsgerichtliche Klageart in § 21 Abs. 1 BDSG-E angesprochen ist. Nach Abs. 1 „*hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen*“. Es wird jedoch nicht spezifiziert, worauf genau dieser Antrag inhaltlich gerichtet sein muss, also etwa auf Feststellung der Gültigkeit/Ungültigkeit oder aber Prüfung der Gültigkeit/Ungültigkeit oder Vorlage an den Europäischen Gerichtshof. In § 21 Abs. 6 S. 1 BDSG-E wird auf § 47 Abs. 5 S. 1 VwGO verwiesen, bei dem es um die Normenkontrolle und um

³⁷ BR Drs. 171/1/16.

³⁸ Vgl. hierzu: *Piltz*, Bundesrat: Gesetzesvorschlag für ein neues Klagerecht der Datenschutzbehörden gegen Privacy Shield, abrufbar unter: <https://www.delegedata.de/2016/05/bundesrat-gesetzesvorschlag-fuer-ein-neues-klagerecht-der-datenschutzbehoerden-gegen-privacy-shield/>.

³⁹ EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 61 (Schrems).

⁴⁰ EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 62 (Schrems).

⁴¹ EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 62 (Schrems).

⁴² EuGH, Urt. v. 10.01.2006 – C-344/04, Rn. 29 (IATA und ELFAA).

ein „Antrag über die Gültigkeit“ von Satzungen oder Rechtsverordnungen geht. Aus dieser Gesamtschau kann sich ergeben, dass der Antrag tatsächlich auf die Gültigkeit Bezug nehmen muss. Wünschenswert wäre jedoch eine Klarstellung.

VIII. § 22 – Verarbeitung besonderer Kategorien personenbezogener Daten

Wie auch derzeit gilt für die Verarbeitung besonders „sensibler“⁴³ Daten, die besonderen Kategorien personenbezogener Daten, ein Verarbeitungsverbot, das nur in eng begrenzten Ausnahmefällen (vgl. Art. 9 Abs. 2 DSGVO) durchbrochen werden darf. Diese personenbezogenen Daten dürfen nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in der DSGVO dargelegten besonderen Fällen zulässig.⁴⁴ Hierbei ist zu berücksichtigen, dass der europäische Gesetzgeber es ausdrücklich gestattet, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt werden können, um die Anwendung der Bestimmungen der DSGVO anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist.⁴⁵ Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sind aber stets die allgemeinen Grundsätze und andere Bestimmungen der DSGVO zu beachten.

Solche „besonderen Datenschutzbestimmungen“ sieht der deutsche Gesetzgeber in § 22 BDSG-E vor. Er nutzt zulässigerweise die ausdrücklichen Regelungsmöglichkeiten der Art. 9 Abs. 2 lit. b), lit. h), lit. i) und lit. g) DSGVO, um die Vorgaben der DSGVO an das nationale Recht anzupassen.

In § 22 Abs. 2 S. 1 und 2 BDSG-E setzt der Gesetzgeber das Erfordernis um, entweder „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ oder „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen. Hinsichtlich der Vorgabe in § 22 Abs. 2 S. 2 Nr. 1 BDSG-E („technisch organisatorische Maßnahmen“) ist jedoch unklar, was konkret mit dieser Formulierung gemeint ist: sind es technische und organisatorische Maßnahmen oder schafft der deutsche Gesetzgeber eine eigene Begrifflichkeit? Dies sollte durch eine entsprechende Ergänzung klargestellt werden.

⁴³ „Sensibel“ ist nicht als Rechtsbegriff zu verstehen, wird jedoch auch vom europäischen Gesetzgeber genutzt, um das besondere Schutzbedürfnis von Daten hervorzuheben.

⁴⁴ ErwG 51 DSGVO.

⁴⁵ ErwG 51 DSGVO.

Die Kritik des Bundesrates, dass die Pflicht zur Umsetzung von Maßnahmen zum Schutz der Rechte und Interessen der Betroffenen in § 22 Abs. 2 S. 1 BDSG-E durch eine Bezugnahme auf die Einwilligung in Art. 9 Abs. 2 lit. a) DSGVO erweitert werden sollte,⁴⁶ teile ich nicht. Die Einwilligung als Erlaubnistatbestand wird durch den deutschen Gesetzgeber nicht in § 22 Abs. 1 BDSG-E als Ausnahme für die Verarbeitung besonderer Kategorien personenbezogener Daten näher ausgestaltet. Für eine auf der Grundlage der Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO erfolgende Datenverarbeitung gelten bereits die allgemeinen Bestimmungen und Grundsätze der DSGVO, mithin etwa auch Art. 32 DSGVO zur Sicherheit der Verarbeitung.

IX. § 24 – Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen

Im Gegensatz zum Referentenentwurf⁴⁷ wurden im vorliegenden Gesetzesentwurf die Möglichkeiten einer zweckändernden Weiterverarbeitung deutlich reduziert. Generell ist es zu begrüßen, dass der deutsche Gesetzgeber im Bereich der zweckändernden Weiterverarbeitung Gebrauch von der Öffnungsklausel in Art. 6 Abs. 4 DSGVO macht. Denn auch im geltenden Recht sind solche zweckändernden Datenverarbeitungen zulässig (vgl. 28 Abs. 2 BDSG).

Mit Blick auf eine Weiterverarbeitung für andere Zwecke ist durchaus umstritten, ob Mitgliedstaaten im nationalen Recht eine eigene Rechtsgrundlage für diese Weiterverarbeitung schaffen dürfen und ob Art. 6 Abs. 4 DSGVO eine solche Ermächtigung enthält. Für eine solche Ermächtigung spricht insbesondere der Wortlaut von Art. 6 Abs. 4 DSGVO. Dieser unterscheidet zwei Situationen: zum einen jene, wenn die Verarbeitung zu einem anderen Zweck auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten beruht und zum anderen, wenn dies nicht der Fall ist, welche Kriterien der Verantwortliche zu berücksichtigen hat, um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Der erste Teil des Abs. 4 geht davon aus, dass entweder eine Einwilligung der betroffenen Person vorliegt oder, dieser Einwilligung gleichgestellt, eine Rechtsvorschrift der Mitgliedstaaten existiert, auf der die Verarbeitung zu einem anderen Zweck beruht. Bei der Einwilligung handelt es sich unstreitig um eine Rechtsgrundlage bzw. ein Erlaubnistatbestand (vgl. Art. 6 Abs. 1 lit. a) DSGVO). In der Aufzählung des Art. 6 Abs. 4 wird die „Rechtsvorschrift der Union oder der Mitgliedstaaten“ dem Erlaubnistatbestand der Einwilligung

⁴⁶ BR Drs. 110/17 (B), S. 19.

⁴⁷ Zu den dort noch viel weitergehenden Möglichkeiten für eine Verarbeitung zu anderen Zwecken: Piltz, Referentenentwurf zum BDSG-neu – Kurzanalyse zur zweckändernden Weiterverarbeitung nach § 23 BDSG-neu, abrufbar unter: <https://www.delegedata.de/2016/11/referentenentwurf-zum-bdsg-neu-kurzanalyse-zur-zweckaendernden-weiterverarbeitung-nach-§-23-bdsg-neu/>.

gleichgestellt. Dies spricht meines Erachtens dafür, dass auch der Bezug auf die „Rechtsvorschrift“ einen Erlaubnistatbestand umfasst, der sich aus dem Recht der Mitgliedstaaten ergibt.

Art. 6 Abs. 4 DSGVO stellt gewisse Anforderungen an die nationale Rechtsvorschrift, die eine zweckändernde Weiterverarbeitung gestattet. Die Rechtsvorschrift muss eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellen. Zu diesen Zielen gehören: die nationale Sicherheit; die Landesverteidigung; die öffentliche Sicherheit; die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit; den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren; die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe; Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind; den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; die Durchsetzung zivilrechtlicher Ansprüche.

Im Ergebnis muss man, möchte man die Vereinbarkeit des vorgeschlagenen § 24 BDSG-E mit der DSGVO feststellen, prüfen, ob alle in § 24 BDSG-E aufgeführten Tatbestände diese Anforderungen erfüllen. Zudem müssen die Erlaubnistatbestände jeweils notwendig und verhältnismäßig sein, um die oben benannten Ziele zu schützen.

Nach § 24 Abs. 2 Nr. 1 BDSG-E ist die Weiterverarbeitung zulässig, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist. Diese Regelung ist von Art. 23 Abs. 1 DSGVO abgedeckt. Nach § 24 Abs. 2 Nr. 2 BDSG-E ist die Weiterverarbeitung zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche. Diese Ausnahme ist nur zum Teil von Art. 23 Abs. 1 lit. j) DSGVO abgedeckt. Dort wird auf die „Durchsetzung **zivilrechtlicher** Ansprüche“ (Hervorhebung durch den Autor) verwiesen.⁴⁸ § 24 Abs. 2 Nr. 2 BDSG-E geht jedoch dem Wortlaut nach darüber hinaus, indem allgemein „rechtliche“ Ansprüche umfasst sind und nicht nur zivilrechtliche.⁴⁹ Die Norm sollte entsprechend den Vorgaben des Art. 23 Abs. 1 lit. j) DSGVO angepasst werden.

⁴⁸ Diese Formulierung geht im Übrigen auf den Vorschlag der deutschen Delegation im Rat der Europäischen Union zurück, vgl. Ratsdokument 14270/1/14 REV 1, 24.20.2014, dort Fn. 100.

⁴⁹ So auch die Kritik des Bundesrates, BR Drs. 110/17 (B), S. 21 f.

Für nicht gerechtfertigt halte ich die Kritik des Bundesrates und den damit zusammenhängenden Änderungsvorschlag, in § 24 Abs. 1 Nr. 2 nach dem Wort „Ansprüche“ die Wörter „gegenüber der betroffenen Person“ einzufügen.⁵⁰ Weder aus dem Wortlaut des Art. 21 Abs. 1 lit. j) DSGVO noch aus den Erwägungsgründen ergibt sich, dass zivilrechtliche Ansprüche allein gegenüber der betroffenen Person bestehen sollen.

X. § 26 – Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 BDSG-E entspricht dem bekannten § 32 BDSG. In § 26 BDSG-E wird im Ergebnis für den Beschäftigtendatenschutz nur das festgeschrieben, was bisher in Deutschland gilt.

§ 26 BDSG-E stützt sich auf Art. 88 DSGVO. Dabei handelt es sich um eine fakultativ nutzbare und keine verpflichtende Öffnungsklausel. Nach Art. 88 Abs. 1 DSGVO können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext“ vorsehen.

Es stellt sich jedoch die Frage, ob es sich bei § 26 Abs. 1 BDSG-E tatsächlich um „spezifischere Vorschriften“ handelt oder ob der Entwurf nicht dahinter zurückbleibt. Der europäische Gesetzgeber hatte, dies wird aus der beispielhaften Aufzählung von Verarbeitungssituationen in Art. 88 Abs. 1 DSGVO deutlich, tatsächlich Konkretisierungen der allgemeinen Datenschutzvorgaben der DSGVO für bestimmte Lebenssachverhalte und damit zusammenhängende Datenverarbeitungen angedacht. So etwa für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz. Regelungen zu solch spezifischen Situationen und Verarbeitungszwecken enthält § 26 BDSG-E jedoch nicht. § 26 Abs. 1 S. 1 BDSG-E nennt nur allgemein die „Zwecke des Beschäftigungsverhältnisses“. Dieser allgemeine Zweck ist aber ohnehin von Art. 88 DSGVO vorausgesetzt, in dessen Rahmen dann speziellere Zweck und zugrundeliegende Datenverarbeitungen und damit zusammenhängende Rechte der Betroffenen festgelegt werden sollen. Möglicherweise erfüllt § 26 Abs. 1 BDSG-E also nicht die Voraussetzungen der Öffnungsklausel des Art. 88 Abs. 1 DSGVO, da eine Spezifizierung nicht im Sinne der DSGVO erfolgt. Diesbezüglich wird eine klarstellende Überarbeitung der Vorschrift angeregt.

⁵⁰ Vgl. BR Drs. 110/17 (B), S. 22 f.

Zudem gilt es auch hier die jüngste Rechtsprechung des EuGH zur Beschränkung der Verarbeitungsmöglichkeiten im nationalen Recht zu beachten.⁵¹ Mitgliedstaaten dürfen die Tragweite der Erlaubnistatbestände nicht national verändern. Zwar spricht der Wortlaut von § 26 Abs. 1 S. 1 BDSG-E nicht absolut eindeutig dafür, dass die Datenverarbeitung im Beschäftigungskontext allein zulässig sei soll, wenn die in § 26 Abs. 1 BDSG-E vorgesehenen Voraussetzungen gegeben sind. Denn es wird, anders als etwa in § 4 Abs. 1 S. 1 BDSG-E, nicht vorgeschrieben, dass die Verarbeitung „nur“ zulässig ist. Jedoch sollte der Gesetzgeber darüber nachdenken, klarstellend darauf hinzuweisen, dass mit § 26 Abs. 1 BDSG-E nicht ausgeschlossen ist, dass eine Datenverarbeitung im Beschäftigungskontext stets auf einen der Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO gestützt werden kann.

Ob der deutsche Gesetzgeber die Vorgaben der DSGVO wirklich nur „spezifiziert“ oder über eine Spezifizierung hinausgeht, könnte man im Hinblick auf die Regelung in § 26 Abs. 2 S. 3 BDSG-E in Frage stellen. Danach bedarf die Einwilligung grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der deutsche Gesetzgeber kreiert damit eine formelle Voraussetzung für die Einwilligung im Beschäftigungsverhältnis.⁵² Begründet wird diese Regelung damit, dass hierdurch die Nachweispflicht des Arbeitgebers im Sinne von Art. 7 Abs. 1 DSGVO konkretisiert werde. Jedoch erscheint fraglich, ob die Schaffung einer zusätzlichen Voraussetzung für die Wirksamkeit der Einwilligung tatsächlich noch als „Spezifizierung“ angesehen werden kann. Zudem gesteht auch der Gesetzgeber in der Begründung ein, dass es sich nicht um eine Spezifizierung im Sinne des Art. 88 Abs. 1 DSGVO handelt, sondern um eine solche des Art. 7 Abs. 1 DSGVO. Auch der Bundesrat empfiehlt die Streichung des Schriftformerfordernisses, wenn auch aus Gründen eines potentiell erhöhten bürokratischen Aufwandes.⁵³ Die gleiche Kritik lässt sich für die Vorgabe in § 26 Abs. 2 S. 4 BDSG-E vorbringen, nach dem der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären hat. Auch diese Regelung scheint über eine reine Spezifizierung der Vorschriften der DSGVO für Datenverarbeitungen im Beschäftigungsverhältnis hinauszugehen und tatsächlich eher zusätzlicher Voraussetzungen für die Datenverarbeitung aufzustellen. Die Information der betroffenen Person in Textform ist in Art. 7 Abs. 3 DSGVO nicht vorgesehen.

Für sinnvoll erachte ich den Vorschlag des Bundesrates, § 26 Abs. 1 S. 2 BDSG-E in der Weise anzupassen, dass nach den Wörtern "Zur Aufdeckung von Straftaten" die Wörter "oder anderer schwerer Verfehlungen" sowie nach den Wörtern "eine Straftat" die Wörter "oder eine andere

⁵¹ EuGH, Urt. v. 19.10.2016 – C-582/14 (Breyer); vgl. hierzu auch die Anmerkungen zu § 4 BDSG-E unter C. III.

⁵² So ausdrücklich die Gesetzesbegründung, BT Drs. 18/11325, S. 97.

⁵³ BR Drs. 110/17 (B), S. 24.

schwere Verfehlung" eingefügt werden.⁵⁴ Hierdurch würde insbesondere für die Praxis rechtliche Sicherheit bei internen Ermittlungsmaßnahmen und damit zusammenhängende Datenverarbeitungen geschaffen, ohne dass damit eine besondere Einschränkung der Betroffenenrechte verbunden wäre.

XI. § 29 – Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

In § 29 Abs. 3 S. 1 BDSG-E macht der Gesetzgeber von der Öffnungsklausel des Art. 90 DSGVO Gebrauch und beschränkt die Untersuchungsbefugnisse der Datenschutzbehörden, soweit die Inanspruchnahme der Befugnisse die Geheimhaltungspflicht verletzen würde.

Entgegen anderen Ansichten ist diese Beschränkung verhältnis- und zweckmäßig.⁵⁵ In Art. 90 Abs. 1 DSGVO sieht der europäische Gesetzgeber gerade die Möglichkeit vor, ausgewählte Untersuchungsbefugnisse (jene nach Art. 58 Abs. 1 lit. e) und f) DSGVO) zu beschränken. Ohne diese Einschränkung der Befugnisse der Aufsichtsbehörden kann es in der Praxis zu einer Kollision mit Pflichten des Geheimnisträgers kommen. Ausdrücklich nur für diesen Fall sieht § 29 Abs. 3 S. 1 BDSG-E eine Beschränkung vor. Die Ausgestaltung dieser Beschränkung in der Form eines gänzlichen Ausschlusses der Untersuchungsbefugnisse in konkreten Situationen ist von der Regelungsmöglichkeit des Art. 90 Abs. 1 DSGVO gedeckt.⁵⁶

XII. § 32 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Die Beschränkungen der Informationspflichten (§§ 32, 33 BDSG-E) stützt der Gesetzgeber auf Art. 23 Abs. 1 DSGVO. Wie auch im Fall der zweckändernden Weiterverarbeitung, sind in diesem Fall die Anforderungen des Art. 23 Abs. 1 und Abs. 2 DSGVO zu beachten.

Nach § 32 Abs. 1 Nr. 1 BDSG-E besteht die Pflicht zur Information der betroffenen Person gemäß Art. 13 Abs. 3 DSGVO (Fall der Weiterverarbeitung) ergänzend zu der in Art. 13 Abs. 4 DSGVO

⁵⁴ BR Drs. 110/17 (B), S. 23 f.

⁵⁵ Kritisch: Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 25; Unabhängigen Datenschutzbehörden der Länder: Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz!, abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/pm_der_DSBen_zum_BDSG-neu.pdf.

⁵⁶ Piltz, in: Gola, DS-GVO, 2017, Art. 90 Rn. 10.

genannten Ausnahme nicht, wenn die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person als gering anzusehen ist.

Zunächst ist darauf hinzuweisen, dass diese Beschränkung im BDSG-E sich nicht auf die „normale“ Informationspflicht nach Art. 13 Abs. 1 und 2 DSGVO bezieht, sondern spezifisch nur den Fall der Weiterverarbeitung betrifft. Dennoch ist die Beschränkung kritisch zu sehen.

Der Gesetzgeber scheint in § 32 Abs. 1 Nr. 1 BDSG-E auf den Grundgedanken des Art. 14 Abs. 5 lit. b) DSGVO („die Erteilung dieser Informationen sich als unmöglich erweist“) abstellen und diesen in den Regelungsbereich des Art. 13 DSGVO übertragen zu wollen. Es handelt sich bei den Ausnahmen des Art. 13 und Art. 14 DSGVO jedoch um strukturell unterschiedliche Situationen.⁵⁷ Art. 14 Abs. 5 DSGVO erfasst Situationen, wenn Daten nicht beim Betroffenen erhoben werden. Art. 13 DSGVO bezieht sich jedoch auf Fälle der Direkterhebung, um die es auch in der Ausnahmegvorschrift des § 32 Abs. 1 BDSG-E gehen soll. Im Endeffekt setzt sich der Gesetzgeber damit in § 32 Abs. 1 BDSG-E über die Vorgaben von Art. 13 Abs. 4 und Art. 14 Abs. 5 DSGVO hinweg.

Es hat durchaus seinen Sinn, dass die Ausnahme des Art. 14 Abs. 5 lit. b) DSGVO nicht in Art. 13 DSGVO genannt ist. Bei einer Direkterhebung beim Betroffenen soll es verständlicherweise weniger Ausnahmen von der Informationspflicht geben, denn für den Verantwortlichen ist es in dieser Situation (direkter Kontakt mit dem Betroffenen) einfacher, die Informationen zu erteilen. Dieses Prinzip unterläuft § 32 Abs. 1 BDSG-E.

Gegen die in § 32 Abs. 1 Nr. 1 BDSG-E vorgeschlagene Ausnahme spricht zudem die Systematik der DSGVO. In Art. 13 Abs. 4 DSGVO (im Fall der Direkterhebung) existiert allein eine Ausnahme (wenn der Betroffene die Informationen bereits besitzt). Diese Ausnahme gibt es auch im Art. 14 Abs. 5 lit. a) DSGVO (der Fall, wenn Daten nicht beim Betroffenen erhoben werden). Dies zeigt, dass der europäische Gesetzgeber manche Ausnahmen in beiden Situationen als begründbar und vertretbar ansah und entsprechend aufnahm, andere Ausnahmen, die alleine in Art. 14 Abs. 5 lit. b) DSGVO existieren, aber explizit nicht in Art. 13 Abs. 4 DSGVO für Situationen der Direkterhebung geltend lassen wollte.

Wie schon im Rahmen der vorgeschlagenen Regelungen zur Weiterverarbeitung (vgl. unter C. IX.), sollte auch in § 32 Abs. 1 Nr. 4 BDSG-E das Wort „rechtlicher“ durch „zivilrechtlicher“ ersetzt werden. Der Wortlaut des insoweit zu beachtenden Art. 23 Abs. 1 lit. j) DSGVO bezieht sich ausdrücklich

⁵⁷ Vgl. auch die Kritik des Bundesrates, BR Drs. 110/17 (B), S. 34 f.

allein auf „zivilrechtliche“ Ansprüche.⁵⁸ Das Abstellen auf „rechtliche“ Ansprüche würde über den in der Ausnahmegvorschrift des Art. 23 Abs. 1 lit. j) DSGVO festgelegten Regelungsbereich für nationale Vorschriften hinausgehen. Ebenfalls wie im Rahmen der Stellungnahme zu § 24 BDSG-E halte ich jedoch die Kritik und den Anpassungsvorschlag des Bundesrates, in § 32 Abs. 1 Nr. 4 BDSG-E nach dem Wort „Ansprüche“ die Wörter „gegenüber der betroffenen Person“ einzufügen, nicht für angebracht. Weder aus dem Wortlaut des Art. 21 Abs. 1 lit. j) DSGVO noch aus den Erwägungsgründen ergibt sich, dass zivilrechtliche Ansprüche allein gegenüber der betroffenen Person bestehen sollen.

XIII. § 35 – Recht auf Löschung

In § 35 Abs. 1 S. 1 BDSG-E schränkt der Gesetzgeber das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Art. 17 Abs. 1 DSGVO ein. Zwar ist eine nationale Beschränkung des Betroffenenrechts der Löschung aus Art. 17 Abs. 1 DSGVO grundsätzlich über die Regelung des Art 23 Abs. 1 DSGVO vorgesehen und möglich. Jedoch wird aus dem Gesetzesentwurf und insbesondere auch der Gesetzesbegründung nicht deutlich, welches der in Art. 23 Abs. 1 DSGVO abschließend aufgezählten Ziele mit dem Vorschlag in § 35 Abs. 1 S. 1 BDSG-E erreicht werden soll. Der Gesetzgeber verweist in der Begründung auf Art. 23 Abs. 2 lit. c) DSGVO. Dieser Verweis geht jedoch zur Begründung der Beschränkung fehl, da in Art. 23 Abs. 2 DSGVO die Anforderungen an die nationale Maßnahme festgelegt werden, jedoch nicht das in jedem Fall erforderliche Ziel, welches eine solche Maßnahme erreichen will. Diese Ziele finden sich allein in Art. 23 Abs. 1 DSGVO.

Welches der in Art. 23 Abs. 1 DSGVO genannten Ziele mit § 35 Abs. 1 S. 1 BDSG-E erreicht werden soll, bleibt unklar und es steht zu befürchten, dass mit dieser Beschränkung des Lösungsrechts keines der dort aufgezählten Ziele verfolgt wird. Der in § 35 Abs. 1 S. 1 BDSG-E benannte Grund für die Beschränkung, dass die Löschung wegen der besonderen Art der Speicherung überhaupt nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, findet sich in dieser Form nicht als Ziel in der Auflistung in Art. 23 Abs. 1 DSGVO. § 35 Abs. 1 S. 1 BDSG-E sollte vor diesem Hintergrund, um einen Verstoß gegen die DSGVO zu vermeiden, entsprechend auf eine Zielvorgabe angepasst oder gestrichen werden.⁵⁹

XIV. Einwilligung Minderjähriger

⁵⁸ So auch der Bundesrat, BR Drs. 110/17 (B), S. 35 f.

⁵⁹ So auch der Bundesrat mit einem Anpassungsvorschlag, BR Drs. 110/17 (B), S. 39 f.

Macht der deutsche Gesetzgeber, meines Erachtens dem Grunde nach durchaus berechtigterweise, von vielen Öffnungsklauseln der DSGVO Gebrauch, so wird die Regelungsmöglichkeit des Art. 8 Abs. 1 DSGVO hinsichtlich der Festlegung einer Altersgrenze bei der Einwilligung durch Minderjährige jedoch nicht genutzt. Mir ist durchaus bewusst, dass es schwierig erscheint, eine fixe Altersgrenze festzulegen, ab der davon ausgegangen werden darf, dass Minderjährige selbst über die Verwendung ihrer personenbezogenen Daten entscheiden können. Andererseits existiert hier die Möglichkeit, eine im Datenschutzrecht bisher kontrovers diskutierte und bisher letztendlich unbeantwortete Frage anzugehen. Die Festlegung einer Altersgrenze würde in diesem Bereich für Rechtssicherheit sorgen. Dass eine verbindlich gesetzliche Entscheidung zur Altersgrenze nicht auf allseitigen Zuspruch stoßen wird, dürfte klar sein. Meines Erachtens überwiegen jedoch die Vorteile, eine (insbesondere für die datenverarbeitenden Stellen, aber gerade auch die betroffenen Minderjährigen und Eltern) verbindliche Vorgabe hinsichtlich der Altersgrenze zu etablieren. Bestenfalls sollte eine solche Festlegung im gegenseitigen Einvernehmen mit europäischen Mitgliedstaaten erfolgen, um auf diese Weise einen EU-weiten Gleichlauf der Altersgrenze zu statuieren.

Falls der Bundesgesetzgeber bewusst keine Regelung zur Einwilligung Minderjähriger getroffen hat und damit implizit zu verstehen gibt, dass seiner Ansicht nach wirksame Einwilligungen erst mit Vollendung des 16. Lebensjahres abgegeben werden können (vgl. Art. 8 Abs. 1 DSGVO), sollte darüber nachgedacht werden, zumindest diese Erwägung in der Gesetzesbegründung aufzunehmen.⁶⁰ Jedoch sollte hierbei im Blick behalten werden, dass sich der deutsche Gesetzgeber in weit sensitiveren Lebensbereichen dazu entschlossen hat, eine niedrigere Altersgrenze anzusetzen. So etwa nach § 36 Abs. 1 S. 1 SGB I, wonach Personen, die das 15. Lebensjahr vollendet haben, Anträge auf Sozialleistungen stellen können. Oder in § 2 Abs. 2 Transplantationsgesetz, nach dem mit Vollendung des 16. Lebensjahres in die Organspende eingewilligt werden kann und bereits ab dem vollendeten 14. Lebensjahr ein entsprechender Widerspruch erklärt werden kann.

D. Rechtliche Würdigung einzelner Aspekte der Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680

Neben der von der Öffentlichkeit mit weitaus mehr Aufmerksamkeit bedachten DSGVO wurde gleichzeitig auch die Richtlinie (EU) 2016/680 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 (JI-RL) verabschiedet. Mit

⁶⁰ In der deutschen Literatur wird derzeit, soweit keine gesetzliche Vorgabe existiert, jedoch wohl zumeist von einer Altersgrenze von 14 Jahren ausgegangen, wobei es auf die Einsichtsfähigkeit im Einzelfall ankommt, vgl. *Schulz*, in: *Gola, DS-GVO*, 2017, Art. 8 Rn. 10.

den §§ 45 bis 85 BDSG-E setzt der deutsche Gesetzgeber die Regelungen der JI-RL gemeinsam mit den Anpassungen zur DSGVO im neuen BDSG-E um.

Erstmals wird mit der JI-RL eine Unionsregelung für Datenverarbeitungen im Bereich der Gefahrenabwehr und Strafverfolgung existieren.⁶¹ Anders als bei der DSGVO, sind die Regelungen der JI-RL zwingend durch den deutschen Gesetzgeber in nationales Recht zu überführen. Die JI-RL ist „nur“ hinsichtlich des zu erreichenden Ziels verbindlich (Art. 288 Abs. 3 AEUV). Ziele der JI-RL sind nach ErwG 93 JI-RL die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten und den ungehinderten Austausch personenbezogener Daten im Verkehr zwischen den zuständigen Behörden innerhalb der Union zu gewährleisten. Diese Ziele werden in Art. 1 Abs. 2 JI-RL noch einmal ausdrücklich wiederholt und dem deutschen Gesetzgeber damit quasi als Leitlinie bei seiner Umsetzungsarbeit mit auf den Weg gegeben.

I. Mindestharmonisierung durch die JI-RL

Im Gegensatz zur DSGVO (vgl. oben B. III.) bezwecken die Vorgaben der JI-RL nur eine Mindestharmonisierung (wenn auch auf hohem Niveau) der Datenschutzvorgaben in ihrem Anwendungsbereich. Betroffene Personen sollen damit einen unionweit einheitlichen Schutz genießen (ErwG 15 JI-RL). Mitgliedstaaten ist es aber ausdrücklich gestattet (Art. 1 Abs. 3 JI-RL), Garantien (also gesetzliche Regelungen) festzulegen, die strenger sind also jene der JI-RL (vgl. auch ErwG 15). Die Mitgliedstaaten dürfen also bei der Umsetzung der JI-RL das Schutzniveau⁶² nach oben „durchbrechen“. ⁶³ Diese Möglichkeit der Schutzniveauerhöhung spielt auch im Rahmen des hier vorliegenden Gesetzesentwurfs eine Rolle.

II. § 46 Nr. 17 – Einwilligung

In § 46 Nr. 17 JI-RL definiert der Gesetzgeber die datenschutzrechtliche Einwilligung legal, indem er die Definition aus Art. 4 Nr. 11 DSGVO übernimmt. Die JI-RL selbst enthält keine Definition der Einwilligung, schließt sie als Erlaubnistatbestand für die Verarbeitung in ihrem Anwendungsbereich aber auch nicht aus. Dies ergibt sich aus ErwG 35 JI-RL, der Situationen benennt, in denen die Einwilligung nicht als freiwillig erteilt angesehen werden kann. Jedoch wird auch ausdrücklich darauf verwiesen, dass es Situationen geben kann, in denen die Einwilligung als Erlaubnistatbestand in

⁶¹ Kühling/Martini *et al.*, Die DSGVO und das nationale Recht, 2016, S. 5.

⁶² Wobei es meines Erachtens teilweise schwierig sein kann, datenschutzrechtliche Normen danach zu bewerten, ob das Schutzniveau gesenkt oder erhöht wird; denn es kommt bei einer solchen Bewertung, wie so oft, auf die Perspektive an.

⁶³ Stellungnahme des Juristischen Dienstes des Rates, Ratsdokument 15712/14, 18.11.2014.

Betracht kommt. Dass der deutsche Gesetzgeber hier auf die Definition der DSGVO zurückgreift, halte ich (insbesondere im Hinblick auf eine Vereinheitlichung der Anforderungen) für richtig. Nicht teilen kann ich daher die Kritik des Bundesrates, der die Übernahme der Definition aus der DSGVO mit dem Hinweis bemängelt, dass bei der Normierung von Anforderungen an eine wirksame Einwilligung der strenge Maßstab der DSGVO auf den Anwendungsbereich der Richtlinie übertragen wird.⁶⁴ Gerade wenn sich Betroffene den Strafverfolgungsbehörden gegenüber sehen und in die Verarbeitung ihrer Daten einwilligen sollen, halte ich hohe rechtliche Anforderungen für die Rechtmäßigkeit der Verarbeitung durch die Behörden für sinnvoll. Auch die Kritik, dass durch die neue Definition „noch striktere Vorgaben“ gemacht werden, verfährt nicht. Wie oben erläutert, ist es dem deutschen Gesetzgeber ausdrücklich gestattet, das Schutzniveau im Vergleich zu den harmonisierten Vorgaben der JI-RL zu erhöhen.

III. § 49 – Verarbeitung zu anderen Zwecken

In § 49 S. 2 BDSG-E regelt der Gesetzgeber die Weiterverarbeitung von zu Zwecken des § 45 BDSG-E erhobenen Daten (also jenen, die in den Anwendungsbereich der JI-RL fallen) zu anderen als in § 45 BDSG-E genannten Zwecken. Es handelt sich mithin um Zwecke, die außerhalb des Anwendungsbereichs der JI-RL liegen. Für diese Weiterverarbeitung ist grundsätzlich die DSGVO einschlägig, vgl. ErwG 34 JI-RL. § 49 S. 2 BDSG-E verweist aber nicht auf die DSGVO, sondern allein auf eine „Rechtsvorschrift“. Eventuell sollte der Gesetzgeber, wie in ErwG 34 JI-RL spezifiziert, klarstellen, dass es sich sowohl um eine nationale als auch insbesondere eine Rechtsvorschrift des EU-Rechts handeln kann.

IV. § 57 – Auskunftsrecht

In § 57 Abs. 2 BDSG-E legt der Gesetzgeber fest, wann keine Auskunft gegenüber Betroffenen erteilt werden muss. Dem Wortlaut nach („Absatz 1 gilt nicht...“) nimmt der Gesetzgeber personenbezogene Daten in bestimmten Verarbeitungssituation per se aus dem Anwendungsbereich des Auskunftsrechts heraus. Ob eine solche Herausnahme bestimmter personenbezogener Daten von der JI-RL gedeckt ist, erscheint zumindest fraglich. Selbst wenn man aber grundsätzlich von der Anwendbarkeit des Auskunftsrechts ausgeht, begegnet § 57 Abs. 2 BDSG-E Bedenken. Mit der Vorschrift wird das Auskunftsrecht in jedem Fall vollständig eingeschränkt. Eine solche vollständige Einschränkung ist grundsätzlich möglich und in Art. 15 Abs. 1 JI-RL vorgesehen.

⁶⁴ BR Drs. 110/17 (B), S. 43.

Jedoch muss die einschränkende gesetzliche Maßnahme einem der in Art. 15 Abs. 1 lit. a) bis e) JI-RL aufgeführten Zwecke dienen. Die Gesetzesbegründung zu § 57 Abs. 2 BDSG-E verhält sich aber nicht dazu, welcher Zweck mit der Einschränkung verfolgt wird. Eine Einschränkung in Fällen, in denen die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist, findet sich in der Aufzählung des Art. 15 Abs. 1 JI-RL nicht. Ich würde daher anregen, den mit der Einschränkung verfolgten Zweck i.S.d. Art. 15 Abs. 1 JI-RL genau zu bezeichnen oder aber § 57 Abs. 2 BDSG-E zu überarbeiten.

V. § 65 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten

Abweichend von Art. 30 Abs. 1 JI-RL bezieht sich der deutsche Gesetzgeber in § 65 Abs. 1 BDSG-E (und auch in anderen Regelungen) nicht auf ein „Risiko“, sondern die „Gefahr“ für Rechtsgüter natürlicher Personen. In allgemeinen Sprachgebrauch mögen diese Begrifflichkeiten synonym verwendet werden. In der Wissenschaft und Fachkreisen, werden beide Begriffe jedoch unterschiedlich verstanden und definiert.⁶⁵ Warum der Gesetzgeber vom Begriff „Risiko“ Abstand nimmt, ergibt sich aus der Gesetzesbegründung nicht. Ich schlage daher entweder die Aufnahme einer Erläuterung zur Abweichung gegenüber der JI-RL oder eine entsprechende Anpassung des § 65 BDSG-E (und auch anderer betroffener Vorschriften) vor.

VI. § 83 – Schadensersatz und Entschädigung

Meiner Auffassung nach zurecht sieht § 83 BDSG-E keine Begrenzung des Schadensersatzbetrages der Höhe nach vor. Ein solcher Höchstbetrag wird in Art. 56 JI-RL nicht festgelegt und auch nicht als Regelungsoption für die Mitgliedstaaten vorgesehen. Der Anregung des Bundesrates, im weiteren Gesetzgebungsverfahren zu prüfen, ob unter Geltung der JI-RL Spielräume für eine gesetzliche Höchstgrenze verbleiben,⁶⁶ würde ich vor dem Hintergrund eines möglichen Verstoßes gegen die Vorgaben der JI-RL nicht entsprechen. So gibt ErwG 88 JI-RL generell vor, dass Schäden, die einer Person aufgrund einer Verarbeitung entstehen, von dem Verantwortlichen oder einer anderen nach dem Recht der Mitgliedstaaten zuständigen Behörde ersetzt werden sollen. Zudem verlangt der europäische Gesetzgeber in ErwG 88 JI-RL, dass die betroffenen Personen einen vollständigen und

⁶⁵ Bundesinstitut für Risikobewertung, „Risiko“ oder „Gefahr“? Experten trennen nicht einheitlich, abrufbar unter: http://www.bfr.bund.de/de/presseinformation/2010/04/_risiko_oder_gefahr_experten_trennen_nicht_einheitlich-48560.html.

⁶⁶ BR Drs. 110/17 (B), S. 43 f.

wirksamen Schadenersatz für den erlittenen Schaden erhalten müssen. Jede Schaffung eines Höchstbetrages birgt das Risiko, dem Ziel eines „wirksamen Schadenersatzes“ entgegenzustehen.

Berlin, den 22. März 2017

Dr. Carlo Piltz



Stellungnahme

zum Gesetzentwurf der Bunderegierung

Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU
(DSAnpUG-EU)

BT-Drucksache 18/11325

erstellt von
Rechtsanwalt Andreas Jaspers,
Geschäftsführer der Gesellschaft für
Datenschutz und Datensicherheit e.V.

I. Grundsätzliches

Grundsätzlich ist Kernregelung des DSAnpUG-EU, die Neufassung des BDSG, zu begrüßen, weil es dazu beiträgt, die zu Recht kritisierte Unterkomplexität der DS-GVO durch differenzierte und am bisherigen BDSG orientierte Regelungen zu konkretisieren und praxisgerecht auszugestalten.

Ein verfassungsrechtliches Kernproblem ist die Kompetenz der Mitgliedstaaten bei der Ausfüllung von Öffnungsklauseln in der Grundverordnung. Der Entwurf legt diese Klauseln aus, um Rechtssicherheit zu schaffen. Dies ist sinnvoll, da die Zulässigkeitsnormen und die Ausgestaltung der Betroffenenrechte in der DS-GVO oftmals nur unter großem administrativen Aufwand oder gar nicht umsetzbar sind. Dem Vorwurf, die Neufassung des BDSG konterkariere den Willen der DS-GVO, lässt sich entgegenhalten, dass die „Grund“-Verordnung als neuartige Verordnungsform mit ihren zahlreichen Öffnungen und verordnungsuntypischen, sehr weiten Formulierungen, den Mitgliedstaaten gerade ermöglichen will, Konkretisierungen zu schaffen.

Der deutsche Gesetzgeber entscheidet mit der Neufassung des BDSG über wirtschaftlich und politisch sehr relevante Fragen. Damit regelt er im Rahmen der Öffnungsklauseln Sachverhalte, die ansonsten nach der DS-GVO die Datenschutzaufsichtsbehörden der EU im sehr mächtig ausgestalteten Datenschutzausschuss entscheiden würden. Den Aufsichtsbehörden fehlt jedoch weitgehend die demokratische Legitimation für Entscheidungen zur Datenverarbeitung von grundsätzlicher Bedeutung. Die Entscheidungen des Datenschutzausschusses kann in Regel abschließend erst der EuGH überprüfen. So gesehen schafft der Ansatz des Entwurfs der Bunderegierung neben Rechtssicherheit in der Anwendung der Normen in Deutschland zumindest im Anwendungsbereich des Rechts innerhalb der Öffnungsklauseln auch mehr demokratische Legitimation.

II. Zu Vorschriften in der Neufassung des BDSG

1. Zulässigkeit der Datenverarbeitung

Zur Zweckänderung

Die Regelung des § 24 BDSG-E gestattet nicht öffentlichen Stellen, unter bestimmten Voraussetzungen die Verarbeitung personenbezogener Daten über die restriktiven Kompatibilitätsanforderungen des Art 6 Abs. 4 DS-GVO hinaus zu einem anderen Zweck, als zu demjenigen, zu dem die Daten erhoben wurden.

Die Nummern 1 und 2 des Abs. 1 (Gefahrenabwehr, Geltendmachung rechtlicher Ansprüche) bilden hierbei im Wesentlichen die bestehende Rechtslage ab.

Eine Begrenzung der Nr. 2 auf zivilrechtliche Ansprüche des Verantwortlichen, die vom Bundesrat vorgeschlagen wird (BR-Drs. 110/17 Nr. 21), greift zu kurz. Interessengerecht ist es, Verantwortliche zu berechtigen, auch bei öffentlich-rechtlichen Ansprüchen personenbezogene Daten zu übermitteln.

Diese Ansprüche sollten auch nicht auf Ansprüche des Verantwortlichen gegenüber der betroffenen Person beschränkt bleiben, wie es vom Bundesrat gefordert wird (BR-Drs. 110/17 Nr. 22). Da nachträgliche Datenweitergaben an Dritte in der Regel nicht mit dem Erhebungszweck kompatibel sind, bedarf es einer Regelung, die auch bei berechtigten Ansprüchen Dritter hierzu eine Rechtsgrundlage bieten. Als Beispiel können Gläubigeranfragen zur Zwangsvollstreckung oder Schadensersatzansprüche Dritter gegen eigene Arbeitnehmer genannt werden. Grenzen der Weiterverarbeitung werden im Regierungsentwurf des § 24 Abs. 1 BDSG-E durch die Interessenabwägung gesetzt.

Zum Beschäftigtendatenschutz

§ 26 BDSG-E setzt die in Art. 88 DS-GVO enthaltene Öffnungsklausel für Datenverarbeitungen im Beschäftigungskontext um. Dieses ist als Schritt zu mehr Rechtssicherheit zu begrüßen. Mit der bisher ergangenen arbeitsgerichtlichen Rechtsprechung und dem umfangreichen Schrifttum ist ein stabiles Fundament für die zukünftige Rechtsanwendung gelegt.

In der Kommunikation mit den Beschäftigten sollte der zunehmenden Bedeutung von digitalen Arbeitsabläufen Rechnung getragen werden und deshalb die Textform statt Schriftform in Absatz 2 bei der Einwilligung als Voraussetzung normiert werden.

Die in § 26 Abs. 3 BDSG-E enthaltene Regelung zur Verarbeitung sensibler Daten im Beschäftigungsverhältnis zur Erfüllung gesetzlicher Pflichten sollte zur Klarstellung auch den Zweck „Pflichten aus dem Steuerrecht“ als Rechtfertigungsgrund aufnehmen, da z.B. die Verarbeitung von Daten über den Familienstand und die Religionszugehörigkeit im Rahmen des Beschäftigungsverhältnisses gewährleistet bleiben muss.

Klarstellende Bedeutung hat auch die Regelung in § 26 Abs. 4 BDSG-E, wonach die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch auf der Grundlage von Kollektivvereinbarungen zulässig bleibt. Dies entspricht auch Erwägungsgrund 155 DS-GVO.

Zu Datenübermittlungen an Auskunftseien und zum Scoring

Die Regelung in § 31 BDSG-E nimmt die Vorschriften des derzeit geltenden BDSG auf (§§ 28a, 28b BDSG). Der Rekurs auf etablierte Verfahrensweisen als Schritt zu mehr Rechtssicherheit - sowohl zugunsten der Betroffenen als auch der verantwortlichen Stellen - ist zu begrüßen.

2. Pflichten der Verantwortlichen

Zu den Transparenzpflichten

§ 33 Abs. 1 Nr. 2 lit. a BDSG-E schränkt die Pflicht zur Information der betroffenen Person bei Zweckänderungen ein, sofern die Informationserteilung voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Dies ist praxisgerecht, da anderenfalls investigative Maßnahmen bei Verdacht auf kriminelle Handlungen dem Betroffenen angekündigt werden müssten.

Zusätzlich sollten die bisherigen Ausnahmeregelungen des § 33 Abs. 2 Nr. 2, Nr. 7a, und 7b, 8a und 8b BDSG zu gesetzlichen Aufbewahrungspflichten und zur Übernahme von Daten aus öffentlichen Quellen übernommen werden. Viele Unternehmen (z.B. Kreditinstitute) sind aufgrund der Vorgaben zur Compliance und zur Geldwäschebekämpfung gehalten, Daten auch aus öffentlichen Quellen zu erheben. Eine Unterrichtung der davon Betroffenen könnte im Spannungsfeld zu den Zwecken Compliance und Geldwäschebekämpfung stehen. Deshalb sollten diese bisherigen Ausnahmetatbestände fortgeführt werden, zumindest bei Verfolgung der genannten Zwecke.

Zur Auskunft

Die in § 34 Abs. 1 BDSG-E vorgesehenen Ausnahmen zur Auskunft knüpfen an den heutigen § 33 Abs. 2 BDSG an und nehmen Daten von der Auskunftspflicht aus, die nur aufgrund von Aufbewahrungsvorschriften gespeichert sind. Diese Daten sind zu sperren, d.h. aus dem produktiven Datenbestand zu entfernen und ggfs. zu archivieren. Bei gesetzlichen Aufbewahrungsvorschriften ergibt sich

dies aus § 35 Abs. 1 i.V.m. Art. 17 Abs. 3 DS-GVO, bei satzungsmäßigen oder vertraglichen Aufbewahrungsvorschriften aus der Pflicht zum Ausschluss der Verarbeitung durch geeignete technische und organisatorische Maßnahmen gem. § 24 Abs. 1 Nr. 2 BDSG-E. Weder für das Unternehmen noch für den Betroffenen haben diese gesperrten Daten eine persönlichkeitsrechtsbeeinträchtigende Wirkung. Eine zweckwidrige Weiterverarbeitung dieser gesperrten Daten unter Bußgeldbewährung ist im Gegensatz zur Darstellung des Bundesrates nicht zu befürchten. Das Auskunftsrecht auch auf nur aufbewahrungspflichtige Daten zu erweitern, würde einen unverhältnismäßigen Aufwand bedeuten. Dasselbe gilt für Daten, die nur zu Zwecken der Datensicherung oder Datenschutzkontrolle gespeichert sind (siehe nachfolgend).

Zur Löschung

Das Recht auf Löschung wird in § 35 BDSG-E auf die Sperrvorschriften des § 35 Abs. 3 BDSG zurückgeführt. Insofern wird aus der Einschränkung der Verarbeitung nach Art. 18 DS-GVO, die nur als Betroffenenrecht ausgestaltet ist, eine ergänzende Pflicht des Verantwortlichen. Praxisrelevanz hat dieser Rückgriff auf das BDSG z.B. bei der Datensicherung. Sämtliche, z.T. umfangreiche Tages-, Wochen- und Monatssicherungen müssten für ein zu löschendes Datum mit großem administrativen Aufwand der IT korrigiert werden. Dies wäre unverhältnismäßig. Konsequenz ist insofern auch die Beibehaltung der Sperrpflicht nicht nur bei gesetzlichen (Art. 17 Abs. 3 lit. b DS-GVO), sondern auch bei vertraglichen oder satzungsmäßigen Aufbewahrungspflichten. Dadurch werden Pflichtenkollisionen vermieden.

Ein weiterer Gesichtspunkt von Praxisrelevanz dieser Vorschrift ist Gestaltung von Datenbanken. Dort sind Daten mit unterschiedlichen Zweckbestimmungen aus Gründen der referenziellen Integrität miteinander verknüpft. Eine Teillöschung ist deshalb bei Standardanwendungen aufgrund ihrer Architektur systemtechnisch nicht möglich. Für diesen Fall muss ebenfalls eine Berufung auf § 35 BDSG-E möglich sein.

3. Aufsichtsbehörden und Sanktionen

One-stop-shop in Deutschland

Wie auch vom Bundesrat unter Ziffer 12 zu § 19 BDSG-E (vgl. BR-Drs.110/17) vorgeschlagen, sollte der „one-stop-shop“-Ansatz der DS-GVO auch bei innerstaatlichen Sachverhalten mit bundesweiter Bedeutung etabliert werden. Denn für grenzüberschreitende Sachverhalte innerhalb der Europäischen Union gelten spezielle Bestimmungen zur grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden (vgl. Artikel 56 und 60 ff. DS-GVO). Dementsprechend sollte § 19 BDSG-E wie vom Bundesrat vorgeschlagen ergänzt werden, um eine Regelung zur federführenden Zuständigkeit einer Datenschutzbehörde in den Fällen zu erhalten, in denen Aufsichtsfragen über die Grenzen eines Bundeslandes hinaus Bedeutung haben (z.B. bundesweit agierende Unternehmen oder länderübergreifend einheitlich nutzbare Produkte).

Akkreditierung von Zertifizierungsstellen

Eine klare Zuständigkeitsregelung für die Durchführung der Akkreditierung ist zu begrüßen. Da die Zertifizierung in der DS-GVO eine zentrale Position einnimmt, ist es wichtig, die Akkreditierungshürde und die daraus entstehenden Kosten für die mittelständische Wirtschaft im Blick zu halten und von einer Überregulierung Abstand zu nehmen.

Der in § 39 BDSG-E vorgeschlagene zweistufige Akkreditierungsweg über die Deutsche Akkreditierungsstelle GmbH (DAkkS) und die zuständige Datenschutzaufsichtsbehörde führt aber zu mehr Bü-

rokratie und Kosten für die zu zertifizierenden Unternehmen. In der Sache erscheint dieser Weg auch nicht notwendig zu sein, denn Art. 43 Abs. 1 DS-GVO sieht ausdrücklich eine einstufige Akkreditierung bei einer Datenschutzaufsichtsbehörde vor.

Stand bei der Errichtung einer deutschen Akkreditierungsstelle Produktprüfungen im Vordergrund (Erg. 48 VERORDNUNG (EG) Nr. 765/2008), so handelt es sich beim Datenschutz in erster Linie um eine Prüfung von Abläufen. Insofern hängt die Prüfqualität von dem verwendeten Prüfstandard ab und nicht von der Arbeit im "Laboren". Dazu haben die deutschen Datenschutzaufsichtsbehörden selber umfassendes Know-how aufgebaut, belegt durch Projekte wie z.B. das „Datenschutzsiegel in Nordrhein-Westfalen“, „Gütesiegel Datenschutz M-V“ und die Arbeiten des ULD. Insofern erscheint eine einstufige Akkreditierung direkt bei den Datenschutzaufsichtsbehörden sachgerechter und im Interesse von bezahlbaren Zertifikaten auch für die mittelständische Wirtschaft geboten.

Zu den Sanktionen

Die Art. 33 und 34 DS-GVO verpflichten den Verantwortlichen zur Meldung von Datenschutzvorfällen. Zugleich garantieren jedoch Art. 14 Abs. 3 lit. g IPbPR und Art. 6 Abs. 1 Satz 1 MRK die Selbstbelastungsfreiheit, den sog. nemo-tenetur-Grundsatz. § 42 Abs. 4 BDSG-E und § 43 Abs. 2 BDSG-E führen deswegen die derzeit geltende Regelung in § 42a Satz 6 BDSG fort, wonach solche Meldungen nicht in Bußgeld- oder Strafverfahren verwendet werden dürfen. Die GDD begrüßt, dass dem Konflikt zwischen Meldepflicht und Selbstbelastungsfreiheit auf diese Weise Rechnung getragen werden soll.

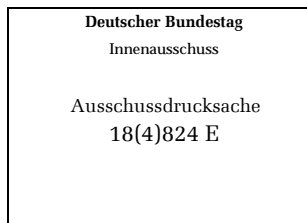
Die geplanten Vorschriften berücksichtigen jedoch nicht, dass Meldepflichtiger und Bußgeldpflichtiger nicht identisch sein müssen. Ist der Verantwortliche etwa eine juristische Person, kann immer noch gegen den persönlich Handelnden vorgegangen werden. Von daher ist ein weitreichendes Verwendungsverbot gesetzlich zu verankern, wie es derzeit nach herrschender Meinung in § 42a Satz 6 BDSG und § 97 Abs. 1 Satz 3 InsO interpretiert wird.

4. Zum Datenschutzbeauftragten

Begrüßenswert ist, dass die bislang geltenden Bestellvoraussetzungen für einen betrieblichen Datenschutzbeauftragten unverändert übernommen werden sollen. Mit Blick auf seine unabhängige Aufgabenwahrnehmung wurde auch der besondere Kündigungsschutz beibehalten. Ebenso wurde die besondere Schweigepflicht, die zugleich ein Schweigerecht ist, adaptiert.

Bonn, den 22.März 2017

Prof. Dr. Heinrich Amadeus Wolff
Rudolf-Ditzen-Weg 12
13156 Berlin
Tel: 030/48097948
Mobil: 0163 9012445
Fax: 030/43738903



dienstl.
Universität Bayreuth
Universitätsstr. 30
95447 Bayreuth
Mail: HeinrichWolff@t-online.de

Schriftliche Stellungnahme zu dem Gesetzentwurf 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) – BT-Drs. Drucksache 18/11325

als Vorbereitung für die öffentliche Anhörung vor dem Innenausschuss des Deutschen Bundestages am Montag, den 27. März 2017, von 10:30 bis 12:30 Uhr im Paul-Löwe-Haus, Raum E400, Konrad-Adenauer-Straße 1, 10557 Berlin

Berlin, den 23.03.2017

Die ehrenvolle Einladung des Innenausschusses erreichte mich, ohne nennenswerte Vorwarnung, am Freitag den 17. März 2017 gleichzeitig mit der Bitte, die schriftliche Stellungnahme möglichst bis zum 23. März 2017 abzugeben. Die beiliegende Bundestagsdrucksache wies zugleich einen Umfang von 134 Seiten auf. Angesichts dieser Eckdaten ist es leider nicht möglich, eine, der Bedeutung der Sache eigentlich notwendige, Stellungnahme zu allen Einzelheiten abzugeben. Die folgenden Gesichtspunkte besitzen daher etwas Selektives, wofür schon im Voraus um Nachsicht gebeten wird. Es sei erlaubt, zunächst mit einer allgemeinen Betrachtung der Struktur des Gesetzes und seiner generellen Rechtfertigung zu beginnen (I.), anschließend einige übergreifende Fragen anzusprechen (II.), um dann auf eine Auswahl von Einzelproblemen überzuwechseln (III.).

I. Allgemein

1. Besonderheiten

Der vorliegende Gesetzentwurf zeichnet sich in mehrfacher Hinsicht aus:

- Zunächst setzt er Unionsrecht um, aber nicht eine Richtlinie, sondern eine Verordnung, die aber aufgrund zahlreicher Öffnungsklauseln konkretisierungsfähig und konkretisierungsbedürftig ist. Gleichzeitig ist die Verordnung aber auch an anderen Stellen einerseits so vage (hinsichtlich der Rechtsgrundlagen) und an anderen Stellen wieder so strikt (hinsichtlich der Betroffenenrechte, der technischen und organisatorischen Pflichten für den Verantwortlichen und hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten), dass es einem förmlich unter den Nägeln brennt, im Rahmen der Öffnungsklauseln auch in einem Aufwasch, das Unionsrecht etwas zu korrigieren, was unionsrechtlich aber unzulässig ist.
- Weiter bildet das Datenschutzrecht eine Querschnittsmaterie, die fast die gesamte Rechtsordnung erfasst. Werden hier Fehler gemacht, können entweder ganze Wirtschaftsbereiche erheblich leiden bzw. die Normunterworfenen in die Illegalität getrieben werden oder umgekehrt die Privatsphäre einer Vielzahl von Personen schlimmstenfalls irreparabel beeinträchtigt werden.
- Drittens stehen sich oftmals grundrechtsgeprägte Sichtweisen und wirtschaftlich geprägte Interessen unversöhnlich gegenüber.

All dies führt dazu, dass faktisch jede vernehmbare Stimme „etwas am Gesetzentwurf zu meckern“ hat, weil das Umsetzungsrecht zu weit bzw. nicht weit genug geht, dass Unionsrecht nicht halbherzig oder zu engstirnig befolgt, die Grundrechte oder alternativ die Wirtschaftsbelange zu gering beachtet werden oder die in der Verordnung enthaltene Vorgabe so unsinnig sei, dass man sie ignorieren müsse. So ist es schon ungewöhnlich, dass es erstens drei Referentenentwürfe zu einem Gesetz gibt (August 2016, November 2016 und Januar 2017) und darüber hinaus der Bundesrat einen schier nicht enden wollenden Änderungskatalog vorgelegt hat (BR-Drs. 110/17), der nach Einschätzung des Unterzeichners teilweise auf ganz unterschiedlichen Wertungen (einmal grundrechtsbetont, dann wirtschaftsbetont dann wieder exekutivorientiert) zu sein scheint.

Aus der Sicht eines Außenstehenden ist die Aufregung nicht so recht nachvollziehbar. Der Entwurf zum DSAnpUG-EU macht aus den vorgegebenen Situationen mit das Beste, was möglich war.

2. Ausprägung des Gesetzes

Der Entwurf ist dabei von folgenden Eckpunkten geprägt:

- Bis Mai 2018 muss das BDSG geändert werden. Die Vorstellung, man könne trotz der Datenschutz-Grundverordnung alles beim Alten belassen, um abzuwarten, was komme, stünde einem juristisch unverantwortlichen Blindflug gleich. Aus diesem Grund sieht der Entwurf ein Inkrafttreten auch erst ab Mai 2018 vor.
- Der Gesetzentwurf enthält ganz überwiegend Normen, die Fragenkreise behandeln, die durch das Recht der Mitgliedstaaten unionsrechtlich behandelt werden müssen; über das „Wie“ kann man sicherlich an vielen Stellen streiten, das „Ob“ dürfte aber nicht ernsthaft bestreitbar sein. Gewissermaßen nicht zwingend sind die Regeln zu dem rein nationalen Raum und zu den Verarbeitungsregeln, bei denen von einer echten Öffnungsklausel Gebrauch gemacht wird und die gewissermaßen aus dem alten BDSG hinübergenommen werden, die da etwa sind § 31 BDSG und § 42 f BDSG.
- Der Entwurf lebt von folgenden Grundstrukturen:
 - soweit es geht, orientiert sich der Neuentwurf an alten Regelungen des BDSG;
 - er nimmt die Vorrangigkeit des Unionsrechts ernst und bildet eine aus sich heraus unvollständige Rechtsgrundlage – der Kodifikationscharakter ist dahin;
 - er macht von den Öffnungsklauseln selbstbewusst, aber nicht flächendeckend Gebrauch;
 - er zögert nicht, das Unionsrecht auch in den Teilen beim Wort zu nehmen, die uns bisher fremd waren, z.B. die kategorische Trennung von Zweckänderung und kompatible Verarbeitung/ die kategoriale Trennung von besonderen Datenkategorien mit den überraschenden Folgen, dass im sensiblen Bereich die Mitgliedstaaten Regelungsmöglichkeiten besitzen/ die Unabhängigkeit und Klagemöglichkeiten der Aufsichtsbehörden/ die besonderen Verarbeiter- und Betroffenenkategorien im Richtlinienbereich;
 - er versucht im Bereich der Betroffenenrechte den Verantwortlichen entgegenzukommen. Dafür ist es wiederum beim Betriebsbeauftragten strenger als es unionsrechtlich zwingend ist.
 - er enthält einige alte Regelungen, bei deren Weiterleben man durchaus etwas überrascht sein kann, wie insbesondere die Regeln zur Videoüberwachung zu Auskunftsdateien und Scoring.
 - nicht immer erscheint er in sich ausgewogen, so sind etwa die Regelungen zum betrieblichen Datenschutzbeauftragten ausführlicher als sie unionsrechtlich sein

müssten, während bei den allgemeinen Regeln zur Aufsichtsbehörde das nationale Recht sich wieder enthalten zeigt.

- Der Gesetzentwurf enthält eine klare Struktur. Es gibt vier Teile. Einen Teil für den Bereich der Verordnung, einen Teil für den Bereich der Richtlinie Inneres und Sicherheit, einen Teil für den verbleibenden nationalen Bereich und einen allgemeinen Teil für alle. Die Struktur dieses Gesetzes zeugt von einer dogmatischen Klarheit, die von wissenschaftlicher Seite nicht nur überzeugt, sondern angenehm überrascht. Offen gestanden war ich persönlich überrascht, dass die Ministerialbürokratie so etwas Schönes hervorbringen kann. Ich hatte damit gerechnet, dass nur die Grundverordnung ausgefüllt wird und ansonsten nichts aufgenommen wird. Aus meiner Erfahrung als Sachverständiger kenne ich selten so systematisch überzeugende Ansätze.

3. Die Systematik des BDSG-E

Im Einzelnen gilt:

a) Verordnungsteil

Der Teil der Datenschutz-Grundverordnung enthält Regeln, die unstreitig notwendig sind, wie die nationale Ausgestaltung der Aufsichtsbehörden, die Abstimmung für den Vertreter im Datenschutzausschuss, die Installierung des betrieblichen Datenschutzbeauftragten oder mehr als nahe liegend, wie die Relativierung der Rechte der Betroffenen. Es wird wegen Art. 6 Abs. 3 VO (EU) 2016/679 (im Folgenden: DS-GVO) im öffentlichen Bereich noch weiteren bereichsspezifischen Datenschutz geben und wegen Art. 6 Abs. 1 lit. e) DS-GVO in Verbindung mit Art. 6 Abs. 3 DS-GVO auch im privaten Bereich. Die Notwendigkeit eines weiteren bereichsspezifischen Datenschutzes ändert aber nichts an dem Erfordernis, die allgemeinen Fragen der Verordnung an einer zentralen Stelle zu regeln, auch schon deshalb, weil dort teilweise andere Dinge geregelt werden dürften, wie etwa die Rechtfertigung der Verarbeitung und Hürden für die Weitergabe und spezifische Speicherbedingungen, sowie Löschungsfristen. Auch soweit sie die gleichen Fragen regeln wie der Teil zwei des BDSG bleibt es dennoch sinnvoll, zunächst das BDSG zu erlassen, weil dann die spezifischen Regeln sich auf das beschränken können, was abweichend von der allgemeinen Regel notwendig ist. Es entspricht einer allgemeinen gesetzgeberischen Logik, zunächst den allgemeinen Teil einer Kodifikation zu formulieren und erst anschließend den besonderen Teil.

b) Umsetzung der Richtlinie

Man könnte darüber streiten, ob die Richtlinie einen eigenen allgemeinen Teil benötigt oder nicht die Realisierung in den Sicherheitsgesetzen genügt. Die Aufnahme in das BDSG erscheint aber richtig. Die Umsetzung zur Richtlinie kann sich nicht auf Änderungen in den Sicherheitsgesetzen beschränken, weil unklar ist, wie die Richtlinie genau von der Datenschutz-Grundverordnung abzugrenzen ist und es daher einer Auffangregelung bedurfte. Auch hier bleibt zudem der Gedanke, dass es sinnvoll ist, identische Regelungsstrukturen auch in einem allgemeinen Gesetz zusammenzufassen.

c) Rein nationaler Raum

Am Wichtigsten erscheint aber der Hinweis, dass es auch weiterhin zwingend einen rein nationalen Bereich geben wird, der nach menschlichem Ermessen sich als ein Teil des öffentlichen Bereichs darstellen wird. Dieser verbleibende nationale Teil folgt schon aus der begrenzten Kompetenz des Unionsrechts. Art. 16 AEUV gibt der Union für Handeln der Mitgliedstaaten im Datenschutzbereich eine Regelungskompetenz nur, sofern die

Mitgliedstaaten im „Anwendungsbereich des Unionsrechts“ handeln. Fraglich ist, welche Bereiche dadurch ausgeklammert werden. Unstreitig fällt heraus der Bereich staatliche Sicherheit i.S.v. Art. 4 Abs. 2 S. 3 EUV, der enger ist als der Bereich der öffentlichen Sicherheit und wohl die Bereiche Militär- und Nachrichtendienste erfassen dürfte. Auf die Wiederholung des Art. 4 Abs. 2 EU wird man den Begriff „Anwendungsbereich“ aber schon aus systematischen Gründen kaum beschränken können. Diesen nationalen Bereich regeln §§ 1-4 BDSG und § 85 BDSG nur rudimentär. Geregelt sind dort: Zuständigkeiten, Begriffsbestimmungen, behördlicher Datenschutzbeauftragter, BfDI und eine allgemeine Rechtsgrundlage.

Nicht geregelt ist aber Vieles, insbesondere etwa:

- Zulässigkeit der Einwilligung,
- Zulässigkeit der Verarbeitung bei gesetzlicher Pflicht,
- Anforderung an die Zweckänderung,
- Schutz für besondere Arten von Daten und vor Profiling,
- Datengeheimnis,
- Rechte der Betroffenen,
- technische und organisatorische Anforderungen an den Verantwortlichen ,
- Zulässigkeit der Auftragsverarbeitung.

Der Entwurf vertraut offenbar auf bereichsspezifische Regelungen. Da kein Mensch genau weiß, wo die Grenzen von Art. 16 AEUV enden, ist das Vertrauen, man werde schon eine relevante Regelung haben, durchaus gewagt. Auch wenn das Risiko nicht groß ist, dass eine Lücke entsteht, ist die gegenwärtige Fassung mit dem absoluten Torso-Charakter des rein nationalen Bereichs auch systematisch sehr ausgewogen.

Man sollte daher prüfen, ob nicht in § 85 Abs. 4 BDSG-E oder alternativ in § 86 BDSG-E neu subsidiär auf §§ 46-83 BDSG-E verwiesen wird.

Der Verweis kann nicht so falsch sein, weil es ja nur den öffentlichen Bereich von Bundesbehörden treffen kann und da die Richtlinienumsetzung nahe liegt. Man kann überlegen, die §§ 70, 72-74 BDSG-E ggf. herauszunehmen, weil sie unionsrechtliche Besonderheiten sind, die wir bisher so im nationalen Recht nicht kannten.

II. Übergreifende Fragen

1. Kompetenzfrage

a) Vertretungsregelung im EDA

Nicht ganz einfach ist die Bestimmung der Gesetzgebungskompetenz für die Regelung des Abstimmungsverhaltens der Aufsichtsbehörden untereinander und der Bestimmung des Vertreters im europäischen Datenschutzausschuss.

Die DS-GVO schafft einen Europäischen Datenschutzausschuss, in den jeder Mitgliedstaat eine Behörde entsendet. Für den Fall mehrerer nationaler Aufsichtsbehörden verpflichten Art. 51 Abs. 3 DS-GVO und Art. 68 DS-GVO mitsamt (EG 119) die Mitgliedstaaten, die erforderlichen nationalen Regelungen für den gemeinsamen Vertreter aufzustellen.

Das nationale Recht muss drei Fragen klären: (1) wer die Regeln erlassen darf, (2.) wer in dem EDA wann Deutschland vertreten darf und (3.) wie er sich vorab mit den anderen abzustimmen

hat. Die erste Frage betrifft die Gesetzgebungskompetenz, die der Entwurf im Ergebnis zutreffend beim Bund sieht und die zweite betrifft die Verwaltungskompetenz, die bei Bund und Land mit unterschiedlichen Gewichten gemeinsam liegt und bei der es daher eines kompetenzschonenden Einigungsverfahrens bedarf. Auch das setzt der Entwurf in einer denkbaren und möglichen Form um.

Der Bundesrat bemängelt, dass die Zuständigkeit des Verstreters nicht auch greift, wenn der Vollzug der Verordnung in die Landeszuständigkeit fällt. Dies wäre bei Fragen des privaten Bereichs in aller Regel der Fall. Eine entsprechende Erweiterung des § 17 Abs. 2 BDSG-E und § 18 Abs. 2 BDSG-E ist denkbar, aber nicht zwingend.

Für einen Einbezug der Vollzugszuständigkeit in die Zuständigkeit des Landesvertreters spricht:

- bei der Zuständigkeit im EDA geht es in der Regel gerade um Vollzug;
- auf Landesebene liegen die Erfahrungen im Vollzugsbereich;
- die innerstaatlich betroffenen Verwaltungskompetenzen liegen bei den Ländern.

Für eine Aufrechterhaltung der gegenwärtigen Fassung spricht:

- eine Kontinuität in der Vertretung im EDA bringt Verhandlungsvorteile;
- die Betrachtung des Bund-Land-Verhältnisses als widerstreitende Interessenlage ist verkürzt;
- im EDA geht es auch um Interessen, die Deutschland als ganzes treffen und dann ist eine starke einheitliche Anlaufstelle vom Vorteil;
- eine interne Abstimmung ist immer erforderlich, gleich ob der Gemeinsame Vertreter oder der Vertreter zuständig ist; ob der Vertreter des Landes L sich nun über die BfDI als Gemeinsame Vertreterin ärgert oder über den Hamburger Beauftragten als Stellvertreter, ist ihm eher gleich;
- die Parallelität zu Art. 23 Abs. 4 ff. GG würde aufgegeben werden.

Im Kern sind beide Wege bechreitbar und es bleibt eine politische Frage.

b) Presserecht

aa) Die Kompetenzfrage

Das gegenwärtige BDSG enthält eine Regelung zum Datenschutz im Pressewesen in § 41 BDSG. Der Gesetzentwurf enthält keine Regelung mehr. In der Gesetzesbegründung wird darauf hingewiesen, der Landesgesetzgeber sei zuständig (BT-Drs. 18/11325, S. 79). Mit dieser Zurückhaltung hinsichtlich einer presserechtlichen Regelung aus kompetenziellen Gründen steht der Gesetzgeber nicht alleine. Auch die Literatur, die sich mit der Erfüllung des Art. 85 Abs. 2 DS-GVO auseinandersetzt bzw. die sich zu Art. 9 DS-GVO geäußert hat, geht davon aus, die Regelungen, bezogen auf die Verarbeitung für journalistische Zwecke, verlangen nach einem Kompetenztitel für das Presserecht.

Bei näherer Betrachtung ist allerdings die Ansicht, dem Bund stünde keine Gesetzgebungskompetenz zu, in dieser Form nicht wirklich überzeugend. Der Unterzeichner hat die Frage der Gesetzgebungskompetenz des Bundes für das Pressewesen gemeinsam mit Johannes Weberling im Auftrag verschiedener Presseverbände in einem Rechtsgutachten geprüft, das sich gerade in der Finalisierung befindet. Die Verfasser kommen dabei zu dem Ergebnis, dass zutreffender Ansicht nach, entgegen der ganz überwiegenden Ansicht, dem Bund sehr wohl eine Gesetzgebungskompetenz für das Pressewesen zusteht und zwar kurzgefasst aus folgenden Gründen:

Sondernormen datenschutzrechtlicher Art, die den Regelungsauftrag des Art. 85 Abs. 2 DS-GVO ausfüllen, liegen im Überschneidungsbereich der Gesetzgebungskompetenzen des Bundes für den Datenschutz im privaten Bereich und im Bereich der Gesetzgebungskompetenzen der Länder für das Presserecht. Es handelt sich daher um Regelungen, die sowohl dem einen Gesetzgebungstitel als auch dem anderen zugeschrieben werden können. Als Regel für die Zuordnung einer Regelung zu einer Gesetzgebungskompetenz hat das Bundesverfassungsgericht folgende allgemeine Regelung aufgestellt:

bb) Die Zuordnung einer bestimmten Regelung zu einer Kompetenznorm geschieht anhand von unmittelbarem Regelungsgegenstand, Normzweck, Wirkung und Adressat der zuzuordnenden Norm sowie der Verfassungstradition (vgl. BVerfGE 7, 29 <44>; 28, 21 <32>; 33, 125 <152 f.>; 106, 62 <105>). Für die Auslegung hat daher auch die bisherige Staatspraxis großes Gewicht (vgl. BVerfGE 33, 125 <152 f.>; 61, 149 <175>; 68, 319 <328>; 106, 62 <105>; 109, 190 <213>). Bei der Zuordnung einzelner Teilregelungen eines umfassenden Regelungskomplexes zu einem Kompetenzbereich dürfen die Teilregelungen nicht aus ihrem Regelungszusammenhang gelöst und für sich betrachtet werden. Kommt ihre Zugehörigkeit zu verschiedenen Kompetenzbereichen in Betracht, so ist aus dem Regelungszusammenhang zu erschließen, wo sie ihren Schwerpunkt haben. Dabei fällt insbesondere ins Gewicht, wie eng die fragliche Teilregelung mit dem Gegenstand der Gesamtregelung verbunden ist. Eine enge Verzahnung und ein dementsprechend geringer eigenständiger Regelungsgehalt der Teilregelung sprechen regelmäßig für ihre Zugehörigkeit zum Kompetenzbereich der Gesamtregelung (vgl. BVerfGE 97, 228 <251 f.>).

BVerfG, Ut. v. 12.03.2008, 2 BvF 4/03, juris Rn. 80 - Hessisches Privatrundfunkgesetz

So konnte ein strafprozessuales Zeugnisverweigerungsrecht der Presse nicht auf dem Kompetenztitel der Presse durch die Länder eingeführt werden, da es sich um eine Frage des gerichtlichen Verfahrens handelte, für die eine abschließende Bundesregelung bestand. Ausschlaggebend für diese Zuordnung war die wesensmäßige und historische Zugehörigkeit des Zeugnisverweigerungsrechts zum Gebiet des Prozessrechts.

BVerfG, Beschl. v. 13.02.1974, 2 BvL 11/73, Rn. 23 f.

Ausgearbeiteter, aber inhaltlich vergleichbar ist das Verhältnis von Art. 74 Abs. 1 Nr. 11 GG zu der Kulturhoheit der Länder. Die Filmabgabe nach dem Filmförderungsgesetz durfte auf Art. 74 Abs. 1 Nr. 11 GG gestützt werden. Das Gesetz sei nach seinem objektiven Regelungsgehalt auf die Förderung der deutschen Filmwirtschaft und des deutschen Films ausgerichtet, das auch die kreativ-künstlerische Qualität des deutschen Films zum Förderziel bestimmt.

BVerfG, Ut. v. 28.01.2014, 1 BvR 1561/12 u.A., juris Rn. 102 ff., - Filmabgabe

Dabei ist Filmabgabe nur ein Beispiel von vielen;

Der Bund durch auf der Grundlage seiner Gesetzgebungskompetenz für das Recht der Wirtschaft Religionsgesellschaften in eine Abgabepflicht einbeziehen, (vgl. BVerfGE 55, 274 <309>),... auf der Grundlage der Gesetzgebungskompetenz für die öffentliche Fürsorge (Art. 74 Abs. 1 Nr. 7 GG) gesetzliche Regelungen gegen die Verbreitung jugendgefährdender Schriften treffen (vgl. BVerfGE 31, 113 <117>), die warenverkehrsbezogene Gesetzgebungskompetenz aus Art. 73 Abs. 1 Nr. 5 GG für ein bestimmte Filme betreffendes Verbringungsverbot (vgl. BVerfGE 33, 52 <60 ff.>) und die Strafrechtskompetenz aus Art. 74 Nr. 1 GG a.F. für ein Verbot der öffentlichen Vorführung pornographischer Filme gegen Entgelt nutzen (vgl. BVerfGE 47, 109 <110, 115 ff.>, ohne Thematisierung der Kompetenzfrage) und auf der Grundlage des Kompetenztitels "Sozialversicherungsrecht" (Art. 74 Abs. 1 Nr. 12 GG) das Künstlersozialversicherungsgesetz erlassen (vgl. BVerfGE 75, 108 <146>).

Vgl. BVerfG, Ut. v. 28.01.2014, 1 Br. 1561/12 u.A., juris Rn. 105 – Filmabgabe.

bb) Die Anwendung dieser Grundsätze auf die vorliegende Konstellation

Ob auf dieser Grundlage Ausnahmeregelungen für die Presse vom Bund oder vom Land zu erlassen sind, ist nicht eindeutig feststellbar. Für beide Ansichten lassen sich Argumente finden.

Für eine Zuordnung einer der Umsetzungsregeln zu Art. 85 Abs. 2 DS-GVO zu der Kompetenz der Länder spricht:

- es sollen gerade die Besonderheiten der Presse beachtet werden;
- die Norm betrifft den eigentlichen Pressebereich in Form der Verarbeitung von Informationen (sofern sie personenbezogene Daten sind);
- historisch wurde in Deutschland die Regelung dieser Art als eine Regelung zum Presserecht qualifiziert;
- die überwiegende Ansicht geht von der Zuordnung zum Presserecht aus;
- Adressaten sind die Presseunternehmen;
- die Länder sind ebenso wie der Bund unmittelbar an das Europarecht gebunden.

Für die entgegengesetzte Ansicht sprechen:

- es geht um eine Ausnahme von einer Regelungskompetenz (privater Datenschutz), für die dem Bund die Kompetenz zusteht;
- es geht zugleich um eine Ausnahmeregelung von einer Gesamtkodifikation, die einen datenschutzrechtlichen Schwerpunkt hat; es geht daher um eine Annexregelung zu einem größeren Regelungskomplex; der Bund muss aufgrund der Verordnung den Datenschutz reformieren;
- Adressat der Ausnahmeregelungen sind Wirtschaftsunternehmen (Presseunternehmen), also auch Private;
- die Regelung, die erlassen werden soll, besitzt dem Inhalt nach datenschutzrechtlichen Inhalt. Die Regelungen sind dem Gegenstand nach auf personenbezogene Daten bezogen. Der Schwerpunkt liegt auf dem Datenschutzrecht. Dies sieht man auch an der Formulierung des Art. 85 Abs. 2 DS-GVO. Es sollen Ausnahmen vom Datenschutzrecht erlassen werden. Es geht um die Berücksichtigung der Meinungsfreiheit bei der Regelung des Datenschutzes und es geht nicht um die Berücksichtigung des Datenschutzes bei den Regelungen zur Meinungsfreiheit. Nur hinsichtlich der Standards wird aufgrund der Besonderheit des Presserechts Rückgriff genommen;
- Der Bezug zum Datenschutz ist auch daran erkennbar, dass Meinungsfreiheit, Informationsfreiheit und die Spezialbereiche von Journalismus, Literatur und Kunst in einem Atemzug genannt werden, obwohl sie als Fachmaterien in den Mitgliedstaaten durchaus unterschiedlichen Gesetzgebungskompetenzen zugewiesen sein können.
- In anderem Zusammenhang hat der Bund auch Regelungen zur Verarbeitung erlassen bzw. will sie im künftigen BDSG erlassen, obwohl es um Materien geht, die der Sache nach in Landeszuständigkeit stehen (vgl. § 27 BDSG-E).

Es ist daher entgegen der herrschenden Meinung nicht wahrscheinlich, dass das Bundesverfassungsgericht eine Sonderregelung des Bundes im BDSG, zur Umsetzung von Art. 82 Abs. 2 DS-GVO wegen einer fehlenden Gesetzgebungskompetenz des Bundes für nichtig erklären würde.

cc) Keine Regelungspflicht

Eine Regelungspflicht des Bundes wird man dabei annehmen müssen, wenn nur der Bund den Regelungsauftrag aus Art. 85 Abs. 2 DS-GVO erfüllen könnte. Dies wird man aber nicht annehmen können. Die Länder besitzen ebenfalls Regelungskompetenz. Es ist durchaus möglich, dass Bund und Länder Regelungen zur gleichen Frage auf der Grundlage verschiedener

Kompetenztitel regeln können, ansonsten wäre auch die Kollisionsnorm des Art. 31 GG von einem wesentlichen Anwendungsbereich befreit.

Angesichts der überregionalen Wirkung von Poesetätigkeit wäre es allerdings schon sehr nahe liegend, wenn einheitliche Regelungen für die Verarbeitung von Daten vorlägen. Würde jetzt das Land A die alte Freistellung der Presse i.S.v. § 41 BDSG iVm Art. 85 DS-GVO übernehmen und ein anderes Land B nicht oder in substantiell anderer Form, wäre das nicht sehr glücklich.

Eine ursprünglich angenommene Gefahr des Vakuums bis zum Erlass der Landesregelungen schließt der Bund aus, indem das BDSG-E gemäß Art. 8 das BDSG alt erst mit Wirkung zum Mai 2018 aufhebt.

Vorschlag

Es wird vorgeschlagen, eine bundeseinheitliche Ausfüllung des Art. 85 DS-GVO für das Pressewesen aufzunehmen.

c) Allgemeines Polizeirecht

§ 40 Abs. 1 BDSG-E erweckt den Eindruck, weiter zu reichen, als er kompetenziell kann. § 40 Abs. 1 BDSG-E beruht auf Art. 74 Abs. 1 Nr. 11 GG. Die Kontrolle des Datenschutzes von Privaten, die Datenverarbeitung nicht zu wirtschaftlichen Zwecken verfolgen, aber dennoch in den Anwendungsbereich der Datenschutz-Grundverordnung fallen (Homepage einer Privatperson) ist darauf aber nicht zu stützen:

Beispiel: Der ehrenamtliche Mitarbeiter M. stellt Fotos des letzten Vereinstuniers auf die Homepage des Turnsportvereins. Die Interessensabwägung i.S.v. Art. 6 Abs. 1 lit. f) Verordnung geht zu Gunsten der betroffenen Person aus. Die zuständige Aufsichtsbehörde möchte M. das daher untersagen. Sie kann sich dafür nicht auf § 40 BDSG-E stützen, vielmehr ist hier Landesrecht maßgeblich, da es um allgemeines Polizeirecht geht, das hoffentlich eine ergänzende Norm vorweist.

2. Abgrenzung Verordnung – Richtlinie

Die Abgrenzung zwischen der Richtlinie Justiz und Inneres und der Datenschutz-Grundverordnung ergibt sich aus dem Unionsrecht. Aus diesem Grunde wiederholt § 45 BDSG-E den Text von Art. 1 RL 2016/680. Schwierig sind zwei Fragen:

- inwiefern gilt die Richtlinie für präventives Handeln?
- ist das Ordnungswidrigkeitenrecht Strafrecht i.S.d. Richtlinie?

§ 45 BDSG-E beantwortet die erste Frage ausdrücklich, die zweite konkludent. Datenverarbeitung zur Verfolgung von Ordnungswidrigkeiten werden vollständig erfasst, präventives Handeln nur, wenn es von Behörden vorgenommen wird, die auch für Strafverfolgung zuständig sind, d.h. von den Vollzugsbehörden nicht aber den Ordnungsbehörden. Im Umkehrschluss aus § 45 BDSG-E kann man folgern, dass die Verhütung von Ordnungswidrigkeiten nicht von § 45 BDSG-E erfasst werden soll, mit der Folge, dass die Abwehr von Gefahren für die öffentliche Sicherheit nur von solchen Behörden wahrgenommen werden kann, die gleichzeitig auch die Kompetenz haben, Straftaten zu verfolgen und zu ahnden. In der Gesetzesbegründung findet sich daher auch der Hinweis, dass die Gefahrenabwehr durch allgemeine Ordnungsbehörden, wie insbesondere den Waffenbehörden und Hygienebehörden nicht unter § 45 gefasst wird (BT-Drs. 18/11325, S. 110 f.).

Diese Auslegung des Anwendungsbereichs der Richtlinie ist, wie alles im Bereich der Konkretisierung der Datenschutzrichtlinie und der Datenschutz-Grundverordnung nicht zweifelsfrei, aber ein verhältnismäßig überzeugender Weg. Wenn der Bund sich dazu entschließt, diese Interpretation durchzuführen, läge es allerdings näher, diese Auslegung noch deutlicher im Normtext und § 45 BDSG-E zum Ausdruck zu bringen. Die Normanwender würden es dem Bund danken. Das prozessuale Risiko, das durch eine noch bestimmtere Norm eintritt, erscheint hinnehmbar.

Es wird daher vorgeschlagen bei § 45 S. 3 hinter „für die öffentliche Sicherheit“ einzufügen „durch die für die Verfolgung von Straftaten zuständigen öffentlichen Stellen“.

3. Ordnungswidrigkeitenrecht

a) Verschuldensfrage - § 41 Abs. 1 OWiG

Gemäß § 41 OWiG ist § 10 OWiG anwendbar, mit der Folge, dass das Handeln des Verantwortlichen vorsätzlich oder fahrlässig sein muss, um als Ordnungswidrigkeit zu gelten. Eine echte Zurechnungsnorm des Verschuldens der Repräsentanten kennt das OWiG aber nicht. § 30 OWiG kann zwar helfen, ist aber nicht ganz passend, weil er eine ergänzende Haftung begründet, es hier um eine originäre geht. Man sollte daher in § 41 Abs. 1 OWiG für die Verschuldenshaftung ausdrücklich auf § 30 OWiG verweisen.

Dies wäre allerdings nur möglich, wenn die Verschuldensvoraussetzungen ein zulässiges Tatbestandsmerkmal bilden. Das ist nicht ganz eindeutig, liegt aber wegen Art. 83 Abs. 8 und 9 DS-GVO und vor allem wegen EG 151 nahe. Man wird vom Begriff der Geldbuße her das Verschulden als begriffsimmanent verstehen können. Ordnungswidrigkeiten gem. Art. 83 DS-GVO setzen daher nach deutschem Verständnis Verschulden voraus. Das Strafrecht in Dänemark wird auch nicht ohne Verschuldenserfordernis auskommen.

b) Haftung der Repräsentanten

Der Referentenentwurf erstreckte die Ordnungswidrigkeitentatbestände, die für die Verantwortlichen gelten, auch auf die Angestellten. Das hat sich nicht durchgesetzt. Fraglich ist, ob die Repräsentanten einer juristischen Person über § 30 OWiG selbst haften sollen. Interpretatorisch wäre das möglich, ob das Gesetz das will, ist unklar. Hier wäre eine Klarstellung gut.

Es wird vorgeschlagen § 41 Abs. 1 BDSG-E um die Regelung zu ergänzen: Für die Zurechnung von Verschulden zu juristischen Person, die Verantwortliche oder Auftragsverarbeiter ist und für die persönlichen Haftung des Handenden gilt § 30 OWiG entsprechend.

4. Videoüberwachung

Der Bundesgesetzgeber hat in § 4 BDSG-E eine spezielle Regelung zur Videoüberwachung erlassen, die für die öffentliche Hand und Private gleichermaßen gilt. Sie ist weiter als die alte Regelung in § 6b BDSG, weil sie auch die Überwachung öffentlicher Plätze durch Private erfasst.

Eine Änderung des BDSG zur Anpassung des § 6b BDSG ist gerade im Gesetzgebungsverfahren (vgl. BT-Drs. 18/11435: Gesetz zur Änderung des Bundesdatenschutzgesetzes - Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)). Die gegenwärtige Fassung lebt davon, dass sie durch Satz 2 versucht, die Abwägungsentscheidung im Sinne von Art. 6 Abs. 1 lit. f) DS-GVO durch eine nationale gesetzgeberische Entscheidung zu beeinflussen, indem sie ein besonderes Gewicht für bestimmte Umstände vorschlägt. Dies ist offensichtlich unionsrechtswidrig. Der Gesetzgeber ist nicht der EuGH.

Der § 4 BDSG-E hat sich im Laufe des Gesetzgebungsverfahrens erheblich verändert. In dem Referentenentwurf von November 2016 war die Videoüberwachung gefährdeter Räume durch Private noch als öffentliche Aufgabe erklärt worden, so dass Art. 6 Abs. 1 lit. e) DS-GVO griff. Das war aus deutscher Sicht ungewohnt, aber aus der Sicht der Verordnung gut vertretbar und insbesondere aus systematischen Gründen für die Gesetzgebung der Länder und für die bereichsspezifische Gesetzgebung als Vorbildwirkung erheblich. Es ist systematisch wichtig, ob der nationale Gesetzgeber im privaten Bereich nur die Möglichkeit haben soll, Rechtsgrundlagen über die Interessensabwägung des Art. 6 Abs. 1 lit. f) DS-GVO hinaus in der Form zu schaffen, dass er für die Privaten Pflichten schafft. Der Gesetzgeber sollte sich die Möglichkeit offen halten, bei Aufgaben im öffentlichen Interesse, Private für eine Datenverarbeitung zu ermächtigen ohne sie dazu zu verpflichten.

Es wird vorgeschlagen § 4 BDSG-E wie folgt zu fassen:

§ 4 Videoüberwachung öffentlich zugänglicher Räume

(1) Für die Videoüberwachung öffentlich zugänglicher Räume gilt:

1. öffentliche Stellen dürfen personenbezogene Daten aus optisch-elektronischen Einrichtungen verarbeiten (Videoüberwachung), wenn es für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgaben des Verantwortlichen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.
2. nicht-öffentliche Stellen dürfen personenbezogene Daten aus optisch-elektronischen Einrichtungen verarbeiten (Videoüberwachung), wenn es zum Schutz von Leben, Gesundheit oder Freiheit von Personen erforderlich ist, die sich in öffentlich zugänglichen großflächigen Anlagen, insbesondere Sport-, Versamlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs aufhalten, und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Bei der Abwägungsentscheidung nach Satz 1 ist der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in Anlagen nach Satz 1 aufhalten, in besonderem Maße zu berücksichtigen.

5. Bonitätsauskunft und das Scoring

Eine weitere Regelung, die es „aus dem alten BDSG“ hinüber geschafft hat, sind die Regelungen zu Bonitätsauskunft und Scoring gemäß § 31 BDSG. Der Gesetzentwurf lässt offen, welche unionsrechtliche Grundlage den Mitgliedstaaten eine Konkretisierung in einem Bereich gestattet, der sonst unter Art. 6 Abs. 1 lit f) DS-GVO fallen würde. Im Referentenentwurf von

November 2016 waren Art. 6 Abs. 4 DS-GVO in Verbindung mit Art. 23 Abs. 1 der Verordnung, das heißt die Ermächtigung zur Regelung über die Zweckentfremdung, als Grund angeführt. Diese Berufung erscheint bei der Übermittlung an Auskunftsdateien zwar grundsätzlich möglich, würde aber bei der Datenverarbeitung zu Scoringzwecken nicht richtig überzeugen. Nach anderer Ansicht soll es sich bei § 31 BDSG-E um eine Verbraucherschutznorm handeln. Allein der Charakter den Verbraucherschutz zu verwirklichen, würde allerdings nicht eine Befreiung von den Anforderungen der Datenschutzverordnung ermöglichen. Die Datenschutz-Grundverordnung kennt Abgrenzungen zu anderen Richtlinien, wie etwa in Art. 95 DS-GVO, die Richtlinie zum Verbraucherschutz ist ausdrücklich nicht genannt. Die Verordnung geht davon aus, dass die Pflichten aus unionsrechtlichen Rechtsquellen grundsätzlich die Vorgaben der DS-GVO einhalten müssen. Das gilt auch für die Verbraucherrichtlinie. Art. 6 Abs. 3 DS-GVO gibt ausreichend Raum. Möglich wäre es auch hier, sich wieder auf Art. 6 Abs. 1 lit. e) BDSG-E in Verbindung mit Art. 6 Abs. 3 DS-GVO zu stützen, wenn man der Auffassung wäre, die Scoringstellen würden eine Aufgabe von öffentlichem Interesse wahrnehmen. Wenn man diese Konstruktion aber schon bei der Videoüberwachung nicht wählt, wird man sie beim Scoring kaum übernehmen können.

Es ist aus wissenschaftlicher Sicht schon erstaunlich, sich bei den Betroffenenrechten um jeden Halbsatz zu streiten, dann aber im Bereich der Bonitätsauskunft und Scoring, Verarbeitungsgrundlage von großer Tragweite mit völlig offener Rechtfertigung einfach durchzuwinken, weil der entsprechende Wirtschaftsbereich es wünscht.

Ändern wird man die Norm rein praktisch nicht mehr können, toll ist dieser unterschiedliche Umgang mit Partikularinteressen nicht.

Schön wäre es, §§ 31 BDSG-E so zu formulieren, dass die Rechtfertigung der Bonitätsübermittlung durch Art. 6 Abs. 4 i.V.m. Art. 23 DS-GVO und des Scoring durch Art. 6 Abs. 1 lit. e) DS-GVO möglich ist.

6. Verhältnis der Aufsichtsbehörden mit anderen Behörden

Das BDSG hatte die Sanktionierung der Verletzung der Datenschutzbestimmungen noch nicht in der Weise primär in die Hände der Aufsichtsbehörde gegeben, wie die Datenschutz-Grundverordnung. Die Konzentration auf die Aufsichtsbehörden in der Datenschutz-Grundverordnung erscheint unglücklich, da Datenschutzverstöße oft bei Gelegenheit der sonstigen Kontrollen auftreten. Der Gesetzentwurf nimmt das Problem in § 40 Abs. 6 BDSG-E zur Kenntnis insofern, als dass die Gewerbeordnung unberührt bleibt. Dies dürfte etwas zu eng sein. Auch das sonstige Wirtschaftsrecht im weiteren Sinne, wie etwa das Recht auf freien Beruf oder das Recht der Banken und die dort bestehenden Aufsichtsstrukturen sollten Datenschutzverstöße prüfen dürfen.

Weiter sind die anderen Behörden zur Verfolgung von Ordnungswidrigkeiten i.S.d. DS-GVO nicht zuständig, eine Erweiterung der Zuständigkeit über die Aufsichtsbehörden hinaus läge aber nahe.

Es sollte daher geprüft werden,

- ob nicht stattdessen ein Verweis in § 40 Abs. 6 BDSG-E aufgenommen wird, nachdem „die Befugnisse anderer Aufsichtsbehörden unberührt bleiben.“

- Und ob nicht die Verfolgung der Ordnungswidrigkeitentatbestände der Verordnung auch weiteren Behörden neben den Aufsichtsbehörden eröffnet werden sollte.

7. Allgemeine Verarbeitungsgrundlage

§ 3 BDSG-E schafft eine einheitliche Rechtsgrundlage für alle Bereiche, angelehnt an Art. 6 Abs. 1 lit. e) DS-GVO. In der Gesetzesbegründung wird auf Art. 6 Abs. 3 DS-GVO verwiesen (BT-Drs. 18/11325, S. 79). Legt man dies zugrunde, dann ist es systematisch aber eigentlich zwingend auch die Norm Art. 6 Abs. 1 lit. c) DS-GVO zu wiederholen.

Man sollte § 3 BDSG-E ergänzen um den Passus „oder zur Erfüllung einer rechtlichen Verpflichtung, die sie unterliegt,“ ...

Dabei könnte man auch diskutieren, die Beschränkung auf öffentliche Stellen entfallen zu lassen. Sie ergibt sich aus dem ausfüllenden Recht von selbst.

III. Einzelfragen

§ 1 Abs. 4 BDSG-E

Für die deutschen Regelungen, bei denen von Öffnungsklauseln Gebrauch gemacht wird, muss das BDSG den Anwendungsbereich festlegen. § 1 Abs. 4 BDSG-E folgt dabei, wie auch das gegenwärtige BDSG, dem Gedanken des Herkunftslandprinzips. Danach werden Verantwortliche aus anderen Mitgliedsstaaten, die keinen territorialen Anknüpfungspunkt in Deutschland haben, aus der dem Anwendungsbereich der Sondernormen herausgenommen. Dies ist sachgerecht.

§ 2 BDSG-E

Der Vorschlag des Bundesrates (BR-Drs. 110/17, S. 4), in § 2 BDSG-E den Begriff „anonymisieren“ zu definieren, wird unterstützt.

§ 6 Abs. 6 S. 3 BDSG-E

Auf Vorschlag des Bundesrates, den Begriff „Schriftstücke“ durch „Dokumente“ zu ersetzen, wird unterstützt, genauso bei § 13 Abs. 3 S. 3 BDSG-E.

§ 6 BDSG-E

Die Rechtsstellung des Datenschutzbeauftragten wird in § 6 BDSG-E konkurrierend zu Art. 38 DS-GVO geregelt. Das Bundesrecht ist dabei für den Datenschutzbeauftragten günstiger als das Unionsrecht, insbesondere weil es der Sache nach, einen Kündigungsschutz vorsieht (§ 6 Abs. 4 BDSG-E). Weiter regelt es die Vertraulichkeit gemäß § 6 Abs. 5 – Abs. 6 BDSG-E. Die detaillierte Regelung in Konkurrenz zum Unionsrecht wirft die Frage der Unionskonformität auf. Art. 37 – 39 DS-GVO enthalten keine ausdrücklichen Öffnungsklauseln. Allerdings verweist Art. 37 DS-GVO durch die ausdrückliche Sonderstellung des behördlichen Datenschutzbeauftragten konkludent

auf die Ausgestaltungsbefugnis der Mitgliedstaaten im Organisationsbereich. Weiter ist durch die Möglichkeit, in weiteren Fällen Datenschutzbeauftragte durch mitgliedstaatliches Recht zu normieren, die Materie insgesamt teilweise dem mitgliedsstaatlichen Recht eröffnet. Geht man von einer Regelungsbefugnis aufgrund der Organisationshoheit der Mitgliedsstaaten aus, dürfte der EG 8 es gestatten wiederholendes Unionsrecht aufzunehmen. Insofern ist von der Unionsrechtskonformität des § 6 BDSG-E im Ergebnis auszugehen.

§ 19 Abs. 2 BDSG-E

Das Unionsrecht sieht vor, dass der Betroffene das Recht hat, jede Aufsichtsbehörde seiner Wahl mit einer Beschwerde zu befassen und diese dann die Beschwerde bescheiden muss (Art. 77 Abs. 2 DS-GVO). Das deutsche Recht definiert diese angerufene Aufsichtsbehörde kurzerhand um, indem die Beschwerde an die zuständige Aufsichtsbehörde weitergereicht wird und dies als die angerufene Behörde definiert wird (§ 19 Abs. 2 BDSG-E).

Das BDSG-E reduziert die unionsrechtlich gegebenen Möglichkeiten gemäß § 19 Abs. 2 BDSG-E ganz erheblich. Danach muss die angerufene Aufsichtsbehörde, die nicht zuständig ist, die Beschwerde an die sachlich zuständige Aufsichtsbehörde weiterreichen. Die empfangene Aufsichtsbehörde wird dann nach deutschem Recht als die Behörde erklärt, bei der die Beschwerde eingereicht wurde. Sie muss dann die Beschwerde bescheiden. Von einer Pflicht, die gleiche Sprache zu verwenden, wie die Behörde, bei der die Beschwerde eingereicht wurde, wird man ausgehen müssen, weil ansonsten die Regelung in § 19 Abs. 2 BDSG-E die Rechte der betroffenen Person erheblich verschlechtern würde. Art. 77 DS-GVO geht erkennbar davon aus, dass die Pflichten gemäß Art. 77 Abs. 2 DS-GVO die Behörde treffen, bei der die Beschwerde eingereicht wurde. Das deutsche Recht versucht nun das Unionsrecht umzudefinieren. Auch wenn die Regelung des § 19 Abs. 2 BDSG-E sachlich vernünftig und einleuchtend ist und insofern glücklicher ist als die Regelung des Art. 77 DS-GVO, ändert § 19 Abs. 2 BDSG-E ohne erkennbaren Grund das Unionsrecht und verstößt somit gegen den Anwendungsrang des Unionsrechts und dürfte eine gerichtliche Überprüfung auf seine Unionskonformität kaum „überleben“.

Angemessene und spezifische Maßnahmen - § 22 Abs. 2 BDSG-E/ § 28 Abs. 1 BDSG-E/ § 37 Abs. 2 BDSG-E

Die Verordnung kennt an verschiedenen Stellen die Konstruktion, dass sie die Mitgliedstaaten zu nationalen Regelungen ermächtigt unter der Bedingung, dass diese dann angemessene Sicherungen zugunsten der Interessen des Betroffenen vorsehen. So etwa bei Art. 9 Abs. 2 lit. b), g), i) DS-GVO, auf die unter anderem § 22 BDSG-E gestützt wird, als auch bei Art. 9 Abs. 2 lit. j) DS-GVO, auf den § 27 BDSG-E gestützt wird, als auch bei Art. 9 Abs. 2 lit. g) DS-GVO auf den § 37 BDSG-E gestützt wird und vergleichbar bei Art. 89 Abs. 1 DS-GVO, auf den § 28 BDSG-E gestützt ist.

Der nationale Gesetzgeber garantiert diese besondere Sicherung nicht so, dass er selbst die Sicherungsmaßnahmen bestimmt, sondern den Verantwortlichen die Erfüllung dieser Voraussetzung auferlegt. Fraglich ist, ob das genügt. Da die Erfüllung dieser Tatbestandsvoraussetzung für die Rechtmäßigkeit der Wahrnehmung der jeweiligen nationalen Sonderregelungen für den Verantwortlichen ist, stellt diese Regelungstechnik im Ergebnis sicher, dass den Betroffenen die spezifischen Maßnahmen im Ergebnis zu Gute kommen oder die Verarbeitung rechtswidrig ist. Es ist daher davon auszugehen, dass diese Regelungstechnik unionsrechtlich noch hinnehmbar ist.

§ 23 BDSG-E

Das BDSG-E macht von der Ermächtigung in Form von Art. 6 Abs. 4 S. 1 i. V. m. Art. 23 DS-GVO insbesondere durch die §§ 23-25 BDSG-E Gebrauch. Dort regelt es die Verarbeitung zu anderen Zwecken durch öffentliche Stellen (§ 23 BDSG-E) durch nicht-öffentliche Stellen (§ 24 BDSG-E) als auch die Datenübermittlung durch öffentliche Stellen (§ 25 BDSG-E). Ursprünglich wollte der Gesetzgeber die Weiterverarbeitung sowohl für öffentliche als auch für nicht-öffentliche Stellen in einer Vorschrift normieren.

Das BDSG kennt in § 23 BDSG-E sieben Fallgruppen, unter denen die Zweckänderung zulässig ist. Es formuliert die Fallgruppen selbstständig und übernimmt nicht den Normtext von Art. 23 DS-GVO, darin liegt unionsrechtlich ein gewisses Risiko.

§ 25 BDSG-E

Das BDSG enthält eine Regelung zur Datenübermittlung durch öffentliche Stellen (§ 25 BDSG-E), nicht aber für private Stellen. Sicher gibt es einen Grund weshalb § 23 BDSG-E durch § 25 BDSG-E ergänzt wird, § 24 BDSG-E aber nicht durch einen § 25a BDSG-E. Leider hat sich dieser Grund dem Unterzeichner aber nicht offenbart.

Unverhältnismäßiger Aufwand - § 27 Abs. 2 BDSG-E

Der BDSG-Entwurf sieht an mehreren Stellen den Ausschluss gewisser Rechte vor, wenn die Erfüllung für den Verantwortlichen einen unverhältnismäßigen Aufwand bedeuten würde, so etwa in § 26 Abs. 1 BDSG-E am Ende (bezogen auf Öffnungsklausel Art. 88 DS-GVO), weiter in § 27 Abs. 2 S. 2 BDSG-E (bezogen auf Art. 89 Abs. 2 DS-GVO), in § 32 Abs. 1 Nr. 1 BDSG-E (bezogen auf Art. 13 DS-GVO) sowie § 34 Abs. 1 Nr. 2 BDSG-E (bezogen auf Art. 14 DS-GVO, hier allerdings mit ausdrücklicher Ermächtigung in Art. 14 Abs. 4 DS-GVO), § 35 Abs. 1 BDSG-E (bezogen auf Art. 17 DS-GVO), § 34 Abs. 1 Nr. 2 BDSG-E (bezogen auf Art. 21 Abs. 1 lit. i) DS-GVO).

Im Fall des Art. 14 DS-GVO (abgesehen von dem wohl nicht relevanten Art. 19 DS-GVO) findet sich in der unionsrechtlichen Grundlage allerdings keine ausdrückliche Ermächtigung den Aufwand zu berücksichtigen.

§ 32 Abs. 1 Nr. 1 BDSG-E

Der Rechtfertigungsgrund von § 32 Abs. 1 Nr. 1 BDSG-E ist unionsrechtlich nicht ganz deutlich. Der Gesetzentwurf nimmt dazu nicht ausdrücklich Stellung. Der Referentenentwurf im November 2016 berief sich auf Art. 14 Abs. 4 DS-GVO analog. Auch Art. 23 Abs. 1 DS-GVO dürfte kaum eingreifen. Es handelt sich daher bei dieser Fallgruppe um eine nationalrechtlich etwas gewagte Vorschrift.

§ 33 Abs. 1 Nr. 2 BDSG-E

Nach dem Referentenentwurf aus November 2016 scheint § 33 Abs. 1 Nr. 2a BDSG-E wiederum auf der Grundlage von Art. 23 Abs. 1 lit. i DS-GVO geschützt zu sein. Auch hier liegt wieder eine zwar logisch mögliche, wertungsmäßig aber großzügige Interpretation des Passus „Rechte oder Freiheiten anderer Personen“ vor.

§ 34 Abs. 1 Nr. 2 BDSG-E

§ 34 Abs. 1 Nr. 2 BDSG-E scheint nach der Begründung des Referentenentwurfs von November 2016 auf Art. 23 Abs. 1 lit. i) DS-GVO gestützt zu sein. Der Schutz des Verantwortlichen vor unverhältnismäßigen Maßnahmen in Randbereichen kann streng genommen als ein Schutz der

Rechte und Freiheiten anderer Personen verstanden werden. Eine gewagte unionsrechtliche Interpretation bildet es dennoch.

§ 35 Abs. 3 BDSG-E

§ 35 Abs. 3 BDSG-E lässt die Löschungspflicht entfallen, wenn der Verantwortliche, das Recht, dem er unterliegt und das gem. Art. 17 Abs. 3 DS-GVO die Ausnahme rechtfertigen soll (BT-Drs. 18/11325), selbst geschaffen hat oder freiwillig mit Dritten eingegangen ist. Dafür kann die betroffene Person aber nichts. Sofern der Verantwortliche nicht verpflichtet war diese Art von Rechtsbindung einzugehen, dürfte Art. 17 Abs. 3 DS-GVO diese Ausnahme nicht rechtfertigen.

Generell ist festzustellen, dass sich das neue BDSG sehr an seine Vorgängerregelungen anlehnt. Dies zeigt sich z.B. durch die Beibehaltung der systematischen Unterscheidung zwischen „öffentlichen Stellen“ und „nicht-öffentlichen Stellen“. Auch im Rahmen der Ausnahmen von den Betroffenenrechten (§§ 32 ff. BDSG-neu) orientiert sich das neue Gesetz stark an den Regelungen des alten BDSG.

§ 36 BDSG-E

Bei § 36 a.E. BDSG-E könnte man Zweifel haben, ob der Ausschluss des Widerspruchsrechts in allen Fällen, in denen eine Rechtsvorschrift zur Verarbeitung verpflichtet, mit Art. 21 DS-GVO vereinbar ist, da dort diese Ausnahme nicht genannt wird. Da § 36 BDSG-E aber der Sache nach Verarbeitungen auf der Grundlage von Art. 6 Abs. 1 lit. c) DS-GVO erfasst und für diese das Widerspruchsrecht nicht greift, dürfte die Regelung möglich sein. Sinnvoll ist sie.

§ 51 BDSG-E

Die Richtlinie Justiz und Inneres kennt als Rechtsgrundlage nur die Erfüllung gesetzlich vorgegebener Aufgaben gemäß Art. 8 JI-RL. Die Einwilligung ist nicht aufgeführt. Im Erwägungsgrund 35 am Ende weist die Richtlinie aber darauf hin, dass die Mitgliedstaaten das Recht behalten, die Einwilligung in bestimmten Situationen als Rechtsgrundlage zu normieren. Glücklicherweise ist dies nicht, weil die Erwägungsgründe den normativen Text des Art. 8 JI-RL Richtlinie nicht verändern können. Die Erwägungsgründe helfen aber, die Reichweite der Ausschließlichkeit der Regeln des Art. 8 JI-RL zu bestimmen. Offenbar geht der Normgeber bei der Richtlinie davon aus, die Bindungswirkung des Art. 8 JI-RL würde die Einwilligung nicht ausschließen. Aus deutscher Sicht ist die Möglichkeit der Einwilligung auch im Anwendungsbereich von § 45 BDSG-E mehr als wünschenswert. Die Möglichkeit einer Alkoholkontrolle durch „Blasen in das Röhrchen“ wäre ohne die Regeln des § 51 BDSG-E rechtlich in Zukunft nicht mehr möglich gewesen.

Heinrich Wolff

(Das Schreiben wurde als Datei versendet und ist nicht unterschrieben)

I. Allgemein	1
1. Besonderheiten	1
2. Ausprägung des Gesetzes	2
3. Die Systematik des BDSG-E	3
a) Verordnungsteil	3
b) Umsetzung der Richtlinie	3
c) Rein nationaler Raum	3
II. Übergreifende Fragen	4
1. Kompetenzfrage	4
a) Vertretungsregelung im EDA	4
b) Presserecht	5
c) Allgemeines Polizeirecht	8
2. Abgrenzung Verordnung – Richtlinie	8
3. Ordnungswidrigkeitenrecht	9
a) Verschuldensfrage - § 41 Abs. 1 OWiG	9
b) Haftung der Repräsentanten	9
4. Videoüberwachung	9
5. Bonitätsauskunft und das Scoring	10
6. Verhältnis der Aufsichtsbehörden mit anderen Behörden	11
7. Allgemeine Verarbeitungsgrundlage	12
Man sollte § 3 BDSG-E ergänzen um den Passus „oder zur Erfüllung einer rechtlichen Verpflichtung, die sie unterliegt,“...	12
III. Einzelfragen	12
§ 1 Abs. 4 BDSG-E	12
§ 2 BDSG-E	12
§ 6 Abs. 6 S. 3 BDSG-E	12
§ 6 BDSG-E	12
§ 19 Abs. 2 BDSG-E	13
Angemessene und spezifische Maßnahmen - § 22 Abs. 2 BDSG-E/ § 28 Abs. 1 BDSG-E/ § 37 Abs. 2 BDSG-E	13
§ 23 BDSG-E	14
§ 25 BDSG-E	14
Unverhältnismäßiger Aufwand - § 27 Abs. 2 BDSG-E	14
§ 32 Abs. 1 Nr. 1 BDSG-E	14
§ 33 Abs. 1 Nr. 2 BDSG-E	14
§ 34 Abs. 1 Nr. 2 BDSG-E	14
§ 35 Abs. 3 BDSG-E	15
§ 36 BDSG-E	15
§ 51 BDSG-E	15



2^B Advice
The Privacy Benchmark

ÖFFENTLICHE ANHÖRUNG
27.3.2017

BUNDESTAGSINNENAUSSCHUSS ZU
DSANPUG-EU, BT-DRUCKSACHE 18/1325

INHALTSVERZEICHNIS

INHALTSVERZEICHNIS.....	2
HERAUSFORDERUNG FÜR DIE DATENSCHUTZ-PRAXIS.....	3
1 DEUTSCHE DATENSCHUTZSTANDARDS ENTFALLEN:.....	5
2 ZU DEN REGELUNGEN DES GESETZENTWURFES IM EINZELNEN	6
2.1 ZU § 4 VIDEOÜBERWACHUNG ÖFFENTLICH ZUGÄNGLICHER RÄUME.....	6
2.2 ZU § 5 BENENNUNG.....	6
2.3 ZU § 7 AUFGABEN.....	7
2.4 ZU § 17 VERTRETUNG IM EUROPÄISCHEN DATENSCHUTZAUSSCHUSS, ZENTRALE ANLAUFSTELLE	7
2.5 ZU §26 DATENVERARBEITUNG FÜR ZWECKE DES BESCHÄFTIGUNGSVERHÄLTNISSES	8
2.6 ZU § 30 VERBRAUCHERKREDITE	8
2.7 ZU § 31 SCHUTZ DES WIRTSCHAFTSVERKEHRS BEI SCORING UND BONITÄTSAUSKÜNFTEN	8
2.8 ZU § 43 BUßGELDVORSCHRIFTEN	10

HERAUSFORDERUNG FÜR DIE DATENSCHUTZ-PRAXIS

Mit dem In-Kraft-Treten der EU-Datenschutzgrundverordnung (Art. 99¹) sind die geänderten Anforderungen an das Datenschutzmanagement in den betroffenen Unternehmen und Behörden abzubilden. Mit dem Wirksamwerden der DSGVO **am 25. Mai 2018 sind alle Regelungen direkt und ohne nationale Umsetzungsanforderung** in ganz Europa gültig.

Das Jahr 2017 muss demzufolge genutzt werden, um die geänderte Rechtslage zu analysieren und davon ausgehend:

- a) Maßnahmen zur Anpassung der Datenschutzmanagementprozesse innerhalb des Unternehmens/der Behörde,
- b) Maßnahmen zur Anpassung von Vertragswerken mit Auftrags(daten)verarbeitern/Auftraggebern und
- c) Maßnahmen zur Anpassung der Produkte und Dienstleistungen festzulegen, soweit diese personenbezogene Daten nutzen.

Der hierfür vorgesehene Umsetzungszeitrahmen von zwei Jahren ist bereits knapp bemessen – und schon jetzt fast abgelaufen ohne die erforderlichen nationalen Umsetzungen.

Die Unternehmen, Behörden, Datenschutzbeauftragten, Aufsichtsbehörden und Landesgesetzgeber benötigen deshalb schnell Rechtsklarheit zu allen nationalstaatlichen Umsetzungsrechtsakten auf Basis der Erlaubnisnormen der EU-DSGVO.

Das Datenschutzrecht erfährt gegenwärtig die größte Änderung der letzten 20 Jahre. Aus nationalen Regelungen zur Umsetzung des Rechtes auf informationelle Selbstbestimmung werden europäische Regeln zur Gewährleistung der Freizügigkeit des Datenverkehrs auch für personenbezogene Daten, die auch internationale Standards setzen. Die EU-Datenschutzgrundverordnung² ist nach mehr als 4jähriger Diskussion am **25. Mai 2016** in Kraft getreten. Sie sieht einen zweijährigen Anpassungszeitraum vor.

Damit bleibt den Unternehmen und Behörden nur noch ein kurzes Zeitfenster, um

¹ Artikelnummerierungen ohne weitere Bezeichnung sind immer solche der DSGVO, EG Nummer bezieht sich immer auf die Erwägungsgründe der DSGVO, §§ ohne Bezeichnung beziehen sich immer auf das BDSG

² 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); L 119/4 Amtsblatt der Europäischen Union vom 4.5.2016

- alle bestehenden Datenverarbeitungsprozesse auf ihre weitere Zulässigkeit hin zu prüfen,
- alle Auftragsdatenvereinbarungen auf eine neue Rechtsgrundlage zu stellen,
- die neuen Informations- und Dokumentationspflichten umzusetzen,
- Prozesse zur Einhaltung der strengeren terminlichen und verfahrensrechtlichen Anforderungen einzuführen bzw. zu überarbeiten.

Bis zum 25. Mai 2018 müssen alle nationalen Datenschutzvorschriften auf den Prüfstand und ggf. neu erlassen werden. Da im Datenschutzrecht auch weiterhin der Grundsatz „Verbot mit Erlaubnisvorbehalt“ (Art. 5 DSGVO) gilt, sind ab dann alle Datenverarbeitungsprozesse unzulässig, die ausschließlich auf den gegenwärtigen deutschen Regelungen beruhen.

Darüber hinaus wird die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung (Polizei, Justiz) durch eine Richtlinie neu geregelt, die bis zum **6. Mai 2018** in nationales Recht umgesetzt werden muss.

Diese Umsetzung soll durch den

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)

erfolgen, zu dem ich wie folgt Stellung nehmen darf:

1 DEUTSCHE DATENSCHUTZSTANDARDS ENTFALLEN:

Für die Praxis wichtige spezifische Normen des bisherigen Bundesdatenschutzgesetzes (BDSG alt) **entfallen** mit der EU-DSGVO:

- § 4 Abs. 2 BDSG alt: Prinzip der Direkterhebung beim Betroffenen;
- § 4 d Abs. 4 BDSG alt: Meldung von Verfahren bei der Aufsichtsbehörde, bei denen geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder der Markt- oder Meinungsforschung gespeichert werden;
- § 4 d Abs. 5,6 BDSG alt: Vorabkontrolle von besonders risikoreichen Verfahren durch den Datenschutzbeauftragten;
- § 4g Abs. 2 Satz 2 BDSG alt: Verzeichnisse für Jedermann;
- § 5 BDSG alt : Verpflichtung auf das Datengeheimnis;
- Einwilligungsfähigkeit eines Kindes auch ohne elterliche Zustimmung bei Einsichtsfähigkeit
- § 28 Abs. 3 BDSG alt: Regelung zur Datenverarbeitung für Werbung;
- § 28a BDSG alt: Zulässigkeitsregelung für die Meldung von Negativ-/Positivdaten in den Auskunftsbestand von Auskunftsteilen;
- § 28b BDSG alt: Transparenzvorschriften beim Scoring;
- § 29 BDSG alt: Verarbeitung für fremde Geschäftszwecke (Adresshändler, Auskunftsteile);
- § 30 BDSG alt: Verarbeitung für fremde Geschäftszwecke in anonymisierter Form;
- § 30a BDSG alt: Verarbeitung für Markt- und Meinungsforschung;
- §§ 28a, 28b, 34 Abs. 2 und 4 BDSG alt: Regelungen zu Datenübermittlungen an Auskunftsteile, Scoring, Auskunft

Der Bundesgesetzgeber sollte hier – wie es der Bundesinnenminister als politische Zielstellung des Gesetzentwurfes wiederholt bezeichnete – den Status Quo so weit wie möglich erhalten. Dies gelingt mit dem vorliegenden Entwurf nur in wenigen Punkten. Vielmehr werden wichtige, in oft langen politischen Diskussionsprozessen erzielte Kompromisse zwischen der verschiedenen berechtigten Interessenlagen ohne Not aufgelöst.

2 ZU DEN REGELUNGEN DES GESETZENTWURFES IM EINZELNEN

2.1 ZU § 4 VIDEOÜBERWACHUNG ÖFFENTLICH ZUGÄNGLICHER RÄUME

„Bei der Videoüberwachung von 1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder 2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhaltigen Personen als ein besonders wichtiges Interesse.“

Der Zweck dieser Regelung erschließt sich nicht. An die Definition als „besonders wichtiges Interesse“ knüpfen keine Rechtsfolgen an.

In der Begründung heißt es hierzu: „Absatz 1 Satz 2 schreibt die bisherige Regelung des § 6b Absatz 1 Satz 2 BDSG a. F. fort, die mit dem Entwurf eines Videoüberwachungsverbesserungsgesetzes in das BDSG a. F. aufgenommen werden soll. Soweit der Betreiber eine Videoüberwachung einsetzen möchte und die Schutzgüter Leben, Gesundheit oder Freiheit in den dort genannten Anlagen betroffen sein können, wird durch die Formulierung „gilt als...ein besonders wichtiges Interesse“ die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme geprägt.“

Hier soll also einer Entscheidung vorgegriffen werden, die eine Abwägungsentscheidung dem Grunde nach überflüssig machen würde. Auch die Relativierung in Absatz 2 „zum frühestmöglichen Zeitpunkt“ führt zu einer völlig unklaren und willkürlich auslegbaren Rechtslage.

Empfehlung: Der bisherige §6b BDSG alt sollte unverändert und nur redaktionell in Absatz 4 angepasst übernommen werden.

2.2 ZU § 5 BENENNUNG

Gem. (1) benennen öffentliche Stellen „eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten“. Dies führt in der Praxis regelmäßig zu Problemen, wenn diese durch Krankheit, Elternzeit oder längere Abwesenheiten an der Ausübung ihres Amtes gehindert ist. Für diese Fälle sollte – wie es eine Reihe von Landesdatenschutzgesetzes bereits vorschreiben – auch eine Stellvertreterin zu benennen sein.

Empfehlung: §5 (1) ist wie folgt zu ändern: „Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten **sowie eine Stellvertreterin oder einen Stellvertreter.**“

§5 (5) ist wie folgt zu ändern: „Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten **sowie der Stellvertreterin oder des Stellvertreters** und teilt diese Daten der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.“

2.3 ZU § 7 AUFGABEN

Zu den Aufgaben des Datenschutzbeauftragten gehört es nach der DSGVO nicht mehr, das Verfahrensverzeichnis zu führen, die Datenschutzfolgenabschätzung durchzuführen oder den öffentlichen Teil des Verfahrensverzeichnisses auf Antrag Jedermann zur Verfügung zu stellen. Damit werden den Datenschutzbeauftragten die wesentlichen Instrumente zur Durchsetzung der Datenschutzerfordernungen genommen. Dies ist vor dem Hintergrund zu erklären, dass die Funktion des Datenschutzbeauftragten in Europa unbekannt und durch die DSGVO nur in wenigen Ausnahmefällen eingeführt wird. Es spricht jedoch nichts dagegen, diese Aufgaben im neuen BDSG fortzuführen.

Empfehlung: §7 sollte wie folgt geändert werden:

„(1) Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

Neu 3. Durchführung der Datenschutz-Folgenabschätzung gemäß § 67 dieses Gesetzes

Neu 6. Führung des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30

Neu 7. Zugänglichmachung des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 auf Antrag für Jedermann mit Ausnahme der Angaben nach Abs. 1 Satz 2 Buchstabe g.“

2.4 ZU § 17 VERTRETUNG IM EUROPÄISCHEN DATENSCHUTZAUSSCHUSS, ZENTRALE ANLAUFSTELLE

Der Europäische Datenschutzausschuss koordiniert und entscheidet in Fragen der Datenschutzaufsicht im nicht-öffentlichen Bereich. Für die Aufsicht in diesem Bereich sind in weit überwiegendem Umfang die Landesaufsichtsbehörden zuständig, die über die erforderliche Sachkunde und Sachnähe verfügen. Aus diesem Grund wäre die in Absatz 2 des Entwurfes vorgesehene Ausnahmeregelung der Übertragung der Aufgabenwahrnehmung auf die oder den Ländervertreter der Regelfall.

Empfehlung: §17 ist wie folgt zu ändern:

“(1) Gemeinsamer Vertreter im Europäischen Datenschutzausschuss und zentrale Anlaufstelle ist die oder der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (gemeinsamer Vertreter). Die oder der Bundesbeauftragte für Datenschutz und Informationsfreiheit ist die ständige Stellvertreterin oder der ständige Stellvertreter des gemeinsamen Vertreters und leitet die Geschäftsstelle, die bei der Bundesbeauftragten oder dem Bundesbeauftragten errichtet wird.

(2) Der gemeinsame Vertreter überträgt in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche der Bund allein das Recht zur Gesetzgebung hat, oder welche die Einrichtung oder das Verfahren von Bundesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss.

2.5 ZU §26 DATENVERARBEITUNG FÜR ZWECKE DES BESCHÄFTIGUNGSVERHÄLTNISSES

Der Entwurf soll in Absatz 1 die Datenverarbeitung auf der Grundlage von Kollektivvereinbarungen ermöglichen, verfehlt diese Ziel jedoch wesentlich, indem dort die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis auf der Basis einer Kollektivvereinbarung nur dann erlaubt wird, wenn diese für die Ausübung oder Erfüllung der sich hieraus „ergebenden Rechte und Pflichten der Interessenvertretung“ erforderlich ist. Diese Regelung privilegiert mithin ausschließlich die Datenverarbeitung durch die Interessenvertretung. Diese Regelung steht damit im Widerspruch zu Absatz 4 des Entwurfes und sollte klarstellend korrigiert werden.

Empfehlung: §26 ist wie folgt zu ändern:

„(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Aufgaben erforderlich ist.“

2.6 ZU § 30 VERBRAUCHERKREDITE

Die bisher bestehende Pflicht zur Meldung von Verfahren bei der Datenschutzaufsichtsbehörde, bei denen geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder der Markt- oder Meinungsforschung gespeichert werden, entfällt aufgrund der Neuregelungen in Art. 30 DSGVO. Diese Meldepflicht stellt eine wichtige Säule der Überwachung dieser besonders sensiblen Datenverarbeitungen durch die Aufsichtsbehörden dar und sollte deshalb dringend beibehalten werden.

Empfehlung: §39 ist wie folgt zu ergänzen:

„(1a) Diese Stellen haben die Verzeichnisse der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO der zuständigen Datenschutzaufsichtsbehörde rechtzeitig anzuzeigen und alle zur Prüfung der Zulässigkeit erforderliche Angaben zu machen.“

2.7 ZU § 31 SCHUTZ DES WIRTSCHAFTSVERKEHRS BEI SCORING UND BONITÄTSAUSKÜNFTE

Anders als in § 28a BDSG alt gibt es keine konkreten rechtlichen Anforderungen mehr an die Einmeldung von Forderungsdaten in Auskunfteien. Der neue § 31 Abs. 2 regelt nur noch, welche Forderungsdaten für die Score-Berechnung genutzt werden dürfen. Die grundsätzliche und davon unabhängige Frage, welche Forderungsdaten überhaupt an Auskunfteien übermittelt werden dürfen, bleibt künftig ungeregt. Das ist aus Sicht der Verbraucherinnen und Verbraucher ein großer Rückschritt.

Mit § 28a Abs. 2 letzter Satz BDSG entfällt das für Kreditsuchende wichtige Verbot, sog. Konditionenankfragen zu beaufkunen und zu scoren. In § 28a Abs. 2 letzter Satz ist bislang ein von Verbraucher- und Datenschutz in langem Ringen erkämpftes Verbot enthalten: Das Verbot, sog. Konditionenankfragen von Kreditsuchenden in dem Auskunftsdatsatz zu speichern und vor allem: für die Score-Berechnung zu verwenden.

Der neue § 31 Abs. 2 BDSG wird kaum praktische Relevanz haben – das Scoring von Forderungsdaten ist nicht das Problem. Liegen zu potentiellen Vertragspartnern bereits negative Zahlungserfahrungen vor, benötigen die Unternehmen keine Score-Werte, sondern wissen bereits aufgrund der Negativeintragungen, dass das Ausfallrisiko hoch ist. Score-Berechnungen sind daher für die Wirtschaft vor allem interessant, soweit es um Verbraucherinnen und Verbraucher geht, zu denen keine konkreten Einträge vorliegen. In diesen Fällen werden häufig verhaltensunabhängige Daten etwa zu Geschlecht, Alter und Wohnort (Wohnumfeldbewertung) für das Scoring genutzt. Die in § 31 Abs. 2 BDSG geregelten Forderungsdaten sind daher auch aus Sicht des Datenschutzes nicht die problematischen. Insoweit ist die Bedeutung des neuen § 31 Abs. 2 umgekehrt proportional zum Verlust, den die Betroffenen durch die Streichung des bisherigen § 28a BDSG alt erleiden werden.

Die bislang wichtigste rechtliche Einschränkung des Scoring (§ 28b Nr. 2 BDSG alt) entfällt – die allgemeine Anforderung in § 31 Abs. 1 BDSG ist kein adäquater Ersatz. Nach § 28b Nr. 2 BDSG alt dürfen nur die personenbezogenen Daten in eine Score-Berechnung einfließen, die auch außerhalb des Score-Verfahrens für den damit verfolgten Zweck genutzt werden dürfen. Während § 28b Nr. 1 BDSG alt als notwendige, aber nicht hinreichende Bedingung die statistische Relevanz jedes Score-Merkmals fordert, ist daher der § 28b Nr. 2 derzeit das entscheidende rechtliche Korrektiv. Deswegen ist es bislang unzulässig, für das Bonitäts-Scoring etwa Vornamen (wie in Frankreich teilweise geschehen), die Anzahl der Umzüge (Adressänderungen) oder (wie früher ebenfalls bei der SCHUFA) die Anzahl der datenschutzrechtlichen Selbstauskünfte nach § 34 BDSG alt zu verwenden – auch wenn sie mathematisch-statisch durchaus dafür geeignet wären.

Diese rechtliche Anforderung ist umso wichtiger, als nun Score-Anbieter auf den Markt drängen, die allgemein zugängliche Daten aus Facebook, Twitter und sonstigen Sozialen Netzwerken für die Score-Berechnung nutzen (Kreditech, Lenddo, LendUp, Wonga, Cignifi).

Die allgemeine Anforderung in § 31 Abs. 1 BDSG ist insbesondere in den Fällen kein adäquater Ersatz, in denen die Daten – wie in den oben genannten Beispielen – rechtmäßig erhoben wurden und nun „nur“ zweckändernd in die Score-Berechnung einfließen sollen. Denn mit den allgemeinen Regelungen der DSGVO zur Zweckänderung werden die Aufsichtsbehörden die zweckändernde Verwendung für das Scoring nicht unterbinden können.

Die speziellen Transparenz- und Betroffenenrechte der Verbraucherinnen und Verbraucher zum Scoring entfallen (insb. § 34 Abs. 2 und Abs. 4, § 35 BDSG). Die bisherigen bereichsspezifischen Regelungen zur Transparenz beim Scoring

(Auskunftsrecht, Kennzeichnung von Schätzdaten) sowie zur Sperrung und Löschung von Auskunftseidaten wurden nicht übernommen.

Empfehlung: Der § 31 BDSG ist wie folgt zu ändern:

Die Regelungen der bisherigen §§ 28 a, 28b, 29 und 34 (2), (4) und 35 BDSG alt sind redaktionell angepasst zu übernehmen.

2.8 ZU § 43 BUßGELDVORSCHRIFTEN

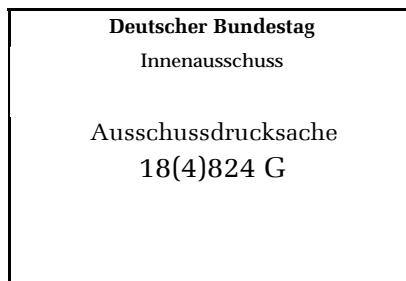
Der Gesetzentwurf will in §43 (3) BDSG auch weiterhin die Behörden und öffentlichen Stellen entgegen der Regelung der DSGVO von der Bußgeldandrohung ausnehmen. Hierfür ist weder ein Grund, noch ein legitimes Interesse erkennbar. Die Öffnungsklausel des Artikels 83 Absatz 7 DSGVO muss nicht zwingend umgesetzt werden. Vielmehr erscheint es angesichts der ständig zunehmenden Datenübermittlungen zwischen nicht-öffentlichen und öffentlichen Stellen geboten, hier für eine Gleichbehandlung zu sorgen. Um dem Argument der Haushaltsneutralität zu begegnen kann eine Zweckbindung der Bussgeldeinnahmen gesetzlich geregelt werden.

Empfehlung: Der §43 Abs. 3 ist wie folgt zu ändern: „(3) Werden gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 Geldbußen verhängt fließen die Einnahmen der Verbesserung der Öffentlichkeitsarbeit der Aufsichtsbehörden zu.“

Bonn, 23.03.2017



Karsten Neumann



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

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

An den

Innenausschuss des
Deutschen Bundestages

Per E-Mail an: innenausschuss@bundestag.de

Datum: 25. März 2017

**Stellungnahme zum
Gesetzentwurf 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), BT-Drucksache 18/11325,**

**vorgelegt zur Anhörung des Innenausschusses des Deutschen
Bundestags am 27. März 2017 in Berlin**

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@](mailto:Hartmut.Aden@hwr-berlin.de)

hwr-berlin.de

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

www.foeps-berlin.org

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Mitwirkung an der Anhörung. Meine Stellungnahme beschränkt sich absprachegemäß auf die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 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 [...]*.

Bedauerlicherweise hat diese Richtlinie in der öffentlichen Wahrnehmung seit der gemeinsamen Einbringung der Entwürfe durch die Europäische Kommission Anfang 2012 zumeist im Schatten der Datenschutzgrundverordnung gestanden. Dies ist insbesondere angesichts der hohen praktischen Relevanz zu bedauern, die der Datenaustausch zwischen Sicherheitsbehörden seit den 1990er Jahren und verstärkt im Zusammenhang mit der Terrorismusbekämpfung der letzten Jahre erlangt hat.

Das Datenschutzrecht für die polizeiliche Zusammenarbeit in der Europäischen Union entsprach bisher weder dem Stand der Zusammenarbeitspraxis noch der technischen Entwicklung. Der jetzt abzulösende Rahmenbeschluss stammt noch aus der ehemaligen „Dritten Säule“, also der

Seiten insgesamt

1/8

Seite 129 von 365
Berliner Volksbank

Konto 884 101 52 40



reinen Regierungszusammenarbeit. Die Technik der Datenverarbeitung und die Praxis der Zusammenarbeit zwischen den hier relevanten Behörden der Mitgliedstaaten (Polizei u. a.) haben sich in den letzten Jahren erheblich weiterentwickelt. Der transnationale Informationsaustausch hat sich in Zeiten gestiegener Risiken und Gefahren für die Sicherheit zu einem zentralen Instrument entwickelt. Die ausgeweitete Praxis ist aber auch mit Risiken für die Grundrechte der Bevölkerung verbunden, insbesondere für die informationelle Selbstbestimmung und die daran anknüpfenden Grundrechte im Strafverfahren (Unschuldsvermutung; Schutz vor willkürlichen Freiheitsentziehungen etc.). Diese Grundrechtspositionen lassen sich nur durch rigorose Maßnahmen zur Gewährleistung der Qualität der hier verarbeiteten personenbezogenen Daten schützen, die Fehlinformationen, Verwechslungen oder unberechtigte Datenverarbeitung verhindern. Solche Maßnahmen liegen zugleich im Interesse der Sicherheitsbehörden selbst, da Reibungsverluste durch veraltete oder unrichtige Daten so vermieden werden können.¹ Daher ist die Harmonisierung durch die Richtlinie (EU) 2016/680 ein wichtiger Schritt.

Zu ausgewählten Aspekten des Entwurfs für die Umsetzung dieser Richtlinie nehme ich im Folgenden Stellung. Der vorliegende Gesetzentwurf wirft konzeptionelle Fragen für eine adäquate, in der Praxis handhabbare Umsetzung der Richtlinienvorgaben auf (A). Er spiegelt verbliebene Unzulänglichkeiten der Richtlinie selbst wider (B), enthält aber auch diverse Mängel und nicht ausgeschöpfte Regelungspotentiale, die der Deutsche Bundestag im Rahmen des Umsetzungsspielraums noch korrigieren kann (C).

A) Konzeptionelle Problematik der Richtlinienumsetzung in das deutsche Recht

Problematisch ist bereits die für die Richtlinienumsetzung vorgeschlagene Systematik. Statt ein anwendungsfreundliches Datenschutzgesetz „aus einem Guss“ zu schaffen, trennt der vorliegende Gesetzentwurf die

¹ Näher hierzu: Aden, Hartmut (2014) *Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem*, in: Der moderne Staat, Zeitschrift für Public Policy, Recht und Management (7. Jg., Nr. 1), S. 55-73; ders. (2015) *Police information sharing and data protection in the European Union before and after the Treaty of Lisbon*, in: Hartmut Aden (Hrsg.), *Police Cooperation in the European Union under the Treaty of Lisbon – Opportunities and Limitations*, Baden-Baden (Nomos, Schriftenreihe des Arbeitskreises Europäische Integration, Band 83), S. 209-216.



Anpassung des deutschen Rechts an die Datenschutzgrundverordnung ganz unnötig von der Umsetzung der Richtlinie 2016/680. Gesetzgebungstechnisch ungewöhnlich schlägt der Entwurf damit „zwei Gesetze in einem“ vor. Indes verfolgte das Anfang 2012 von der Europäischen Kommission vorgelegte EU-„Datenschutzpaket“ die Intention, einen Datenschutz „aus einem Guss“ zu schaffen. Die Trennung in Richtlinie und Verordnung sollte lediglich den Mitgliedstaaten etwas größere Gestaltungsspielräume für das Datenschutzrecht im Polizei- und Strafverfolgungsbereich überlassen.

- Der vorliegende Entwurf spiegelt dagegen eher die Zuständigkeitsverteilung für die beiden EU-Rechtsakte in einer arbeitsteilig organisierten Ministerialverwaltung wider als eine ambitionierte, an der Schaffung systematischer Rechtsgrundlagen orientierte Gesetzgebung. Chancen für die Schaffung eines einheitlichen, benutzerfreundlichen Datenschutzrechts werden damit vertan. Wesentlich sinnvoller erschiene es, allgemeine Fragen wie Definitionen und Grundsätze in einem gemeinsamen allgemeinen Teil voranzustellen und sodann in einem besonderen Teil zunächst die Anpassung an die Datenschutzgrundverordnung und sodann die Umsetzung der Richtlinie vorzunehmen. Trotz des Nebeneinanders unmittelbar geltender Verordnungsinhalte und umsetzungsbedürftiger Richtlinienvorgaben ist eine Vereinheitlichung der Begrifflichkeiten und allgemeiner Prinzipien im Interesse kohärenter Rechtsanwendung sinnvoll. Dies betrifft zumindest die §§ 45 bis 47 der Entwurfsfassung. Nur so bleibt das Gesetz in der Praxis handhabbar, insbesondere auch für Polizeibedienstete auf Sachbearbeiterebene.²
-

Empfehlung: *Der Deutsche Bundestag sollte die allgemeinen Datenschutzgrundlagen aus der Richtlinie (insbesondere §§ 45 bis 47 des Entwurfs) mit Teil 1, Kapitel 1 (§ 1 bis 2) zu einem kohärenten „allgemeinen Teil“ des Gesetzes zusammenführen.*

² Zur Überforderung der Polizeipraxis durch überkomplizierte rechtliche Grundlagen: Aden, Hartmut (2013), *Polizei und das Recht: Stressquelle oder Stressvermeidung?*, in: Rainer Prätorius & Lena Lehmann (Hrsg.), *Polizei unter Stress?*, Frankfurt/Main: Verlag für Polizeiwissenschaft, S. 15-34.

B) Defizite in der EU-Richtlinie und Korrekturmöglichkeiten im Rahmen der deutschen Gesetzgebung

Einige Defizite des vorliegenden Gesetzentwurfs sind bereits in der Richtlinie (EU) 2016/680 angelegt. Da es sich um eine Richtlinie handelt, kann der Deutsche Bundestag diese Defizite jedenfalls teilweise durch eigene gesetzgeberische Impulse kompensieren. Zwei dieser Defizite seien hier exemplarisch hervorgehoben.

1. Fehlende Anwendbarkeit für die EU-Agenturen und ihre Zusammenarbeit mit den mitgliedstaatlichen Behörden

Gemäß Art. 2 Abs. 2 der RL (EU) 2016/680 bezieht sich ihr Anwendungsbereich nicht auf die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union. Damit sind auch die für Sicherheitsfragen eingerichteten EU-Agenturen (insbesondere Europol, Frontex, eu-LISA, CEPOL) nicht erfasst. Dies ist vor dem Hintergrund der ursprünglichen Absicht, einen einheitlichen Datenschutzrahmen in der EU zu schaffen, inkonsequent – und angesichts einer bisher für jede Agentur unterschiedliche Datenschutzarchitektur³ bedauerlich. Hier wird die EU-Gesetzgebung in einem weiteren Gesetzgebungsschritt für mehr Kohärenz und einheitlich höhere Schutzstandards sorgen müssen.

Dies hindert indes den Deutschen Bundestag nicht daran, bereits jetzt einheitliche (Mindest-)Standards für den Datenaustausch der Sicherheitsbehörden des Bundes mit EU-Agenturen „vor die Klammer zu ziehen“.

2. Verweis auf mitgliedstaatliche Gesetze: zu viele „Hintertüren“ für die Datenverarbeitungspraxis

Die Richtlinie verfolgt die regulatorische Grundlinie, dass die Datenverarbeitung von Sicherheitsbehörden durch rechtliche Grundlagen legitimiert werden kann und muss. Dieser regulatorische Ansatz ist als solcher nicht zu beanstanden und angesichts der hohen Bedeutung der Ressource Information für Sicherheitsbehörden kaum vermeidlich. Erforderlich wären dagegen klarere materiell-rechtliche Grenzen für die Datenerhebung und -verarbeitung. Diese müssen nun von der mitgliedstaatlichen Gesetzgebung etabliert werden – die Richtlinie enthält zahlreiche Verweisungen

³ Näher hierzu Aden, Hartmut (2014) *Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem*, a.a.O.



auf mitgliedstaatliche Gesetze. Auch für das deutsche Recht gibt es hier noch erheblichen Entwicklungsbedarf. Der vorliegende Gesetzentwurf liefert hierfür leider keine über die Mindestvorgaben der Richtlinie hinausgehenden Ansätze.

C) Nachbesserungsmöglichkeiten des Deutschen Bundestags für die Richtlinienumsetzung

Der Deutsche Bundestag hat im Gesetzgebungsverfahren die Chance, eine Reihe konkreter Verbesserungen an dem vorliegenden Entwurf vorzunehmen. Einige hiervon seien exemplarisch aufgeführt.

1. Nicht nur den Richtlinientext abschreiben, sondern die Umsetzung in die deutsche Rechtssystematik gewährleisten

Der vorliegende Entwurf orientiert sich bis in Detailformulierungen hinein stark am Text der Richtlinie. Dies entspricht einer bedauerlichen Tendenz, die auch auf anderen Rechtsgebieten zu beobachten ist: Aus Sorge vor Interpretationsstreitigkeiten, eventuellen Vertragsverletzungsverfahren und manchmal auch vor einer über die EU-Vorgaben hinausgehenden Umsetzung werden Richtlinieninhalte wörtlich in die Umsetzungsgesetzgebung übernommen. Dabei ist es gerade der Sinn einer Richtlinie gemäß Art. 288 AEUV, den Mitgliedstaaten die Einpassung in ihre spezifische Rechtssystematik und –terminologie zu ermöglichen.

Beispiel: In Art. 3 Abs. 1c der RL (EU) 2016/680 heißt es: „Die Mitgliedstaaten sehen vor, dass personenbezogene Daten dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind.“ Diese sprachlich missglückte Formulierung der offiziellen deutschsprachigen Richtlinienfassung wurde einfach in den vorliegenden Entwurf hineinkopiert. In § 47 Nr. 3 des Entwurfs heißt es: Personenbezogene Daten müssen „dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sein.“ In der deutschen Rechtssystematik müsste eine für die Rechtsanwendung in den Sicherheitsbehörden ohne Weiteres verständliche Formulierung dagegen ungefähr wie folgt lauten: Personenbezogene Daten „dürfen nur verarbeitet werden, soweit diese Verarbeitung für das Erreichen des Verarbeitungszwecks (zwingend) erforderlich ist und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck steht.“

Dieses Beispiel zeigt, dass der gesamte Entwurf noch einmal gründlich bezüglich seiner Übereinstimmung mit der deutschen Rechtssystematik und –terminologie überprüft werden sollte.

Empfehlung: *Der Deutsche Bundestag sollte die wörtlich aus der deutschsprachigen Richtlinienfassung übernommenen Formulierungen des Gesetzentwurfs einer gründlichen Überprüfung auf ihre Vereinbarkeit mit der deutschen Rechtssystematik und –terminologie unterziehen.*

• **2. Zweckänderungsvorschrift (§ 49) nicht mit dem Bestimmtheitsgebot vereinbar**

Die Zweckbindung folgt unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechte-Charta). Sie ist damit ein zentraler Grundsatz für die Datenverarbeitung in Deutschland und in der EU, auch und gerade für den Sicherheitsbereich. Sicherheitsbehörden können für einen bestimmten Zweck erhobene Daten nicht nach Belieben für andere Zwecke verwenden. Zweckänderungen stellen vielmehr erneute Grundrechtseingriffe dar und bedürfen daher einer klaren gesetzlichen Grundlage. Art. 9 der RL (EU) 2016/680 regelt dies den üblichen Standards entsprechend.

Die Umsetzung in § 49 des Entwurfs genügt nicht den Anforderungen des grundgesetzlichen Bestimmtheitsgebots. Der pauschale Verweis in § 49 Satz 1 (Entwurfssatzung) auf die in § 45 genannten „Zwecke“ ist viel zu allgemein und unbestimmt. Denn dort sind die nur sehr allgemein genannten Zwecke „Verhütung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten“ genannt. Die neue Regelung würde es ermöglichen, im Rahmen des Verhältnismäßigen vorhandene Datenbestände zwischen diesen verschiedenen Aufgabenbereichen und Zweckbestimmungen hin- und herzuschieben. Eine solche Zweckänderungsgeneralklausel fiel sogar erheblich hinter den heutigen Stand der spezialgesetzlichen Zweckänderungsvorschriften in der Strafprozessordnung, den Polizeigesetzen und anderen Fachgesetzen zurück. Das Bestimmtheitsgebot erfordert vielmehr spezialgesetzliche Zweckänderungsregelungen. Im Hinblick auf das Wesentlichkeitsprinzip für gravierende Grundrechtseingriffe können diese nur in anderen Parlamentsgesetzen erlassen werden. Das neue Bundesdatenschutzgesetz sollte ausschließlich auf diese verweisen.



Empfehlung: *Der Deutsche Bundestag sollte die Entwurfsfassung des § 49 durch einen Verweis auf spezialgesetzliche, vom Parlament zu erlassene Regelungen ersetzen, in denen die Zwecke, zu denen Daten ebenfalls verarbeitet werden dürfen, im Sinne des Bestimmtheitsgebots präzise zu benennen sind.*

3. Besonders sensible Daten:

Die Verarbeitung besonders sensibler personenbezogener Daten stellt für die Betroffenen einen schweren Grundrechtseingriff dar: Informationen zur rassischen und ethnischen Herkunft, zu religiösen oder weltanschaulichen Überzeugungen, genetische und biometrische Daten sowie Informationen zur Gesundheit oder zum Sexualleben dürfen daher auch von Sicherheitsbehörden nur ausnahmsweise und mit besonderer Vorsicht verarbeitet werden. Art. 10 der RL (EU) 2016/680 erkennt an, dass dieser Ausnahmecharakter auch einer besonderen rechtlichen Absicherung bedarf.

Die vorgeschlagene Umsetzungsregelung in § 48 des Entwurfs könnte so interpretiert werden, dass eine Verarbeitung solcher Daten bereits dann zulässig ist, wenn die dort genannten Voraussetzungen und nur beispielhaft aufgeführten Verfahrensvorkehrungen getroffen werden. Dies würde indes der Schwere des Grundrechtseingriffs durch die Verarbeitung derartiger Daten nicht gerecht. Vielmehr sind im Hinblick auf das grundgesetzliche Bestimmtheitsgebot die Zwecke, für die solche Daten ausnahmsweise erhoben und weiter verarbeitet werden dürfen, in den Fachgesetzen konkret darzulegen. Wegen der Eingriffsintensität erfordert das Wesentlichkeitsprinzip auch hier parlamentsgesetzliche Regelungen.

Empfehlung: *Der Deutsche Bundestag sollte klarstellen, dass die Verarbeitung besonders sensibler Daten (Art. 10 der RL (EU) 2016/680) nur zulässig ist, wenn der konkrete Zweck in einem Parlamentsgesetz (Fachgesetz) zugelassen ist.*

4. Auskunftsrechte: Rechte der Betroffenen klarer sichern

Die Auskunftsrechte der betroffenen Personen sind in Art. 14 und 15 der RL (EU) 2016/680 geregelt und in Deutschland zusätzlich durch das Grundrecht auf informationelle Selbstbestimmung geschützt. Art. 15 ermöglicht zwar Einschränkungen des Auskunftsrechts. Diese sind aber im Lichte der grundrechtlichen Verbürgungen auszugestalten.



In § 57 Abs. 7 der Entwurfsfassung wird eine Konstruktion gewählt, in der die oder der Bundesdatenschutzbeauftragte in Fällen der Auskunftsverweigerung die mit der Auskunftserteilung verbundene Kontrolle bezüglich der Korrektheit der Daten und der Rechtmäßigkeit der Verarbeitung für die Betroffenen wahrnimmt. Diese Konstruktion ist grundsätzlich geeignet, das Spannungsverhältnis zwischen berechtigten Auskunfts- und Kontrollbegehren der Betroffenen und in manchen Fällen berechtigten Geheimhaltungsanliegen der Sicherheitsbehörden aufzulösen. Die Ausnahmeklausel, nach der diese Stellvertretung im Einzelfall durch die zuständige oberste Bundesbehörde wegen Gefährdung „der Sicherheit des Bundes oder eines Landes“ verweigert werden kann (Abs. 7 Satz 3), ist dagegen nicht mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vereinbar. Denn die oder der Bundesbeauftragte verfügt über genügend vertrauenswürdigen und sicherheitsüberprüftes Personal, um diese Aufgabe auch in solchen besonderen Fällen zuverlässig zu erfüllen. Die Ausnahmeklausel ist daher verfassungsrechtlich nicht gerechtfertigt. Auch in dem hier maßgeblichen Art. 17 der RL (EU) 2016/680 ist eine solche Ausnahme nicht vorgesehen, so dass die Umsetzung insofern auch nicht den Anforderungen des EU-Rechts genügt.

Darüber hinaus böte es sich an, dass der Deutsche Bundestag die Rechte der Betroffenen dadurch stärkt, dass die oder der Bundesdatenschutzbeauftragte für diese und andere Fälle ein Klagerecht gegen aus ihrer Sicht rechtswidrige Behördenentscheidungen erhält.

Empfehlung: *Der Deutsche Bundestag sollte die Sicherheitsklausel aus § 57 Abs. 7 Satz 3 des Entwurfs streichen und der oder dem Bundesdatenschutzbeauftragten zudem ein Klagerecht zur Durchsetzung von Betroffenenrechten einräumen.*

Fazit: Ich empfehle dem Deutschen Bundestag, den Entwurf nur nach gründlicher Überarbeitung zu verabschieden.

Gez. Prof. Dr. Hartmut Aden



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag

Innenausschuss

Ausschussdrucksache
18(4)788

Andrea Voßhoff

Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

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

An den
Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn
Ansgar Heveling, MdB

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

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL referat11@bdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 03.03.2017
GESCHÄFTSZ. 11-100/044#0115

Nachrichtlich:

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

Herrn Stephan Mayer, MdB
Herrn Armin Schuster, MdB
Herrn Burkhard Lischka, MdB
Herrn Gerold Reichenbach, MdB
Frau Ulla Jelpke, MdB
Herrn Jan Korte, MdB
Frau Irene Mihalic, MdB
Herrn Dr. Konstantin v. Notz, MdB

BETREFF **Entwurf eines Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU
(DSAnpUG-EU), BT-Drs. 18/11325**

HIER Positionspapier der Bundesbeauftragten für den Datenschutz und die
Informationsfreiheit

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

zu dem anstehenden parlamentarischen Beratungsverfahren zum Gesetzentwurf der
Bundesregierung "Gesetz zur Anpassung des Datenschutzrechts an die Verordnung
(EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680", BT-Drs. 18/11325,
überreiche ich in der Anlage das Positionspapier der BfDI zu Ihrer Kenntnisnahme.
Ich möchte Sie bitten, das Schreiben an alle Ausschussmitglieder zu übersenden.



SEITE 2 VON 2

Sollten die Berichterstatter der Fraktionen es wünschen, bin ich selbstverständlich gern bereit, in Ihren Arbeitsgruppen zu dem Gesetzentwurf Stellung zu nehmen.

Mit freundlichen Grüßen

Andrea Voßhoff



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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)

Bundestags-Drucksache 18/11325

Positionen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Bonn, den 3. März 2017

Vorbemerkung

Die Bundesregierung hat dem Deutschen Bundestag den von ihr am 1. Februar 2017 beschlossenen Entwurf eines Datenschutzanpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU, BT-Drs. 18/11325) vorgelegt.

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

I. Artikel 1 (Entwurf BDSG-neu)

1. Befugnisse der BfDI im Bereich der JI-Richtlinie

§ 16 Abs. 2 BDSG-neu-E lautet:

„Stellt die oder der Bundesbeauftragte bei Datenverarbeitungen durch öffentliche Stellen des Bundes zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber der zuständigen obersten Bundesbehörde und fordert diese zur Stellungnahme innerhalb einer von ihm oder ihr zu bestimmenden Frist auf. Die oder der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Bundesbeauftragten getroffen worden sind. Die oder der Bundesbeauftragte kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.“

Vorschlag BfDI:

§ 16 Abs. 2 wird wie folgt gefasst:

„(2) Stellt die oder der Bundesbeauftragte bei Datenverarbeitungen durch öffentliche Stellen des Bundes zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, ist Absatz 1 entsprechend anwendbar.“

Begründung:

In § 16 Abs. 2 BDSG-E sind die Befugnisse der BfDI im Geltungsbereich der Richtlinie für Polizei und Justiz (DS-RL) und in den Bereichen außerhalb des Geltungsbereichs des EU-Rechts geregelt. Danach soll nach dem Willen der Bundesregierung der status quo erhalten bleiben. **Die BfDI bliebe beschränkt auf Beanstandungen. Für den Geltungsbereich der DS-RL ist das europarechtswidrig.** Art. 47 Abs. 2 DS-RL beinhaltet die Verpflichtung zu wirksamen Abhilfebefugnissen und Art. 47

Abs. 5 DS-RL die Verpflichtung, Möglichkeiten einer gerichtlichen Klärung zu regeln. Beides enthält die vorgeschlagene Regelung nicht.

Das Instrument der Beanstandung ist nicht verbindlich und nicht durchsetzbar. Vertritt der Verantwortliche bzw. dessen Aufsichtsbehörde eine andere Rechtsauffassung als die Datenschutzaufsicht, besteht keine Möglichkeit der Durchsetzung oder Einleitung einer gerichtlichen Klärung der Frage, ob die betreffende Verarbeitung rechtswidrig ist. Die BfDI kann in dieser Konstellation keine wirksame Abhilfe herbeiführen. Um den Befugnissen Wirksamkeit zu verleihen, bedarf es – wie im Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) – der Möglichkeit, verbindliche Anordnungen zu treffen.

2. Vertretung im Europäischen Datenschutzausschuss; Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder (§ 17 Abs. 2, § 18 Abs. 2 BDSG-neu-E)

a) § 17 Abs. 2 BDSG-neu lautet:

„Der gemeinsame Vertreter überträgt in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss.“

b) § 18 Abs. 2 BDSG-neu-E lautet:

„(2) Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vor. Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, legt in Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, der Stellvertreter den Vorschlag für einen gemeinsamen Standpunkt fest. In den übrigen Fällen fehlenden Einvernehmens nach Satz 2 legt der gemeinsame Vertreter den Standpunkt fest. Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. Der Bund und jedes Land haben jeweils eine Stimme. Enthaltungen werden nicht gezählt.“

Vorschlag BfDI:

a) Zu § 17 Abs. 2:

Beibehaltung des Regierungsentwurfs

b) § 18 Abs. 2 wird wie folgt gefasst:

„(2) Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter ei-

nen Vorschlag für einen gemeinsamen Standpunkt vor. Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, legt in Angelegenheiten, die die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das Recht der Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, der Stellvertreter den Vorschlag für einen gemeinsamen Standpunkt fest. In den übrigen Fällen fehlenden Einvernehmens nach Satz 2 legt der gemeinsame Vertreter den Standpunkt fest. Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. Der Bund und jedes Land haben jeweils eine Stimme. Enthaltungen werden nicht gezählt. Abweichend von den Sätzen 1 bis 5 legt die oder der Bundesbeauftragte den gemeinsamen Standpunkt fest, wenn es sich um Angelegenheiten handelt, die ausschließlich in ihrer Zuständigkeit liegen.“

Begründung:

- a) Das den Vorschlägen der §§ 17 Abs. 2, 18 Abs. 2 BDSG-neu-E zugrundeliegende Verständnis des Regierungsentwurfs stellt sicher, dass die deutschen Datenschutzaufsichtsbehörden im europäischen Kontext mit einer starken Stimme sprechen und tariert die verschiedenen Interessen von Bund und Ländern auf eine sinnvolle und angemessene Weise aus. Die BfDI spricht sich deshalb dafür aus, diese Grundarchitektur beizubehalten. Im Bundesrat diskutierte Vorschläge, die Gewichte zulasten des Bundes zu verschieben, würden die Position der deutschen Datenschutzaufsichtsbehörden in europäischen Angelegenheiten unnötig schwächen und sind daher abzulehnen.

Der Regierungsentwurf trägt dem in Art. 23 GG und im EUZBLG verankerten Grundsatz Rechnung, dass dem Bund grundsätzlich die Aufgabe zusteht, die Interessen des Gesamtstaates in Angelegenheiten der EU zu vertreten. Nach den dort festgelegten Maßstäben wird die Außenvertretung der Bundesrepublik Deutschland in der Regel vom Bund wahrgenommen. Dies ist nur dann anders, wenn die ausschließliche Gesetzgebungskompetenz der Länder in den Gebieten der schulischen Bildung, der Kultur und des Rundfunks betroffen ist. Der Regierungsentwurf geht zugunsten der Länder bereits über diesen Ansatz hinaus, indem er dem Ländervertreter entsprechende Befugnisse nicht nur für alle Fälle der ausschließlichen Gesetzgebungskompetenz der Länder, sondern auch für das Verfahren von Landesbehörden einräumt.

Die im Regierungsentwurf vorgesehene starke Stellung der BfDI muss wegen der Vollzugskompetenz der Länder von starken verfahrensmäßigen Mitwirkungs- und Einflussmöglichkeiten der Datenschutzaufsichtsbehörden der Länder flankiert werden. Diese werden durch den Regierungsentwurf in angemessener Weise garantiert, indem § 18 Abs. 2 BDSG-neu-E zum einen vorsieht, dass die federführende Behörde den Vorschlag für den gemeinsamen Standpunkt festlegt und in allen Fällen die Möglichkeit besteht, dass der gemeinsame Standpunkt mehrheitlich von den Aufsichtsbehörden beschlossen wird.

Bei der Frage der Vertretung im EDSA ist zu berücksichtigen, dass dessen Entscheidungen die Auslegung der DSGVO maßgeblich steuern und zum Teil auch verbindlich festlegen werden. Seine Beschlüsse werden in der Regel über den Einzelfall hinauswirken. Insofern sind von seinen Beschlüssen nicht nur die Datenschutzaufsichtsbehörden der Länder, sondern alle deutschen Datenschutzaufsichtsbehörden betroffen, zumal die BfDI auf den Gebieten von Telekommunikation und Post ebenfalls Zuständigkeiten im nicht-öffentlichen Bereich hat. Zudem gibt es – beispielsweise beim Beschäftigtendatenschutz, bei Fragen der Videoüberwachung oder im Bereich der Verarbeitung personenbezogener Daten zu Forschungs- oder Statistikzwecken – vielfache Überschneidungen oder gemeinsame Zuständigkeiten der Aufsichtsbehörden von Bund und Ländern. Dem würde es nicht gerecht, wenn Deutschland jeweils nur von einem Ländervertreter repräsentiert wird. Bei der Vertretung in europäischen Angelegenheiten kommt es auf die Interessen des Gesamtstaates an. So wie in allen Fragen der europäischen Integration muss deshalb auch hier der Bund dafür einstehen und die Länder im Rahmen ihrer nationalen Vollzugskompetenzen verfahrensmäßig einbinden.

Jede Verschiebung der im Regierungsentwurf vorgesehenen Architektur zulasten des Bundes hätte zudem zwangsläufig Auswirkungen auf die nach § 17 Abs. 1 BDSG-neu-E bei der BfDI angesiedelte zentrale Anlaufstelle. Würde der Gesetzgeber den Datenschutzaufsichtsbehörden der Länder bei der Vertretung im EDSA eine stärkere Rolle zuschreiben, stellt sich die Frage, ob die Länder nicht auch die zentrale Anlaufstelle in gleicher Weise finanziell stärker ausstatten müssten.

Schließlich sichert die Wahrnehmung der Rolle des gemeinsamen Vertreters durch die BfDI – aufgrund der bisher seit mehr als 20 Jahren wahrgenommenen Vertretung in der Artikel 29 Datenschutzgruppe – die notwendige Kontinuität. Die in dieser Zeit gewachsenen Erfahrungen und Ressourcen sind eine gute Grund-

lage für den zu erwartenden komplexen Anpassungsprozess der besonderen föderalen Aufsichtsstruktur in Deutschland an die künftigen Abstimmungsmechanismen im Europäischen Datenschutzausschuss.

- b) Das im Gesetzentwurf vorgesehene Verfahren zur Festlegung eines gemeinsamen Standpunktes stellt grundsätzlich einen angemessenen Ausgleich zwischen den Interessen des Bundes und der Länder her. Sofern es sich allerdings um Angelegenheiten im Bereich der exklusiven Zuständigkeit der BfDI handelt (d. h. im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Erbringung von Post- oder Telekommunikationsdiensten) führt die in Satz 4 vorgesehene Mehrheitsentscheidung zu unbilligen Ergebnissen. Die BfDI könnte in diesen Fällen immer von den Landesaufsichtsbehörden überstimmt werden, obwohl diese keine Zuständigkeit haben. Diese Konstellation ist auch nicht mit dem umgekehrten Fall vergleichbar, da die BfDI allein bei einer Zuständigkeit der Landesaufsichtsbehörden nicht in der Lage wäre, das Ländervotum zu überstimmen. Auch im Verhältnis der Landesaufsichtsbehörden untereinander stellt sich das Problem nicht, da die Möglichkeit der Mehrheitsentscheidung nicht im Falle der Federführung, sondern nur dann gilt, wenn ohnehin mehrere oder alle Landesaufsichtsbehörden betroffen sind.

3. Ausschluss der Anordnung der sofortigen Vollziehung bei Maßnahmen gegenüber Behörden (§ 20 Abs. 7 BDSG-neu-E)

§ 20 Abs. 7 BDSG-neu-E lautet:

„Die Aufsichtsbehörde darf gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der Verwaltungsgerichtsordnung anordnen.“

Vorschlag BfDI:

Streichung.

Begründung:

Durch die Norm wird die Anordnung der sofortigen Vollziehung gegenüber Behörden ausgeschlossen. Dies ist nicht akzeptabel und die Begründung überzeugt nicht. Auch im öffentlichen Bereich wird es Fälle geben, in denen die Anordnung der sofortigen Vollziehung notwendig ist, um die Rechte der Betroffenen zu wahren. Angesichts der Dauer verwaltungsgerichtlicher Streitigkeiten ist diese Möglichkeit in dringenden Eilfällen unverzichtbar. Ordnet die BfDI beispielsweise die Beseitigung einer Sicherheitslücke in einem IT-System einer Behörde an, darf eine Klage der Behörde dagegen nicht dazu führen, dass dieser Zustand während der Dauer des Rechtsstreits nicht beseitigt wird. Würde die Anordnung der sofortigen Vollziehung zugelassen, wie im allgemeinen Verwaltungsrecht vorgesehen, hätten die Behörden wie jeder andere Adressat der aufsichtsbehördlichen Maßnahme die Möglichkeit, gem. § 80 Abs. 5 VwGO die Wiederherstellung der aufschiebenden Wirkungen zu beantragen.

4. Verarbeitung zu anderen Zwecken durch öffentliche Stellen (§ 23 Abs. 1 BDSG-neu-E)

§ 23 Abs. 1 BDSG-neu-E lautet:

„(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

- 1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,*
- 2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,*
- 3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,*
- 4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,*
- 5. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,*
- 6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder*
- 7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.“*

Vorschlag BfDI:

§ 23 Abs. 1 wird wie folgt gefasst:

„(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu

demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, ~~es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,~~
4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
5. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, ~~soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.~~

und sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. “

Begründung:

Wie auch bei der Verarbeitung zu anderen Zwecken durch nicht öffentliche Stellen (§ 24 BDSG-neu-E) sollte bei der zweckändernde Verarbeitung durch öffentliche Stellen in allen von den Nummern 1 bis 7 des § 23 Abs. 1 genannten Varianten als Korrektiv eine Interessenabwägung vorgesehen werden. Der Regierungsentwurf schreibt eine solche Interessenabwägung nur in § 23 Abs. 1 Nr. 3 und Nr. 7 BDSG-neu-E vor. Die Erforderlichkeit einer Interessenabwägung ergibt sich schon daraus, dass - wie in der Gesetzesbegründung ausgeführt- den Mitgliedstaaten durch die Verordnung Regelungsspielraum nur insoweit gewährt wird, als die nationale Rege-

lung eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme“ zum Schutz der in Art. 23 genannten Ziele darstellt. Die Verhältnismäßigkeit gebietet es, neben den in § 23 Abs. 1 Nr. 1 bis 7 BDSG-neu-E genannten Rechtsgüter auch die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung einzubeziehen. Beispielsweise wäre sonst jede zweckändernde Datenverarbeitung durch öffentliche Stellen zulässig, wenn sie zur Sicherung des Steueraufkommens erforderlich ist (Nr. 5), unabhängig von der Höhe der Steuerschuld und der Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung der betroffenen Person.

5. Untersuchungsbefugnisse der Aufsichtsbehörden bei Geheimhaltungspflichten (§ 29 Abs. 3 BDSG-neu-E)

§ 29 Abs. 3 BDSG-neu-E lautet:

„(3) Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.“

Vorschlag BfDI:

§ 29 Abs. 3 wird wie folgt gefasst:

„(3) Die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 erstrecken sich auch auf Berufs- und besondere Amtsgeheimnisse. Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen diese Befugnisse nur insoweit, als ihre Inanspruchnahme zur Ausübung der Datenschutzaufsicht unabdingbar ist. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.“

Begründung:

Die im Entwurf der Bundesregierung vorgesehenen Einschränkungen der Befugnisse auf Zugang zu personenbezogenen Daten und den Geschäftsräumen und Datenverarbeitungsanlagen von Berufsgeheimnisträgern sind insgesamt zu unpräzise und lassen einen weiten Interpretationsspielraum zu. Auch die Gesetzesbegründung liefert keine präzisen Hinweise zur Auslegung der Norm. Es ist deshalb zweifelhaft, ob § 29 Abs. 3 BDSG-neu-E tatsächlich notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen und damit den Anforderungen der Öffnungsklausel des Art. 90 DSGVO gerecht wird. Vielmehr besteht die Gefahr, dass beispielsweise Ärzte oder Rechtsanwälte den Beschäftigten der Aufsichtsbehörden unter Berufung auf ihre Geheimhaltungspflicht und § 29 Abs. 3 BDSG-neu-E pauschal den Zugang zu ihren

Geschäftsräumen und Datenverarbeitungsanlagen verwehren könnten. Das würde im Ergebnis dazu führen, dass gar keine Datenschutzkontrolle mehr stattfinden würde, was einen Verstoß gegen die DSGVO darstellen würde und auch nicht von dem in der Gesetzesbegründung zitierten Urteil des Bundesverfassungsgerichts bezweckt ist.

Die vorgeschlagene alternative Formulierung würde hingegen in Satz 1 zunächst klarstellen, dass sich die Datenschutzkontrolle – wie im geltenden Recht – auch auf besondere Amtsgeheimnisse und Berufsgeheimnisse erstreckt. Hinsichtlich der Berufsgeheimnisse stellt Satz 2 einen Ausgleich zwischen den Geheimhaltungspflichten und der Datenschutzkontrolle her, indem der Zutritt zu den Geschäftsräumen und der Zugang zu den gespeicherten Daten auf das notwendige Maß beschränkt wird. Sollte die Aufsichtsbehörde dabei Kenntnis von Daten erlangen, die unter das Berufsgeheimnis fallen, ist durch § 29 Abs. 3 Satz 2 BDSG-neu-E gewährleistet, dass diese Daten von der Aufsichtsbehörde nicht weitergegeben oder offenbart werden.

6. Einschränkungen von Betroffenenrechten

Der Entwurf des BDSG-neu enthält in Kapitel 2 einige Paragraphen, die die in der DSGVO vorgesehenen Betroffenenrechte einschränken. Zwar lässt Art. 23 DSGVO Beschränkungen grundsätzlich zu, allerdings nur unter strengen Voraussetzungen, die im Entwurf des BDSG-neu nicht immer eingehalten werden. Dies gilt insbesondere für die folgenden Normen:

- **§ 32 Abs.1 Nr. 5 BDSG-neu-E**

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

...

5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.“

Vorschlag BfDI:

Streichung von § 32 Abs. 1 Nr. 5.

Begründung:

Die Norm eröffnet ihrem Wortlaut nach einen weiten Spielraum, in dem auf die Information der betroffenen Person verzichtet werden kann. Zwar stellt die Begründung klar, dass sich die Ausnahme nur auf spezifische Fälle im Kontext der öffentlichen Sicherheit bezieht. Dies ist aber bereits durch § 32 Absatz 1 Nummern 2 und 3 abgedeckt. „Vertraulichkeit“ als solche ist kein Schutzgut im Sinne von Artikel 23 DSGVO, vielmehr sind bestimmte Zwecke der Datenverarbeitung zu schützen, was – wie dargelegt – bereits durch die Nummern 2 und 3 sichergestellt wird.

- **§ 33 Abs. 1 Nr. 1 Buchstabe a) BDSG-neu-E**

§ 33 Abs. 1 Nr. 1 Buchstabe a) BDSG-neu-E lautet:

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Falle einer öffentlichen Stelle

- a) *die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679 gefährden würde.*“

Vorschlag BfDI:

Streichung von § 33 Abs. 1 Nr. 1 Buchstabe a).

Begründung:

Der Tatbestand erfüllt nicht die Anforderungen an die Verhältnismäßigkeit, wie sie von Artikel 23 DSGVO gefordert werden. Das pauschale Abstellen auf eine Gefährdung der Aufgabenerfüllung in Verbindung mit dem Verweis auf Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung sind nicht ausreichend. Vielmehr müssten zumindest konkrete Fallgestaltungen in den Normtext aufgenommen werden. Andernfalls ist die Nummer zu streichen.

• **§ 33 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu-E**

§ 33 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu-E lautet:

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahmen nicht, wenn die Erteilung der Information

1. im Falle einer nicht-öffentlichen Stelle

- a) *allgemein anerkannte Geschäftszwecke des Verantwortlichen erheblich gefährden würde, es sei denn dass das Interesse der betroffenen Person an der Informationserteilung überwiegt.*“

Vorschlag BfDI:

Streichung von § 33 Abs. 1 Nr. 2 Buchstabe a).

Begründung:

Die erhebliche Gefährdung der Geschäftszwecke des Verantwortlichen rechtfertigt trotz der verankerten Interessenabwägung in dieser Allgemeinheit nicht die Einschränkung der Informationspflicht. Es bedarf vielmehr einer konkreten Bezugnahme auf die Tatbestände des Artikels 23 Abs. 1 der DSGVO und die Einschränkung muss

der Prüfung standhalten, ob es sich dabei um eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme handelt. Ob hiermit reine Privatinteressen überhaupt geschützt werden können, erscheint zweifelhaft. Auch die vorgesehene Interessenabwägung hilft letztlich zur Rechtfertigung der Beschränkung nicht weiter, da der Verantwortliche zunächst ohne Weiteres das Nicht-Überwiegen der Interessen der betroffenen Person behaupten kann.

7. § 48 BDSG-neu-E (Verarbeitung besonderer Kategorien personenbezogener Daten)

§ 48 BDSG-neu-E lautet:

„(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein

- 1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,*
- 2. die Festlegung von besonderen Aussonderungsprüffristen,*
- 3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,*
- 4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,*
- 5. die von anderen Daten getrennte Verarbeitung,*
- 6. die Pseudonymisierung personenbezogener Daten,*
- 7. die Verschlüsselung personenbezogener Daten.*
- 8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.“*

Vorschlag BfDI:

§ 48 wird wie folgt gefasst:

„Die Verarbeitung besonderer Kategorien von Daten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt.“

Begründung:

Der Inhalt des Vorschlags der Bundesregierung geht nicht über die Vorgaben der Richtlinie hinaus und stellt keine Konkretisierung dar. In welchen Fällen Polizei- und Strafverfolgungsbehörden sensitive Daten speichern dürfen, sollte ausschließlich in den Fachgesetzen geregelt werden.

8. § 49 BDSG-neu-E (Zweckbindung)

§ 49 BDSG-neu-E lautet:

„Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.“

Vorschlag BfDI:

§ 49 wird wie folgt gefasst:

„Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als demjenigen, zu dem sie erhoben wurden, ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt.“

Begründung:

Diese Vorschrift betrifft die zentralen Aussagen zur Zweckbindung im Urteil des Bundesverfassungsgerichts zum BKAG (BVerfG NJW 2016, 1781). Die Vorschrift ist nicht mit den Aussagen des Urteils vereinbar. Die Zwecke der Gefahrenabwehr und der Strafverfolgung werden nicht hinreichend differenziert. Zudem bleiben die Aussagen sogar hinter § 481 StPO zurück, der seinerseits nicht mehr den verfassungsrechtlichen Anforderungen entspricht. Das BVerfG hält eine Übermittlung personenbezogener Daten aus eingriffsintensiven Ermittlungsmaßnahmen zum einen nur für zulässig, wenn ein gleichgewichtiger Rechtsgüterschutz besteht. Darüber hinaus muss sich aus einem hinreichend spezifischen Anlass ein konkreter Ermittlungsansatz ergeben. Ein lediglich potentieller Ermittlungsansatz oder gar eine allgemeine Nützlichkeit ist nicht ausreichend. Vor diesem Hintergrund sollten die Anforderungen an die Zulässigkeit von Zweckänderungen konkret im Fachrecht geregelt werden.

9. § 64 Absätze 2 und 3 BDSG-neu-E (Anforderungen an die Sicherheit der Datenverarbeitung)

§ 64 Absätze 2 und 3 BDSG-neu-E lauten:

„(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich ist. Die Maßnahmen nach Satz 1 sollen dazu führen, dass

- 1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt wird und*
- 2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.*

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

- 1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),*
- 2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),*
- 3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),*
- 4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),*
- 5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle),*
- 6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),*
- 7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),*
- 8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird (Transportkontrolle),*

9. Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellbarkeit),
 10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
 11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
 12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
 13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
 14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennbarkeit).
- Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.“

Vorschlag BfDI:

Aufnahme eines neuen Absatzes 2 statt der bisherigen Absätze 2 und 3.

„(2) Dabei ist insbesondere zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können und in das Verfahren eingegriffen werden kann (Authentizität und Intervention),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).“

Begründung:

Die Norm beinhaltet Regelungen, die sich an den ersten Datenschutzgesetzen aus den 1970er und 1980er Jahren orientieren und die inzwischen fachlich als veraltet

anzusehen sind. So geht § 64 Abs. 3 Nr. 2 BDSG-neu-E beispielsweise an den technischen Möglichkeiten vorbei. Man kann zwar durch Verschlüsselung versuchen, einen Unbefugten vom Datenzugriff abzuhalten, wie man das Kopieren, Löschen, usw. verhindern will, bleibt aber offen. Es wird deshalb die oben dargestellte, zeitgemäße Alternativregelung vorgeschlagen.

10. § 76 Abs. 3 BDSG-neu-E (Verwendung von Protokolldaten)

§ 76 Abs. 3 BDSG-neu-E lautet:

„(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.“

Vorschlag BfDI:

Abs. 3 wird wie folgt gefasst:

„(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten verwendet werden.“

Begründung:

Protokollierung ist eine Verfahrenssicherung, die den Grundrechtseingriff der Datenverarbeitung abmildern soll. Sie darf deshalb nicht ihrerseits zu zusätzlichen Grundrechtseingriffen führen. Dies schließt die allgemeine Verwertung für die Strafverfolgung aus. Art. 25 Abs. 2 DS-RL, der erst im Trilog um die Möglichkeit der Nutzung von Protokolldaten für Strafverfahren ergänzt wurde, kann nicht dahingehend ausgelegt werden, dass eine Verwendung für jegliches Strafverfahren zulässig sein soll. Dies wäre mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Für die Verfolgung von Straftaten, die durch die Verwendung der personenbezogenen Daten begangen wurden, ist eine solche Regelung nicht erforderlich. Denn dieser Zweck ist bereits von der Zweckbestimmung „Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ erfasst. Die Richtlinie soll die nationale Verarbeitung begrenzen, nicht zu einer Erweiterung der Datenverarbeitung führen. Insofern sollte die Verwendung für Strafverfahren gestrichen werden.

II. Artikel 4 (Änderung des BND-Gesetzes)

1. § 32 BNDG-E (Unabhängige Datenschutzkontrolle)

In der Begründung zu § 32 BNDG-E (S. 69) wird Folgendes ausgeführt:

„Das in § 26a Absatz 3 Nr. 2 Bundesverfassungsschutzgesetz geregelte Zutrittsrecht zu allen Diensträumen bezieht sich nur auf die vom Bundesnachrichtendienst genutzten Räume. Räume, welche beispielsweise bei gemeinsam genutzten Dienststellen ausschließlich durch andere Einrichtungen genutzt werden, sind keine Diensträume des Bundesnachrichtendienstes. Insoweit besteht folglich auch kein Betretungsrecht nach dieser Vorschrift.“

Vorschlag BfDI:

Streichung der vorgenannten Sätze

Begründung:

Die Entwurfsbegründung lässt sich aus dem Wortlaut des in Bezug genommenen § 26 a Abs. 3 Nr. 2 BVerfSchG nicht herleiten und steht in Widerspruch zum geltenden Recht (vgl. §§ 24 Abs. 4 Satz 1 Nr. 2 BDSG i.V.m. § 1 Abs. 5 Satz 2 BDSG). Nach § 1 Abs. 5 Satz 2 i.V.m. Satz 4 BDSG gilt das BDSG – und damit auch das Zutrittsrecht der BfDI –, wenn eine verantwortliche Stelle, die außerhalb der EU (d.h. in einem Drittstaat) „belegen ist“ (§ 1 Abs. 5 Satz 2 BDSG), im Inland personenbezogene Daten erhebt, verarbeitet oder nutzt und nicht nur Datenträger zum Zweck des Transits durch das Inland einsetzt. Befinden sich demnach in einer Liegenschaft des BND im vorgenannten Sinne Räume, die z.B. ausschließlich von einem Nachrichtendienst eines Drittstaates genutzt werden, sind dies nach geltendem Recht Räume, zu denen die BfDI zutrittsberechtigt ist.

Die Entwurfsbegründung widerspricht den verfassungsrechtlichen Vorgaben zur Gewährleistung einer umfassenden und effizienten Kontrolle durch die BfDI und der der BfDI vom Bundesverfassungsgericht zugewiesenen Kompensationsfunktion zum Schutz der Grundrechte der Betroffenen. Die BfDI muss die Befugnis haben, eine behauptete Unzuständigkeit bezüglich des Zutrittsrechts überprüfen zu dürfen.

Zugunsten des BfV und des MAD existieren keine vergleichbaren Begründungen.

2. § 32a BNDG-E (Anwendung des Bundesdatenschutzgesetzes)

§ 32a Abs. 1 Nr. 1 lit. b) BNDG-E lautet:

„b) findet § 14 Absatz 2 mit der Maßgabe Anwendung, dass sich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur an die Bundesregierung sowie an die für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien (Parlamentarisches Kontrollgremium, Vertrauensgremium, G 10-Kommission, Unabhängiges Gremium) wenden darf; eine Befassung der für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien setzt voraus, dass sie oder er der Bundesregierung entsprechend § 16 Absatz 2 Satz 1 Bundesdatenschutzgesetz zuvor Gelegenheit gegeben hat, innerhalb einer von ihr oder ihm gesetzten Frist Stellung zu nehmen;“

BfDI-Vorschlag:

Streichung von § 32a Abs. 1 Nr. 1 lit. b). Lit. a) wird dann unmittelbar zu Nr. 1.

Begründung:

§ 32 a Abs. 1 Nr. 1 lit. b) BNDG-E schränkt das geltende Recht (vgl. § 26 Abs. 2 Satz 3 BDSG) – das von § 14 Abs. 2 BDSG-neu fortgeschrieben wird – zu Lasten der BfDI und des Deutschen Bundestages verfassungswidrig ein. Nach diesem Regelungsvorschlag soll § 14 Abs. 2 BDSG-neu, wonach sich die BfDI – ebenso wie nach geltendem Recht (vgl. § 26 Abs. 2 Satz 3 BDSG) – von sich aus an den Deutschen Bundestag oder seine Ausschüsse wenden kann, in Bezug auf die den BND betreffende Sachverhalte nur mit der Maßgabe gelten, dass sich die BfDI nur an die Bundesregierung sowie an die für die Kontrolle des BND zuständigen Gremien (PKGr, G 10, Vertrauensgremium, Unabhängiges Gremium) wenden darf – und auch nur sofern der Bundesregierung entsprechend § 16 Abs. 2 Satz 1 des Gesetzentwurfs zuvor Gelegenheit zur Stellungnahme gewährt worden ist.

Dies bedeutet, dass sich die BfDI im Gegensatz zum geltenden Recht den BND betreffend nicht mehr an den Deutschen Bundestag oder seine Ausschüsse wenden dürfte – und damit insbesondere nicht an den Innenausschuss oder einen Untersuchungsausschuss des Deutschen Bundestages, der z.B. BND-relevante Sachverhalte aufklären soll.

Diese Beschränkung steht nicht nur in Widerspruch zu verfassungsgerichtlichen Vorgaben. Sie widerspricht auch der durch den Europäischen Gerichtshof geforderten Unabhängigkeit der BfDI. Zudem beschränkt diese Regelung in unzulässiger Weise das Informationsrecht des Parlaments und seiner Ausschüsse.

In Bezug auf das BfV und den MAD enthält der Gesetzentwurf keine vergleichbaren Einschränkungen für die BfDI.

Die hier vorgeschlagene Streichung würde zu einer unmittelbaren Anwendbarkeit des § 14 Abs. 2 BDSG-neu führen und damit den oben beschriebenen verfassungsrechtlichen Ansprüchen genügen.

Neben den vorgenannten grundsätzlichen Kritikpunkten sieht die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an weiteren Stellen Änderungsbedarf. Dazu gehören folgende Punkte:

- **Art. 1, § 4 BDSG-neu-E:** Die Schaffung einer nationalen Regelung zur Videoüberwachung durch nicht-öffentliche Stellen ist europarechtlich zweifelhaft. Die wortgleich aus dem Entwurf des Videoüberwachungsverbesserungsgesetzes übernommenen Änderungen tragen nicht zu einer Erhöhung der öffentlichen Sicherheit bei und sind daher unnötig.
- **Art. 1, § 27 Abs. 2 Satz 2 BDSG-neu-E:** Das Recht auf Auskunft bei der Verarbeitung personenbezogener Daten zu Forschungszwecken sollte nicht schon dann entfallen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand darstellt, da das Auskunftsrecht häufig die einzige Möglichkeit für den Betroffenen darstellt, Transparenz herzustellen.
- **Art. 2, § 26a Abs. 2 BVerfSchG-E:** Zur Vermeidung von Kontrolllücken sowie zur sachgerechten Abgrenzung zwischen den Kompetenzen der BfDI einerseits und der G-10-Kommission andererseits bedarf es einer Neuregelung des § 15 Abs. 5 Satz 2 G 10.

gez.

Andrea Voßhoff

Nr. 23/16
Dezember 2016

Stellungnahme des Deutschen Richterbundes zum Referentenentwurf für ein Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU)

Deutscher Richterbund
Haus des Rechts
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

A. Tenor der Stellungnahme

Mit dem vorgelegten Referentenentwurf ist eine Absenkung des derzeit in Deutschland geltenden Datenschutzniveaus zu befürchten.

Der Gesetzentwurf erscheint aufgrund der gleichzeitigen Umsetzung von Datenschutz-Grundverordnung und JI-Richtlinie strukturell unübersichtlich und für den Rechtsanwender schwer verständlich.

Datenschutzrechtliche Regelungen für den justiziablen Bereich sollten bereichsspezifisch in den jeweiligen Verfahrensordnungen geregelt werden, insbesondere im Bereich des Ermittlungs- und Strafverfahrens.

Verfasser der Stellungnahme:
Marco Rech, Richter am Oberlandesgericht,
Mitglied des Präsidiums

B. Bewertung im Einzelnen

Aufgrund des Umfangs des geplanten Gesetzentwurfs und der – auch vom Bundesministerium des Innern festgestellten – Komplexität der zu regelnden Materie kann der Gesetzentwurf nicht vertieft innerhalb der gesetzten Frist von knapp elf Arbeitstagen in allen Details geprüft werden. Der Deutsche Richterbund nimmt daher nur zu einzelnen Punkten wie folgt vorläufig Stellung:

Mit dem Gesetzentwurf soll in einem Zuge sowohl das deutsche Datenschutzrecht an die Verordnung (EU) 2016/679 (nachfolgend: DS-GVO) angepasst werden als auch die Richtlinie (EU) 2016/680 (nachfolgend: JI-Datenschutz-RL) zumindest teilweise umgesetzt werden, indem das Bundesdatenschutzgesetz umfassend neu gefasst wird. In diesem Zusammenhang sollen auch Änderungen im Bundesverfassungsschutzgesetz, MAD-Gesetz, BND-Gesetz und Sicherheitsüberprüfungsgesetz erfolgen. All dies erscheint im Hinblick auf den Umfang der zu ändernden Regelungen als auch im Hinblick auf den unterschiedlichen Anwendungsbereich von DS-GVO und JI-Datenschutz-RL und die Komplexität der Regelungsmaterie strukturell schwierig. Der Gesetzentwurf ist überfrachtet; der Regelungsinhalt ist aus sich heraus nur schwer verständlich. Die vorgeschlagenen Regelungen dürften selbst für einen fachkundigen Rechtsanwender vielfach nur schwierig zu erfassen sein.

Insgesamt steht – trotz der bei den Verhandlungen zur DS-GVO vorhandenen Bestrebungen zum Erhalt des aktuell geltenden hohen Datenschutzniveaus im nationalen Recht – zu befürchten, dass es mit den vorgeschlagenen Regelungen insgesamt zu einer Absenkung des Datenschutzniveaus in Deutschland kommt. Der Grundsatz der Datensparsamkeit wird nicht ausreichend deutlich. Auch bestehen nach dem Gesetzentwurf umfangreiche Möglichkeiten, erhobene Daten zu anderen Zwecken, als denen, zu denen diese erhoben wurden, zu verwenden, hier insbesondere zum Zwecke des Profilings durch private Stellen, aber auch zum Zwecke der Rasterung zum Zwecke der Gefahrenabwehr bzw. Strafverfolgung durch öffentliche Stellen. Der bisher geltende Zweckbindungsgrundsatz wird damit untergraben. Auch sollen die Informations-, Auskunfts-, Löschungs- und Widerspruchsrechte der Betroffenen im privaten Bereich über die DS-GVO hinaus eingeschränkt werden, was verfassungsrechtlich bedenklich erscheint.

Unionsrechtlich erscheint im hohen Grade problematisch, ob eine Wiederholung der Definitionen im Anwendungsbereich der DS-GVO zulässig ist. Die Begründung zu § 2 BDSG-E überzeugt insoweit nicht.

Im Hinblick auf das Ermittlungs- und Strafverfahren sollte eine Umsetzung der JI-Datenschutz-RL nicht im Bundesdatenschutzgesetz, sondern weitgehend im Rahmen der StPO erfolgen. Im Rahmen der Umsetzung ist sicherzustellen, dass der durch die JI-Datenschutz-RL vorgegebene Schutz der Daten aller Betroffenen in die Regelungen zu entsprechenden Ermittlungsmaßnahmen in die StPO eingearbeitet wird, hier insbesondere auch in Bezug auf Akteneinsichtsrechte und Aktenlöschungsfristen. Auch sollte zunächst im Detail geprüft werden, inwieweit es weiterer Vorgaben eines Datenschutzrechtes im Strafverfahrensrecht – aber auch in den anderen Verfahrensordnungen – bedarf. Entsprechende Ausführungen sind der Gesetzesbegründung nicht in ausreichendem Umfang zu entnehmen. Jedenfalls darf es für das Strafverfahrensrecht nicht zu einer Vermischung der Rechtsschutzmöglichkeiten gegen (straf-)prozessuale Maßnahmen und den datenschutzrechtlichen Beanstandungsmöglichkeiten kommen.

Die Regelungen zur Bestellung eines behördlichen Datenschutzbeauftragten bei Gericht und Staatsanwaltschaften können so nicht überzeugen. Bei Gerichten soll ein zu benennender Datenschutzbeauftragter nicht für die im Rahmen der justiziellen Tätigkeit zu verarbeitenden Daten zuständig sein. Anders soll dies bei Staatsanwaltschaften sein, bei denen der Datenschutzbeauftragte für alle Daten zuständig sein soll. Dies kann inhaltlich nicht überzeugen, auch wenn die Differenzierung europarechtlich wohl gerechtfertigt werden kann. Aus Sicht des Deutschen Richterbundes macht es keinen Unterschied, ob eine Staatsanwaltschaft dieselben Daten im Rahmen eines Ermittlungsverfahrens oder ein Gericht im Rahmen eines Gerichtsverfahrens speichert. Derselbe Widerspruch findet sich in § 55 BDSG-E. Der Deutsche Richterbund plädiert insofern dafür, den Aufgabenkreis des behördlichen Datenschutzbeauftragten bei den Staatsanwaltschaften entsprechend dem gerichtlichen Datenschutzbeauftragten zu bestimmen.

§ 46 BDSG-E enthält eine Regelung zu Zweckänderungen, geht aber nicht auf die besonderen Daten des § 45 BDSG-E ein. Damit könnte der Eindruck entstehen, dass besondere Daten nach § 45 BDSG-E, wenn sie erst einmal erhoben sind, immer zu anderen Zwecken genutzt werden können, wenn die Voraussetzungen des § 43 BDSG-E vorliegen. Zumindest zur Klarstellung sollte in § 46 BDSG-E geregelt werden, dass die besonderen Daten für andere Zwecke bei dem Dritten nur dann genutzt werden dürfen, wenn auch die Voraussetzungen des § 45 BDSG-E gegeben sind.

Im Hinblick auf die noch nicht abgeschlossene Abstimmung des Gesetzentwurfs innerhalb der Bundesregierung und den erfahrungsgemäß daraus resultierenden Änderungen behält sich der Deutsche Richterbund im weiteren Verfahren eine weitere Stellungnahme vor.

Der Deutsche Richterbund ist mit mehr als 16.000 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.

Stellungnahme zum Gesetzentwurf 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)

der Verfasser

Deutsche Forschungsgemeinschaft

Fraunhofer-Gesellschaft

Helmholtz-Gemeinschaft

Leibniz-Gemeinschaft

Max-Planck-Gesellschaft

Max Weber Stiftung

Medizinischer Fakultätentag

Rat für Sozial- und Wirtschaftsdaten

TMF - Technologie- und Methodenplattform für die vernetzte medizinische
Forschung

Verband der Universitätsklinika Deutschlands

Stand 16. Februar 2017

Stellungnahme zum Gesetzentwurf der Bundesregierung

I. Vorbemerkung

Die EU-Verordnung 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 (EU-Datenschutzgrundverordnung) wird am 25. Mai 2018 in allen Mitgliedsstaaten der Europäischen Union unmittelbar gelten. Zur Umsetzung der darin enthaltenen Öffnungsklauseln und Regelungsaufträge werden Anpassungen am bislang geltenden Bundesdatenschutzgesetz (BDSG) notwendig, die mit dem Entwurf dieses Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) adressiert werden. Darüber hinaus dient der Gesetzentwurf auch der Umsetzung der EU-Richtlinie 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung und Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Am 1. Februar 2017 beschloss das Kabinett den Regierungsentwurf „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)“.

Die Verfasser dieser Stellungnahme bilden einen großen Teil der Forschungslandschaft Deutschlands, der entweder mittelbar oder unmittelbar durch die öffentliche Hand getragen wird, ab. Sie verstehen sich daher als Vertreter der gemeinsamen Interessen der öffentlich finanzierten Forschung in Deutschland.

Diese Stellungnahme bezieht sich vorrangig auf die für die wissenschaftliche Forschung relevanten Inhalte des Artikel 1 des Gesetzentwurfes der Bundesregierung (nachfolgend DSAnpUG-EU - E) in der Bundesrat-Drucksache 110/17 vom 02. Februar 2017.

II. Grundlegende Bewertung

Die Verfasser begrüßen die in den Gesetzentwurf der Bundesregierung als § 27 DSAnpUG-EU - E eingegangenen Regelungen für die wissenschaftliche Forschung grundsätzlich.

Der Gesetzentwurf eröffnet die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken ohne Einwilligungserklärung unter Schaffung angemessener und spezifischer Maßnahmen zur Wahrung der Betroffenenrechte, die in § 22 Absatz 2 DSAnpUG-EU - E beschrieben werden. Die Verfasser befürworten die im Gesetz enthaltene Abwägung zwischen dem Interesse der betroffenen Person und dem der Forschungseinrichtung.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Für die Durchführbarkeit einiger Forschungsvorhaben bleibt es unabdingbar, dass Rechte der Betroffenen eingeschränkt werden können. Dies nutzen Forschungseinrichtungen bereits bisher nicht leichtfertig und nur dann, wenn das Forschungsziel nicht auf anderem Wege erreicht werden kann. Das Bundesdatenschutzgesetz in der alten Fassung enthält vergleichbare Vorschriften und folgt dem Grundsatz der Grundrechteabwägung zwischen der Forschungsfreiheit und der informationelle Selbstbestimmung. Die Verfasser bewerten die Umsetzung dieser Einschränkungen der Betroffenenrechte im Gesetzentwurf der Bundesregierung noch als unzureichend. Darüber hinaus weisen die Verfasser darauf hin, dass durch die gewählte Ausformulierung der Einschränkung der Betroffenenrechte Rechtsunsicherheit bei den Anwendern entsteht.

Neben der Anpassung des Bundesdatenschutzgesetzes als allgemeines Datenschutzrecht des Bundes, ist eine umfangreiche Überarbeitung der entsprechenden landesgesetzlichen Regelungen zu erwarten.

Die aus Anwendersicht und aus Sicht des europäischen Gesetzgebers gewünschte Harmonisierungswirkung der EU-Datenschutzgrundverordnung kann aufgrund der verteilten Gesetzgebungskompetenz des Bundes und der Länder in ihren faktischen Ausprägungen in Deutschland unterschiedlich sein. Die Verfasser empfehlen den nationalen Gesetzgebern daher nachdrücklich, eine einheitliche Ausgestaltung der für die wissenschaftliche Forschung relevanten Regelungen zu treffen, um eine bundeslandübergreifende Forschung mit gleichen Datenschutzstandards zu gewährleisten. Dies gilt insbesondere für die Landesdatenschutzgesetze sowie die Krankenhaus- und Statistikgesetze der Länder.

III. Stellungnahme im Einzelnen

1. Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten stellt die EU-Datenschutzgrundverordnung unter besonderen Schutz. Der Gesetzentwurf der Bundesregierung verpflichtet die für die Datenverarbeitung Verantwortlichen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Diese finden Eingang in den **§ 22 Absatz 2 Absatz 2 DSAnpUG-EU - E**. Die Verfasser begrüßen den Regelungsansatz sowie die vorgeschlagenen Maßnahmen und empfehlen dem Gesetzgeber die Klarstellung, dass diese in Form eines Datenschutzkonzeptes zu dokumentieren sind. Dies stellt nach Einschätzung der Verfasser keine zusätzliche Dokumentationsaufgabe dar, sondern fasst die Anforderungen, auch im Sinne der in Artikel 5 Absatz 2 der EU-Datenschutzgrundverordnung aufgeführten Rechenschaftspflichten in verständlicher und handhabbarer Weise zusammen.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Bereits heute gibt es eine Vielzahl von Forschungsorganisationen, Aufsichtsbehörden und Projektträgern, die die Erstellung von Datenschutzkonzepten für Forschungsvorhaben voraussetzen. Auch die Ethikkommissionen beschäftigen sich verstärkt mit dem Thema Datenschutz und interessieren sich vor Votierung einzelner Forschungsvorhaben für die eingerichteten Schutzmaßnahmen in den Forschungsorganisationen.

Die Aufnahme des Begriffs „Datenschutzkonzept“ im Kontext von Forschungsvorhaben mit besonderen Kategorien personenbezogener Daten erscheint den Verfassern als sinnvolle Präzisierung des eigentlichen Regelungswillens dieser Vorschrift.

Formulierungsvorschlag für § 22 Absatz 2 DSAnpUG-EU - E

„In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen und in einem Datenschutzkonzept zu beschreiben. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

- 1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,*
- 2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,*
- 3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,*
- 4. Benennung einer oder eines Datenschutzbeauftragten,*
- 5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,*
- 6. Pseudonymisierung personenbezogener Daten,*
- 7. Verschlüsselung personenbezogener Daten,*
- 8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,*
- 9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder*
- 10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.*

Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 1 Buchstabe b keine Anwendung.“

Stellungnahme zum Gesetzentwurf der Bundesregierung

2. Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Der **Absatz 1 des § 27 DSAnpUG-EU - E** eröffnet die Möglichkeit der Verarbeitung besonderer Kategorien personenbezogener Daten ohne Einwilligung der betroffenen Person zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken.

Dies kann beispielsweise in der Sozialforschung der Fall sein, wenn entsprechende personenbezogene Daten von Behörden oder Körperschaften des öffentlichen Rechts an Forschungseinrichtungen übermittelt werden, die diese dann bei Vorliegen der Voraussetzungen, jedoch ohne separate Einwilligungserklärung der betroffenen Personen, unmittelbar zu Forschungszwecken nutzen.

In der biomedizinischen Forschung gibt es eine Reihe von Beispielen, in denen aus technischen, organisatorischen oder auch ethischen Gründen die Einholung einer Einwilligungserklärung nicht möglich oder nicht angemessen erscheint. Genannt sei hier beispielsweise die Frage des Umgangs mit bereits bestehenden genetischen Daten und Biomaterialproben, die gerade nicht auf der Grundlage einer Einwilligungserklärung erhoben wurden. Die Einholung einer nachträglichen Einwilligungserklärung ist zumindest dann ausgeschlossen, wenn die Identität der betroffenen Person nicht mehr hergestellt werden kann. Zudem kann die nachträgliche Einholung einer Einwilligungserklärung das Recht eines Probanden auf Nicht-Wissen verletzen, zum Beispiel wenn bestehende Daten für ein neues Forschungsprojekt aufgrund der Entdeckung eines Risiko-Markers für Demenz genutzt werden sollen.

Für die Fälle, bei denen eine informierte Einwilligungserklärung nicht eingeholt werden kann, ist eine gesetzliche Grundlage mithin unerlässlich, die eine Abwägung aller relevanten Interessen ermöglicht. Darüber hinaus werden die für die Datenverarbeitung Verantwortlichen in diesen Fällen verpflichtet, umfangreichen Garantien zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß § 22 Absatz 2 DSAnpUG-EU - E zu treffen.

§ 27 Absatz 2 DSAnpUG-EU - E schränkt die Rechte auf Auskunft, Berichtigung, eingeschränkter Verarbeitung sowie das Recht auf Widerspruch von betroffenen Personen insoweit ein, als die Einschränkung der Betroffenenrechte notwendig ist und diese Rechte die Umsetzbarkeit von Forschungsvorhaben ernsthaft beeinträchtigen oder unmöglich machen würden. Aus Sicht der Verfasser birgt diese Vorschrift erhebliche Rechtsunsicherheit bei ihrer praktischen Anwendung. Auch unter Zuhilfenahme der Gesetzesbegründung (Seite 98, Bundesrat Drucksache 110/17 vom 02. Februar 2017) bleibt unklar, in welchen Fällen Forschungsvorhaben unmöglich oder ernsthaft beeinträchtigt wären.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Zumindest in medizinischen Forschungsvorhaben wird in der Tat regelmäßig ein Votum der zuständigen Ethikkommission eingeholt. Dies gilt jedoch nicht für Vorhaben aus anderen Forschungsbereichen, zum Beispiel der Sozialforschung oder psychologischen Forschung.

Zudem könnte die Beschränkung der Betroffenenrechte, insbesondere des Auskunftsrechtes, durch das Recht auf Datenübertragbarkeit gemäß Artikel 20 der EU-Datenschutzgrundverordnung aktuell umgangen werden, da § 27 Absatz 2 DSAnpUG-EU - E hierzu keine entsprechende Regelung enthält.

Die Verfasser empfehlen dem Gesetzgeber eine entsprechende Klarstellung in die Gesetzesbegründung aufzunehmen, aus der hervorgeht, welche Kriterien zur Einschränkung der Betroffenenrechte herangezogen werden können. Weiter wäre eine Klarstellung hilfreich, dass auch eine Einschränkung von Betroffenenrechten zu deren eigenem Schutz erforderlich sein kann. So können durch Analysemethoden aus personenbezogenen Daten neue Daten und gegebenenfalls besondere Kategorien personenbezogener Daten entstehen, die dem Selbstbild der betroffenen Person widersprechen könnten. Die Auskunft dieser Daten an die betroffene Person, könnte aus ethischen Erwägungsgründen unangebracht sein, da sie die betroffene Person erheblich belasten könnte. Weiterhin kann das Recht auf Auskunft während eines Vorhabens der Verhaltensforschung eine methodische Hürde darstellen, wenn die betroffene Person zur Durchführung des Forschungsvorhabens keine Information über dessen Verlauf erhalten darf, da sonst das Forschungsziel nicht erreicht werden kann.

Der Gesetzgeber eröffnet mit § 630 g Absatz 1 BGB bereits heute die Einschränkung der Betroffenenrechte bei der Einsichtnahme in die Patientenakte, soweit dieser Einsichtnahme erhebliche therapeutische Gründe entgegenstehen. Diesem allgemeinen Rechtsgedanken folgend, empfehlen die Verfasser dem Gesetzgeber eine entsprechende Ergänzung des § 27 Absatz 2 DSAnpUG-EU - E vorzusehen.

Formulierungsvorschlag für § 27 Absatz 2 DSAnpUG-EU - E

„Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde oder wenn die Auskunftserteilung dem Wohl der betroffenen Person nach therapeutischen, ethischen oder moralischen Erwägungsgründen zuwiderläuft oder schaden könnte.“

Stellungnahme zum Gesetzentwurf der Bundesregierung

Mit **§ 27 Absatz 3 DSAnpUG-EU - E** werden die für die Datenverarbeitung Verantwortlichen verpflichtet, die umfangreichen Garantien zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß § 22 Absatz 2 DSAnpUG-EU - E umzusetzen sowie die besonderen Kategorien von personenbezogenen Daten frühestmöglich zu anonymisieren. Im Kontext der Anonymisierung einzelner besonderer Kategorien personenbezogener Daten sehen die Verfasser eine verbleibende Rechtsunsicherheit - so beispielhaft bei genetischen Daten aus Biomaterialproben oder Bilddaten aus der Magnetresonanztomographie oder der gespeicherten Stimmenprobe. Aus diesem Grund empfehlen die Verfasser dem Gesetzgeber diese Vorschrift um die tatsächliche Möglichkeit des Anonymisierens nach dem Stand der Technik zu ergänzen.

Formulierungsvorschlag für § 27 Absatz 3 DSAnpUG-EU - E

„Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen ~~sind~~ sollten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ~~möglichst zu anonymisierten~~ werden, sobald dies nach dem Forschungs- oder Statistikzweck und dem Stand der Technik möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.“

Der **Absatz 4 des § 27 DSAnpUG-EU - E** bestimmt, dass für die Datenverarbeitung Verantwortliche personenbezogene Daten nur dann veröffentlichen dürfen, wenn die betroffene Person eingewilligt hat, oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Die Verfasser empfehlen dem Gesetzgeber, diese Vorschrift um den Anwendungsfall, dass die Daten bereits öffentlich zugänglich sind, zu erweitern.

Formulierungsvorschlag für § 27 Absatz 4 DSAnpUG-EU - E

„Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat, ~~die personenbezogenen Daten bereits allgemein zugänglich sind~~ oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“

Stellungnahme zum Gesetzentwurf der Bundesregierung

3. Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Die Verfasser empfehlen dem Gesetzgeber, die Rechtsgrundlagen zur Verarbeitung für Zwecke von Beschäftigungsverhältnissen nach **§ 26 DSAnpUG-EU - E** um zwei Anwendungsbereiche zu erweitern.

So fehlt aus Sicht der Verfasser in dem von der Bundesregierung vorgelegten Gesetzentwurf eine Rechtsgrundlage zur Verarbeitung dieser Daten zu Zwecken der Datenschutzkontrolle, den Tätigkeiten der Innenrevision sowie zur Datensicherung und Sicherung des ordnungsgemäßen Betriebes von Datenverarbeitungssystemen. Diese Regelungslücke kann derzeit lediglich im Anwendungsbereich des Bundesbeamtengesetzes durch dessen §§ 106, 107 aufgefangen werden.

Weiter empfehlen die Verfasser dem Gesetzgeber die Schaffung einer Rechtsgrundlage, um personenbezogene Daten von Beschäftigten für die Ausübung gesetzlicher Prüfungsrechte verarbeiten zu dürfen. Hintergrund einer solchen Anpassung ist zum Beispiel das Prüfrecht von Zuwendungsgebern, die sich dabei auf § 40 Absatz 1 Satz 3 Bundeshaushaltsordnung stützen. Die Verfasser vertreten die Rechtsauffassung, dass die Bundeshaushaltsordnung die Regelungen des Bundesdatenschutzgesetzes nicht verdrängen kann, da sie nicht den Schutz personenbezogener Daten regelt. Die Einwilligungserklärung als alternative Rechtsgrundlage für das Offenbaren personenbezogener Beschäftigtendaten, eignet sich nach Auffassung der Verfasser grundsätzlich nicht, da diese unter dem Vorbehalt des jederzeitigen Widerrufs durch den Beschäftigten steht. Das Prüfrecht der Zuwendungsgeber darf jedoch nicht von der freiwilligen und widerruflichen Einwilligungserklärung der Beschäftigten abhängen. Nach Einschätzung der Verfasser dürfte dieser Regelungsbedarf nicht ausschließlich für Forschungseinrichtungen, sondern mutmaßlich für alle Zuwendungsgeber und -empfänger relevant sein.

Formulierungsvorschlag für § 26 DSAnpUG-EU - E

„(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung

Stellungnahme zum Gesetzentwurf der Bundesregierung

nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Eine Verarbeitung für andere als die in Absatz 1 Satz 1 sowie Absatz 3 Satz 1 genannten Zwecke liegt nicht vor, wenn personenbezogene Daten von Beschäftigten ausschließlich für Zwecke der Datenschutzkontrolle oder zur Ausübung eines gesetzlich oder durch vergleichbare Vorschriften der Europäischen Union vorgesehenen Prüfungsrechts genutzt werden. Gleiches gilt, soweit im Rahmen der Datensicherung oder der Sicherung des ordnungsgemäßen Betriebes eines Datenverarbeitungssystems eine nach dem Stand der Technik nicht oder nur mit unverhältnismäßigem Aufwand zu vermeidende Kenntnisnahme von personenbezogenen Daten von Beschäftigten erfolgt.

Stellungnahme zum Gesetzentwurf der Bundesregierung

(7) Verantwortliche gewähren dem oder der Datenschutzbeauftragten Zugang zu personenbezogenen Daten von Beschäftigten sowie zur Personalakte. Zugang haben ferner die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse nur auf diesem Weg und nicht durch Auskunft aus der Personalakte gewinnen können. Jede Einsichtnahme nach Satz 2 ist aktenkundig zu machen. Die Beteiligungsrechte der Interessenvertretung der Beschäftigten bleiben unberührt.

(8) Die Absätze 1 bis 7 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(9) Beschäftigte im Sinne dieses Gesetzes sind:

- 1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeiterinnen und Leiharbeiter im Verhältnis zum Entleiher,*
- 2. zu ihrer Berufsbildung Beschäftigte,*
- 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),*
- 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,*
- 5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz leisten,*
- 6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,*
- 7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.*

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.“

Stellungnahme zum Gesetzentwurf der Bundesregierung

IV. Die Verfasser



Deutsche Forschungsgemeinschaft e. V.
Kennedyallee 40
53175 Bonn

Peter Dörel

Datenschutzbeauftragter

Telefon +49 (228) 885 - 2801
eMail peter.doerel@dfg.de

Die Deutsche Forschungsgemeinschaft e. V. (DFG) ist die zentrale Selbstverwaltungsorganisation der deutschen Wissenschaft. Mitglieder der DFG sind Hochschulen, andere Einrichtungen der Forschung von allgemeiner Bedeutung, Akademien der Wissenschaften und wissenschaftliche Verbände. Die Hauptaufgabe der DFG ist die Förderung selbstbestimmter, nach ihrer wissenschaftlichen Qualität ausgewählter Forschungsprojekte in Universitäten und anderen von der Öffentlichen Hand getragenen Forschungseinrichtungen. Detaillierte Informationen zu den Aufgaben und zur Struktur der DFG sind dem Internet zu entnehmen.



Fraunhofer-Gesellschaft zur Förderung der
angewandten Forschung e. V.
Hansastraße 27 c
80686 München

Ralph Harter

Datenschutzbeauftragter

Telefon +49 (89) 1205 - 2045
eMail ralph.harter@zv.fraunhofer.de

Die Fraunhofer-Gesellschaft verfolgt den Zweck, die angewandte Forschung zu fördern. Sie führt in diesem Rahmen frei gewählte Forschungsvorhaben, von Bund und Ländern übertragene Aufgaben und Vertragsforschung durch.

Stellungnahme zum Gesetzentwurf der Bundesregierung



Hermann von Helmholtz-Gemeinschaft
Deutscher Forschungszentren e. V.
Ahrstraße 45
53175 Bonn

Ronny Repp

Vorsitz Arbeitskreis der Datenschutz-
beauftragten der außeruniversitären
Forschungseinrichtungen

Telefon +49 (228) 43302 - 430
eMail ronny.repp@dzne.de

Die Helmholtz-Gemeinschaft Deutscher Forschungszentren leistet Beiträge zur Lösung großer und drängender Fragen von Gesellschaft, Wissenschaft und Wirtschaft durch wissenschaftliche Spitzenleistungen in sechs Forschungsbereichen: Energie, Erde und Umwelt, Gesundheit, Schlüsseltechnologien, Materie sowie Luftfahrt, Raumfahrt und Verkehr. Sie ist mit rund 38.000 Mitarbeiterinnen und Mitarbeitern in 18 Forschungszentren die größte Wissenschaftsorganisation Deutschlands.



Wissenschaftsgemeinschaft
Gottfried Wilhelm Leibniz e. V.
Chausseestraße 111
10115 Berlin

Jasmine Henz

Justiziarin

Telefon +49 (30) 206049 - 27
eMail henz@leibniz-gemeinschaft.de

Die Leibniz-Gemeinschaft verbindet 91 selbständige Forschungseinrichtungen. Ihre Ausrichtung reicht von den Natur-, Ingenieur- und Umweltwissenschaften über die Wirtschafts-, Raum- und Sozialwissenschaften bis zu den Geisteswissenschaften. Leibniz-Institute widmen sich gesellschaftlich, ökonomisch und ökologisch relevanten Fragen. Sie betreiben erkenntnis- und anwendungsorientierte Forschung, auch in den übergreifenden Leibniz-Forschungsverbünden, sind oder unterhalten wissenschaftliche Infrastrukturen und bieten forschungsbasierte Dienstleistungen an. Die Leibniz-Gemeinschaft setzt Schwerpunkte im Wissenstransfer, vor allem mit den Leibniz-Forschungsmuseen. Sie berät und informiert Politik, Wissenschaft, Wirtschaft und Öffentlichkeit. Leibniz-Einrichtungen pflegen enge Kooperationen mit den Hochschulen unter anderem in Form der Leibniz-WissenschaftsCampi, mit der Industrie und anderen Partnern im In- und Ausland. Sie unterliegen einem transparenten und unabhängigen Begutachtungsverfahren. Aufgrund ihrer gesamtstaatlichen Bedeutung fördern Bund und Länder die Institute der Leibniz-Gemeinschaft gemeinsam.

Stellungnahme zum Gesetzentwurf der Bundesregierung



Max-Planck-Gesellschaft zur Förderung der
Wissenschaften e. V.
Hofgartenstraße 8
80539 München

Heidi Schuster
Datenschutzbeauftragte
Telefon +49 (89) 2108 - 1554
eMail heidi.schuster@gv.mpg.de

Die Max-Planck-Gesellschaft ist eine Wissenschaftsorganisation mit langer Tradition: Seit mehr als 60 Jahren steht sie für exzellente, erkenntnisorientierte Grundlagenforschung in den Lebens-, Natur- und Geisteswissenschaften. Sie hat 1948 die Nachfolge der bereits 1911 errichteten Kaiser-Wilhelm-Gesellschaft angetreten, in der neben Planck schon namhafte Forscher wie Albert Einstein oder Otto Hahn tätig waren. So wie diese damals, stoßen Max-Planck-Forscherinnen und Forscher auch heute immer wieder in neue Dimensionen des Wissens vor – 18 von ihnen wurden dafür bislang mit dem Nobelpreis ausgezeichnet. Auch deshalb genießt die Max-Planck-Gesellschaft mit ihren 83 Forschungsinstituten großes Ansehen im In- und Ausland.

Max Weber Stiftung

Deutsche
Geisteswissenschaftliche
Institute im Ausland

Max Weber Stiftung
Deutsche Geisteswissenschaftliche Institute
im Ausland
Rheinallee 6
53173 Bonn

Reinhard Hiß
Datenschutzbeauftragter
Telefon +49 (228) 37786 - 14
eMail hiss@maxweberstiftung.de

Die Max Weber Stiftung zählt zu den maßgeblichen Trägern deutscher geisteswissenschaftlicher Forschung im Ausland. Sie unterhält weltweit zehn wissenschaftlich autonome Institute, die eine Brückenfunktion zwischen den Gastländern und Deutschland einnehmen und eine wichtige Rolle in der internationalen Wissenschaftslandschaft spielen. Als multipolares Netzwerk treiben die Institute die Internationalisierung der Wissenschaft gemeinsam voran.

Stellungnahme zum Gesetzentwurf der Bundesregierung



MFT Medizinischer Fakultätentag der
Bundesrepublik Deutschland e. V.
Alt-Moabit 96
10559 Berlin

Dr. Frank Wissing

Generalsekretär

Telefon +49 (30) 64498559 - 0
eMail wissing@mft-online.de

Der MFT Medizinische Fakultätentag ist der Zusammenschluss der medizinischen Fakultäten in Deutschland. Seine 37 Mitglieder betreiben Lehre und klinische Forschung auf international anerkanntem Niveau zum Wohle der Patienten und zur Sicherung des medizinischen und wirtschaftlichen Fortschritts. Ihre Partner vor Ort sind die Universitätskliniken. Sie gewährleisten damit die flächendeckende medizinische Versorgung der Zukunft. Durch exzellente Leistungen der Grundlagenforschung und der patientenbezogenen Forschung stärken sie die Wissenschaftslandschaft maßgeblich. Gemeinsam werben die hochschulmedizinischen Einrichtungen jährlich mehr als 1,5 Milliarden Euro Drittmittel für Forschungsvorhaben ein.

RatSWD.

Rat für Sozial- und
Wirtschaftsdaten

Rat für Sozial- und Wirtschaftsdaten
Geschäftsstelle
Chausseestraße 111
10115 Berlin

Claudia Oellers

Leiterin der Geschäftsstelle

Telefon +49 (30) 206049 - 1228
eMail coellers@ratswd.de

Der Rat für Sozial- und Wirtschaftsdaten (RatSWD) ist ein unabhängiges Gremium bestehend aus empirisch arbeitenden Wissenschaftlerinnen und Wissenschaftlern sowie Vertreterinnen und Vertretern wichtiger Datenproduzenten. Er wurde 2004 vom Bundesministerium für Bildung und Forschung eingerichtet mit der Zielsetzung die Forschungsdateninfrastruktur für die empirische Forschung nachhaltig zu verbessern und somit zu ihrer internationalen Wettbewerbsfähigkeit beizutragen. Der RatSWD hat sich als institutionalisiertes Forum des Austauschs und der Vermittlung zwischen den Interessen der Wissenschaft und Datenproduzenten etabliert und erfüllt dabei eine wichtige Rolle als Kommunikations- und Koordinations-Plattform. Das Gremium nimmt in den Sozial-, Verhaltens und Wirtschaftswissenschaften in Bezug auf die Standardsetzung und Qualitätssicherung sowie die weitere Entwicklung der Forschungsdatenzentren und Datenservicezentren eine beratende und initiiierende Funktion wahr.

Stellungnahme zum Gesetzentwurf der Bundesregierung



TMF - Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e. V.
Charlottenstraße 42
10117 Berlin

Sebastian Claudius Semler
Geschäftsführer

Telefon +49 (30) 2200247 - 0
eMail info@tmf-ev.de

Die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. ist die Dachorganisation für die medizinische Verbundforschung in Deutschland. Sie ist die Plattform für den interdisziplinären Austausch und die projekt- wie standortübergreifende Zusammenarbeit von Wissenschaftlern, die gemeinsam die organisatorischen, rechtlich-ethischen und technologischen Probleme der modernen medizinischen Forschung identifizieren und lösen. Die Lösungen reichen von Gutachten, generischen Konzepten und IT-Anwendungen über Checklisten und Leitfäden bis zu Schulungs- und Beratungsangeboten. Die TMF stellt diese Lösungen frei und öffentlich zur Verfügung.



Verband der Universitätsklinika
Deutschlands e. V. (VUD)
Alt-Moabit 96
10559 Berlin

Ralf Heyder
Generalsekretär

Telefon +49 (30) 3940517 - 0
eMail info@uniklinika.de

Der Verband der Universitätsklinika Deutschlands e. V. (VUD) repräsentiert die 33 deutschen Universitätsklinika. Diese sind eine tragende Säule des Gesundheitssystems und stehen für eine Krankenversorgung auf höchstem Niveau sowie für Spitzenforschung und die Einführung neuer Behandlungsmethoden. Zudem sichern die Universitätsklinika, gemeinsam mit den medizinischen Fakultäten, die Ausbildung künftiger Generationen von Ärzten und Wissenschaftlern. Gemeinsam mit außeruniversitären Partnern führen sie neue medizinische Methoden in das Gesundheitssystem ein.

Stellungnahme zum Gesetzentwurf 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)

Ergänzung zu § 27 Absatz 3 DSAnpUG-EU - E

Artikel 89 Absatz 1 EU-DS-GVO verlangt technische und organisatorische Maßnahmen als Garantien für den Schutz der Rechte und Freiheiten der betroffenen Personen. Als mögliche Maßnahmen benennt er die Pseudonymisierung und Anonymisierung von Forschungsdaten. Die englische Fassung dieses Artikels verwendet offensichtlich bewusst **Sollvorschriften** (vgl. Satz 3 und 4) hinsichtlich dieser beiden Maßnahmen. Die von der Bundesregierung getroffene Formulierung im § 27 Absatz 3 DSAnpUG-EU - E sieht hingegen eine **Verpflichtung zur Anonymisierung** der Forschungsdaten vor.

Die Verordnung ermöglicht den Mitgliedstaaten auf der Grundlage des Artikel 9 Absatz 4 EU-DS-GVO die Schaffung zusätzlicher Bedingungen und Beschränkungen bei der Verarbeitung von genetischen, biometrischen und Gesundheitsdaten. Diese werden jedoch nicht durch § 27 Absatz 3 DSAnpUG-EU - E geschaffen, denn die Norm bezieht sich auf alle besonderen Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 EU-DS-GVO.

Zwischenfazit: Die Verpflichtung zur Anonymisierung von Forschungsdaten geht über den Regelungswillen des Europäischen Gesetzgebers hinaus.

Die Folgen einer Verpflichtung zur Anonymisierung können empfindliche und weitreichende Auswirkungen für die Forschung haben. Beispiele für Forschungsdaten, die der besonderen Kategorie personenbezogener Daten angehören, sind etwa genetische Daten aus **Biomaterialproben** oder diese Biomaterialproben selbst, aber auch **Bilddaten** zum Beispiel aus der Magnetresonanztomographie, Computertomographie oder gespeicherte **Stimmenproben**. Diese Beispiele sind nicht abschließend, sollen aber veranschaulichen, dass diese Forschungsdaten genutzt werden, die sich nach dem Stand der Technik nicht anonymisieren lassen. Würden Forschungseinrichtungen die Anonymisierung von zum Beispiel Biomaterialproben erreichen wollen, wäre dies nach dem Stand der Technik nur mit dem endgültigen Vernichten der Biomaterialproben möglich.

Vorwiegend in biomedizinischen Forschungsvorhaben werden gerade die voran genannten Forschungsdaten regelmäßig benötigt und unter der Verwendung von seit Jahren **etablierten Pseudonymisierungsverfahren** verarbeitet. Außerdem werden zusätzliche Schutzmaßnahmen getroffen, z. B. die Verarbeitung der personenidentifizierenden Daten (z. B. Name, Adresse) durch eine Treuhandstelle. Biomaterialproben und Bilddaten werden also bewusst ohne die identifizierenden Daten und dafür mit einer eindeutigen Proben- bzw. Bildnummer verarbeitet um sie in unterschiedlichen Forschungsvorhaben nutzbar zu machen. Dabei ist der tatsächliche Forschungszweck im Voraus nicht immer definierbar. Die mit den Biomaterialproben arbeitenden Forscher erhalten keinen Zugang zu den personenidentifizierenden Daten, da diese bei einer Treuhandstelle gespeichert werden. Diese erweiterten Maßnahmen sind flächendeckend üblich und stellen insoweit bereits eine gesteigerte Form der Unkenntlichmachung von Forschungsdaten dar und ermöglichen einen mit dem Ziel der Anonymisierung vergleichbaren Schutz der betroffenen Personen.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Der Artikel 5 Absatz 1 lit. b lässt grundsätzlich eine Weiterverarbeitung zu Forschungszwecken zu. In Forschungsvorhaben, bei denen frühzeitig anonymisiert werden müsste, wäre eine Rekontaktierung zur Erhebung weiterer oder neuer personenbezogener Daten unmöglich. Die Forschungseinrichtungen müssten demnach aufwendig neu und damit doppelt erheben, da die ursprünglichen Forschungsdaten dann bereits anonymisiert wurden.

Die Rekontaktierung kann auch aus medizinischen Gründen angezeigt sein, zum Beispiel, wenn sich aus den bereits erhobenen Forschungsdaten erkennen lässt, dass die betroffene Person an einer lebensbedrohlichen Erkrankung leidet, welche jedoch nach dem Stand der Medizin behandelbar ist. Die Feststellung einer solchen Erkrankung kann durchaus nach Erreichen des Forschungszwecks eintreten. Zudem können neue Therapieoptionen für bestimmte Patientengruppen gefunden werden, die anhand der Forschungsdaten herausgefiltert und im pseudonymen Zustand durch die Verbindung mit den identifizierenden Daten auch wieder kontaktiert werden können.

Zwischenfazit: Nicht alle Forschungsdaten können nach dem Stand der Technik anonymisiert werden. Eine Weiterverarbeitung personenbezogener Daten zu Forschungszwecken ist mit einer Verpflichtung zur Anonymisierung nicht vereinbar. Die Pseudonymisierung ist der Anonymisierung bei der Anwendung erweiterter technischer und organisatorischer Maßnahmen zum Schutz der betroffenen Personen in vielen Forschungsvorhaben vorzuziehen.

Formulierungsvorschlag für § 27 Absatz 3 DSAnpUG-EU - E

„Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen ~~sind~~ sollten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ~~möglichst zu~~ anonymisiert ~~ten~~ werden, sobald dies nach dem Forschungs- oder Statistikzweck und dem Stand der Technik möglich ist, es sei denn, berechnigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.“

Stellungnahme zum Gesetzentwurf 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)

Ergänzung zu § 27 Absatz 2 DSAnpUG-EU - E

Artikel 89 Absatz 2 EU-DS-GVO ermöglicht es dem nationalen Gesetzgeber, Ausnahmen der Betroffenenrechte vorzusehen, wenn personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden. Die Beschränkung der Betroffenenrechte setzt voraus, dass die Verwirklichung der Forschungszwecke voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt wird und die Beschränkung für die Erfüllung des Forschungszwecks notwendig ist.

Mit § 27 Absatz 2 Satz 1 DSAnpUG-EU - E werden die Ausnahmen der Betroffenenrechte aus Artikel 89 Absatz 2 EU-DS-GVO festgelegt. Sie betreffen das Recht auf Auskunft gemäß Artikel 15 EU-DS-GVO, das Recht auf Berichtigung laut Artikel 16 EU-DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 EU-DS-GVO sowie das Recht auf Widerspruch entsprechend Artikel 21 EU-DS-GVO.

§ 27 Absatz 2 Satz 2 DSAnpUG-EU - E präzisiert die Beschränkung des Auskunftsrechts gemäß Artikel 15 EU-DS-GVO. Er macht jedoch zur Bedingung, dass die Daten für wissenschaftliche Forschungszwecke erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Die Gesetzesbegründung verweist zum Satz 2 auf die Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i EU-DS-GVO.

§§ 34 Absatz 7 in Verbindung mit 33 Absatz 2 Satz 1 Nummer 5 sowie § 19a Absatz 2 Nummer 2 **BDSG** sehen bereits heute auf Grundlage von Artikel 11 Absatz 2 **EG-Datenschutzrichtlinie** 95/45/EG **gleichlautende Einschränkungen des Auskunftsrechts** und des Rechts auf Benachrichtigung vor, wenn die uneingeschränkte Umsetzung dieser Rechte im Rahmen von Forschungsvorhaben mit einem unverhältnismäßigen Aufwand verbunden wäre.

Entsprechende Ausnahmen vom Recht auf Auskunft bedeuten keine neuen oder gar weitergehenden Ausnahmen zu Lasten der betroffenen Personen. Sie bleiben jedoch für die wissenschaftliche Forschung, insbesondere im Bereich der medizinischen Forschung, weiterhin unverzichtbar.

Die Auskunftserteilung gemäß Artikel 15 EU-DS-GVO, **insbesondere die Herausgabe** von wissenschaftlichen Daten an die betroffene Person aufgrund des Artikel 15 Absatz 3 EU-DS-GVO, würde in bestimmten Fällen zu einem **unverhältnismäßigen Aufwand** für Forschungseinrichtungen führen.

Gemäß **Artikel 12 Absatz 1 EU-DS-GVO** müssen Mitteilungen nach Artikel 15 EU-DS-GVO **präzise, transparent, verständlich und in einer leicht zugänglichen Form** an die betroffene Person übermittelt werden. Diese Anforderungen würden einen enormen Aufwand für die Forschungseinrichtung ausmachen, wenn die personenbezogenen Daten durch neue Technologien und Verfahren entstanden oder derart komplex sind, dass eine verständliche Mitteilung an die betroffene Person kaum umsetzbar ist. Hinzu kommt, dass Forschungsdaten häufig in Datenformaten verarbeitet werden, die eine leicht zugängliche Form überwiegend ausschließen.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Darüber hinaus würde die **uneingeschränkte Auskunft** nach den Vorgaben des Artikel 12 EU-DS-GVO im Falle **von genetischen Forschungsdaten** nach Artikel 3 Nummer 13 EU-DS-GVO zu einer **vom nationalen Gesetzgeber mutmaßlich nicht gewünschten** Situation führen. Die Mitteilung von genetischen Daten ist im Gendiagnostikgesetz an besondere Vorkehrungen zum Schutz der betroffenen Personen geknüpft. Die wissenschaftliche Forschung ist allerdings vom Geltungsbereich des Gendiagnostikgesetzes bewusst ausgenommen. Eine Anwendung von Schutzmaßnahmen, die dem Gendiagnostikgesetz entsprechen würden, kommt im Forschungskontext schon allein deshalb nicht in Frage, da die Erhebung der genetischen Daten typischerweise mit Hilfe von Verfahren erfolgt, die nicht als Grundlage für eine genetische Untersuchung und Beratung geeignet sind. Dazu können **neue Tumormarker oder Analyseverfahren** gehören, die noch **im Entwicklungsstadium** sind. Die Anwendung anderer Verfahren und die Umsetzung einer umfassenden genetischen Beratung würde zu **nicht tragbaren Aufwänden** für Forschungseinrichtungen führen. Insofern würde die Mitteilung von genetischen Daten aus Forschungsvorhaben nach Artikel 15 EU-DS-GVO im **Widerspruch zu** dem vom Gendiagnostikgesetz intendierten **Schutzniveau** für die betroffenen Personen stehen.

Die Mitteilung von Forschungsdaten **muss also im Einzelfall zum Wohle der betroffenen Person ausbleiben können**, wenn personenbezogene Daten aus neuen ungesicherten diagnostischen Verfahren entstehen beziehungsweise wenn diese Mitteilung zu einer erheblicher Verunsicherung der betroffenen Person führen könnte.

Der Schutz der körperlichen und geistigen Gesundheit der betroffenen Person ist in Artikel 3 Absatz 1 EU-Grundrechtecharta verbrieft. Dies entspricht in Deutschland dem Grundrecht auf körperliche Unversehrtheit nach Artikel 2 Absatz 2 Satz 1 GG.

Im direkten Behandlungszusammenhang erkennt § 630 g Absatz 1 **BGB** diese Besonderheit an und **schützt** Patientinnen und Patienten **vor der Einsichtnahme** in Behandlungsdaten, wenn diese ihnen einen **erheblichen therapeutischen Schaden** zufügen könnte. Auch **Landeskrankenhausgesetze beinhalten Ausnahmen vom Auskunftsrecht zum Schutz des Patienten**. So regelt § 36 Absatz 5 Satz 3 Landeskrankenhausgesetz Rheinland-Pfalz, dass das Auskunftsrecht im Interesse der Gesundheit des Patienten begrenzt werden kann. Ähnliche Regelungen finden sich zudem in den Landeskrankenhausgesetzen von Berlin, Brandenburg und Bayern.

Fazit Weder Ausnahmen vom Auskunftsrecht wegen unverhältnismäßigem Aufwand, noch Einschränkungen zum Schutz der betroffenen Person, stellen neuartige Regelungsansätze dar. Vielmehr gibt es in aktuellen Gesetzen bereits entsprechende Vorschriften.

Ein unverhältnismäßiger Aufwand, der durch die Erfüllung des Auskunftsrechts betroffener Personen entsteht, führt dazu, dass die voraussichtliche Verwirklichung der Forschungszwecke unmöglich gemacht oder ernsthaft beeinträchtigt wird.

Ausnahmen vom Auskunftsrecht müssen zudem zum Schutz der betroffenen Person vorgesehen werden.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Formulierungsvorschlag für § 27 Absatz 2 DSAnpUG-EU - E

„Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde oder wenn die Auskunftserteilung dem Wohl der betroffenen Person nach therapeutischen, ethischen oder moralischen Erwägungsgründen zuwiderläuft oder Schaden könnte.“

Stellungnahme
zu Artikel 1, § 31 BDSG-E,
des Entwurfs der Bundesregierung für ein
Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU¹),
BR-Drs. 110/17, vom 2. Februar 2017

I) Allgemeine Bemerkungen

Der Verband „Die Wirtschaftsauskunfteien e.V.“ (im Folgenden „DW“) vertritt die Interessen der großen deutschen Wirtschaftsauskunfteien. Zu den Mitgliedern zählen die Unternehmen Bisnode Deutschland GmbH, Bürgel Wirtschaftsinformationen GmbH & Co. KG, Creditreform Boniversum GmbH, IHD Gesellschaft für Kredit- und Forderungsmanagement mbH, infoscore Consumer Data GmbH, SCHUFA Holding AG und der Verband der Vereine Creditreform e.V.. Zusammen beschäftigen sie deutschlandweit mehr als 10.000 Mitarbeiter, erteilen pro Jahr rd. 400 Mio. Bonitäts- und Bilanzauskünfte an 250.000 Unternehmen in Deutschland und erwirtschaften im Jahr einen Umsatz von mehr als 1 Mrd. €.

Die Wirtschaftsauskunfteien begrüßen grundsätzlich das Bestreben der Bundesregierung, die im Zuge der BDSG-Novelle 2009/2010 eingeführten §§ 28a, 28b BDSG auch nach Wirksamwerden der EU-Datenschutz-Grundverordnung (EU-DSGVO) zu erhalten. So kann die Rechtssicherheit, die die Regelungsarchitektur der §§ 28a und b BDSG für Wirtschaft und Verbraucher geschaffen hat, zumindest teilweise auch unter dem Regime der EU-DSGVO aufrechterhalten werden.

II) Zu Art. 1, § 31 BDSG-E Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

1) Zu § 31 Abs. 1 BDSG-E

Unsere Mitglieder unterstützen die Schaffung des § 31 Abs. 1 BDSG-E, der im Wesentlichen dem heutigen § 28b BDSG entspricht. Auf diese Weise wird die Ermittlung sowie Verwendung von Wahrscheinlichkeitswerten/Bonitätsauskünften und damit die Arbeit von Wirtschaftsauskunfteien, denen in der Gesetzesbegründung zutreffender Weise eine tragende Rolle für die Funktionsfähigkeit der Wirtschaft zugeschrieben wird, auf eine rechtssichere und in der Praxis erprobte Grundlage gestellt.

¹ Vollständiger Titel: „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)“

2) Zu § 31 Abs. 2 BDSG-E

Die Intention des Entwurfes, den Regelungsgehalt des § 28a Abs. 1 BDSG auch unter der Geltung der EU-DSGVO fortzuschreiben, wird ebenfalls grundsätzlich begrüßt.

Hauptanliegen der Wirtschaftsauskunfteien bei der Diskussion um die Anpassung des BDSG an die EU-DSGVO war und ist es, die im BDSG für deren Tätigkeit geschaffene Regelungsarchitektur so weit wie möglich zu erhalten. Ausgehend von dieser Prämisse erschien der Ansatz im Referentenentwurf des Gesetzes, die Bezeichnung und die Rechtsfolge des § 28a BDSG (Datenübermittlung an Auskunfteien) zu übernehmen, plausibel und auch dogmatisch überzeugend, da europarechtliche Vorgaben und mögliche Konkretisierungen in einen angemessenen Ausgleich gebracht werden, während für weitergehende Einschränkungen dagegen kein Raum mehr bestehen dürfte. Dass die Rechtsfolge im Regierungsentwurf nun bei der „Verwendung eines Wahrscheinlichkeitswerts“ ansetzt, trägt unserem Anliegen gleichwohl Rechnung, als die Voraussetzungen des § 31 Abs. 2 BDSG-E weitgehend mit denen des § 28a Abs. 1 BDSG identisch sind. Damit ist Rechtssicherheit für alle Beteiligten hinsichtlich der auf dieser Grundlage in der Praxis etablierten Prozesse auch für die Zukunft gewährleistet.

Gleichwohl besteht hinsichtlich eines Aspekts klarstellender Änderungsbedarf:

In § 31 Abs. 2 S. 1 Nr. 4 c) und Nr. 5 BDSG-E wird vom „Gläubiger“ statt - wie bisher in § 28a BDSG - von „verantwortlicher Stelle“ gesprochen. An dieser Stelle sollte die Formulierung des § 28a Abs. 1 S. 1 Nr. 4 c) und Nr. 5 BDSG beibehalten und auf die Einführung des Begriffs „Gläubiger“ verzichtet werden.

Es ist erklärtes Ziel des Entwurfes, den „materiellen Schutzstandard der §§ 28a und 28b BDSG“ fortzuschreiben. Die Verwendung des Begriffs „Gläubiger“ könnte aber nun die Frage aufwerfen, ob z. B. auch Inkassounternehmen, die eine Forderung im Namen des Gläubigers geltend machen, wie bisher auch weiterhin berechtigt sein sollen, an Stelle bzw. im Auftrag des Gläubigers Informationen an Auskunfteien zu übermitteln. Wir gehen davon aus, dass nicht beabsichtigt ist, durch die Aufnahme des Begriffs „Gläubiger“ diese bewährte Praxis zu ändern. Zur Vermeidung etwaiger diesbezüglicher Zweifel sollte daher eine Klarstellung erfolgen. Eine solche könnte z. B. durch eine passivische Formulierung erreicht werden:

4. bei denen

.....

c) der ~~Gläubiger~~ den Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist ~~hat~~ und

.....

5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der ~~Gläubiger~~ den Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist ~~hat~~.

Hilfsweise könnte eine entsprechende Klarstellung auch in den Gesetzesmaterialien erfolgen.

Wir wären dankbar, wenn diese Anregung bei den weiteren Beratungen über den Gesetzentwurf entsprechend berücksichtigt würde.

Neuss, den 01.03.2017

Dr. Thomas Riemann

Deutscher Bundestag
Vorsitzender des Innenausschusses
Herrn Ansgar Heveling, MdB
Obleute im Innenausschuss
Herrn Armin Schuster, MdB
Herrn Burkhard Lischka, MdB
Frau Ulla Jelpke, MdB
Frau Irene Mihalic, MdB
Platz der Republik 1
11011 Berlin

ausschließlich per E-Mail

Institut der Wirtschaftsprüfer
in Deutschland e. V.

Wirtschaftsprüferhaus
Tersteegenstraße 14
40474 Düsseldorf
Postfach 32 05 80
40420 Düsseldorf

TELEFONZENTRALE:
+49 (0) 211 / 45 61 - 0

FAX GESCHÄFTSLEITUNG:
+49 (0) 211 / 4 54 10 97

INTERNET:
www.idw.de

E-MAIL:
info@idw.de

BANKVERBINDUNG:
Deutsche Bank AG Düsseldorf
IBAN: DE53 3007 0010 0748 0213 00
BIC: DEUTDE33XXX
USt-ID Nummer: DE119353203

Düsseldorf, 07.03.2017

651

**Regierungsentwurf eines Gesetzes zur Anpassung des Datenschutzrechts
an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU)
2016/680 (BT-Drs. 18/11325)**

Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Obleute,

im Vorfeld der Anhörung möchten wir zu dem Regierungsentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (im Folgenden: RegE) Stellung nehmen.

Wir begrüßen, dass einige Vorschläge aus unserer Stellungnahme vom 07.12.2016 zum Referentenentwurf berücksichtigt wurden.

Neben verbliebenen Unsicherheiten bezüglich der Geheimhaltungspflicht bleibt der RegE allerdings an manchen Stellen hinter den europarechtlichen Möglichkeiten zur Durchsetzung der berufsrechtlichen Geheimhaltungspflicht und zum Schutz vertraulicher Mandanteninformationen zurück. Ein Ausschöpfen der Schutzmöglichkeiten ist für die Ausübung des Wirtschaftsprüferberufs wie auch der anderen freien Berufe von größter Bedeutung, da auf diese Weise das Rechtsgut des persönlichen Lebens- und Geheimbereichs des Mandanten, Patienten etc. geschützt bleibt.

GESCHÄFTSFÜHRENDER VORSTAND:
Prof. Dr. Klaus-Peter Naumann,
WP StB, Sprecher des Vorstands;
Dr. Klaus-Peter Feld, WP StB;
Dr. Daniela Kelm, RA LL.M.

Seite 193 von 365

Seite 2/4 zur Stellungnahme vom 07.03.2017 an den Innenausschuss des Bundestags

Zur Stützung der strafrechtlich bewehrten berufsrechtlichen Geheimhaltungspflicht und zur rechtstechnischen Klarstellung haben wir folgende Anmerkungen und regen folgende Änderung zu Artikel 1 (Bundesdatenschutzgesetz) des Regierungsentwurfs an.

1. Einschränkung des bisherigen Schutzes der Geheimhaltungspflicht

Bisher hatten Spezialnormen, wie z.B. die Wirtschaftsprüferordnung und andere berufsrechtliche Ordnungen Vorrang vor dem BDSG. Aufgrund der EU-rechtlichen Normenhierarchie hat nunmehr die DS-GVO als EU-Verordnung Geltungsvorrang. Damit tritt – ohne Nutzung der mitgliedstaatlichen Öffnungsklauseln, insbesondere des Art. 23 Abs. 1 DS-GVO – das „allgemeine“ Datenschutzrecht der DS-GVO vor etwaige deutsche Spezialgesetze.

Die o.g. Öffnungsklausel des Art. 23 Abs. 1 DS-GVO erlaubt Beschränkungen der Betroffenenrechte in den Art. 12 bis 22, 34 sowie 5 DS-GVO.

Der RegE macht von den Beschränkungsmöglichkeiten des Art. 23 DS-GVO nur in Bezug auf Artt. 13 bis 15 und 34 DS-GVO und dort teilweise auch nur lückenhaft Gebrauch.

Die weiterhin nur eingeschränkte Nutzung der Ausnahmemöglichkeiten des Art. 23 Abs. 1 DS-GVO und der Vorrang der DS-GVO führen dazu, dass der bisherige Schutz der berufsrechtlichen Geheimhaltungspflicht ohne sachlichen oder rechtlichen Grund eingeschränkt wird. Dies, obwohl die DS-GVO gerade den „berufsständischen Regeln reglementierter Berufe“ eine besondere Bedeutung beimisst, indem zu ihrem Schutz ausdrücklich eine Ausnahmeregel in Art. 23 Abs. 1 Buchst. g DS-GVO geschaffen wurde.

Es ist im Übrigen nicht ersichtlich, ob der Entwurf überhaupt Art. 23 Abs. 1 Buchst. g DS-GVO beachtet hat. Der Entwurf erwähnt im Gesetzestext lediglich die Schutznormen der Art. 14 Abs. 5 und 34 Abs. 3 DS-GVO, die aber ohnehin durch die DS-GVO vorgegeben sind. Und in den Begründungen verweist der Entwurf auf Art. 23 Abs. 1 Buchst. i DS-GVO („den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“), nicht aber auf Buchst. g („die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe“).

Vor diesem Hintergrund haben wir folgende Anmerkungen und sehen folgende Änderungen für angebracht.

2. Zu § 29 BDSG-E

2.1. Zu § 29 Abs. 1 Satz 1 BDSG-E – gesetzliche und vertragliche Geheimhaltungspflicht

Seite 3/4 zur Stellungnahme vom 07.03.2017 an den Innenausschuss des Bundestags

Wir begrüßen die überarbeitete Fassung des § 29 Abs. 1 Satz 1 BDSG-E, möchten aber mangels ausdrücklicher Klarstellung im Gesetz darauf hinweisen, dass wir den Verweis auf die Ausnahmetatbestände des Art. 14 Abs. 5 DS-GVO so verstehen, dass mit „gemäß dem Recht der Mitgliedstaaten“ sowohl die gesetzliche wie auch die vertragliche Geheimhaltungspflicht gemeint sind. Zum deutschen Rechtskorpus gehören Berufs-, Straf- und Vertragsrecht, und alle drei Rechtsgebiete können zum Schutz des Geheimbereichs der Mandanten herangezogen werden. Die Geheimhaltungspflicht gilt zugunsten der Mandanten unabhängig davon, ob ihr der Berufsträger selbst unterliegt, sein Gehilfe oder ein anderer Verantwortlicher, der hinter dem Berufsträger steht und in rechtlich zulässiger Weise zum Kreis der zur Geheimhaltung Verpflichteten gehört – und somit unabhängig von der rechtlichen Grundlage.

2.2. Zu § 29 Abs. 1 Satz 2 BDSG-E – gesetzliche und vertragliche Geheimhaltungspflicht

Wir verstehen den Verweis auf „nach einer Rechtsvorschrift oder ihrem Wesen nach“ so, dass damit eine gesetzliche und eine vertragliche Geheimhaltungspflicht gemeint sind, so dass der bisherige gesetzliche und vertragliche Schutz von vertraulichen Mandantendaten in Deutschland aufrechterhalten wird.

2.3. Zu § 29 Abs. 1 Sätze 3 und 4 BDSG-E – Interessenabwägung

Anmerkung

Wir begrüßen, dass der RegE dem Grundsatz nach von der Ausnahmemöglichkeit nach Art. 23 Abs. 1 DS-GVO Gebrauch gemacht hat, die Benachrichtigungspflicht nach Art. 34 DS-GVO zugunsten der Geheimhaltungspflicht zu beschränken. Wie in Punkt 2.2. dargelegt, gehen wir davon aus, dass hier die gesetzlich wie auch vertraglich begründete Geheimhaltungspflicht erfasst sind.

Kritisch zu sehen ist allerdings, dass § 29 Abs. 1 Satz 4 BDSG-E die Geheimhaltungspflicht zur Disposition stellt und ohne sachlich erkennbaren Grund die europarechtlich gewährten Ausnahmemöglichkeiten wieder einschränkt. Für den Berufsgeheimnisträger selbst aber auch im Streitfall für ein Gericht ist eine Interessensabwägung bezüglich der berufsrechtlichen Geheimhaltungspflicht von Berufsgeheimnisträgern problematisch. Der Berufsgeheimnisträger ist nicht „Herr der Geheimhaltungspflicht“. Er kann nur durch eine gesetzliche Regelung oder vom Mandanten von seiner Geheimhaltungspflicht befreit werden. Und nur das wird ein Richter feststellen können. Es besteht praktisch kein Ermessensspielraum, aufgrund dessen der Berufsgeheimnisträger oder ein Gericht entscheiden könnte, „ob die Interessen der betroffenen Person, insbesondere unter

Seite 4/4 zur Stellungnahme vom 07.03.2017 an den Innenausschuss des Bundestags

Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.“

Darüber hinaus wäre eine solche Interessenabwägung für den Wirtschaftsprüfer auch nicht praktikabel und führt zu Rechtsunsicherheit, da eine solche Abwägung eine Quelle potentieller Rechtsstreitigkeiten mit den Betroffenen wäre.

Vorschlag

§ 29 Abs. 1 Satz 4 BDSG-E sollte gestrichen werden.

2.4. Zu § 29 Abs. 3 BDSG-E – Datenlöschung nach unbefugter Kenntnisnahme

Anmerkung

Wir begrüßen die deutlicher formulierte Beschränkung der Behördenbefugnisse zugunsten des vertrauensbedürftigen Mandanten. Zur Sicherstellung, dass eine Behörde vertrauliche Mandantendaten, die sie ohne Befugnis erlangt hat, nicht nutzt, sollte die Behörde – in Anlehnung an § 160a StPO und § 24u Bundeskriminalamtgesetz – zur Löschung der Daten verpflichtet sein.

Vorschlag

Nach § 29 Abs. 3 Satz 2 BDSG-E sollte ein neuer Satz 3 folgenden Inhalts eingefügt werden:

„Die Daten sind unverzüglich zu löschen; die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.“

Wir wären Ihnen sehr verbunden, wenn Sie unsere Anmerkungen bei den weiteren Beratungen berücksichtigen.

Mit freundlichen Grüßen



Dr. Kelm



Rindermann, RA StB

Fachleiterin Steuern und Recht

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. -

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)812

Stellungnahme

zum Gesetzentwurf für ein

Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU)

Berlin, 13. März 2017

Ansprechpartner: RA Sebastian Schulz, Leiter Rechtspolitik & Datenschutz

Der Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) repräsentiert als die **Interessenvertretung der Online- und Versandhandelsbranche** Unternehmen aller Größen und Handelsformen (Online, Multichannel, Katalog, TV-Shopping, Plattformhändler und -betreiber). Mit seinen über 500 Mitgliedern steht der bevh für **rund 75% des gesamten Branchenumsatzes** auf dem deutschen Markt. Darüber hinaus sind dem Verband mehr als 130 Dienstleister aus dem Umfeld der E-Commerce-Branche angeschlossen.

Im Einzelnen nehmen wir **zu Artikel 1 des o.g. Entwurfs** wie folgt Stellung:

1. Zum Erfordernis eines nationalen Anpassungsgesetzes

Die EU-Datenschutzgrundverordnung (DS-GVO) ist **für den Rechtsanwender eine Herausforderung**, die mit vielen Unwägbarkeiten verbunden ist. Obwohl im Vergleich zum aktuell noch geltenden Recht auf materiell-rechtlicher Ebene kaum neue Vorgaben zu verzeichnen sind, wird durch die erforderliche Neubewertung der nunmehr **autonom-europarechtlich auszulegenden Vorgaben** eine rechtskonforme Umsetzung zum Glücksspiel. Hinzu kommt, dass die durch den EU-Verordnungsgeber gewählte technikneutrale, maximal-abstrahierende Gesetzestechnik das Gegenteil von Rechtsklarheit und -sicherheit darstellt. Das dem Datenschutzrecht ohnehin immanente Interpretationsrisiko verlagert sich durch die DS-GVO nochmals stärker auf den Rechtsanwender, was insbesondere vor dem Hintergrund des neu eingeführten drakonischen Sanktionsrahmens als überaus bedenklich erscheint.

Vor diesem Hintergrund ist ein **nationales Begleitgesetz**, das in den Grenzen der Vorgaben der DS-GVO Konkretisierungen des europäischen Rechtsrahmens vornimmt, zweifellos **zu begrüßen**. Dies gilt umso mehr, als es sich bei geschätzten 75% des vorliegenden Entwurfs allein um obligatorische, d.h. nach der DS-GVO bzw. der neuen EU-Datenschutzrichtlinie zwingend zu regelnde Aspekte handelt. Allerdings geben wir zu bedenken, dass der Gesetzgeber an dieser Stelle mit großer Besonnenheit vorgehen muss. Konkretisierungen bewirken nicht allein ein

Mehr an Rechtssicherheit. Typischerweise geht mit Begleitgesetzen auch eine **Sperrwirkung** einher, namentlich dort, wo ausgewählte Teilbereiche durch das Begleitgesetz explizit und damit abschließend geregelt werden. Insbesondere bei der Ausgestaltung von Artikel 6 Absatz 4 DS-GVO (unten 3.), aber auch etwa im Bereich des Beschäftigtendatenschutzes (unten 5.) kann dies in der Praxis zu erheblichen Folgeproblemen führen, die durch den Gesetzgeber möglicherweise so nicht intendiert waren.

2. Zu §§ 17f.; §§ 40f. BDSG-E | Nationale Datenschutzaufsichtsbehörden

Der Gesetzentwurf macht Vorgaben für das Verfahren zur internen Beschlussfassung zwischen den 18 Datenschutzaufsichtsbehörden in Deutschland. Die feingranularen Regelungen in § 18 BDSG-E adressieren jedoch allein die Kompetenzverteilung (i) zur Vorlage eines Entwurfes für einen gemeinsamen Standpunkt bei fehlender Einigungsfähigkeit sowie (ii) zur Verhandlungsführung im Europäischen Datenschutzausschuss (Art. 68 DS-GVO). Vorgaben für die in der Praxis primär relevante Frage des internen Beschlussverfahrens zwischen den Aufsichtsbehörden des Bundes und der Länder, etwa zum Abstimmungsprozess bei (länder-)grenzüberschreitenden Sachverhalten, zu erforderlichen Quoren, einzuhaltenden Fristen usw. fehlen vollständig. Es ist bezeichnend, dass sich auf europäischer Ebene 28 Mitgliedstaaten auf geordnete, straffe und die eigenen Kompetenzen nicht unwesentlich beschneidende Verfahren verständigen konnten, vergleichbare Regeln auf der Ebene des nationalen Rechts hingegen weiterhin fehlen (sollen). Die hieraus resultierende Rechtsunsicherheit ist für die Daten verarbeitende Wirtschaft aber auch für die Behörden selbst überaus unerfreulich. In Anlehnung an das in den Art. 60ff. DS-GVO geregelte sog. Kohärenzverfahren und unter Berücksichtigung der Rechtsprechung des EuGH zur Unabhängigkeit der Datenschutzaufsicht sollten auch **für Abstimmungsprozesse der nationalen Datenschutzaufsichtsbehörden konkrete Vorgaben** erlassen werden. Zur Vermeidung von Entscheidungen allein am „grünen Tisch“ sollte im Zuge dessen, angelehnt an den Vorgaben von §§ 47f. GGO, eine **obligatorische Befassung der jeweils betroffenen Kreise** vorgesehen werden.

Losgelöst von den vorstehend dringend anzuregenden Ergänzungen sollte perspektivisch endlich der politische Wille zur **Abschaffung der föderalen Zersplitterung der Datenschutzaufsicht im nicht-öffentlichen Bereich** gefasst werden. In einem vereinten Europa, das im Bereich des Datenschutzes sowohl in materiell-rechtlicher Hinsicht als auch auf der Ebene der Rechtsdurchsetzung über einen vollharmonisierten Rechtsrahmen verfügt, erscheint die allein in Deutschland gelebte Praxis einer sachlichen wie regionalen Aufspaltung der aufsichtsrechtlichen Zuständigkeiten als anachronistisch und als zunehmend nicht mehr praktikabel.

3. Zu § 24 BDSG-E | Weiterverarbeitung nach Zweckänderung

Entsprechend der Vorgaben in § 24 BDSG-E sollen personenbezogene Daten in nur zwei Fallkonstellationen zu einem anderen als dem ursprünglichen Erhebungszweck weiterverarbeitet

werden dürfen. Die Entwurfsverfasser wählen an dieser Stelle den denkbar engsten Weg zur Umsetzung der Vorgaben von Art. 6 Abs. 4 DS-GVO. Blicke es bei dieser engen Vorgabe, hätte dies in der Praxis weitreichende negative Auswirkungen. So muss insbesondere die Streichung der noch im Vorentwurf enthaltenen Möglichkeit, eine **Weiterverarbeitung auch auf Grundlage einer allgemeinen Interessenabwägung** zu gestatten, rückgängig gemacht werden. Sollte es an dieser Stelle nicht zu einer Fortführung des geltenden Rechts¹ kommen, bleiben die Rechtsanwender auf lange Sicht auf die in der Praxis schlechterdings nicht zu handhabenden Vorgaben des sog. Kompatibilitätstest des Art. 6 Abs. 4 DS-GVO angewiesen. Einwänden, wonach es dem nationalen Gesetzgeber verwehrt sein soll, auf Grundlage von Art. 6 Abs. 4 DS-GVO auch eine allgemeine Interessenabwägungsklausel als Erlaubnistatbestand im mitgliedstaatlichen Recht zu schaffen, sind unbegründet und verkennen die praktische Relevanz einer solchen Norm. Über die **Beibehaltung des Korrektivs eines schutzwürdigen Ausschlussinteresses** der betroffenen Person würde den Vorgaben von Art. 23 DS-GVO ersichtlich angemessen Rechnung getragen, wobei zum Zwecke der Stärkung der Rechte der betroffenen Person der Abwägungsmaßstab des § 28 Abs. 2 a. E. BDSG auch auf die Abwägung mit den Interessen des Verantwortlichen ausgeweitet werden könnte.

4. Zu § 26 BDSG-E | Beschäftigtendatenschutz

a. Ausschluss der allg. Interessenabwägungsklausel; § 26 Abs. 1 BDSG-E

Dass sich die Entwurfsverfasser für eine grundsätzliche Fortführung der Vorgaben aus § 32 BDSG entschieden haben, ist **zu begrüßen**. Die zu dieser Vorschrift ergangene Rechtsprechung des Bundesarbeitsgerichts wird so auch in Ansehung der DS-GVO grundsätzlich weiter Bestand haben können und für Rechtssicherheit sorgen. Die Vorschrift kann dennoch nicht frei von Kritik sein. So ist erstens fraglich, ob der vollständige **Ausschluss der allgemeinen Interessenabwägung im Beschäftigungsverhältnis** mit den übrigen Vorgaben der DS-GVO vereinbar ist. Art. 88 Abs. 1 DS-GVO gestattet dem nationalen Gesetzgeber allein „spezifischere“ Vorschriften zur Datenverarbeitung im Beschäftigungsverhältnis zu erlassen. Gemeint sind Konkretisierungen der in den Artikeln 6 und 9 DS-GVO normierten Erlaubnistatbestände. Macht der nationale Gesetzgeber von dieser Öffnungsklausel Gebrauch, darf dies aber nicht zu einem (teilweisen) vollständigen Ausschluss einzelner Erlaubnistatbestände führen. Anderenfalls droht die Norm infolge ihrer Unvereinbarkeit mit Art. 6 Abs. 1 DS-GVO und in Ansehung der Rechtsprechung des EuGH² für nichtig erklärt zu werden. Empfohlen wird daher ein Zusatz, wonach die Datenverarbeitung im Beschäftigungskontext **auch auf Grundlage der allgemeinen Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO** zulässig ist. Erfolgt diese Klarstellung nicht, ist im überaus praxisrelevanten Bereich des Beschäftigtendatenschutzes eine weitere Verstärkung des zu Recht beklagten datenschutzrechtlichen Flickenteppichs innerhalb der EU zu besorgen,

¹ Vgl. § 28 Abs. 2 Nr. 1 iVm § 28 Abs. 1 S. 1 Nr. 2 BDSG (Interessen des Verantwortlichen); § 28 Abs. 2 Nr. 2 a) BDSG (Drittinteressen).

² Vgl. EuGH, Urt. v. 19.10.2016 – 582/14 („Breyer“).

da in Mitgliedstaaten, in denen die Regelungsoption des Art. 88 DS-GVO nicht wahrgenommen wird, weiterhin und ganz selbstverständlich Datenverarbeitungen im Beschäftigungsverhältnis auch auf Grundlage der allgemeinen Interessenabwägungsklausel des Art. 6 Abs. 1 Buchst. f) DS-GVO vorgenommen werden.

b. Formerfordernis der Einwilligungserklärung; § 26 Abs. 2 BDSG-E

Dass im Beschäftigungskontext abgegebene Einwilligungserklärungen grundsätzlich der **Schriftform** bedürfen sollen, erscheint im Zeitalter der Digitalisierung als **anachronistisch und als zu bürokratisch**. Die durch die Entwurfsverfasser angeführte Begründung, wonach hierüber die Nachweispflicht des Arbeitgebers im Sinne von Art. 7 Abs. 1 DS-GVO konkretisiert werden sollte, ist redundant. Eine solche besteht ohnehin und unabhängig vom Kontext der Datenverarbeitung. Kann der für die Verarbeitung Verantwortliche den erforderlichen Nachweis nicht führen, eröffnet sich für diesen ein nicht unerhebliches Sanktionsrisiko, weshalb hier schon aus eigenem Interesse Wert auf Nach- und Beweisbarkeit zu legen ist. Für die Schaffung spezifischer Formvorschriften besteht insoweit bereits kein Regelungsbedürfnis. Wird ein solches gleichwohl angenommen, erscheint eine Vorgabe zur Einholung einer **Einwilligung in Textform** als zureichend und zeitgemäß, da hierüber auch Einwilligungserklärungen in Form von Klickboxen, per Email usw. ausreichen würden. Die Befassungspflicht des Beschäftigten bliebe auch in diesen Konstellationen erhalten; dem Schutzgedanken der Norm würde weiterhin Rechnung getragen.

c. Verengung der Zulässigkeit einwilligungsbasierter Datenverarbeitung; § 26 Abs. 2 BDSG-E

Dass Einwilligungen nur dann einen wirksamen Erlaubnistatbestand darstellen, wenn neben der Informiertheit auch die Freiwilligkeit der Abgabe sichergestellt ist, ist eine Grundvoraussetzung. Auch die DS-GVO macht an gleich mehreren Stellen die Relevanz der Freiwilligkeit der Einwilligung deutlich. Ob vor diesem Hintergrund Konkretisierungen dieses Grundsatzes durch den nationalen Gesetzgeber überhaupt erforderlich sind, darf bezweifelt werden. Nachgerade problematisch werden solche Konkretisierungen aber dann, wenn hierüber ausgewählte Bereiche einer einwilligungsbasierten Datenverarbeitung rechtlich oder faktisch geradewegs entzogen werden. Mag die Formulierung in § 26 Abs. 2 S. 2 BDSG-E zwar davon sprechen, dass Einwilligungen im Beschäftigungsverhältnis „insbesondere“ bei für den Beschäftigten vorteilhaften bzw. bei gleichgelagerten Interessen als freiwillig angesehen werden können, wird hierüber doch eine Intention des Gesetzgebers deutlich, die die Zulässigkeit von Einwilligungen, die nicht in diese Kategorien fallen, unnötig erschwert. So ist insbesondere **unklar, wann noch von gleichgelagerten Interessen ausgegangen werden kann**. Auch ein Blick in die Gesetzesbegründung hilft an dieser Stelle nicht. Im Gegenteil kann an dieser Stelle bezweifelt werden, dass ein Beschäftigter im Rahmen einer einwilligungsbasierten Veröffentlichung seiner Bilddaten im Intranet eines Unternehmens stets ein dem Veröffentlichungsinteresse des Arbeitgebers gleichrangiges Interesse hat. Umgekehrt verkennt die aktuell gewählte Formulierung, die auf das Vorliegen synallagmatischer Interessen hindeutet, dass sich die

Gleichrangigkeit der betroffenen Interessen in der Praxis oftmals erst aus einer Gesamtschau ergibt, im Rahmen derer sich „Geben und Nehmen“ in Summe die Waage halten. Es wird daher angeregt, die Sätze 1 und 2 in § 26 Abs. 2 BDSG-E **zu streichen oder zumindest insoweit zu ergänzen**, als dass sich die Gleichrangigkeit der Interessen „aus einer Gesamtschau“ ergeben kann.

5. Zu § 31 BDSG-E | Auskunftswesen und Scoring

Anders als durch die Gesetzesbegründung suggeriert, regelt § 31 Abs. 2 BDSG-E nicht mehr die Modalitäten der Einmeldung, d.h. der Datenübermittlung an Auskunftswesen, sondern die Zulässigkeit der Verwendung eines durch eine Auskunftswesen ermittelten Wahrscheinlichkeitswertes. Streng am Wortlaut orientiert soll nunmehr die Verwendung eines von einer Auskunftswesen ermittelten Wahrscheinlichkeitswertes vom Vorliegen bestimmter Kriterien abhängig gemacht werden. Gemeint und orientiert an der Gesetzesbegründung ist aber wohl eine Fortführung des Schutzgedankens von § 28a BDSG und damit eine Regulierung der Zulässigkeit der Datenübermittlung an Auskunftswesen. Die Entwurfsfassung macht auch allein bei einer so vorgenommenen Interpretation Sinn, da Auskunftswesen typischerweise keine Kenntnis über die Tatbestandsvoraussetzungen des § 31 Abs. 2 S. 1 BDSG-E haben. Zu dem vermeintlich gewollten Ergebnis der Fortführung des status quo, das im Sinne eines **Mehr an Rechtssicherheit** grundsätzlich auch zu begrüßen ist, kommt der Rechtsanwender allerdings nur noch „über Umwege“.

Entscheidet sich der deutsche Gesetzgeber für die beschriebene Neuformulierung sollte **zumindest der Wortlaut** von § 31 Abs. 2 S. 1 Nr. 4 Buchst. c) und Nr. 5 BDSG-E **angepasst werden**. Gerade im Online- und Versandhandel werden im Falle von Zahlungstörungen Schuldner nicht selten durch eingeschaltete Dritte, etwa durch mit der Forderungsdurchsetzung beauftragte Dienstleister kontaktiert und durch diese über ihre Rechte informiert. Solche Unternehmen sind aber nicht selbst Gläubiger der offenen Forderung. Eine strenge allein am Wortlaut der Norm erfolgende Auslegung könnte mithin zu unerwünschten Ergebnissen führen. Konkret wird daher folgende Änderung angeregt:

§ 31 Abs. 2 S. 1 Nr. 4

[...]

c) der ~~Gläubiger den~~ Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftswesen unterrichtet **worden ist**

§ 31 Abs. 2 S. 1 Nr. 5

deren zugrundeliegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der ~~Gläubiger den~~ Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftswesen unterrichtet **worden ist**.

6. Zu § 32f. BDSG-E | Betroffenenrechte

Dass über die §§ 32f. BDSG-E die heute existierenden Ausnahmen von grundsätzlich bestehenden Rechten der betroffenen Person fortgeführt werden sollen, ist nicht nur **sinnvoll**, sondern auch in Ansehung der betroffenen Grundrechte des für die Verarbeitung Verantwortlichen dringend **erforderlich**. Einwände, wonach die angedachten Beschränkungen über die bereits existierenden Ausnahmen hinausgingen und insoweit das bestehende Schutzniveau unterminieren würden, sind schlichtweg falsch. Im Gegenteil werden einzelne, heute existierende Ausnahmen gerade nicht in den Gesetzestext des künftigen BDSG übernommen. Dies ist unverständlich und sachlich nicht zu rechtfertigen. Wir setzen uns deshalb für eine **1:1-Übernahme sämtlicher heute existierender Ausnahmetatbestände** ein. Die §§ 32f. BDSG-E bedürfen insoweit der nachfolgenden Ergänzungen:

- Übernahme von § 33 Abs. 2 Nr. 2 BDSG in § 33 BDSG-neu
- Übernahme von § 33 Abs. 2 Nr. 7a und 7b BDSG in § 33 BDSG-neu

7. Zu § 37 BDSG-E | Automatisierte Einzelentscheidungen

Die in § 37 BDSG-E vorgenommene Formulierung ist in mehrfacher Hinsicht missglückt. Zum einen stellt sich bereits die Frage, mit welcher Begründung der Gesetzgeber derart offensichtlich **Partikularinteressen einer einzelnen Branche** zu entsprechen versucht. Dies ist umso verwunderlicher, als die allein zugunsten der Versicherungsbranche vorgeschlagene Norm **schlichtweg überflüssig** ist. Die in § 37 Abs. 1 BDSG-E geregelten Fälle werden vom Regelungsgehalt des Art. 22 DS-GVO nämlich gar nicht erfasst. Es besteht daher bereits kein Bedürfnis, die Konstellation einer automatisierten Entscheidung auf Grundlage „verbindlicher Entgeltregelungen“ aus dem Anwendungsbereich von Art. 22 DS-GVO wieder herauszulösen.

Begründung: Betroffene Personen dürfen nach Art. 22 Abs. 1 DS-GVO keiner Entscheidung „unterworfen werden“. Ein solches „**Unterworfen sein**“, liegt aber nur dann vor, wenn der Verantwortliche die Bedingungen der Verarbeitung und damit die Grundlagen der automatisierten Entscheidung einseitig festlegt. Erforderlich ist somit, dass die Datenverarbeitung zu einer von der betroffenen Person nicht beeinflussten Entscheidung führt und der Computer nicht nur lediglich etwas ausführt, was auf Grundlage feststehender Parameter vorgezeichnet ist. Letzteres ist aber bei verbindlichen Entgeltregelungen, auf die kein Einfluss genommen werden kann, ersichtlich der Fall.

Des Weiteren werden nach dem Wortlaut von Art. 22 Abs. 1 DS-GVO **nur beeinträchtigende (rechtliche) Wirkungen**, d.h. nur solche, die Rechtspositionen der betroffenen Person negativ beeinflussen, **erfasst**. Eine solche Auslegung entspricht auch dem Schutzzweck der Norm; vor einer vollständig begünstigenden Entscheidung muss der Einzelne nicht geschützt werden. Die DS-GVO ist an dieser Stelle im Vergleich zu Art. 15 Abs. 1 RL 95/46/EG, nach dem sich

„beeinträchtigend“ noch allein auf die „Entscheidung“, nicht aber auch auf die „rechtliche Folge“ erstreckt, präziser. Eine andere Lesart hätte zur Folge, dass der Ordnungsgeber rechtliche Wirkungen per se als erheblich beeinträchtigend einstufen würde oder aber die in einer rechtlichen Wirkung immanent liegende gestaltende Wirkung zum gesonderten Maßstab erhebt. Beides erscheint als unsinnig. Eine auf Grundlage von Art. 22 Abs. 2 lit. b DS-GVO grundsätzlich denkbare, § 6a Abs. 2 Nr. 1 BDSG vergleichbare Ausnahmegesetzgebung im nationalen Recht für die betroffene Person begünstigende automatisierte Entscheidungen ist danach nicht erforderlich.

Wird der letztgenannte Aspekt durch den nationalen Gesetzgeber anders bewertet, wird eine branchenoffene, nicht an Partikularinteressen orientierte Formulierung angemahnt. Hier allein Partikularinteressen einer einzelnen Branche zu entsprechen, ist inakzeptabel. Vielmehr sollten dann automatisierte Entscheidungen **in allen Branchen** von der Regelung des Art. 22 Abs. 1 DS-GVO ausgeschlossen sein, wenn dem Begehren der betroffenen Person vollumfänglich stattgegeben wurde.

Vorab per E-Mail: ansgar.heveling@bundestag.de

Herrn
Ansgar Heveling MdB
Vorsitzender
Innenausschuss des
Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Arbeits- und Tarifrecht

arbeitsrecht@arbeitgeber.de

T +49 30 2033-1200
F +49 30 2033-1205

14. März 2017
0910-1703-012/Bal

Sehr geehrter Herr Vorsitzender,

am 9. März 2017 hat der Bundestag den Gesetzentwurf zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung in erster Lesung beraten. Der Innenausschuss wird sich voraussichtlich am 26. April 2017 hiermit befassen. Wir begrüßen sehr, dass die Anpassung des deutschen Rechts an die europäischen Vorgaben zeitnah abgeschlossen werden soll.

Die vorgesehene Neufassung des Bundesdatenschutzgesetzes hat allerdings Auswirkungen auf den Beschäftigtendatenschutz. Insbesondere die in § 26 Absatz 2 BDSG-neu aufgeführten Vorgaben zur Einwilligung halten wir für missglückt. Sie können die Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis in Frage stellen. Eine Beschränkung der Möglichkeit, in den Gebrauch der eigenen Daten einzuwilligen, widerspricht dem Geist der Datenschutz-Grundverordnung. Der Beschäftigte muss „Herr über seine Daten“ bleiben. Zudem ist die Vorgabe, dass die Einwilligung grundsätzlich in Schriftform zu erfolgen hat, in Zeiten digitaler Kommunikation nicht angemessen.

Kritisch sehen wir besonders auch die Ausweitung des Beschäftigtenbegriffs um Leiharbeitnehmer. Leiharbeitnehmer sind bereits durch die allgemeinen Vorgaben geschützt.

Anliegend übersenden wir Ihnen unsere Stellungnahme, in der wir diese sowie weitere Aspekte näher ausgeführt haben, die einer Änderung bedürfen. Wir bitten Sie, diese Stellungnahme den Mitgliedern des Ausschusses zukommen zu lassen.

Mit freundlichen Grüßen



Thomas Prinz



Eva Barlage-Melber

BDA | Bundesvereinigung der
Deutschen Arbeitgeberverbände

Mitglied von BUSINESSEUROPE

Hausadresse:
Breite Straße 29 | 10178 Berlin

Briefadresse:
11054 Berlin

www.arbeitgeber.de

Beschäftigtendatenschutz vernünftig anpassen

Stellungnahme zum Gesetzentwurf zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung – Datenschutz-Anpassungs- und Umsetzungsgesetz EU

2. März 2017

Zusammenfassung

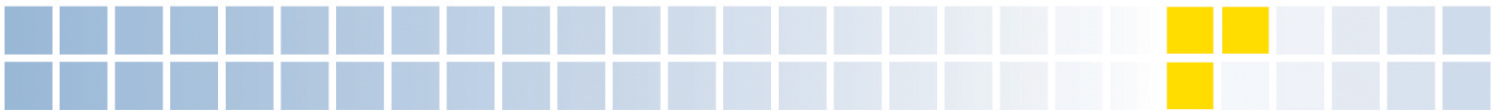
Mit der Verabschiedung der Datenschutz-Grundverordnung hat die Europäische Union einen wichtigen Schritt hin zu einem einheitlichen Datenschutzrecht in Europa gemacht. Die BDA hat diesen Grundansatz begrüßt, da durch den europäischen Binnenmarkt die grenzüberschreitende Tätigkeit von Unternehmen täglich gelebte Realität ist. Einheitliche europäische Regelungen zum Datenschutz können dazu beitragen, dass grenzüberschreitende wirtschaftliche Aktivitäten unbürokratisch durchgeführt werden können. Von den in der Datenschutz-Grundverordnung enthaltenen Öffnungsklauseln für mitgliedstaatliche Regelungen sollte deshalb nur zurückhaltend Gebrauch gemacht werden.

Der Beschäftigtendatenschutz bedarf vor dem Hintergrund der technischen Entwicklungen einer grundlegenden Reform. Themen wie „Big-Data-Anwendungen“ oder die Einordnung des Arbeitgebers als Telekommunikationsanbieter müssen stärker in das Blickfeld genommen werden. Gleichzeitig ist es wichtig, dass der Prozess der Anpassung des nationalen Rechts an die Vorgaben der Datenschutz-Grundverordnung zügig abgeschlossen wird, damit die Unternehmen schnell Rechtsklarheit erlangen, um innerhalb der kurzen Übergangsfrist bis zum 25. Mai 2018 ihre internen Prozesse an die komplexen Vorgaben der Datenschutz-Grundverordnung sowie des nationalen Rechts anpassen zu können.

Deshalb setzt die BDA sich dafür ein, die gegenwärtige Rechtslage zum Beschäftigtendatenschutz, wie sie insbesondere durch § 32 und § 3 Abs. 11 BDSG widergespiegelt wird, im Rahmen eines ersten Umsetzungsschritts beizubehalten.

Die Vorteile der Datenschutz-Grundverordnung dürfen nicht dadurch zunichte gemacht werden, dass die dort vorgesehenen Öffnungsklauseln dafür genutzt werden, auf nationaler Ebene komplizierte, rechtsunsichere und überflüssige Regelungen im Bereich des Beschäftigtendatenschutzes einzuführen.

Das gilt insbesondere für die im Gesetzentwurf vorgesehenen Vorgaben zur Einwilligung im Beschäftigungsverhältnis. Der Gesetzentwurf gewichtet im Hinblick auf die Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis nicht ausreichend, dass mit der Erteilung einer Einwilligung die betroffene Person ihr Grundrecht auf informationelle Selbstbestimmung ausübt und nicht etwa auf dieses Grundrecht verzichtet. Die Vorgaben der Grundverordnung zur Einwilligung führen zu einem angemessenen Schutzniveau. Eine weitergehende nationale Regelung ist abzulehnen. Zudem wäre die angestrebte Aufrechterhaltung des Schriftformerfordernisses der Einwilligung in Zeiten, in denen das „papierlose Büro“ vielfach gelebte Realität in den Unternehmen ist, ein rückwärtsgewandtes und nicht praxistaugliches Signal für den Beschäftigtendatenschutz.



Für die Verhandlung von Kollektivvereinbarungen ist es wesentlich, dass den Parteien ein weiter Verhandlungsspielraum zugestanden wird. Eine solche Klarstellung ist insbesondere vor dem Hintergrund der veränderten Sanktionsfolgen und dem Auslegungsbedarf vieler Vorschriften der Datenschutz-Grundverordnung erforderlich. Der Verweis auf Artikel 88 Abs. 2 sollte hingegen gestrichen werden.

Der Gesetzgeber sollte von einer Ausdehnung des bereits sehr weiten datenschutzrechtlichen Beschäftigtenbegriffs um Leiharbeitnehmer Abstand nehmen. Leiharbeitnehmer sind ausreichend geschützt.

Zudem ist es wichtig, dass im Hinblick auf geheimhaltungsbedürftige Daten Arbeitgebervereinigungen, die als Bevollmächtigte im arbeitsgerichtlichen Verfahren tätig werden, Berufsgeheimnisträgern gleichgestellt werden.

Im Einzelnen

Datenverarbeitung im Beschäftigungsverhältnis - § 26 BDSG-neu

Nach Art. 88 der Datenschutz-Grundverordnung (DS-GVO) können die Mitgliedstaaten Vorschriften zur Datenverarbeitung im Beschäftigtenverhältnis vorsehen. Eine Verpflichtung hierzu besteht nicht.

Den Unternehmen wird mit der Datenschutz-Grundverordnung auferlegt, sich innerhalb der kurzen Zeitspanne von zwei Jahren auf ein neues Datenschutzrecht einzustellen. Dies stellt bereits für große Unternehmen eine erhebliche Herausforderung dar. Gleichzeitig müssen für den Beschäftigtendatenschutz weiterhin 28 unterschiedliche nationale Rechtsordnungen eingehalten werden. Veränderte Vorgaben zum Beschäftigtendatenschutz zu diesem Zeitpunkt sind eine unnötige und übermäßige Zusatzbelastung für die Unternehmen.

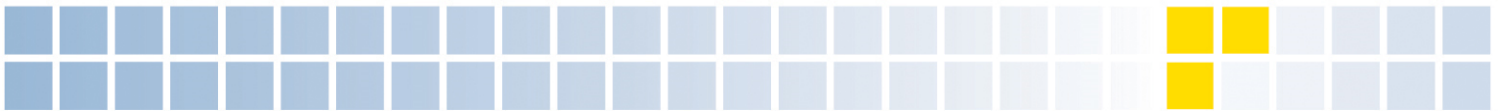
Der Gesetzgeber sollte das Rangverhältnis der nationalen Vorgaben zum Beschäftigtendatenschutz zu den Regelungen der Datenschutz-Grundverordnung klarstellen. Es

muss dabei sichergestellt sein, dass neben § 26 BDSG-neu auch Artikel 6 Abs. 1 DS-GVO als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten anwendbar ist, wenn personenbezogene Beschäftigtendaten zu anderen Zwecken als dem Beschäftigungsverhältnis verarbeitet werden – z. B. für die Abwicklung von Sonderleistungen wie Mitarbeiterversicherungen, Fahrzeugprogramme. Im Gesetzentwurf wird in § 1 Abs. 5 BDSG-neu ausgeführt, dass das BDSG-neu dann keine Anwendung findet, soweit die Datenschutz-Grundverordnung unmittelbar gilt. Zudem ergibt sich aus der Gesetzessystematik von Verordnung und nationalem Recht, dass Artikel 6 Abs. 1 DS-GVO weiterhin einschlägig sein kann. Um gleichwohl vorhandene Rechtsunsicherheit in dieser wichtigen Frage zu vermeiden, ist die Klarstellung erforderlich, dass Artikel 6 Abs. 1 DS-GVO für den Beschäftigtendatenschutz als Rechtsgrundlage für die Datenverarbeitung zu anderen Zwecken angewendet werden kann.

1. Verarbeitung für Zwecke des Beschäftigungsverhältnisses

Der Gesetzentwurf lehnt sich in § 26 Abs. 1 BDSG-neu teilweise an die heutigen Vorgaben von § 32 Abs. 1 BDSG an. Das ist grundsätzlich zu begrüßen. Ergänzt wird der Text um Ausführungen zu Rechten und Pflichten der Interessenvertretung der Beschäftigten. Diese Ergänzung ist überflüssig. Auf den Betriebsrat bezogen ergibt sich die Grundlage sowie der Umfang der zulässigen Datenverarbeitung heute aus den Vorschriften des BetrVG. Es ist davon auszugehen, dass dies auf der Grundlage von § 1 Abs. 2 BDSG-neu auch in Zukunft möglich sein wird. Sollten hieran Zweifel bestehen, sollten diese im Rahmen von § 1 Abs. 2 BDSG-neu gelöst werden und nicht durch § 26 BDSG-neu. Ergeben sich Rechte und Pflichten der Interessenvertretung der Beschäftigten auf der Grundlage von Kollektivvereinbarungen, so stellt § 26 Abs. 4 BDSG-neu sicher, dass dies auch in Zukunft möglich sein wird.

Die in § 26 Abs. 1 BDSG-neu aufgenommene Legaldefinition von „Kollektivvereinbarung“ sollte in § 26 Abs. 4 BDSG-neu ver-



schoben werden. Sie ist in § 26 Abs. 1 BDSG-neu fehl am Platze, da sie dazu führt, dass das Thema „Kollektivvereinbarungen“ unnötig auf zwei Absätze aufgeteilt wird.

Wenn der Gesetzgeber es für notwendig erachtet, den heutigen Gesetzestext des § 32 Abs. 1 BDSG abzuändern, so sollte er vielmehr klarstellen, dass Arbeitgeber auch dann einem konkreten Verdacht auf eine schwere Vertragspflichtverletzung zielgerichtet nachgehen können, wenn diese unterhalb der Schwelle zur Strafbarkeit liegt. Dass dies notwendig ist, zeigt ein Urteil des LArbG Baden-Württemberg (20. Juli 2016, 4 Sa 61/15), das auf der Grundlage des Wortlauts von § 32 BDSG die Auffassung vertreten hat, dass Arbeitgeber dann konkreten Anhaltspunkten nicht nachgehen dürfen, wenn sich diese nur auf schwere Pflichtverletzungen und nicht auf Straftaten beziehen. Das BAG hat jedoch in einer aktuellen Entscheidung klargestellt, dass nicht nur der konkrete Verdacht einer strafbaren Handlung, sondern auch einer anderen schweren Verfehlung zu Lasten des Arbeitgebers ausreichend sein kann, um einen Eingriff in das Recht auf informationelle Selbstbestimmung zur rechtfertigen (BAG, 22. September 2016, 2 AZR 848/15). Dies zeigt, dass eine gesetzgeberische Klarstellung im o. g. Sinne angezeigt ist.

2. Einwilligung

Eine eigenständige Regelung zur Einwilligung im Beschäftigungsverhältnis ist nicht erforderlich. Die Vorgaben in § 26 Abs. 2 BDSG-neu sollten gestrichen werden. Die Vorgaben der Grundverordnung führen bereits zu einem angemessenen Schutzniveau.

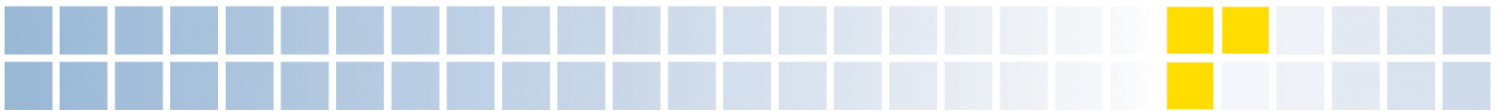
Die Möglichkeit, Daten auf der Grundlage einer Einwilligung verarbeiten zu können, ist gerade in den Fällen wichtig, in denen kein Betriebsrat besteht, der eine Betriebsvereinbarung zur Datenverarbeitung abschließen könnte, oder wenn Personengruppen betroffen sind, die von einer solchen Vereinbarung nicht erfasst werden.

§ 26 Abs. 2 BDSG-neu geht insbesondere auf die **Freiwilligkeit** der Einwilligung ein.

Solche Vorgaben zur Freiwilligkeit der Einwilligung sind nicht erforderlich, stellt doch die Datenschutz-Grundverordnung in Erwägungsgrund 32 fest, dass eine Einwilligung eine freiwillige Handlung ist. Näher wird der Aspekt der Freiwilligkeit in Erwägungsgrund 43 zu Artikel 7 DS-GVO betrachtet. Es wird dort u. a. ausgeführt, dass eine Einwilligung nur in besonderen Fällen keine Rechtsgrundlage für die Datenverarbeitung sein kann, z. B. wenn ein klares Ungleichgewicht wie beim Verhältnis Behörde – betroffene Person besteht. Der europäische Gesetzgeber hat ganz bewusst die ursprüngliche Vorgabe der EU-Kommission nicht übernommen, die eine Einwilligung im Beschäftigungsverhältnis kritisch gesehen hatte. Der Wille des europäischen Gesetzgebers muss auf nationaler Ebene berücksichtigt werden. Das ist durch § 26 Abs. 2 BDSG-neu nicht gegeben.

Dass ein klares Ungleichgewicht im Arbeitsverhältnis grundsätzlich nicht gegeben ist, ergibt sich auch aus der Rechtsprechung des BAG. Das BAG hat mit seiner Entscheidung vom 11. Dezember 2014 (8 AZR 1010/13) anerkannt, dass die Erteilung einer Einwilligung im Beschäftigungsverhältnis möglich ist. Das BAG führt aus, dass auch im Rahmen eines Arbeitsverhältnisses Arbeitnehmer sich grundsätzlich frei entscheiden können, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen. Dem stünde weder die grundlegende Tatsache, dass Arbeitnehmer abhängig Beschäftigte sind, noch das Weisungsrecht des Arbeitgebers entgegen. Mit den konkreten Vorgaben in § 26 Abs. 2 BDSG-neu, wann vom Vorliegen einer freiwilligen Einwilligung ausgegangen wird, wird demgegenüber zu Unrecht unterstellt, dass eine Einwilligung grundsätzlich nicht freiwillig erfolgt.

Mit der Erteilung einer Einwilligung übt der betroffene Grundrechtsträger sein Grundrecht auf informationelle Selbstbestimmung aus. Es geht hierbei gerade nicht darum, dass auf dieses Grundrecht verzichtet wird. Nachdem der Beschäftigte sogar sein Beschäftigungsverhältnis jederzeit auflösen kann, muss er erst recht „Herr über seine Daten“ sein. Es ist davon auszugehen, dass eine Einwilligung freiwillig erteilt wird. Nur bei



begründeten Zweifeln sollte geprüft werden, ob eine besondere Situation vorliegt, die der freiwilligen Erteilung einer Einwilligung entgegenstehen könnte. Dies würde auch der Struktur der Datenschutz-Grundverordnung entsprechen, die in Erwägungsgrund 43 ihren Niederschlag gefunden hat. Eine solche Prüfung kann nur bezogen auf den Einzelfall erfolgen. Die Vorgabe bestimmter Kriterien kann dem nicht gerecht werden.

Konkrete Vorgaben im Gesetzestext, wann eine freiwillige Einwilligung vorliegen kann, sind ebenso abzulehnen, wie die in der Gesetzesbegründung zu § 26 Abs. 2 BDSG-neu aufgeführten Beispiele, wann z. B. die Gewährung eines Vorteils vorliegt. Hierdurch können nicht alle denkbaren Fälle einer Einwilligung abgedeckt werden. So würde sich z. B. die Frage stellen, ob die heute zulässige Einwilligung zur Datenverarbeitung, um die Dienstleistungsqualität in Telefonieabteilungen festzustellen, noch zulässig wäre. Zudem schaffen solche Vorgaben zusätzliche Rechtsunsicherheit. So wäre z. B. zu diskutieren, ob automatisch von gleichgelagerten Interessen ausgegangen werden kann, wenn sie in einer Kollektivvereinbarung wie einer Betriebsvereinbarung niedergelegt sind.

Die Vorgaben im Hinblick auf ein **Schriftformerfordernis** im Rahmen der Erteilung einer Einwilligung sind verfehlt.

Die Datenschutz-Grundverordnung sieht keine Verpflichtungen im Hinblick auf Formerfordernisse wie Schriftform und Textform vor. Wie Erwägungsgrund 32 ausführt, kann eine Einwilligung vielmehr z. B. schriftlich, mündlich oder in elektronischer Form erklärt werden. Es ist kein Grund ersichtlich, warum diese für alle Einwilligungen geltenden Bewertungen und Vorgaben der Datenschutz-Grundverordnung nicht auch für das Beschäftigungsverhältnis Anwendung finden sollen.

Gemäß Art. 88 Abs. 1 DS-GVO können die Mitgliedstaaten „spezifischere Vorschriften“ vorsehen. Die Vorgabe konkreter Formvorschriften geht über eine Konkretisierung der o. g. europäischen Vorgaben hinaus und

überschreitet somit den von der Datenschutz-Grundverordnung gesetzten Rahmen.

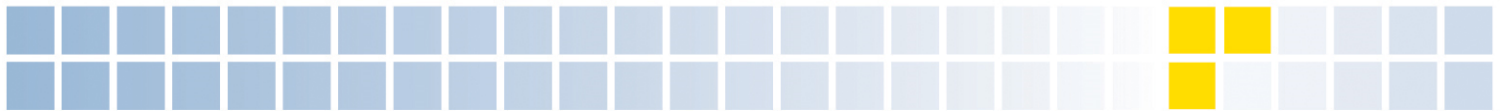
§ 26 Abs. 2 Satz 3 BDSG-neu legt für die Einwilligung ein Schriftformerfordernis fest, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. In Zeiten voranschreitender Digitalisierung, in denen das „papierlose Büro“ vielfach gelebte Realität in den Unternehmen ist, wäre ein solches Schriftformerfordernis ein rückwärtsgewandtes und nicht praxistaugliches Signal für den Beschäftigtendatenschutz.

Sollte entgegen der hier vertretenen Auffassung gleichwohl ein Formerfordernis für die Erteilung einer Einwilligung festgelegt werden, so sollte allenfalls Textform gemäß § 126b BGB vorgeschrieben werden. Damit könnte der Verantwortliche ausreichend nachweisen, dass der Betroffene eingewilligt hat. Die Schutzvorkehrung, die mit dem Schriftformerfordernis verknüpft ist, ist im Falle der Einwilligung hingegen nicht notwendig, da die Einwilligung gem. Artikel 7 Abs. 3 DS-GVO jederzeit widerrufen werden kann.

3. Besondere Kategorien personenbezogener Daten von Beschäftigten

Grundsätzlich ist zu begrüßen, dass der Gesetzgeber von den mitgliedstaatlichen Regelungsmöglichkeiten des Artikels 9 Abs. 1 DS-GVO Gebrauch machen will. In vielen Bereichen ist es unerlässlich, dass besondere Kategorien von Daten verarbeitet werden. Ein Beispiel hierfür sind Untersuchungen wie Alkoholkontrollen, um zu gewährleisten, dass sicherheitsempfindliche Verfahrensvorgänge ungestört ablaufen können.

Eine eigenständige Regelung hierzu in § 26 BDSG-neu ist hingegen abzulehnen. Der Gesetzgeber geht bereits in § 22 BDSG-neu auf die Verarbeitung besonderer Kategorien personenbezogener Daten ein. Es ist nicht ersichtlich, warum dieser Bereich aufgeteilt werden soll, indem neben § 22 BDSG-neu in § 26 BDSG-neu eine eigenständige Regelung zu diesem Bereich bezogen auf Daten von Beschäftigten geschaffen werden soll. Eine solche Aufteilung würde vielmehr we-



gen Abgrenzungsfragen zu unnötiger Rechtsunsicherheit führen.

Dass es hier Abgrenzungsprobleme geben wird, zeigt bereits die Anmerkung in der Gesetzesbegründung auf, wonach die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses auch die Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit einschließen „kann“. Eine solche „Kann-Formulierung“ in der Gesetzesbegründung schafft nicht die notwendige Rechtssicherheit. Hierfür ist es notwendig, die Vorgaben von Artikel 9 Abs. 1 b) DS-GVO in § 22 BDSG-neu zu integrieren und auf die Sonderregelung in § 26 Abs. 3 BDSG-neu zu verzichten.

Diese unnötigen Abgrenzungsschwierigkeiten werden auch dadurch deutlich, dass im Rahmen von § 26 Abs. 3 BDSG-neu die Vorgaben von § 22 Abs. 2 BDSG-neu, Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen, angewendet werden müssen. Dies soll jedoch gemäß § 22 Abs. 2 Satz 3 BDSG-neu dann nicht gelten, wenn § 22 Abs. 1 b) BDSG-neu einschlägig ist. Bezogen z. B. auf die Beurteilung der Arbeitsfähigkeit, die nach der Gesetzesbegründung sowohl unter § 26 Abs. 3 als auch unter § 22 Abs. 1 b) BDSG-neu fallen kann, wäre unklar, ob § 22 Abs. 2 BDSG-neu angewendet werden muss oder nicht.

4. Kollektivvereinbarungen

Der europäische Gesetzgeber hat in der Datenschutz-Grundverordnung zu Recht klar gestellt, dass Kollektivvereinbarungen, wie insbesondere Betriebsvereinbarungen und Tarifverträge, eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein können, vgl. Artikel 88 iVm Erwägungsgrund 155 DS-GVO. Die Tarifautonomie sowie die Betriebspartnerschaft sind wesentliche Grundlagen des deutschen Arbeitsrechts.

Artikel 88 Abs. 1 DS-GVO spricht davon, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften vorsehen können. Es ist deshalb zu begrüßen, dass der Ge-

setzentwurf in § 26 Abs. 4 vorsieht, dass die Verarbeitung personenbezogener Daten auf der Grundlage von Kollektivvereinbarungen zulässig ist. Dass Kollektivvereinbarungen eine Datenverarbeitung rechtfertigen können, entspricht bereits heute der geltenden Rechtslage, wonach gemäß § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf der Grundlage einer „anderen Rechtsvorschrift“ zugelassen wird.

Darüber hinaus ist es wesentlich, dass klar gestellt wird, dass beiden Parteien einer Kollektivvereinbarung ein *weiter* Verhandlungsspielraum zugestanden wird. Eine solche Klarstellung ist insbesondere vor dem Hintergrund der veränderten Sanktionsfolgen und dem Auslegungsbedarf vieler Vorschriften der Datenschutz-Grundverordnung erforderlich. Die Verhandlungspartner benötigen Rechtssicherheit. Bereits heute ergibt sich aus § 75 Abs. 2 BetrVG die Verpflichtung von Arbeitgebern und Betriebsräten, die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern. Wie dieser Schutz konkret ausgestaltet wird, sollte auch zukünftig den gleichrangigen Verhandlungspartnern überlassen bleiben.

Für einen weiten Verhandlungsspielraum spricht zudem Artikel 88 Abs. 2 DS-GVO selbst. Die Aussage von Artikel 88 Abs. 2 DS-GVO, dass z. B. die menschliche Würde, berechnete Interessen und Grundrechte gewahrt werden müssen, wäre unnötig, wenn durch Kollektivvereinbarungen die Vorgaben der Datenschutz-Grundverordnung nur konkretisiert werden könnten. Denn durch die Grundverordnung selbst werden bereits berechnete Interessen und Grundrechte sowie die menschliche Würde gewahrt. Der ausdrückliche Hinweis hierauf macht vielmehr deutlich, dass der europäische Gesetzgeber für Kollektivvereinbarungen auch Abweichungen von den Vorgaben der Datenschutz-Grundverordnung zulassen wollte, die wiederum den in Artikel 88 Abs. 2 DS-GVO gesetzten Grenzen unterliegen sollten.

In der Gesetzesbegründung wird ausgeführt, dass den Verhandlungsparteien ein „Ermessensspielraum im Rahmen des geltenden



Rechts einschließlich der Verordnung (EU) 2016/679“ zusteht. Das ist ein richtiger Ansatz, der weiter ausgeführt werden sollte.

Ein Verweis auf Artikel 88 Abs. 2 DS-GVO für Kollektivvereinbarungen ist nicht notwendig. Er würde nur die Rechtssicherheit gefährden. Bereits nach heutigem Recht wird gemäß § 75 Abs. 2 BetrVG in den von Kollektivvereinbarungen ganz überwiegend angesprochenen Betriebsvereinbarungen die freie Entfaltung der Persönlichkeit der Arbeitnehmer geschützt und gefördert. Damit wird bestätigt, dass die Freiheitsrechte des Grundgesetzes auch im Betrieb gelten. Ein Verweis auf Artikel 88 Abs. 2 DS-GVO ist auch europarechtlich nicht angezeigt.

5. Einhaltung von Verarbeitungsgrundsätzen

Die Datenschutz-Grundverordnung geht dem nationalen Recht vor. Damit findet z. B. Artikel 5 DS-GVO unmittelbar Anwendung. Ein ausdrücklicher Hinweis u. a. auf diesen Artikel in § 26 Abs. 5 BDSG-neu wäre nur dann sinnvoll, wenn man davon ausginge, dass diese Regelungen andernfalls im Beschäftigungsverhältnis nicht eingreifen würden. Solche Anhaltspunkte finden sich jedoch weder im Gesetzestext noch in der Gesetzesbegründung.

6. Anwendungsbereich

Die Vorgabe, dass § 26 Abs. 1 bis 6 BDSG-neu auch dann anzuwenden ist, wenn Daten verarbeitet werden, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen, ist abzulehnen.

Die Aufnahme einer solchen Regelung würde der Grundentscheidung der Datenschutz-Grundverordnung zum sachlichen Anwendungsbereich widersprechen. Artikel 2 Abs. 1 DS-GVO sieht vor, dass die Verordnung für die Verarbeitung personenbezogener Daten gilt, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Begriff „Dateisystem“ wird in Artikel 4 Nr. 6 DS-GVO definiert und umfasst strukturierte Sammlungen personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. § 26 Abs. 7 BDSG-neu zielt hinge-

gen auf jede Form der Verarbeitung ab. Nachdem nach Artikel 88 Abs. 1 DS-GVO nur „spezifischere Vorschriften“ durch die Mitgliedstaaten vorgesehen werden können, ist es bedenklich, wenn von solchen grundlegenden Regelungen der Verordnung abgewichen werden soll.

7. Beschäftigtenbegriff

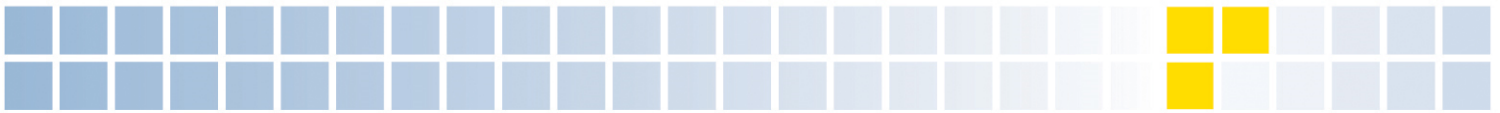
Leiharbeitnehmer sind Arbeitnehmer des Verleihers und haben mit diesem ein auf einem Arbeitsvertrag basierendes Beschäftigungsverhältnis. Leiharbeitnehmer sind somit „Beschäftigte“ des Verleihers. Damit hat ein Leiharbeitnehmer als Beschäftigter des Verleihers nicht weniger Rechte als die Beschäftigten des Entleihers, nur der Bezugspunkt ist ein anderer. Deshalb ist die in § 26 Abs. 8 Nr. 1 BDSG-neu vorgesehene Ausweitung des Beschäftigtenbegriffs auf Leiharbeitnehmer abzulehnen.

Es ist selbstverständlich, dass auch Leiharbeitnehmern gegenüber dem Entleiher das Recht auf informationelle Selbstbestimmung zusteht, das Ausfluss des allgemeinen Persönlichkeitsrechts ist. Ein Leiharbeitnehmer kann somit auch gegenüber dem Entleiher über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen. Eine Ausweitung des Beschäftigtenbegriffs auf Leiharbeitnehmer ist deshalb nicht geboten.

Eine Ergänzung des Beschäftigtenbegriffs um Leiharbeitnehmer könnte auch mitbestimmungsrechtliche Auswirkungen haben. § 87 BetrVG findet dann Anwendung, wenn ein Beschäftigungsverhältnis sowie ein Arbeitsvertrag zum Arbeitgeber besteht, auch wenn es im Einzelnen Abweichungen geben mag. Hieran fehlt es beim Leiharbeitnehmer gerade. Es ist kein Grund ersichtlich, warum von diesen beiden Voraussetzungen abgewichen werden soll.

Geheimhaltungspflicht unterliegende Daten - § 29 BDSG-neu

Es ist wichtig, dass auch weiterhin die Möglichkeit besteht, geheimhaltungsbedürftige Daten geheim halten zu können.



Dabei ist es geboten, in Bezug auf die Rechte der betroffenen Personen Berufsgeheimnisträger und Arbeitgebervereinigungen gleichzustellen, die als Bevollmächtigte im arbeitsgerichtlichen Verfahren tätig werden. Hierzu muss geregelt werden, dass die flexiblen Vorgaben für Berufsgeheimnisträger wie in Artikel 14 Abs. 5 d) DS-GVO und § 29 BDSG-neu sich auch auf Bevollmächtigte im Sinne des § 11 Abs. 2 Ziffer 4 ArbGG beziehen.

Eine Gleichstellung von Berufsgeheimnisträgern und Arbeitgebervereinigungen als Bevollmächtigte ist bereits heute vielfach gegeben. Aus § 11 Abs. 2 Ziffer 4 ArbGG ergibt sich, dass die Parteien eines Rechtsstreits sich u. a. durch Arbeitgebervereinigungen als Bevollmächtigte vor dem Arbeitsgericht vertreten lassen können. Gemäß § 11 Absatz 4 ArbGG gilt die Gleichstellung ausdrücklich auch für die Instanzen mit Anwaltszwang. Bei einer Vielzahl von weiteren Vorschriften werden Verbandsvertreter in ihren Rechten und Pflichten den Rechtsanwälten gleichgestellt, wie z. B. in § 50 Absatz 2, § 12a Absatz 2 ArbGG.

Ebenso wie bei Rechtsanwälten muss die Vertraulichkeit und Geheimhaltung im Verhältnis auch zwischen der vertretenen Person und den Verbandsvertretern geschützt werden. Um den notwendigen Gleichklang sicherzustellen, ist eine Klarstellung erforderlich, dass der grundsätzlich richtige Ansatz, die Rechte der betroffenen Person in bestimmten Fällen zurücktreten zu lassen, sich auch auf Bevollmächtigte im Sinne des § 11 Abs. 2 Ziffer 4 ArbGG bezieht. Der europäische Gesetzgeber eröffnet mit Artikel 23 DS-GVO den Mitgliedstaaten eine solche Möglichkeit.

Datenschutzbeauftragter - § 38 BDSG-neu

Die Pflicht zur Benennung eines Datenschutzbeauftragten sollte auf die zwingenden Vorgaben von Artikel 37 Abs. 1 der Datenschutz-Grundverordnung zurückgeführt werden.

In Artikel 37 Abs. 1 DS-GVO wird festgelegt, dass ein Datenschutzbeauftragter u. a. zu bestellen ist, wenn die Verarbeitung perso-

nenbezogener Daten zur Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters gehört und dies eine umfangreiche regelmäßige und systematische Überwachung erforderlich macht. Gleiches gilt, wenn es sich um die umfangreiche Verarbeitung von Daten im Sinne von Artikel 9 und 10 DS-GVO als Kerntätigkeit handelt.

Bereits die heutigen Vorgaben zur Bestellung eines Datenschutzbeauftragten gemäß § 4 f BDSG gehen weit über diese Vorgaben hinaus. Die nun im Gesetzentwurf vorgesehene Zahl für eine Benennungspflicht schränkt die heutigen Vorgaben weiter ein. Auch wenn nach Artikel 37 Abs. 4 der Datenschutz-Grundverordnung den Mitgliedstaaten eigenständige Regelungen zugestanden werden, ergibt sich hieraus keine Verpflichtung, eigenständige Regelungen treffen zu müssen. Zudem war bereits im Rahmen des Bürokratieabbaus für das BDSG angedacht worden, die Benennungsvoraussetzungen für Datenschutzbeauftragte weniger streng zu fassen¹.

Vor dem Hintergrund, dass mit der Verordnung eine Harmonisierung des Datenschutzes in der EU angestrebt wird, und die Benennungsverpflichtungen des BDSG gerade für kleine und mittlere Unternehmen eine Belastung darstellen, wäre es sinnvoll, zukünftig auf die Vorgaben von Artikel 37 Abs. 1 DS-GVO abzustellen.

Videoüberwachung - § 4 BDSG-neu

Es ist richtig, die Regelung der Videoüberwachung öffentlich zugänglicher Räume in § 4 BDSG-neu an die veränderten Rahmenbedingungen anzupassen. Angesichts der aktuellen Vorfälle ist es wichtig, Sicherheitsbelange stärker zu berücksichtigen, als dies im bisherigen § 6 b BDSG der Fall ist.

Dieser richtige Ansatz sollte weiter gefasst werden und sich nicht nur auf großflächige Anlagen wie Einkaufszentren, sondern auch auf Einzelhandelsgeschäfte wie Waren- und

¹ Eckpunkte zur weiteren Entlastung der mittelständischen Wirtschaft von Bürokratie, Kabinettsbeschluss vom 11. Dezember 2014, Punkt 21



Kaufhäuser beziehen, die der gleichen Sicherheitslage unterliegen.

§ 4 Abs. 2 BDSG-neu sollte an praktische Notwendigkeiten angepasst werden. Der Gesetzentwurf sieht vor, dass nicht nur der Umstand der Beobachtung, sondern auch Name und Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Das ist nicht praktikabel. Zudem führt die Formulierung „frühestmöglicher Zeitpunkt“ zu Rechtsunsicherheit. Diese Vorgabe sollte man auf die bisherige Regelung des § 6 b Abs. 2 BDSG zurückführen.

Darüber hinaus muss im Hinblick auf gezielte Kontrollen im Beschäftigungsverhältnis darauf hingewiesen werden, dass nach ständiger Rechtsprechung des BAG diese unter bestimmten engen Voraussetzungen rechtmäßig sind. Sie sind zur Aufdeckung von Straftaten z. B. im Einzelhandel von hoher Bedeutung. In der Gesetzesbegründung zu § 26 BDSG-neu wird hingegen im Hinblick auf die zukünftige Ausrichtung des Beschäftigtendatenschutzes suggeriert, dass solche Kontrollen nicht möglich sind. Das ist irreführend.

Datenübermittlung zwischen Konzerngesellschaften

Innerhalb von Konzernen werden Beschäftigtendaten häufig bei einer zentralen Stelle gespeichert, z. B. bei der Muttergesellschaft, um eine einheitliche Personalverwaltung zu gewährleisten.

Nach Artikel 6 Abs. 1 f) und Erwägungsgrund 48 der DS-GVO können Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, wie die Verarbeitung von Beschäftigtendaten, zu übermitteln.

Diese Vorgaben der Datenschutzgrundverordnung sowie die Regelungen zum Begriff „Unternehmensgruppe“ in Artikel 4 Abs. 19

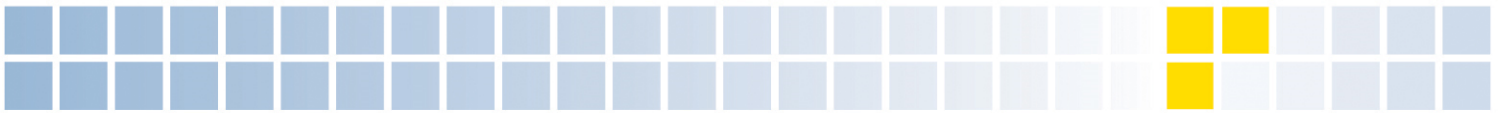
und Erwägungsgrund 37 der DS-GVO legen nahe, dass sowohl Unterordnungskonzerne im Sinne von § 18 Abs. 1 AktG als auch Gleichordnungskonzerne gemäß § 18 Abs. 2 AktG sich auf Artikel 6 Abs. 1 f) der DS-GVO stützen können, um personenbezogene Daten der Beschäftigten innerhalb des Konzerns zu übermitteln. Um in diesem Punkt mehr Rechtssicherheit zu erzielen, wäre es angebracht, wenn im Rahmen der Anpassung des deutschen Rechts an die Vorgaben der Grundverordnung dieses klarstellend bestätigt würde.

Darüber hinaus sollte insgesamt näher auf die Datenübermittlung zwischen Konzerngesellschaften eingegangen werden. In einer solchen Regelung sollte insbesondere festgelegt werden, in welchen Fällen des Beschäftigtendatenschutzes ein „berechtigtes Interesse“ im Sinne von Erwägungsgrund 48 der DS-GVO vorliegt. Ein solches Interesse muss nach der Grundverordnung gegeben sein, um personenbezogene Daten von Beschäftigten innerhalb von Unternehmensgruppen oder Gruppen von Einrichtungen, die einer zentralen Stelle zugeordnet sind, übermitteln zu können. Eine nähere Ausgestaltung dieses unbestimmten Rechtsbegriffs würde zu mehr Rechtssicherheit für die angesprochenen Gruppen führen.

Angemessenheitsentscheidungen - § 21 BDSG-neu

Nachdem der EuGH durch Urteil vom 6. Oktober 2015 die „Safe-Harbor-Entscheidung“ für ungültig erklärt hat (C – 362/14), besteht für die Unternehmen erhebliche Rechtsunsicherheit im Hinblick auf die Übermittlung von personenbezogenen Daten in die USA. In diesem Urteil hat der EuGH auch ein Klage-recht für Kontrollstellen angesprochen. Gleichwohl darf die Wirkung einer Klagemöglichkeit, wie sie § 21 BDSG-neu vorsieht, nicht unterschätzt werden.

Der Angemessenheitsbeschluss der EU-Kommission zum „Privacy Shield“ als Nachfolgeregelung zu „Safe Harbor“ bietet die Möglichkeit, Daten rechtssicher in die USA übermitteln zu können. Durch diesen Beschluss ist es der EU gelungen, das Vertrau-



en in die Rechtmäßigkeit der Datenübermittlung in die USA zumindest im Hinblick auf diesen Übertragungsweg wieder herzustellen. Gleiches gilt für Standardschutzklauseln und Beschlüsse für die Allgemeingültigkeit von genehmigten Verhaltensregeln. Wenn Unternehmen nun befürchten müssen, dass jegliche Aufsichtsbehörde gegen solche Beschlüsse gerichtlich vorgehen kann, würde das gerade zurückgewonnene Vertrauen in die Rechtssicherheit wieder in Frage gestellt.

Deshalb sollte das Klagerecht nur durch die Bundesbeauftragte als zentrale Anlaufstelle im Sinne von § 17 BDSG-neu ausgeübt und nicht jedem Landesdatenschutzbeauftragten eröffnet werden. Die Entscheidung, ob ein solches Klagerecht ausgeübt wird, sollte von allen Datenschutzaufsichtsbehörden gemeinsam getroffen werden.

Generellen Reformbedarf im Auge behalten

Vor dem Hintergrund der Debatte zu „Arbeiten 4.0“ ist die grundlegende Frage zu stellen, wie der Beschäftigtendatenschutz an die technischen Entwicklungen angepasst werden muss, damit er die sich hieraus ergebenden Chancen flankieren kann, ohne dabei zum Hemmschuh für den Einsatz neuer technischer Entwicklungen zu werden. Weitere Verschärfungen gesetzlicher Vorgaben, wie sie sowohl im Gesetzestext als auch in seiner Begründung angesprochen sind, sind der falsche Weg.

Neben den grundlegenden Fragestellungen über die Rolle des Datenschutzes im Rahmen der Debatte um „Arbeiten 4.0“ gibt es beim Beschäftigtendatenschutz eine Reihe weiterer Aspekte, die der Fortentwicklung bedürften. Hierzu gehört zum Beispiel die Klarstellung, dass Arbeitgeber auch dann einem konkreten Verdacht auf eine schwere Vertragspflichtverletzung zielgerichtet nachgehen können, wenn diese unterhalb der Schwelle zur Strafbarkeit liegt. Gleiches gilt für präventive Ermittlungen. Beschäftigtendatenschutz muss die Bekämpfung von Pflichtverletzungen unterstützen. Sie müssen zudem von Anfang an unterbunden werden

können. Hierfür sind rechtssichere gesetzliche Grundlagen erforderlich.

Zudem sollte für den Beschäftigtendatenschutz ein Anreiz dafür gesetzt werden, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Das könnte dadurch geschehen, dass eine solche Anonymisierung oder Pseudonymisierung ohne Einwilligung der betroffenen Person erfolgen kann. Hierdurch könnte der Schutz der ursprünglich betroffenen Person erhöht werden.

Eine Veränderung ist auch im Bereich der Privatnutzung von E-Mail und Internet erforderlich. Es bedarf in diesem Zusammenhang einer gesetzlichen Klarstellung, dass Arbeitgeber in diesem Fall nicht Diensteanbieter im Sinne des TKG und TMG werden. Dies würde zudem der Rechtsprechung verschiedener Instanzgerichte entsprechen (u.a. LArbG Berlin-Brandenburg, Urteil vom 14.1.2016, 5 Sa 657/15).

Eine solche Klarstellung ist längst überfällig. Die laufende Nutzung von E-Mail und Internet wird immer mehr zur Selbstverständlichkeit. Damit steigt auch die Zahl derjenigen Arbeitnehmer, die während der Arbeitszeit auf die private Nutzung von E-Mail und Internet nicht verzichten wollen. Gleichzeitig gibt es viele Unternehmen, die diese private Nutzung - in einem vertretbaren Maß - ihren Mitarbeitern einräumen wollen. Problematisch ist die erlaubte Privatnutzung betrieblicher Kommunikationsmittel jedoch wegen der umstrittenen Frage, ob ein Arbeitgeber hierdurch zum Diensteanbieter im Sinne des TKG und TMG wird. Wäre dies der Fall, würde die Kommunikation dem Fernmeldegeheimnis unterliegen, was auf die Rechtsbeziehung von Arbeitgebern und Arbeitnehmern nicht passt.

Zudem sollte dadurch für mehr Rechtssicherheit gesorgt werden, dass Aufsichtsbehörden stärker mit einer Stimme sprechen, als dies bislang der Fall ist. Ein einheitliches Vorgehen ist gerade für Unternehmen wichtig, die über Standorte in mehreren Bundesländern verfügen. Die föderale Struktur der Bundesrepublik Deutschland, die sich in der



Struktur der Aufsichtsbehörden widerspiegelt, kann zu Unsicherheiten und Standortnachteilen führen. Es müsste vielmehr die Aufsichtsbehörde desjenigen Bundeslandes federführend und allein weisungsbefugt sein, in deren Gebiet die Hauptverwaltung des jeweiligen Unternehmens ansässig ist.

Ansprechpartner:

BDA | DIE ARBEITGEBER

Bundesvereinigung der Deutschen Arbeitgeberverbände

Arbeits- und Tarifrecht

T +49 30 2033-1200

arbeitsrecht@arbeitgeber.de

Die BDA ist die sozialpolitische Spitzenorganisation der gesamten deutschen gewerblichen Wirtschaft. Sie vertritt die Interessen kleiner, mittelständischer und großer Unternehmen aus allen Branchen in allen Fragen der Sozial- und Tarifpolitik, des Arbeitsrechts, der Arbeitsmarktpolitik sowie der Bildung. Die BDA setzt sich auf nationaler, europäischer und internationaler Ebene für die Interessen von einer Mio. Betrieben mit ca. 20 Mio. Beschäftigten ein, die der BDA durch freiwillige Mitgliedschaft in Arbeitgeberverbänden verbunden sind. Die Arbeitgeberverbände sind in den der BDA unmittelbar angeschlossenen 50 bundesweiten Branchenorganisationen und 14 Landesvereinigungen organisiert.



WIRTSCHAFTSPRÜFERKAMMER

Körperschaft des
öffentlichen Rechts

WIRTSCHAFTSPRÜFERKAMMER · Postfach 30 18 82 · 10746 Berlin

Deutscher Bundestag
Innenausschuss
Herrn Ansgar Heveling
– Vorsitzender –
Platz der Republik 1
11011 Berlin

Vorab per E-Mail: innenausschuss@bundestag.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)814

Wirtschaftsprüferhaus
Rauchstraße 26
10787 Berlin
Telefon 0 30/72 61 61-0
Telefax 0 30/72 61 61-212
E-Mail kontakt@wpk.de

Rue des Deux Églises 35
1000 Bruxelles
E-Mail bruessel@wpk.de
www.wpk.de

16. März 2017
Dr. Ferdinand Goltz
Durchwahl: -145

GG 21/2016/867/904
- bitte stets angeben -

**Regierungsentwurf 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-Drs. 18/11325
Stellungnahme der Wirtschaftsprüferkammer**

Sehr geehrter Herr Vorsitzender,

anbei erhalten Sie die Stellungnahme der Wirtschaftsprüferkammer zu o. g. Gesetzentwurf (Anlage).

Wir bitten um Weiterleitung der Stellungnahme an die Mitglieder Ihres Ausschusses und würden uns freuen, wenn unsere Anregungen im weiteren Verfahren berücksichtigt werden.

Für Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

RA Peter Maxi

Dr. Ferdinand Goltz
Referent

Anlage



**Stellungnahme
der Wirtschaftsprüferkammer
zum Regierungsentwurf 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-Drs. 18/11325**

Berlin, den 15. März 2017
GG 21/2016

Ansprechpartner: Dr. Ferdinand Goltz
Wirtschaftsprüferkammer
Postfach 30 18 82, 10746 Berlin
Rauchstraße 26, 10787 Berlin
Telefon: 030 726161-145
Telefax: 030 726161-287
E-Mail: Berufsrecht@wpk.de

www.wpk.de

Geschäftsführer:	RA Peter Maxl	Telefon: 0 30 - 72 61 61-110	Telefax: 0 30 - 72 61 61-104	E-Mail: peter.maxl@wpk.de
	Dr. Reiner J. Veidt	Telefon: 0 30 - 72 61 61-100	Telefax: 0 30 - 72 61 61-107	E-Mail: reiner.veidt@wpk.de

Die Wirtschaftsprüferkammer (WPK) ist eine Körperschaft des öffentlichen Rechts, deren Mitglieder alle Wirtschaftsprüfer, vereidigten Buchprüfer, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften in Deutschland sind. Die WPK 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.

— — —

Wir beschränken unsere Stellungnahme auf Fragestellungen, die unsere Mitglieder betreffen. Von zentralem Interesse für den Berufsstand der Wirtschaftsprüfer/vereidigten Buchprüfer ist die Bewahrung der verschwiegenen Berufsausübung als Wesensmerkmal und Funktionsvoraussetzung der freiberuflichen Berufsausübung, die über ihre Verankerung im einfachen Gesetzesrecht (§ 43 Abs. 1 Satz 1 der Wirtschaftsprüferordnung [WPO]) hinaus auch verfassungsrechtlichen Schutz genießt (BVerfG 12.4.2015, NJW 2005, 1917).

Die Verordnung (EU) 2016/679 (im Folgenden: DS-GVO) enthält im Bereich der Betroffenenrechte (Kapitel 3 Abschnitt 2 bis 4) Vorschriften, die mit der beruflichen Verschwiegenheit unserer Mitglieder kollidieren. Die WPK fordert den Gesetzgeber – wie bereits mit ihrer Stellungnahme zum Referentenentwurf – auch mit der vorliegenden Stellungnahme zum Regierungsentwurf dazu auf, die insbesondere durch Art. 23 Abs. 1 Buchstabe g DS-GVO („Verhütung von Verstößen gegen berufsständische Regelungen reglementierter Berufe“) eröffneten Gestaltungsspielräume dergestalt zu nutzen, dass die Pflicht und damit auch das Recht zur Verschwiegenheit in ihrem derzeitigen Umfang erhalten bleiben.

— — —

Nach Artikel 1 des Gesetzentwurfs wird das Bundesdatenschutzgesetz (BDSG) komplett neu gefasst. In Teil 2 Kapitel 1 Abschnitt 2 (Besondere Verarbeitungssituationen) wird mit § 29 BDSG-E eine Vorschrift verortet, welche Regelungen zur Verarbeitung von Daten beinhaltet, die nach einer Rechtsvorschrift oder ihrem Wesen nach einer Geheimhaltungspflicht unterliegen. Auf Basis von Art. 23 Abs. 1 Buchstabe g und i DS-GVO statuiert Absatz 1 Ausnahmen zu Art. 14 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden), Art. 15 (Auskunftsrecht der betroffenen Person) sowie Art. 34 DS-GVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person). Die Ermächtigung in Art. 90 Abs. 1 DS-GVO aufgreifend, enthält Absatz 3 einschränkende Regelungen zu den Befugnissen der Aufsichtsbehörden gegenüber Berufsheimnisträgern.

- 1.) Nach **§ 29 Abs. 1 Satz 4 BDSG-E** ist abweichend von der Ausnahme nach Satz 3 die betroffene Person nach Art. 34 DS-GVO zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen. Wir weisen darauf hin, dass eine solche Abwägelösung im Bereich gegebenenfalls strafrechtlich relevanten Handelns unsere Mitglieder mit Risiken belastet. Auf der anderen Seite sehen wir auch, dass Art. 23 Abs. 1 DS-GVO lediglich verhältnismäßige Ausnahmebestimmungen der nationalen Gesetzgeber erlaubt. Vor diesem Hintergrund sprechen wir uns dafür aus, die Abwägung zumindest dadurch zu vereinfachen, dass die Interessen der betroffenen Person das Geheimhaltungsinteresse deutlich überwiegen müssen.
- 2.) **§ 29 Abs. 3 Satz 1 BDSG-E** sieht vor, dass die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Art. 58 Abs. 1 Buchstabe e und f DS-GVO nicht bestehen, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten der schweigepflichtigen Person führen würde. Diese Formulierung empfinden wir als unglücklich, da nach unserem Verständnis die Befugnisausübung durch eine Behörde nicht auf Seiten des Betroffenen zu einem Rechtsverstoß führen kann. Wir regen an, eine Formulierung zu verwenden, wonach die Untersuchungsbefugnisse der Aufsichtsbehörde gemäß Art. 58 Abs. 1 Buchstabe e und f DS-GVO nicht bestehen, soweit personenbezogene Daten der Geheimhaltungspflicht unterliegen.
- 3.) Deutlicher zum Ausdruck kommen sollte, dass **§ 29 Abs. 3 Satz 2 BDSG-E** (Geheimhaltungspflicht gilt auch für die Aufsichtsbehörde, wenn diese im Rahmen einer Untersuchung nach Satz 1 Kenntnis von personenbezogenen Daten erlangt, die dem Berufsgeheimnis unterliegen) keine Befugnis begründet, die Untersuchung auf Daten dieser Art zu erstrecken. Es empfiehlt sich die Klarstellung, dass die Regelung nur vorsorglichen bzw. Auffangcharakter hat, also für den Fall geschaffen wurde, dass die Behörde im Rahmen ihrer Untersuchung nach Satz 1 unbeabsichtigt Kenntnis von Daten erlangt, die dem Berufsgeheimnis unterliegen.
- 4.) Nicht nachvollziehen können wir, warum das in **§ 26 Abs. 2 Satz 2 BDSG-E** in der Fassung des Referentenentwurfs enthaltene Verwertungsverbot im Regierungsentwurf gestrichen wurde. Wir regen an, dieses in einen neuen **§ 29 Abs. 3 Satz 3 BDSG-E** aufzunehmen und auf das Verfahren zur Ahndung von Ordnungswidrigkeiten zu erstrecken.
- 5.) Weiteren Ergänzungsbedarf auf Ebene des nationalen Rechts sehen wir unverändert in Bezug auf die im Folgenden genannten, in Kapitel 3 Abschnitt 2 bis 4 DS-GVO geregelt-

ten Betroffenenrechte, die zum Teil mit der Pflicht zur Verschwiegenheit (§ 43 Abs. 1 WPO, § 10 BS WP/vBP), kollidieren. Durch die Regelungen in § 29 Abs. 1 BDSG-E werden zentrale Bereiche (Art. 14, 15 und 34 DS-GVO) zwar bereits von Ausnahmeregelungen im Sinne von Art. 23 Abs. 1 Buchstabe g DS-GVO erfasst. Da die Art. 13 ff. DS-GVO jedoch weiter differenzieren und auch in anderen, speziell geregelten Verarbeitungssituationen Informations- bzw. Auskunftsansprüche des Betroffenen normieren, verbleiben aus unserer Sicht Lücken im Vergleich zur der umfassenden Ausnahmeregelung in §§ 33 Abs. 2 Satz 1 Nr. 3, 34 Abs. 7 BDSG (alt), die es zu schließen gilt.

Im Einzelnen verbleibt aus unserer Sicht in den folgenden Fällen eine Kollision mit der Pflicht zur verschwiegenen Berufsausübung und daher die Notwendigkeit ergänzender, ebenfalls in § 29 BDSG-E zu verortender Ausnahmeregelungen:

a) Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DS-GVO)

Die Informationspflichten nach Artikel 13 Abs. 1 bis 3 DS-GVO können mit der Pflicht zur beruflichen Verschwiegenheit kollidieren, wenn personenbezogene Daten im Rahmen der Auftragsdurchführung im Auftrag des Mandanten bei einem Dritten erhoben werden, soweit der Dritte selbst betroffene Person ist. Zu einer Durchbrechung kann es in diesen Fällen insbesondere kommen, wenn dem Dritten, wie von Art. 13 Abs. 1 Buchstabe c bis e DS-GVO vorgesehen, die Zwecke der Datenverarbeitung, ggf. die berechtigten Interessen des Mandanten sowie die Personen, an die personenbezogene Daten übermittelt werden, umfassend mitgeteilt werden müssten.

§ 32 Abs. 1 Nr. 4 BDSG-E (keine Informationspflicht, wenn diese die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Informationen die Interessen der betroffenen Person überwiegen) reicht nicht aus, um die Informationspflicht mit Blick auf die Tätigkeitssituation speziell des WP/vBP hinreichend zu beschränken. Nicht erfasst wäre z. B. die Konstellation, in der der WP/vBP im Auftrag seines Mandanten (z. B. eines Kaufinteressenten) das Unternehmen eines Einzelkaufmanns (Dritter) analysiert oder bewertet und in diesem Rahmen Informationen zu den wirtschaftlichen Verhältnissen des Einzelkaufmanns unmittelbar bei diesem erhebt. Hier wäre der Dritte nicht Mandant, so dass die Schweigepflicht ihm gegenüber gelten würde, auch wenn die genannten Daten durch den WP/vBP unmittelbar bei ihm erhoben werden.

Die einschränkungslose Anwendung des Art. 13 DS-GVO würde dazu führen, dass der WP/vBP dem Dritten, dessen Daten erhoben wurden, die o. g. Informationen zum Mandatsverhältnis in allen Fällen erteilen muss, ohne dass der Mandant hierauf Einfluss nehmen kann. Dies würde aus unserer Sicht zu einer nicht hinnehmbaren Einschränkung des Vertrauensverhältnisses zwischen Berufsträger und Mandant führen.

b) Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 Satz 2 DS-GVO)

Die Unterrichtung Betroffener über die Identität von Personen, denen gegenüber personenbezogene Daten offengelegt wurden (Art. 19 Satz 2 DS-GVO), kollidiert ebenfalls mit der Pflicht zur verschwiegenen Berufsausübung, wenn im Rahmen der Auftragsdurchführung personenbezogene Daten Dritter, zu denen kein Mandatsverhältnis besteht, erhoben werden. Letzteres ist im Rahmen der Berufsausübung des WP/vBP häufig der Fall (vgl. das unter a) genannte Beispiel oder auch die Erhebung personenbezogener Daten von Mitarbeitern oder Kunden des Mandanten bei diesem).

Die Ausnahmeregelung in Art. 14 Abs. 5 DS-GVO zur Information des Betroffenen ist nach dem Wortlaut der Verordnung auf die Informationspflicht nach Art. 19 Satz 2 DS-GVO nicht anwendbar („Die Absätze 1 bis 4 [des Art. 14] finden keine Anwendung, wenn und soweit...“). Auch § 33 Abs. 1 Nr. 2a BDSG-E hilft schon deswegen nicht weiter, da die Vorschrift wiederum eine Ausnahme lediglich von der Informationspflicht nach Art. 14 DS-GVO normieren will.

c) Nachweis zwingender schutzwürdiger Gründe bei Widerspruch des Betroffenen gegen die Verarbeitung ihn betreffender personenbezogener Daten (Art. 21 Abs. 1 Satz 2 DS-GVO)

Auch soweit der von Art. 21 Abs. 1 Satz 2 DS-GVO geforderte Nachweis zwingender schutzwürdiger Gründe (als Voraussetzung für die weitere Verarbeitung) gegenüber dem der Datenverarbeitung widersprechenden Dritten erbracht wird, kann es zu einer Kollision mit der Verschwiegenheitspflicht kommen. Eine hinnehmbare Lösung wäre aus unserer Sicht, wenn der WP/vBP den Nachweis nicht gegenüber dem widersprechenden Dritten, sondern ausschließlich im berufsaufsichtlichen Verfahren zu führen hätte. Der Wortlaut des Art. 21 Abs. 1 Satz 2 DS-GVO ist insoweit offen.

Wir regen daher auch in diesem Bereich zumindest eine Klarstellung im o. g. Sinne an (Nachweis nicht gegenüber dem betroffenen Dritten, sondern ausschließlich im berufsaufsichtlichen Verfahren gegenüber der zuständigen Berufskammer).

Insgesamt – und um alle denkbaren Kollisionen rechtssicher aufzufangen – regen wir an, eine generalklauselartige Lösung, welche sämtliche Betroffenenrechte in Art. 13 ff. DS-GVO erfasst, in § 29 Abs. 1 BDSG-E aufzunehmen.

Wir hoffen, dass unsere Anregungen im Verlauf des weiteren Gesetzgebungsverfahrens Berücksichtigung finden.

— — —

An:

Deutscher Bundestag

-Innenausschuss

-Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung

-Ausschuss für Recht und Verbraucherschutz

-Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

-Ausschuss Digitale Agenda

Zur Kenntnisnahme:

Bundesministerium für Wirtschaft und Energie – Referat Freie Berufe

Bundesministerium der Justiz und für Verbraucherschutz

Bundesministerium der Finanzen

Bundesanstalt für Finanzdienstleistungsaufsicht

Deutsche Prüfstelle für Rechnungslegung e. V.

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)

GDW Bundesverband deutscher Wohnungs- und Immobilienunternehmen e. V.

Deutscher Steuerberaterverband e. V.

Deutscher Anwaltverein e. V.

Deutscher Notarverein e. V.

Bundesverband der Deutschen Industrie e. V.

Deutscher Industrie- und Handelskammertag e. V.

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Bundesverband Deutscher Banken e. V.

Bundesverband Öffentlicher Banken Deutschlands (VÖB) e. V.

European Federation of Accountants and Auditors for SMEs



Stellungnahme des

**ADM Arbeitskreis Deutscher Markt-
und Sozialforschungsinstitute e.V.**

zu dem

**Entwurf eines Gesetzes zur Anpassung des Da-
tenschutzrechts an die Verordnung (EU) 2016/679
und zur Umsetzung der Richtlinie (EU) 2016/680
(Datenschutz-Anpassungs- und
-Umsetzungsgesetz EU – DSAnpUG-EU)**

(Bundestags-Drucksache 18/11325)

**ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.
Langer Weg 18 60489 Frankfurt am Main
Telefon: 069 978431-36 Telefax: 069 978431-37
E-Mail: office@adm-ev.de Internet: www.adm-ev.de**

Der **ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.** vertritt die Interessen der privatwirtschaftlichen Markt- und Sozialforschungsinstitute in Deutschland. Er wurde im Jahr 1955 gegründet. Gegenwärtig (Stand: März 2017) gehören ihm 75 Institute an, die rund 84 Prozent des Umsatzes der deutschen Markt-, Meinungs- und Sozialforschung (2015: 2.512 Mio. €) erzielen. Zu den satzungsgemäßen Aufgaben des ADM gehören die Wahrung der Anonymität der Studienteilnehmer und die Abgrenzung der Marktforschung von anderen Tätigkeiten, die Durchsetzung der Berufsgrundsätze und Standesregeln sowie die Förderung der Wissenschaftlichkeit der Marktforschung.¹

A. Fokus der Stellungnahme

Die Stellungnahme des ADM 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)** (Bundestags-Drucksache 18/11325) ist auf § 27 BDSG-E fokussiert sowie allgemein auf das Kriterium 'unverhältnismäßiger Aufwand' als Erlaubnistatbestand. Diese gesetzlichen Vorschriften haben unmittelbare Auswirkungen auf die Durchführung von Studien der Markt-, Meinungs- und Sozialforschung.²

B. Empfehlungen

Der ADM hat dazu die folgenden Empfehlungen formuliert. Zuvor wird eine Darstellung der Zielsetzung und Arbeitsweise der Marktforschung gegeben.

¹ Ausführliche Informationen über den ADM sowie seine Aufgaben und Ziele sind auf der Webseite des Verbands www.adm-ev.de zu finden.

² Im Folgenden wird der Begriff „Marktforschung“ in seiner generischen Bedeutung verwendet, die Medien-, Meinungs-, Politik-, Sozial-, Wahlforschung und andere Bereiche einschließend.

Die Empfehlungen im Einzelnen:

1. Der ADM empfiehlt, in § 27 Absatz 1 Satz 1 BDSG-E das Wort ‚erheblich‘ zu streichen, da es zu einer unnötig restriktiven Anwendung des § 27 Absatz 1 führt und die Interessen der Betroffenen anderweitig geschützt werden.
2. Der ADM empfiehlt, im Gesetzentwurf allgemein das Kriterium des ‚unverhältnismäßigen Aufwands‘ als Erlaubnistatbestand zu erhalten und das Vorliegen desselben jeweils begründen zu müssen.
3. Der ADM empfiehlt, in § 27 Absatz 2 Satz 2 BDSG-E das Wort ‚begründet‘ einzufügen, um missbräuchlichen Bezug auf einen ‚unverhältnismäßigen Aufwand‘ zu verhindern und ihn als Erlaubnistatbestand für wissenschaftliche Forschungszwecke zu erhalten.

C. Zielsetzung und Arbeitsweise der Marktforschung

Die Marktforschung ist ausschließlich an generalisierbaren, validen und zuverlässigen Aussagen über das Verhalten und die Einstellungen von nach verschiedenen soziodemographischen und sozioökonomischen Merkmalen abgegrenzten Gruppen der Bevölkerung auf der Grundlage wissenschaftlicher Methoden und Techniken interessiert (**Wissenschaftlichkeitsgebot**). Aussagen über konkrete Einzelpersonen sind nicht Bestandteil der Marktforschung. Sie versucht auch nicht, die Meinungen und das Verhalten von Menschen zu beeinflussen. Die Marktforschung muss deshalb von anderen Tätigkeiten – insbesondere solchen der Werbung und Verkaufsförderung – getrennt durchgeführt werden (**Trennungsgebot**).

Für die jeweilige Zielgruppe einer Studie wird mittels mathematisch-statistischer Verfahren aus vorhandenen Quellen eine Stichprobe potenzieller Teilnehmer gezogen. Die solcherart ausgewählten Personen werden kontaktiert und um die

Teilnahme an der Studie gebeten. Dabei werden sie unter anderem über die Herkunft ihrer Kontaktdaten, den allgemeinen Zweck der Studie und die Freiwilligkeit der Teilnahme informiert. Die Erhebung der Forschungsdaten basiert dann auf der Rechtsgrundlage der Einwilligung der betroffenen Personen.

Nach der Datenerhebung werden die Forschungsdaten von den Kontaktdaten der Studienteilnehmer getrennt und beide mit einer gemeinsamen Kennziffer versehen, d.h. pseudonymisiert, um gegebenenfalls nicht korrekt erhobene Daten aus dem Forschungsdatensatz entfernen und unvollständige Daten – falls methodisch möglich – ergänzen zu können. Nach Abschluss dieser die Forschungsqualität sichernden Maßnahmen werden die Kontaktdaten der Teilnehmer gelöscht und die Forschungsdaten damit anonymisiert. Die Auswertung der erhobenen Daten mittels mathematisch-statistischer Analyseverfahren erfolgt ausschließlich auf der Grundlage der anonymisierten Forschungsdaten (**Anonymisierungsgebot**).

Das Wissenschaftlichkeitsgebot, das Anonymisierungsgebot und das Trennungsgebot sind als allgemein anerkannte berufsethische und berufsständische Grundprinzipien der Profession in der Annahmeerklärung der deutschen Verbände zu dem weltweit akzeptierten Verhaltenskodex der Markt- und Sozialforschung³ kodifiziert.

D. § 27 Absatz 1 BDSG-E „Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken“

Die in § 27 Absatz 1 BDSG-E normierte Ausnahmeregelung soll nur anwendbar sein, wenn die Datenverarbeitung erforderlich ist und die Interessen des Ver-

³ Vgl. dazu die Erklärung für das Gebiet der Bundesrepublik Deutschland zum ICC/ESOMAR Internationalen Kodex für die Markt- und Sozialforschung.

antwortlichen an der Datenverarbeitung diejenigen des Betroffenen erheblich überwiegen. Der ADM befürchtet, dass das Kriterium der Erheblichkeit zu einer unnötig restriktiven Anwendung des § 27 Absatz 1 BDSG-E führt. Die Interessen der Betroffenen werden bereits durch das Kriterium der Erforderlichkeit, das überwiegende Interesse sowie den Hinweis auf die Vorschriften des § 22 Absatz 2 Satz BDSG-E geschützt. Die Öffnungsklausel des Artikel 9 Absatz 2 Buchstabe j DSGVO-EU als Rechtsgrundlage des § 27 Absatz 1 BDSG-E verlangt zudem kein erhebliches Überwiegen der Interessen des Verantwortlichen gegenüber denen des Betroffenen. Der ADM empfiehlt deshalb, in § 27 Absatz 1 Satz 1 das Wort ‚erheblich‘ zu streichen:

„Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung **erheblich** überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.“

E. Generelle Beibehaltung und Begründung des ‚unverhältnismäßigen Aufwands‘ als Erlaubnistatbestand

Der ADM kann die anlässlich der ersten Beratung des von der Bundesregierung eingebrachten Entwurfs eines Datenschutz-Anpassungs- und -Umsetzungsgesetz EU im Deutschen Bundestag am 09. März 2017⁴ vorgebrachten Bedenken hinsichtlich der Missbrauchsmöglichkeiten des unbestimmten Rechtsbegriffs

⁴ Stenografischer Bericht der 221. Sitzung des Deutschen Bundestages in der 18. Legislaturperiode am 9. März 2017 (Plenarprotokoll 18/221)

„unverhältnismäßiger Aufwand“ als Ausnahmetatbestand nachvollziehen. Gleichwohl empfiehlt der ADM, im Gesetzentwurf allgemein das Kriterium des „unverhältnismäßigen Aufwands“ als Erlaubnistatbestand nicht zu streichen, sondern beizubehalten und das Vorliegen desselben jeweils begründen zu müssen.

F. § 27 Absatz 2 BDSG-E „Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken“

Die Verbände der Markt- und Sozialforschung in Deutschland haben in einer gemeinsamen Stellungnahme⁵ zu den in Artikel 89 der Datenschutz-Grundverordnung vorgesehenen Garantien und Ausnahmen für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken betont, dass im Unionsrecht oder im Recht der Mitgliedstaaten keine Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 DSGVO-EU erforderlich sind. Die in der Datenschutz-Grundverordnung normierten Rechte der betroffenen Personen bezüglich ihres Auskunftsrechts, ihres Rechts auf Berichtigung, ihres Rechts auf Einschränkung der Verarbeitung und ihres Widerspruchsrechts machen die Durchführung von wissenschaftlichen Studien der Marktforschung weder unmöglich noch beeinträchtigen sie deren Durchführung erheblich. Gleichwohl begrüßt der ADM im Interesse der Durchführung empirischer Forschung grundsätzlich die Normierung in § 27 Absatz 2 BDSG-E der Ausnahmen von den oben genannten Rechten:

„Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder

⁵ Gemeinsame Stellungnahme der Verbände der Markt- und Sozialforschung in Deutschland zu den in Artikel 89 der Datenschutz-Grundverordnung vorgesehenen Garantien und Ausnahmen vom 13. Mai 2016.

Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung **begründet** einen unverhältnismäßigen Aufwand erfordern würde.“

Die Empfehlung, in § 27 Absatz 2 Satz 2 BDSG-E – wie oben geschehen – das Wort ‚begründet‘ einzufügen, wurde im vorangegangenen Abschnitt E erläutert.

Frankfurt am Main, den 16. März 2017

Stellungnahme

zum Entwurf der Bundesregierung für ein

**„Gesetz zur Anpassung des
Datenschutzrechts an die Verordnung (EU)
2016/679 und zur Umsetzung der Richtlinie
(EU) 2016/680“**

[Stand: 01.02.2017]

Bundestag-Drucksache: 18/11325

Der vfa ist der Wirtschaftsverband der forschenden Pharma-Unternehmen in Deutschland. Er vertritt die Interessen von 44 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 76.000 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 *Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU)* Stellung zu nehmen.

vfa-Position

Das DSAnpUG-EU soll insbesondere der Implementierung der Datenschutzgrundverordnung (EU) 2016/69 (DSGVO) vom 04.05.2016 dienen, die ab dem 25.05.2018 unmittelbar geltendes Recht sein wird. Da die DSGVO mit Ihrem Ansatz der Harmonisierung und Schaffung eines einheitlichen Datenschutzniveaus einen Meilenstein des europäischen Datenschutzrechts darstellt, begrüßt der vfa, dass die Bundesregierung einen Gesetzentwurf zu deren Implementierung in Deutschland vorgelegt hat, was erwarten lässt, dass das parlamentarische Gesetzgebungsverfahren noch in dieser Legislatur zum Abschluss gelangen kann. Das würde in zeitlicher Hinsicht Planungssicherheit für Unternehmen wie auch für die zuständigen Behörden schaffen, wenn ab Mai 2018 die DSGVO in Deutschland umfassend Anwendung finden wird.

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 zum einen für die Herausforderungen der Zukunft, insbesondere im Hinblick auf die digitale Transformation des Gesundheitswesens und den Ausbau der sogenannten Personalisierten Medizin unter Einbeziehung u.a. genetischer Biomarker. Hier bedarf es unserer Einschätzung nach weiterführender 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. Den insoweit erforderlichen gesetzlichen Anpassungen sollte eine öffentliche Debatte mit dem Ziel einer klaren ethischen Grundlage mit gesellschaftlicher Akzeptanz vorausgehen, in die sich der vfa gerne einbringen wird.

Zum anderen ist für forschende Pharmaunternehmen mit Blick auf die jetzt anstehenden Implementierungsschritte der DSGVO wichtig, dass das nationale Regelungssystem – in diesem Fall das neue Bundesdatenschutzgesetz (BDSG-neu) – neben der DSGVO für den Bereich der Forschungs- und Gesundheitsdatenverarbeitung eine praktikable und rechtssichere Grundlage für alle Beteiligten bietet. Dass das BDSG-neu im Zusammenspiel mit der DSGVO im Bereich der Forschungsdatenverarbeitung die Möglichkeiten der Öffnungsklauseln der DSGVO nutzend eine entsprechende Rechtsgrundlage explizit schaffen wird, die im Wesentlichen mit dem geltenden Recht vergleichbare Regelungen vorsieht, ist insoweit zu begrüßen.

Die vorgeschlagenen Regelungen des BDSG-neu sind mehrheitlich sachgerecht und daher zu begrüßen. Dennoch erkennt der vfa Änderungsbedarf in § 22 Abs.1 BDSG-neu aus Klarstellungsgründen sowie in § 27 BDSG-neu im Hinblick auf die dortige Interessenabwägung und auf das dort getroffene Rangverhältnis von Anonymisierung und Pseudonymisierung.

Im Einzelnen:

I. Art.1 DSAnpUG-EU: § 22 Abs. 1 Nr. 1 lit. c BDSG-neu

Der Regierungsentwurf sieht in § 22 Abs. 1 Nr. 1 lit. c BDSG-neu vor, dass die Verarbeitung besonderer Kategorien personenbezogener Daten für öffentliche und nicht-öffentliche Stellen, wenn sie aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Arzneimitteln erforderlich ist, zulässig ist. Der vfa begrüßt die Einführung einer solchen Regelung in das BDSG-neu.

Durch bereits bestehende spezifische arzneimittelrechtliche Vorgaben sind pharmazeutische Unternehmer dazu verpflichtet, ihre im Markt befindlichen Produkte genau zu überwachen und im Falle des Auftretens von Nebenwirkungen diese zu dokumentieren sowie die entsprechenden Meldungen an die zuständigen Bundesoberbehörden weiterzuleiten (**Pharmakovigilanz**). In Abhängigkeit von Anzahl und

Schwere der Nebenwirkungen werden in einem differenzierten Ablauf erforderliche Schritte durch betroffene Hersteller und die zuständigen Behörden zur Gewähr eines hohen Niveaus von Arzneimittelsicherheit eingeleitet und fortgeführt. Grundlage dieser Nebenwirkungsmeldungen sind personenbezogene Daten der betroffenen Patienten und der meldenden Personen (Ärzte, Apotheker, Patienten). Auf Grundlage des noch geltenden Datenschutzrechts kann häufig allein über eine Einwilligungserklärung der betroffenen Personen die Verarbeitung datenschutzrechtskonform durchgeführt werden. Die Einholung einer datenschutzrechtlichen Einwilligungserklärung ist in einer Vielzahl von Fällen der Erhebung von Nebenwirkungsfällen praxisfern, da in diesen Momenten das Patientenwohl und die Arzneimittelsicherheit in erster Linie im Fokus stehen müssen. Zudem ist für die Gewähr einer qualitativ hohen Arzneimittelsicherheit und zur Vermeidung von Mehrfachmeldungen ein und desselben Nebenwirkungsfalles die Erhebung einer nach internationalen Standards festgelegten Anzahl von personenbezogenen Daten einer Person notwendig, was als Widerspruch zum Grundsatz der Datensparsamkeit aufgefasst werden könnte. Dies führt in der Praxis häufig zu Rechtsunsicherheiten und erhöhtem Erklärungsaufwand gegenüber Datenschutzaufsichtsbehörden.

Mit § 22 Abs. 1 Nr. 1 lit. c BDSG-neu als datenschutzrechtliche Ermächtigungsgrundlage für die Verarbeitung von persönlichen Daten in Pharmakovigilanz-Prozessen wird eine erhöhte Rechtssicherheit für pharmazeutische Unternehmen und die Bundesoberbehörden (Bundesinstitut für Arzneimittel und Medizinprodukte sowie Paul-Ehrlich-Institut) geschaffen, die es ermöglicht, die aus Arzneimittelsicherheitsaspekten zwingend notwendigen Nebenwirkungsmeldungen datenschutzrechtskonform durchzuführen. Für den vfa wäre es im Sinne höherer Rechtssicherheit zielführend, wenn in § 22 Abs. 1 Nr. 1 lit. c BDSG-neu klargestellt werden würde, dass damit die Datenverarbeitung in Pharmakovigilanzprozessen nach §§ 62 ff. Arzneimittelgesetz gemeint sei und somit der unbestimmte Rechtsbegriff „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Arzneimitteln“ näher ausgefüllt werden würde.

§ 22 Abs. 1 Nr. 1 lit. c BDSG-neu sollte vor diesem Hintergrund wie folgt gefasst werden:

*c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln **nach §§ 62 – 63j***

Arzneimittelgesetz und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,

Seite 5/8

II. Art.1 DSAnpUG-EU: § 27 BDSG-neu

Der Regierungsentwurf sieht in § 27 BDSG-neu vor, dass abweichend von Art. 9 Abs. 1 DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten für wissenschaftliche Forschungszwecke zulässig sei, wenn die Verarbeitung zur Durchführung wissenschaftlicher Forschung erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der vfa begrüßt, dass Deutschland von der Ermächtigung aus Art. 9 Abs.2 lit. j DSGVO Gebrauch machen will und für die Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen Forschungszwecken eine Rechtsgrundlage zur Verfügung stellt. Dies unterstützt dem Grunde nach den Ansatz zur Verbesserung der Rahmenbedingungen für klinische Forschung in Deutschland und kann zum Erhalt Deutschlands als einem der weltweit führenden Standorte für klinische Forschung beitragen. Die Ergänzung des § 27 Abs.1 BDSG-neu in der Fassung des Regierungsentwurfes um eine Interessenabwägung geht aus Sicht des vfa gegenüber dem Referentenentwurf vom 23. November 2016 (dort § 25 Abs.1) über die Vorgaben des Art. 9 Abs.2 lit. j DSGVO hinaus und erscheint nicht sachgerecht. Ausgehend von diesem Hintergrund möchten wir noch auf folgende Anmerkungen hinweisen und um Beachtung der nachstehenden Änderungsvorschläge bitten:

- § 27 BDSG-neu verlangt für die Datenverarbeitung ohne Einwilligung zu wissenschaftlichen Forschungszwecken eine spezifische Erforderlichkeitsprüfung und eine **Interessenabwägung**, bei der die Forschungsinteressen erheblich überwiegen müssen. Daneben hat der Verantwortliche angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gem. § 22 Abs.2 S.2 BDSG-neu vorzusehen.

Als Ermächtigung für die Einführung von § 27 BDSG-neu wird Art. 9 Abs.2 lit. j (i.V.m. Art. 89 DSGVO) benannt, der jedoch keine Interessenabwägung, wie in § 27 Abs.1 BDSG-neu eingefügt, vorgibt. Unserer Auffassung nach würde der deutsche Gesetzgeber damit die Vorgaben der DSGVO überschreiten und ein „Zuviel“ der Datenverarbeitung zu wissenschaftlichen Forschungszwecken auferlegen. Durch die angemessenen und spezifischen Maßnahmen, die der jeweils Verantwortliche zur Wahrung

der Interessen der betroffenen Person gem. §§ 27 Abs.1 S.2, 22 Abs.2 S.2 BDSG-neu vorzusehen hat, ist unserer Auffassung mittels dieses risikobasierten Ansatzes bereits ein derart hoher Standard erreicht, dass eine Interessenabwägung nicht mehr erforderlich ist. Schließlich legt Art. 6 Abs.1 DSGVO, der bei einer Datenverarbeitung nach § 27 Abs.1 BDSG-neu auch immer erfüllt sein muss, nur für eine seiner Tatbestandsalternativen fest, dass eine Interessenabwägung vorzunehmen ist (und bei dieser Alternative nach Art. 6 Abs.1 lit. f DSGVO genügt bereits das einfache Überwiegen im Vergleich zum erheblichen Überwiegen des § 27 Abs.1 BDSG-neu). Vor diesem Hintergrund schlägt der vfa die Streichung der Interessenabwägung aus § 27 Abs.1 BDSG-neu vor, der dann wie folgt lauten würde:

(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist ~~und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen~~. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

- Der vfa erachtet insbesondere die Klarstellung in der Gesetzesbegründung zu § 27 BDSG-neu, wonach von der in § 27 BDSG-neu geregelten Verarbeitung zugleich die **Weiterverarbeitung** umfasst sei, als zweckdienlich. Denn in vielen Forschungsprojekten der pharmazeutischen Industrie, die unter Umständen sogar von den Arzneimittelzulassungsbehörden – zunehmend insbesondere auch nach erfolgter Zulassung – angefordert werden können, kann es notwendig werden, dass bereits erhobene Gesundheitsdaten zu einem wissenschaftlichen Forschungszweck verarbeitet werden sollen, der von dem ursprünglichen Zweck der Verarbeitung nicht umfasst war. Die Neuregelung ermöglicht derartige Weiterverarbeitungen zu wissenschaftlichen Forschungszwecken im Rahmen der sonstigen datenschutzrechtlichen Anforderungen und schafft Rechtssicherheit in diesem Bereich. Das spart Kosten und verhindert unnötige Doppeluntersuchungen bzw. das aufwendige nachträgliche Einholen von Einwilligungserklärungen.
- Der DSGVO ist zu entnehmen, dass von den Regelungen zur Datenverarbeitung zu wissenschaftlichen Forschungszwecken (Art. 9

i.V.m. mit Art. 89 DSGVO) auch die **privat finanzierte Forschung** umfasst ist. Bereits Erwägungsgrund 159 der DSGVO führt an: *„Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen.“* Der vfa begrüßt und hält es zur Erhöhung der Rechtssicherheit in dieser Frage für zielführend, dass die Gesetzesbegründung zu § 27 BDSG-neu im Regierungsentwurf gleich im ersten Satz klarstellt, dass diese Regelung *„für die öffentliche und private Forschung durch öffentliche und nicht-öffentliche Stellen gilt“*.

- **Pseudonymisierung** ist in der DSGVO legal-definiert als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Voraussetzung ist, dass diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Das Pseudonymisieren ist zudem in der EU-DSGVO als eine primär anzuwendende Technik in der Verarbeitung von Daten zu wissenschaftlichen Forschungszwecken hervorgehoben worden (vgl. Art. 89 Abs.1 DSGVO). Weiterhin ist das Pseudonymisieren seit vielen Jahren in der Praxis ein umfassend etabliertes Standardinstrument im Umgang mit Forschungs- und Gesundheitsdaten.

Dies vorausgeschickt, spricht sich der vfa für folgende Änderung des § 27 Abs. 3 BDSG-neu aus. § 27 Abs. 3 S. 1 und 2 BDSG-neu i.V.m. Art. 9 Abs.1 der DSGVO werten die Pseudonymisierung im Forschungsbereich als gegenüber der Anonymisierung nachrangiges Instrument der Verarbeitung von genetischen oder Gesundheitsdaten. Das sollte aus Sicht des vfa in mehrfacher Hinsicht überdacht werden. Es widerspricht dem aus der DSGVO abgeleiteten Prinzip der Pseudonymisierung als primär anzuwendenden Instrument in der Verarbeitung von Forschungsdaten, wenn nunmehr die Anonymisierung hierfür per Gesetz als primäres Instrument eingestuft wird. Daneben darf nicht vergessen werden, dass ernsthafte wissenschaftliche Zweifel bestehen, ob genetische Daten (auf die sich § 27 Abs. 3 BDSG-neu i.V.m. Art. 9 Abs.1 der DSGVO ausdrücklich bezieht) überhaupt in technischer Hinsicht vollständig anonymisiert werden können. Zudem ist die Pseudo-

nymisierung („Key-Coding“) von erhobenen Daten, die Speicherung der Daten in dieser Form sowie das Aufbewahren der Identifizierungsliste in der klinischen Forschung gesetzlich vorgegeben (vgl. u.a. § 40 Abs. 2a Arzneimittelgesetz), mithin dürfen diese Daten nicht anonymisiert werden; nicht zuletzt deshalb, weil im Falle von unerwarteten Ereignissen mit dem Prüfpräparat der behandelnde Arzt über die rechtlich vorgeschriebene Zeitdauer (10 Jahre nach Beendigung/ Abbruch einer klinischen Studie) in der Lage sein muss, Patienten zu identifizieren und ggfs. zu informieren, für den Fall, dass sie in der klinischen Studie mit dem betreffenden Wirkstoff behandelt wurden. Dies führt zu folgendem Regelungsvorschlag für § 27 Abs. 3 BDSG-neu:

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind bei zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeiteten besonderen Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 ~~zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern~~, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können, gesondert zu speichern (Pseudonymisierung). Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(Stand: 06. März 2017)



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

Berlin, 21.03.2017

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

A. Vorbemerkungen

Mit dem am 01.02.2017 bekannt gewordenen Entwurf für ein „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ (nachfolgend: DSAnpUG-EU) beabsichtigt die Bundesregierung eine Anpassung des Datenschutzrechts an die europäische Rechtsentwicklung auf Bundesebene sowie die Umsetzung der dem nationalen Gesetzgeber in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – nachfolgend: DSGVO) eingeräumten Regelungsmöglichkeiten infolge zahlreicher Ausgestaltungs-, Konkretisierungs- und Ergänzungsklauseln sowie übertragener Regelungsaufträge und -optionen für Ausnahmen.

Zugleich erfolgt 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).

Durch das DSAnpUG-EU wird das bisher geltende Bundesdatenschutzgesetz (BDSG) durch ein neues BDSG abgelöst, das zum 25.05.2018 in Kraft treten soll (Art. 8 Abs. 1 DSAnpUG-EU). Das Vorhaben zieht eine grundlegende Änderung des Datenschutzrechts nach sich. Weiterer gesetzlicher Anpassungsbedarf ergibt sich hinsichtlich der bereichsspezifischen Datenschutzregelungen des Bundes. Diese Anpassung soll jedoch in einem gesonderten Gesetzesvorhaben umgesetzt werden (Begründung zum RegE, S. 67).

Die vorliegende Stellungnahme bezieht sich auf Art. 1 DSAnpUG-EU (nachfolgend: BDSG-E) Teil 1 und Teil 2. Sie würdigt vornehmlich Aspekte, die für die Datenverarbeitung im Gesundheitswesen relevant sind. Die Angaben in dieser Stellungnahme beziehen sich auf den am 01.02.2017 bekannt gewordenen Entwurf der Bundesregierung.

B. Grundlegende Bewertung

Die Bundesärztekammer begrüßt, dass sich der Bundesgesetzgeber dem schwierigen Vorhaben annimmt, den Regelungsaufträgen aus der Datenschutzgrundverordnung nachzukommen und insbesondere Regelungen für die Verarbeitung besonderer Kategorien personenbezogener Daten zu schaffen. Dazu gehört der Bereich der Verarbeitung von Gesundheitsdaten, der aufgrund einer hohen Sensibilität dabei betroffener Daten besonderer Würdigung bedarf. Vor diesem Hintergrund bezieht sich die vorliegende Stellungnahme auf folgende, wesentliche Aspekte:

1. Ein wichtiges Anliegen sollte eine Vereinfachung des vielschichtigen Gesundheitsdatenschutzrechts sein. Mit dem BDSG-E steigt aus Sicht der Anwender und Normadressaten jedoch dessen Komplexität weiter an. Neben der ab dem 25.05.2018 direkt wirkenden DSGVO muss künftig das neue BDSG beachtet werden. Um alle relevanten Rechtsgrundlagen zu erfassen, muss der Rechtsanwender beide Gesetze heranziehen und abgleichen. Außer für ausgewiesene Datenschutzexperten wird eine „**Verständlichkeit und Übersichtlichkeit**“ für den Rechtsanwender, entgegen der Intention des Gesetzgebers (Begründung zum RegE, S. 73), nicht erreicht.

2. Dass eine größere **Akzeptanz und die Durchführbarkeit datenschutzrechtlicher Bestimmungen** erreicht werden, ist zweifelhaft, denn die einschlägigen Voraussetzungen und Bestimmungen lassen sich nur schwer erschließen. Das gilt insbesondere, da neben der DSGVO und dem BDSG-E auch die diversen bereichsspezifischen Datenschutzregelungen in den Fachgesetzen des Gesundheitswesens zu beachten sind. Diese werden wegen der in der DSGVO enthaltenen „Öffnungsklauseln“ voraussichtlich weiterhin Bestand haben. Aufgrund der zahlreichen Verweise aus der DSGVO auf die nationalen Rechtsgrundlagen und infolge der damit erforderlichen Ausgestaltung des Gesundheitsdatenschutzrechts im nationalen Recht ist das Gesundheitsdatenschutzrecht überaus komplex. Ein widerspruchsfreies Regelungswerk, das vorzugsweise die wesentlichen Grundsätze für die Datenverarbeitung im Gesundheitswesen enthält und nur im Hinblick auf die spezifischen Anforderungen auf entsprechende Fachgesetze verweist, wird damit nicht kodifiziert. Soweit möglich, sollte der Gesetzgeber aber **erwägen ein konsistentes Gesundheitsdatenschutzgesetz zu schaffen**.
3. Die unübersichtliche Rechtslage erzeugt **Rechtsunsicherheit**. Das ist vor allem mit Blick auf die möglichen **gravierenden Sanktionen**, die auch niedergelassene Ärzte und Krankenhäuser treffen können, problematisch: Bei Verstößen gegen die neuen Datenschutzbestimmungen werden Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 4 bis 6 DSGVO). Zudem sind die Straf- und Bußgeldvorschriften der §§ 42 f. BDSG-E zu beachten, die Freiheitsstrafe bis zu drei Jahren, Geldstrafen und Geldbußen bis 50.000 Euro vorsehen.
4. Überdies sind die sehr weitgefassten Vorschriften, insbesondere zur Verarbeitung besonderer Kategorien personenbezogener Daten, mit **generalklauselartigen Auffangbestimmungen** nicht geeignet, die Verarbeitung von Gesundheitsdaten auf eine sichere und klare Rechtsgrundlage zu stellen. Das ist nicht zuletzt darauf zurückzuführen, dass der Gesetzgeber den Normtext der Bestimmungen wiederholt, die ihm gerade einen Regelungs-, Ausgestaltungs- und Konkretisierungsauftrag übertragen. Auf diese Weise geschaffene unbestimmte Tatbestandsmerkmale (s. z. B. § 22 Abs. 1 Nr. 1 lit. c und Nr. 2 BDSG-E) und unnötige Auffangtatbestände ohne hinreichend bestimmten Verwendungszweck (s. z. B. § 22 Abs. 1 Nr. 1 lit. a BDSG-E) tragen ebenfalls zur Rechtsunsicherheit bei und können Konflikte im Arzt-Patienten-Verhältnis erzeugen (s. dazu unter II., 1., b., (2.) und (3)).
5. Zudem bedarf es einer sorgfältigen Abstimmung des BDSG-E mit den **Anforderungen für Berufsgeheimnisträger**. Die DSGVO und das BDSG-E betreffen in besonderem Maße auch Angehörige der Heilberufe, zu deren beruflichen Alltag der Zugang zu sensiblen Gesundheitsinformationen gehört. Diese Personen unterliegen daher besonderer Bestimmungen zu Wahrung der in diesem Zusammenhang anvertrauten Geheimnisse.
6. Das BDSG-E ist an einigen Stellen mit anderen Rechtskreisen, wie dem Recht zum Schutz von Berufsgeheimnissen, noch nicht hinreichend abgestimmt: Die parallele **Gesetzgebung zu § 203 StGB** soll eine Erweiterung des Kreises geheimnisverpflichteter Personen um die sog. „mitwirkenden Personen“ zur Folge haben (§ 203 Abs. 4 StGB-E). Das führt z. B. zu möglicherweise vom Gesetzgeber nicht beabsichtigten Privilegierungen dieser Personengruppen im Hinblick auf die Einhaltung technisch-organisatorischer Maßnahmen für den Datenschutz (s. § 22 Abs. 2 S. 3 BDSG, s. dazu unter II., 1., b., (4)). Wegen der Implikationen aus dem Gesetzgebungsverfahren zu § 203 StGB sollte jedenfalls eine Abstimmung der

Voraussetzungen des Datenschutzes mit den Anforderungen des Geheimnisschutzrechts in dem BDSG-E erfolgen.

7. Die Zugriffsmöglichkeiten auf Patientengeheimnisse durch Stellen und Personen, die nicht zu dem Kreis der in das besondere Vertrauensverhältnis einbezogenen Personen gehören, sollte auf ein notwendiges Maß beschränkt werden. Daher sollte bei der Ausgestaltung der Befugnisse von **Aufsichtsbehörden** i. S. d. Art. 90 DSGVO die **Pflicht zur Geheimhaltung** in einem angemessenen Verhältnis zum Recht auf Schutz der personenbezogenen Daten stehen. Auch hier sollte wegen der Wechselwirkungen mit dem Gesetzgebungsverfahren zu § 203 StGB jedenfalls eine Abstimmung mit dem vorliegenden Gesetzgebungsverfahren erfolgen (s. dazu näher unter III.)
8. Den **besonderen beruflichen Pflichten** (insbesondere Dokumentations- und Aufbewahrungspflichten) sollte bei der Ausgestaltung des Datenschutzrechts in angemessener Weise Rechnung getragen werden.
9. Die Ausgestaltung von **Einschränkungen der Betroffenenrechte** aufgrund der in der DSGVO eingeräumten Regelungsmöglichkeiten für Ausnahmen sollte nicht zu Konfliktsituationen im Arzt-Patienten-Verhältnis führen. Durch eine unklare Rechtslage und Auslegungsschwierigkeiten könnte das Vertrauensverhältnis zwischen Arzt und Patient beeinträchtigt werden. Insofern sollten Einschränkungen des Patientenrechts auf Auskunft aus der ärztlich geführten Dokumentation in Einklang mit § 630g BGB stehen. Das Recht auf Datenlöschung sollte in einem angemessenen Verhältnis zu berufsrechtlich vorgeschriebenen Dokumentations- und Aufbewahrungspflichten stehen.

C. Stellungnahme im Einzelnen

I. Anwendungsbereich und Grundsystematik

1. *Verhältnis zu den Berufsgeheimnissen (hier insb. der ärztlichen Schweigepflicht), zu § 1 Abs. 2 S. 3 BDSG-E*

a. Beabsichtigte Neuregelung

§ 1 BDSG-E regelt den Anwendungsbereich des BDSG-E. Dabei wird in § 1 Abs. 2 S. 3 BDSG-E gegenüber dem Referentenentwurf nunmehr zusätzlich normiert, dass die „*Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, [...] unberührt*“ bleibt. Dies entspricht der bisherigen Regelung des § 1 Abs. 3 S. 2 BDSG (vgl. Begründung zum RegE, S. 78).

b. Stellungnahme der Bundesärztekammer

Die Aufnahme der Regelung („Unberührtklausel“) in den Regierungsentwurf entsprechend der Anregung der Kassenärztlichen Bundesvereinigung und der Bundesärztekammer ist sachgemäß und rechtlich geboten, weil dadurch das Verhältnis zu den Vorschriften des besonderen Geheimnisschutzrechts, insbesondere der ärztlichen Schweigepflicht aufgrund

des Strafgesetzbuches und des ärztlichen Berufsrechts (§ 203 StGB, vgl. § 9 MBO-Ä¹), klargestellt und einer Relativierung des besonderen Berufsgeheimnisschutzes vorgebeugt wird. Die Regelung sorgt entsprechend des bisherigen § 1 Abs. 3 S. 2 BDSG für die notwendige Differenzierung der beiden, als eigenständig zu betrachtenden, Regelungsebenen (vgl. i.Ü. Stellungnahme der BÄK zum RefE vom 9.12.2016,² S. 3 f.).

2. Rein deklaratorische Regelung zum Anwendungsvorrang des Unionsrechts, zu § 1 Abs. 5 BDSG-E

a. Beabsichtigte Neuregelung

Mit § 1 Abs. 5 BDSG-E soll klargestellt werden, dass die Vorschriften des BDSG keine Anwendung finden, wenn das Recht der Europäischen Union, im Besonderen der DSGVO, Anwendung finden. In der Begründung zum Regierungsentwurf wird zudem darauf hingewiesen, dass „die unmittelbare Geltung der Verordnung (EU) 2016/679 unberührt“ bleibe (Begründung zum RegE, S. 78).

b. Stellungnahme der Bundesärztekammer

Bei der Regelung des § 1 Abs. 5 BDSG-E handelt es sich zwar nicht um eine Normwiederholung. Die allenfalls deklaratorische Regelung verweist aber auf den selbstverständlichen Anwendungsvorrang des Unionsrechts und ist aus den bereits der Stellungnahme zum Referentenentwurf genannten Gründen entbehrlich (s. Stellungnahme der BÄK zum RefE vom 9.12.2016, S. 4 f.). Im Normtext („*finden keine Anwendung, soweit [die DSGVO] unmittelbar gilt*“) und in der Begründung werden zudem die Kategorien des Anwendungs- und Geltungsvorrangs vermengt, woraus Auslegungsschwierigkeiten resultieren könnten. Die Regelung erscheint widersprüchlich und erzeugt Rechtsunsicherheit über die Frage, welches Recht „gilt“.

c. Änderungsvorschlag der Bundesärztekammer

Streichung von § 1 Abs. 5 BDSG-E.

3. Begriffsbestimmungen, zu § 2 BDSG-E

Positiv bewertet wird die gegenüber dem Referentenentwurf vorgenommene Änderung in § 2 BDSG-E. Die Vorschrift enthält nicht mehr Begriffsbestimmungen, die auch in Art. 4 DSGVO vorzufinden sind. Entsprechend der Anregung der Bundesärztekammer wurden die für die JI-Richtlinie einschlägigen Begriffsbestimmungen im Teil 3 aufgeführt (§ 46 BDSG-E). Diese Systematik schafft mehr Verständlichkeit für den Rechtsanwender, der im

¹ Die (Muster-)Berufsordnung ist nicht geltendes Recht. Rechtswirkung entfaltet die Berufsordnung, wenn sie durch die Kammerversammlungen der Ärztekammern als Satzung beschlossen und von den Aufsichtsbehörden genehmigt wurde.

² Stellungnahme der Bundesärztekammer vom 09.12.2016 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, abrufbar unter: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Stellungnahmen/Datenschutz-Anpassung.pdf.

Anwendungsbereich der DSGVO nur noch die Begriffsbestimmungen in Art. 4 DSGVO heranziehen muss.

II. Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten und deren Verarbeitung im Bereich der Forschung

1. Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten, zu § 22 BDSG-E

a. Beabsichtigte Neuregelung

Mit § 22 BDSG-E sollen Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten für den öffentlichen (Abs. 1 Nr. 1 u. 2) und nicht-öffentlichen Bereich (Abs. 1 Nr. 1) geschaffen werden. Diese Rechtsgrundlagen stellen Ausnahmen zum grundsätzlichen Verarbeitungsverbot gemäß Art. 9 Abs. 1 DSGVO dar und sind auf Art. 9 Abs. 2 DSGVO zurückzuführen (im Einzelnen s. RegE, S. 96 f.).

§ 22 Abs. 1 Nr. 1 lit. a BDSG-E regelt die Verarbeitung von u. a. Gesundheitsdaten im Bereich der sozialen Sicherheit und des Sozialschutzes. § 22 Abs. 1 Nr. 1 lit. b BDSG-E stellt die Rechtsgrundlage für die Verarbeitung dieser Daten, u. a. zum Zweck der Gesundheitsvorsorge und für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich, dar. § 22 Abs. 1 Nr. 1 lit. c BDSG-E betrifft den Bereich der öffentlichen Gesundheit.

§ 22 Abs. 1 Nr. 2 BDSG-E regelt die Verarbeitung von u. a. Gesundheitsdaten, die aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Ferner ist eine Verarbeitung nach § 22 Abs. 1 Nr. 2 BDSG-E z. B. zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit (lit. b) oder aus Gründen der Verteidigung (lit. d) zulässig, wenn sie erforderlich ist und die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen. Eine Verarbeitung aus diesen Gründen erfolgt nur durch öffentliche Stellen.

Gemäß § 22 Abs. 2 BDSG-E sind zudem angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorzusehen. Insbesondere „können“ die unter den Nr. 1 bis 10 aufgeführten Maßnahmen getroffen werden, sofern u. a. der Stand der Technik und die Implementierungskosten berücksichtigt wurden. Ausweislich der Begründung zum Regierungsentwurf, treffen die aufgeführten Maßnahmen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet. Dies gilt gemäß § 22 Abs. 2 S. 3 BDSG-E nicht für eine Verarbeitung nach § 22 Abs. 1 Nr. 1 lit. b BDSG-E (s. a. Begründung zum RegE, S. 97).

b. Stellungnahme der Bundesärztekammer

(1) Allgemeine Anmerkung

Grundsätzlich wird begrüßt, dass der nationale Gesetzgeber von den ihm in der DSGVO eingeräumten Möglichkeiten Gebrauch machen will, Rechtsgrundlagen für die Verarbeitung von „besonderen Kategorien personenbezogener Daten“ (hier: insb. Gesundheitsdaten) zu schaffen. Der Bundesärztekammer ist bewusst, dass der Gesetzgeber dabei vor großen Herausforderungen steht, um ein konsistentes System von Regelungen zu schaffen. Wegen des Rechtscharakters der europäischen Verordnung (Art. 288 UAbs. 2 AEUV), des Anwendungsvorrangs des Unionsrechts, das sich auch in dem „komplexen Mehrebenensystem“ des Datenschutzes auswirkt, gelangen einige Rechtsgrundlagen des

Art. 9 Abs. 2 DSGVO direkt zur Anwendung (Art. 9 Abs. 2 lit. c, e und f DSGVO), andere bedürfen hingegen der Ausgestaltung durch den nationalen Gesetzgeber (Art. 9 Abs. 2 lit. b und g bis j DSGVO). Weiterhin führt schon der Umstand, dass Regelungen für den Gesundheitsdatenschutz einerseits aus der DSGVO und andererseits aus dem BDSG-E zu entnehmen sind, zu einer **unübersichtlichen Regelungslage**. In das System des ohnehin schon überkomplexen Datenschutzes wird insofern mit dem BDSG-E als zusätzlichem „Auffanggesetz“ (Begründung zum RegE, S. 77; § 1 Abs. 2 S. 1 u. 2 BDSG-E) eine weitere Regelungsebene eingefügt. Die damit bewirkte „zersplitterte Rechtslage“ erzeugt erhebliche Rechtsunsicherheit. Um alle relevanten Rechtsgrundlagen zu erfassen, muss der Rechtsanwender stets mehrere Gesetze heranziehen und abgleichen. Dadurch entsteht eine Gemengelage von Vorschriften für den Gesundheitsdatenschutz, die erstens aus der DSGVO, zweitens aus bereichsspezifischen Regelungen und drittens aus dem BDSG heranzuziehen wären (vgl. jetzt auch Begründung zum RegE, S. 96).

Der Bundesgesetzgeber unterlässt es, in § 22 BDSG-E Konkretisierungen vorzunehmen. Die Vorschrift wiederholt nahezu wortgleich den Normtext von Art. 9 Abs. 2 lit. b, g, h und i DSGVO. § 22 Abs. 1 Nr. 1 BDSG-E gibt den Inhalt von Art. 9 Abs. 2 lit. b, h und i DSGVO wieder, wobei § 22 Abs. 1 Nr. 1 lit. a BDSG-E fast wortidentisch Art. 9 Abs. 2 lit. b DSGVO und § 22 Abs. 1 Nr. 1 lit. b BDSG-E mit einer Auslassung und Ergänzung um die Anforderungen von Art. 9 Abs. 3 DSGVO dem Art. 9 Abs. 2 lit. h DSGVO entspricht und § 22 Abs. 1 Nr. 1 lit. c BDSG-E den Inhalt von Art. 9 Abs. 2 lit. i DSGVO wiederholt, der um einen weiteren Halbsatz ergänzt wird. § 22 Abs. 1 Nr. 2 lit. a BDSG-E wiederholt den Inhalt von Art. 9 Abs. 2 lit. g DSGVO.

Es kommt ein **Verstoß gegen das europarechtliche Normwiederholungsverbot** (Art. 4 Abs. 3 und Art. 19 Abs. 1 S. 2 EUV, vgl. EuGH v. 10.10.1973, Rs. 34/73, Variola, Slg. 1973, 981 Rn. 10, 11; *Hatje*, in: Schwarze, EU-Kommentar, 3. Auflage 2012, Art. 4 EUV, Rn. 38; *Schwarze*, in: Schwarze, EU-Kommentar, 3. Auflage 2012, Art. 19 EUV, Rn. 49; s. a. *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 6 ff.) in Betracht, weil weite Teile der europarechtlichen Regelungen lediglich wiedergegeben werden. Ausnahmen vom Normwiederholungsverbot sind zwar möglich (s. EuGH v. 28.3.1985, Rs. C-272/83, Rn. 27): Die punktuelle Wiederholung bestimmter Aspekte aus EU-Verordnungen ist ausnahmsweise zulässig, wenn unionsrechtliche, einzelstaatliche und regionale Vorschriften zusammentreffen und dies „im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten“ liegt. Dies entspricht dem Gedanken des Erwägungsgrundes 8 der DSGVO (vgl. hierzu auch Begründung zum RegE, S. 71 ff.).

Bei der Wiedergabe der Begriffe von Art. 9 Abs. 2 lit. b, g, h und i DSGVO könnte es sich zwar um solche lediglich punktuellen Normwiederholungen handeln, die vom EuGH zugelassen werden. Allerdings ist vom Gesetzgeber augenscheinlich eine Normwiederholung in diesem Sinne gar nicht intendiert. Die Wiederholungen sind nicht erforderlich, um den Regelungsinhalt verständlich zu machen, weil eine Regelung mit dem „Abschreiben“ der Regelungsermächtigung aus dem Verordnungstext gar nicht getroffen wird. Die Wiederholung des Normtextes aus Art. 9 Abs. 2 lit. b, g, h und i DSGVO erfolgt insoweit nicht „innerhalb“ der dem nationalen Gesetzgeber durch „Öffnungsklauseln“ „zugewiesenen Normsetzungskompetenz“ (vgl. *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 7), sondern vollständig an deren Stelle. Diese Wiedergabe des Verordnungstextes dient auch nicht dazu, einen inneren Zusammenhang herzustellen, wie dies anlässlich einer in Betracht zu ziehenden Schaffung einer Gesamtkodifikation für den Gesundheitsdatenschutz (Gesundheitsdatenschutzgesetz) oder im Rahmen der Ausgestaltung bereichsspezifischen Rechts in angemessenem Umfang sinnvoll sein könnte.

Der Gesetzgeber muss jedenfalls den ihm in Art. 9 Abs. 2 lit. b, h und i DSGVO übertragenen **Ausgestaltungs- und Konkretisierungsauftrag** (vgl. auch Begründung zum

RegE, S. 96) **wahrnehmen**. In § 22 BDSG-E wird nicht deutlich, worin die Ausgestaltung und Konkretisierung von Art. 9 Abs. 2 DSGVO durch den Bundesgesetzgeber besteht. Unterschiede zwischen Art. 9 Abs. 2 DSGVO und § 22 BDSG-E sind überwiegend nicht zu erkennen. Eine Spezifizierung unterbleibt. Ungeachtet der Frage eines Verstoßes gegen das Normwiederholungsverbot infolge der bloßen Wiederholung des Normtextes von Art. 9 Abs. 2 DSGVO kommt der nationale Gesetzgeber damit seinem Ausgestaltungs- und Konkretisierungsauftrag nicht nach.

Für die Verarbeitung von Gesundheitsdaten enthält der Regierungsentwurf zudem sehr **allgemein gehaltene Tatbestandsmerkmale**. Mit Blick auf die (gegenwärtig noch nicht absehbare) Anpassung des bereichsspezifischen Datenschutzrechts (sog. Fachrecht), ist noch nicht erkennbar, inwieweit es eines derart unspezifisch **gefassten Auffanggesetzes** für den Datenschutz (§ 1 Abs. 2 S. 1 u. 2 BDSG-E) mit generalklauselartigen Tatbeständen überhaupt bedarf. Bereichsspezifische Gesetze i. S. d. Art. 9 Abs. 2 lit. b und i DSGVO sind insbesondere für den Bereich der „öffentlichen Gesundheit“ (Landesrecht) oder des „Sozialschutzes“ (SGB X) bereits vorhanden. Mit der Schaffung eines Auffanggesetzes bleiben spezifische **Verwendungszwecke** außer Betracht. Insoweit ist eine Konkretisierung durch den nationalen Gesetzgeber erforderlich.

Weil eine Begründung zu § 22 Abs. 1 Nr. 1 lit. a und c BDSG-E dem Gesetzesentwurf nicht zu entnehmen ist, wird nicht ersichtlich, auf welche Bereiche der Datenverarbeitung sich diese Regelung beziehen soll. Ungeachtet etwaiger **Friktionen mit bereichsspezifischem Datenschutzrecht**, z. B. dem Sozialdatenschutzrecht, könnten Kompetenzkonflikte mit Regelungsbereichen auftreten, für welche die **Gesetzgebungskompetenz** den Ländern zukommt.

Nicht verständlich ist, dass nach Auffassung des Gesetzgebers in der Begründung zu § 22 BDSG-E „neben einem Ausnahmetatbestand [gemäß Art. 9 Abs. 2 DSGVO] im Übrigen stets erforderlich [sein soll], dass eine Rechtsgrundlage für die Verarbeitung nach Artikel 6 Absatz 1 [DSGVO] vorliegt.“ (Begründung zum RegE, S. 96). Dies dürfte das System des Verbots (Art. 9 Abs. 1 DSGVO) mit Erlaubnisvorbehalt (Art. 9 Abs. 2 DSGVO) bei der Verarbeitung besonderer Kategorien personenbezogener Daten verkennen; erklärt aber möglicherweise, warum der Gesetzgeber es unterlässt, seinem in Art. 9 Abs. 2 DSGVO vereinzelt übertragenen Ausgestaltungs- und Konkretisierungsauftrag nachzukommen, nach dem er diese Rechtsgrundlagen gerade zu schaffen hätte. Eine „**Verdopplung**“ des **Erfordernisses einer Rechtsgrundlage für die Verarbeitung von u. a. Gesundheitsdaten** durch zusätzliche Heranziehung von Art. 6 Abs. 1 DSGVO ist jedenfalls nicht erforderlich und war schon nach dem Regelungsansatz von Art. 8 RL 95/46/EG, an dem sich Art. 9 DSGVO sichtlich orientiert, nicht geboten.

Sollte der Gesetzgeber entgegen des Wortsinns („ist die Verarbeitung [...] zulässig“) und seiner erklärten Intention („Schaffung einer Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten“, Begründung zum RegE, S. 68) davon ausgehen, dass § 22 BDSG-E keine Rechtsgrundlage für die Datenverarbeitung u. a. von Gesundheitsdaten darstellt, wäre dies sprachlich und systematisch klarzustellen. Die jedenfalls missverständliche Passage sollte anderenfalls aus der Begründung entfernt werden.

(2) Zu § 22 Abs. 1 Nr. 1 BDSG-E

§ 22 Abs. 1 Nr. 1 lit. a BDSG-E, der auf Art. 9 Abs. 2 lit. b DSGVO zurückzuführen ist, regelt die Datenverarbeitung für den Bereich der sozialen Sicherheit und des Sozialschutzes, soweit aus diesem Rechtsbereich erwachsende Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen ist. Eine solche „Generalklausel“ für die Verarbeitung u. a. von

Gesundheitsdaten im Bereich der sozialen Sicherheit und des Sozialschutzes lässt Fragen zur verbleibenden Bedeutung einschlägiger bereichsspezifischer Regelungen im Gesundheitswesen aufkommen, die jeweils für konkrete Verarbeitungssituationen spezifische Rechtsgrundlagen vorsehen. Unter Berücksichtigung von § 1 Abs. 2 S. 1 u. 2 BDSG-E führt eine solche Auffangregelung möglicherweise dazu, das Recht auf informationelle Selbstbestimmung des Patienten auszuhöhlen, weil sämtliche Datenverarbeitungsvorgänge, die nicht auf bereichsspezifische Gesetze gestützt werden können, unter § 22 Abs. 1 Nr. 1 lit. a BDSG-E subsumiert werden. Diese Vorschrift stellt aber keine vergleichbaren Anforderungen; insbesondere bleiben spezifische **Verwendungskontexte** ebenso wie eine **Interessenabwägung** außer Betracht. Insoweit ist eine Konkretisierung durch den Gesetzgeber erforderlich; etwaigen entgegenstehenden Interessen des Betroffenen muss Rechnung getragen werden.

§ 22 Abs. 1 Nr. 1 lit. b BDSG-E stellt die Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten u. a. zum Zweck der Gesundheitsvorsorge und für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich dar. Die Anforderungen für die Verarbeitung von Gesundheitsdaten werden in § 22 Abs. 1 Nr. 1 lit. b BDSG-E, der auf Art. 9 Abs. 2 lit. h DSGVO zurückzuführen ist, nicht näher spezifiziert.

Anders als noch im Referentenentwurf, in dem der Normbestand aus dem BDSG (vgl. die in der ärztlichen Praxis bedeutsame Rechtsgrundlage des § 28 Abs. 7 BDSG; vgl. auch § 13 Abs. 2 Nr. 7 BDSG), weitgehend in das BDSG-E überführt wurde, werden im Regierungsentwurf die von § 28 Abs. 7 S. 2 BDSG vorgesehenen Anforderungen nicht mehr übernommen, die für Verarbeitungsphasen gelten, die keine „Erhebung“ von Gesundheitsdaten i. S. d. § 28 Abs. 7 S. 1 BDSG sind. Nach § 28 Abs. 7 S. 2 BDSG richtet sich die „Verarbeitung und Nutzung“ von Gesundheitsdaten nach den für geheimhaltungspflichtige Personen geltenden Geheimhaltungspflichten. Ob die in § 22 Abs. 1 Nr. 1 lit. b BDSG-E gefundene Formulierung allein darauf zurückzuführen ist, weil die DSGVO nicht mehr zwischen den Verarbeitungsphasen differenziert (Art. 4 Nr. 2 DSGVO) oder ob damit auch inhaltliche Veränderungen intendiert sind bzw. aus welchen Gründen nunmehr von diesen Anforderungen abgesehen wird, ist der Begründung zum Regierungsentwurf jedenfalls nicht zu entnehmen. Dort wird lediglich angegeben, dass die Regelung im wesentlichen § 28 Abs. 7 BDSG entspreche (Begründung zum RegE, S. 97).

Es erfolgt in § 22 BDSE-E stattdessen überwiegend nur eine Wiedergabe des Normtextes von Art. 9 Abs. 2 lit. h DSGVO. Diese Vorschrift der DSGVO kennzeichnet allerdings den Bereich, in welchem der nationale Gesetzgeber seinem Regelungsauftrag nachkommen soll, ohne selbst die hinreichenden Voraussetzungen für eine Rechtsgrundlage zur Verarbeitung u. a. von Gesundheitsdaten aufzuweisen. Der Gesetzgeber müsste insoweit noch konkretisierend tätig werden.

Begrüßt wird hingegen, dass entsprechend der Anregung der Bundesärztekammer in ihrer Stellungnahme zum Referentenentwurf (S. 8) in § 22 Abs. 1 Nr. 1 lit. b BDSG-E nun klargestellt wird, dass eine Datenverarbeitung „aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs“ erfolgen kann (näher Begründung zum RegE, S. 97). Damit wird zutreffend darauf hingewiesen, dass ein Behandlungsvertrag und nicht Verträge des behandelnden Heilberufsangehörigen mit einem Dritten gemeint sind.

Problematisch bleibt **§ 22 Abs. 1 Nr. 1 lit. c BDSG-E**, der auf Art. 9 Abs. 2 lit. i DSGVO zurückzuführen ist und dessen **Hs. 1** eine Rechtsgrundlage für den Bereich der „öffentlichen Gesundheit“ darstellt: Neben der Unbestimmtheit der Tatbestandsmerkmale „schwerwiegende grenzüberschreitende Gesundheitsgefahren“ und „Gewährleistung hoher Qualitäts- und Sicherheitsstandards“ ohne spezifischen Bezug zu einem diese Aspekte betreffenden Regelungsbereich ist das Verhältnis zu anderen, diese Sachverhalte spezifisch

regelnden, sog. Fachgesetzen unklar. Mit Art. 9 Abs. 2 lit. i DSGVO dürften die bereichsspezifischen Gesetze wie z. B. das InfSG oder § 299 SGB V angesprochen sein. Zwar gehen die Spezialgesetze ausweislich § 1 Abs. 2 S. 1 u. 2 BDSG-E dem BDSG-E vor. Der verbleibende Anwendungsbereich von § 22 Abs. 1 Nr. 1 lit. c BDSG-E ist aber aufgrund des Wortsinns nicht erkennbar.

Als Generalklausel für eine Datenverarbeitung, z. B. zum Zwecke der Qualitätssicherung, erscheint die Norm mit Blick auf eine Zweckbestimmung zu unbestimmt. Beschränkungen des Rechts auf informationelle Selbstbestimmung bedürfen einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 65, 1, 44). Insoweit bedarf es nicht lediglich der Wiedergabe der offenen Klauseln aus der DSGVO, die den Bereich kennzeichnen sollen, in welchem der nationale Gesetzgeber regelnd tätig werden soll. Vielmehr müssen klare und hinreichend bestimmte Tatbestandsmerkmale geschaffen werden, die den Zweck der zulässigen Datenverarbeitung kennzeichnen. Nur auf diese Weise kann der den Mitgliedstaaten zugebilligten Ausgestaltungs- und Konkretisierungsaufgabe entsprochen werden. Beispielsweise sollte im Normtext auf Qualitätssicherungsmaßnahmen Bezug genommen werden, für die eine rechtliche Verpflichtung für den Verantwortlichen besteht.

§ 22 Abs. 1 Nr. 1 lit. c **Hs. 2** BDSG-E stellt auf den ersten Blick zusätzliche Anforderungen auf, die von Art. 9 Abs. 2 lit. i DSGVO vorgesehen sind, weil die Mitgliedstaaten „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses“ vorzusehen haben (vgl. auch Begründung zum RegE, S. 97). Die Regelung in der gegenwärtigen Ausgestaltung geht aber über das vom Unionsrecht Geforderte hinaus. Aus Art. 9 Abs. 3 DSGVO lässt sich entnehmen, dass es zur Wahrung des Berufsgeheimnisses nur bei der Verarbeitung nach Art. 9 Abs. 2 lit. h DSGVO als zusätzliche Voraussetzung geboten ist, die Verarbeitung nur durch Personen zuzulassen, die der Berufsgeheimnispflicht unterliegen. Nach Art. 9 Abs. 2 lit. i DSGVO sind indes „angemessene und spezifische Maßnahmen“ zur Wahrung insbesondere des Berufsgeheimnisses vorzusehen. Es wird nicht vorgeschrieben, dass der Verantwortliche diesen Pflichten selbst unterliegen muss.

Demgegenüber begründet § 22 Abs. 1 Nr. 1 lit. c **Hs. 2** BDSG-E offenbar eine Fiktion, wonach für Personengruppen diese Pflichten gelten, die bislang keiner entsprechenden berufs- oder strafrechtlichen Pflicht unterliegen. Alternativ soll mit **Hs. 2** eine Verarbeitung von Daten im Bereich der „öffentlichen Gesundheit“ wohl nur noch durch Personen erfolgen dürfen, die einer solchen Pflicht unterliegen. Dies dürfte nicht den realen Gegebenheiten entsprechen. Es genügt zur Wahrung des Berufsgeheimnisses stattdessen, wenn die Maßnahmen gemäß § 22 Abs. 2 BDSG-E getroffen werden (so auch Begründung zum RegE, S. 97). Die Einhaltung der berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses oder Erstreckung dieser Pflichten auf nicht schweigepflichtige Personen ist entbehrlich; **Hs. 2** muss gestrichen werden.

Zwar könnte § 22 Abs. 1 Nr. 1 lit. c **Hs. 2** BDSG-E eine „zusätzliche Bedingung“ i. S. d. Art. 9 Abs. 4 DSGVO darstellen. Aus Sicht des Personenkreises von Verantwortlichen, der ohnehin zur Einhaltung „insbesondere der berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses“ verpflichtet ist, stellt § 22 Abs. 1 Nr. 1 lit. c **Hs. 2** BDSG-E eine allenfalls deklaratorische Ergänzung dar. Mit Blick auf die zutreffend in den Regierungsentwurf aufgenommene Bestimmung des § 1 Abs. 2 S. 3 BDSG-E ist diese Regelung aber nicht erforderlich und erzeugt entsprechend der vorstehend geäußerten Anmerkungen Missverständnisse für Personengruppen, welche bislang keiner entsprechenden berufsrechtlichen oder strafrechtlich relevanten Pflicht unterliegen.

(3) Zu § 22 Abs. 1 Nr. 2 BDSG-E

§ 22 Abs. 1 Nr. 2 wird im Regierungsentwurf gegenüber dem Referentenentwurf ergänzt um den Aspekt der Interessenabwägung, wonach in den Fällen von Nr. 2 die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen müssen. Diese Ergänzung, die gemäß Art. 9 Abs. 2 lit. g DSGVO erforderlich ist (Begründung zum RegE, S. 97), gilt für § 22 Abs. 1 Nr. 2 lit. a-d BDSG-E und ist sachgerecht.

§ 22 Abs. 1 Nr. 2 lit. a BDSG-E wiederholt den Inhalt von Art. 9 Abs. 2 lit. g DSGVO. Die Regelung ist hochgradig unbestimmt. Mangels aufschlussreicher Gesetzesbegründung bleibt weiterhin offen, was der Gesetzgeber mit dem weiten Begriff des „erheblichen öffentlichen Interesses“ in Verbindung bringt, zu dem die Verarbeitung von Gesundheitsdaten „zwingend erforderlich“ sein muss. In der Begründung zum Referentenentwurf wird ausgeführt, dass dies insbesondere in den Fällen anzunehmen sei, „in denen biometrische Daten zu Zwecken der eindeutigen Identifikation Betroffener verarbeitet werden“ (Begründung zum RegE, S. 97). Die aus Art. 9 Abs. 2 DSGVO übernommenen offenen Klauseln lassen jenseits dieses einen Beispiels insgesamt einen erheblichen Interpretationsspielraum.

Eine Vereinbarkeit mit den durch das Bundesverfassungsgericht aufgestellten Anforderungen der Normklarheit und mit dem rechtsstaatlichen Bestimmtheitsgrundsatz gemäß Art. 20 Abs. 1 GG erscheint hierbei fraglich, wenn „eine Norm die Erhebung sensibler Daten erst ‚durch Auslegung‘ ermöglicht“ (zu § 13 Abs. 2 Nr. 1 BDSG s. *Stender-Vorwachs*, in: Wolff/Brink, BeckOK Datenschutzrecht, § 13, Rn. 25.). Die Erwägungsgründe 52 ff. der DSGVO führen zwar „öffentliche Interessen“ auf. Diese führen bei der Auslegung und Abgrenzung der Normen aber nur bedingt weiter. Hier ist der Gesetzgeber angehalten darzulegen, für welche Zwecke (des erheblichen öffentlichen Interesses) er eine Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten schaffen will. Insbesondere wegen des europarechtlich nicht determinierten Ausgestaltungsbereiches ist es unerlässlich, die verfassungsrechtlichen Anforderungen zur Bestimmtheit und Normenklarheit (s. o.) zu beachten. Daher sollten jedenfalls in der Gesetzesbegründung zu den geschaffenen Rechtsgrundlagen Hinweise für die Auslegung der Normen gegeben werden. Die inhaltlichen Begründungen genügen den europarechtlichen und verfassungsrechtlichen Anforderungen nicht.

Der Gesetzgeber unterlässt es im Übrigen vollständig, für die **§ 22 Abs. 1 Nr. 2 lit. b-d BDSG-E** eine Begründung zu formulieren, sodass zur Auslegung der Begriffe allenfalls auf die zu § 13 Abs. 1 Nr. 1, 5, 6 und 9 BDSG ergangene Rechtsprechung und Kommentarliteratur zurückgegriffen werden kann. Der europäische Regelungshintergrund mit der DSGVO bleibt dabei ausgeblendet. § 22 Abs. 1 Nr. 2 lit. b-d BDSG-E müsste indes im Lichte dieser Verordnung interpretiert werden.

§ 22 Abs. 1 Nr. 2 lit. b-d BDSG-E dürften zudem eine Konkretisierung und Ausgestaltung entsprechend des Regelauftrages gemäß Art. 9 Abs. 2 lit. g DSGVO darstellen, wobei sie den bisherigen Regelungen des § 13 Abs. 1 Nr. 1, 5, 6 und 9 BDSG entsprechen. Die darin verwendeten Tatbestandsmerkmale konkretisieren den Begriff des „erheblichen öffentlichen Interesses“. Weil § 22 Abs. 1 Nr. 2 lit. b-d BDSG-E insoweit Unterfälle von § 22 Abs. 1 Nr. 2 lit. a BDSG-E sein dürften, bedarf es einer Umgestaltung des Tatbestandes von Nr. 2 dergestalt, dass die lit. b-d BDSG-E als Fälle des lit. a abgebildet werden (s. dazu den Änderungsvorschlag).

(4) Zu § 22 Abs. 2 BDSG-E

§ 22 Abs. 2 S. 2 BDSG-E konstituiert „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ i.S.v. Art. 9 Abs. 2 lit. b, g und i DSGVO, die gemäß § 22 Abs. 2 S. 1 BDSG-E vorzusehen sind. Diese Anforderungen gelten nicht verpflichtend für eine Verarbeitung nach § 22 Abs. 1 Nr. 1 lit. b BDSG-E, was zutreffend § 22 Abs. 2 S. 3 BDSG-E klarstellt. Denn Art. 9 Abs. 2 lit. h DSGVO nimmt als „angemessene Garantien“ bereits auf Art. 9 Abs. 3 DSGVO Bezug, was § 22 Abs. 1 Nr. 1 lit. b BDSG-E berücksichtigt.

Personen, die Gesundheitsdaten gemäß § 22 Abs. 1 Nr. 1 lit. b BDSG-E typischerweise verarbeiten, wird ein entsprechendes, nicht zuletzt strafbewehrtes Vertrauen entgegengebracht, wodurch Gefahren des Missbrauchs von Patientendaten wirksam begegnet werden kann. Werden z. B. die in den Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis aufgeführten Anforderungen eingehalten und entsprechende Maßnahmen ergriffen, werden die Grundrechte und Interessen der Patienten hinreichend gewahrt.

Die in § 22 Abs. 2 S. 2 BDSG-E aufgeführten Maßnahmen können gleichwohl auch für eine Datenverarbeitung durch z. B. Ärzte gemäß § 22 Abs. 1 Nr. 1 lit. b BDSG-E eine sinnvolle Orientierung bieten. Im Übrigen ist das Treffen solcher Maßnahmen für Verarbeitungen nach § 22 Abs. 1 Nr. 1 und Nr. 2 BDSG-E verbindlich (§ 22 Abs. 2 S. 1 BDSG-E), wobei die aufgeführten Maßnahmen nicht zwingend sind und auch „andere angemessene und spezifische Maßnahmen getroffen werden“ können (§ 22 Abs. 2 S. 2 BDSG-E: „können“; s. a. Begründung zum RegE zu § 28 BDSG-E, S. 103).

Problematisch erweist sich in diesem Zusammenhang jedoch ein gegenwärtig ebenfalls im Gesetzgebungsverfahren befindliches Gesetz: Mit dem Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (Regierungsentwurf) sollen sog. „mitwirkende Personen“ gemäß **§ 203 Abs. 4 StGB-E** wegen der Zulassung einer Geheimnisoffenbarung durch § 203 Abs. 3 StGB-E folgerichtig in den strafrechtlichen Schutz des § 203 StGB einbezogen werden. Es handelt sich bei diesen Personen um externe Dienstleister, wie z. B. Anbieter von Cloud- oder Fernwartungsdiensten, oder Privatärztliche Verrechnungsstellen. Sie werden durch die Änderung des Strafgesetzbuches zugleich zu „sonstige[n] Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen“ i.S.v. § 22 Abs. 1 Nr. 1 lit. b BDSG-E. Das hat zur Folge, dass sie gemäß § 22 Abs. 2 S. 3 BDSG-E die Voraussetzungen von § 22 Abs. 2 S. 2 BDSG-E nicht einhalten müssen.

Damit müssen externe Dienstleister, deren Datenverarbeitung keine Auftragsverarbeitung i.S.v. Art. 28 DSGVO darstellt (die Rechtswirkungen sind umstr., s. dazu z. B. *Hofmann*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 3, Rn. 251 mwNw.) und damit in Einzelfällen direkt auf § 22 Abs. 1 Nr. 1 lit. b BDSG-E gestützt werden kann (z. B. zur „Verwaltung von Systemen und Diensten“ im Gesundheitsbereich), u. a. keine technischen und organisatorischen Maßnahmen mehr treffen. Bislang werden diese Personengruppen zumeist im Wege einer Auftragsdatenverarbeitung (vgl. § 11 BDSG) von den Personen herangezogen, welche der z. B. ärztlichen Schweigepflicht unterliegen. Dabei hatten diese externen Dienstleister im Rahmen der Auftragsdatenverarbeitung u. a. nach § 9 BDSG technische und organisatorische Maßnahmen zu treffen (§ 11 Abs. 2 BDSG). Durch die Privilegierung aus § 22 Abs. 1 Nr. 1 lit. b BDSG-E i.V.m. § 203 Abs. 4 StGB-E entfällt, anders als noch unter den Voraussetzungen der Auftragsdatenverarbeitung, die

Verpflichtung zur Einhaltung dieser und anderer Maßnahmen zur Sicherstellung des Grundrechtsschutzes der betroffenen Person.

Externe Dienstleister sind anders als Ärzte auch nicht gehalten die die o.g. Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zur ärztlichen Schweigepflicht u. a. zu beachten. Wegen der Implikationen aus dem parallel geführten Gesetzgebungsverfahren sollte eine Abstimmung der Voraussetzungen des Datenschutzes mit den Anforderungen des Geheimnisschutzrechts erfolgen.

Die vorgesehenen Maßnahmen nach **§ 22 Abs. 2 BDSG-E** sind wegen der Orientierung am „Stand der Technik“ und des nicht abschließenden Charakters („insbesondere“) technikoffen, was begrüßt wird. Auf diese Weise lassen sich Schutzmaßnahmen dynamisch an die technischen Entwicklungen anpassen. Die im Regierungsentwurf gegenüber dem Referentenentwurf vorgenommene Erweiterung des nicht abschließenden Katalogs von Maßnahmen in § 22 Abs. 2 S. 2 BDSG-E, die insbesondere aus Art. 24 Abs. 1, Art. 32 Abs. 1, Art. 39 Abs. 1 und Erwägungsgrund 67 DSGVO übernommen worden sind, ist sinnvoll.

c. Änderungsvorschlag der Bundesärztekammer

Eine übersichtlichere Rechtslage könnte nach hiesiger Einschätzung erreicht werden, indem der nationale Gesetzgeber eine **Kodifikation für das Gesundheitsdatenschutzrecht** (Gesundheitsdatenschutzgesetz) einschließlich bereichsspezifischer Regelungen schafft, wofür es freilich der Berücksichtigung der verfassungsrechtlichen Kompetenzordnung bedarf (vgl. dazu *Kühling/Kingreen*, Gesundheitsdatenschutzrecht, 2015, S. 440 ff., S. 463 ff., 468 ff.). Bei dieser Gelegenheit wären ihm auch Ausnahmen vom Normwiederholungsverbot erlaubt, denn der EuGH stellt klar, dass „im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten“ Normen wiederholt werden könnten. In einer Gesamtkodifikation dürfte dieser Fall gegeben sein.

Sollte dem Vorschlag nicht gefolgt werden, ist durch den Gesetzgeber jedenfalls kritisch zu prüfen, ob es weitgefasster Auffangtatbestände wie in § 22 Abs. 1 Nr. 1 und Nr. 2 BDSG-E bedarf oder die vorhandenen bereichsspezifischen Regelungen für den Gesundheitsdatenschutz hinreichender Ausdruck von Art. 9 Abs. 2 lit. b, h und i DSGVO sind. Folgende Änderungen werden insoweit vorgeschlagen:

(1) Zu § 22 Abs. 1 Nr. 1 BDSG-E

§ 22 Abs. 1 Nr. 1 lit. a und c BDSG sind zu streichen, da sich deren Regelungsinhalte in den bereichsspezifischen Gesetzen wiederfinden, für welche Art. 9 Abs. 2 lit. b und i DSGVO eine Regelungsgrundlage bietet. Weiterer Auffangregelungen im BDSG-E bedarf es nicht.

§ 22 Abs. 1 Nr. 1 lit. b und c BDSG-E bedürfen jedenfalls klarer und hinreichend bestimmter Tatbestandsmerkmale. Insoweit ist zumindest eine Konkretisierung erforderlich.

(2) Zu § 22 Abs. 1 Nr. 2 BDSG-E

§ 22 Abs. 1 Nr. 2 ist wie folgt zu ändern:

2. durch öffentliche Stellen, wenn sie aus Gründen eines erheblichen öffentlichen Interesses wie

- a) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit,*
- b) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend oder*
- c) aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf*

dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen

zwingend erforderlich ist und soweit die Interessen des Verantwortlichen an der Datenverarbeitung in den Fällen der Nummer 2 die Interessen der betroffenen Person überwiegen.

Sollte der Vorschlag keine Berücksichtigung finden, bedarf § 22 Abs. 1 Nr. 2 lit. a BDSG-E jedenfalls klarer und hinreichend bestimmter Tatbestandsmerkmale. Insoweit ist zumindest eine Konkretisierung erforderlich.

2. Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten im Bereich der Forschung, zu § 27 BDSG-E

a. Beabsichtigte Neuregelung

§ 27 Abs. 1 BDSG-E regelt die Verarbeitung von personenbezogenen Daten besonderer Art u. a. im Kontext der wissenschaftlichen Forschung. Eine Datenverarbeitung z. B. von Gesundheitsdaten ist danach zulässig, wenn sie zur Durchführung wissenschaftlicher oder historischer Forschung erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

Gemäß § 27 Abs. 1 S. 2 BDSG-E hat der Verantwortliche angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG-E vorzusehen. Ergänzend dazu sieht § 27 Abs. 3 BDSG-E in Anlehnung an § 40 BDSG – bislang aus Gründen der Datensparsamkeit i. S. d. § 3a BDSG – Anforderungen vor, wonach Daten zu anonymisieren sind, „sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.“

§ 27 Abs. 4 BDSG-E sieht in Anlehnung an § 40 Abs. 3 BDSG vor, dass der Verantwortliche personenbezogene Daten nur veröffentlichen darf, „wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“

b. Stellungnahme der Bundesärztekammer

Der mit § 27 BDSG-E intendierte Erhalt der Möglichkeit, personenbezogene Daten besonderer Art, insbesondere zu Zwecken der wissenschaftlichen Forschung, verarbeiten zu können, wird von der Bundesärztekammer begrüßt. Im Wesentlichen wird die Rechtslage gemäß § 28 Abs. 6 Nr. 4 BDSG nachgebildet. Die Ergänzung um den Passus „auch ohne Einwilligung“ im Regierungsentwurf entspricht § 28 Abs. 6 BDSG („soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat“) und stellt damit klar, dass, wie bisher, auch die Einwilligung des Betroffenen bei der Datenverarbeitung im Bereich der Forschung eine hinreichende Legitimationsgrundlage sein kann. Insbesondere durch die Berücksichtigung des Erforderlichkeitsgrundsatzes und des Interesses des Betroffenen findet eine verhältnismäßige Ausgestaltung dieses Tatbestandes statt.

Klargestellt werden sollte aber, dass das „wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens“ (§ 28 Abs. 6 Nr. 4 BDSG) und nicht die (persönlichen)

„Interessen des Verantwortlichen“ (so aber wohl § 27 Abs. 1 BDSG-E) mit dem Interesse des Betroffenen in Abwägung gebracht werden müssen. Nur auf diese Weise wäre die hier einschlägige Interessenkollision von dem Recht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG, Art. 8 EU-GRCh) und dem der Forschungsfreiheit (Art. 5 Abs. 3 S. 1 GG, Art. 13 EU-GRCh) zutreffend abgebildet.

Unverständlich ist auch hier (vgl. schon zu § 22 BDSG-E o. II., 1., b., (1)), dass die Verarbeitung nach § 27 Abs. 1 BDSG-E ausweislich der Gesetzesbegründung zusätzlich das Vorliegen einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO voraussetzen soll, wobei exemplarisch auf die Rechtsgrundlage aus Art. 6 Abs. 1 lit. f DSGVO verwiesen wird, die eine Datenverarbeitung zur „Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten“ zulässt (Begründung zum RegE, S. 102).

Die in Bezug genommene Rechtsgrundlage erfasst schon nicht die Datenverarbeitung im Interesse wissenschaftlicher Forschung. Art. 6 Abs. 1 lit. f DSGVO gilt insbesondere nicht für das Verhältnis von Hoheitsträgern zu Bürgern, sodass die Forschung öffentlicher Stellen darüber kaum legitimiert werden könnte. „Das ‚berechtigte Interesse‘ muss als subjektivrechtliche Position verstanden werden, durch die nur Private berechtigt sind, nicht als Auffangtatbestand für Interessen der Hoheitsträger.“ (Frenzel, in: Paal/Pauly, DSGVO, 2017, Asr. 6, Rn. 23). Zudem dient die Bestimmung nicht als Auffangregel für Datenverarbeitungsprozesse, die nicht unter die anderen Tatbestände von Art. 6 Abs. 1 DSGVO gefasst werden können. Nicht zuletzt sind vielmehr vorrangig die speziellen Rechtsgrundlagen heranzuziehen, die im Kontext der Verarbeitung besonderer Kategorien personenbezogener Daten einschlägig sind. Für die wissenschaftliche Forschung ermöglicht Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DSGVO dem nationalen Gesetzgeber, Rechtsgrundlagen vorzusehen.

Vor diesem Hintergrund dürfte das System des Verbots (Art. 9 Abs. 1 DSGVO) mit Erlaubnisvorbehalt (Art. 9 Abs. 2 DSGVO) bei der Verarbeitung besonderer Kategorien personenbezogener Daten in der Begründung zum Regierungsentwurf verkannt worden sein. Es sind demnach neben § 27 BDSG-E gerade keine weiteren Rechtsgrundlagen aus Art. 6 DSGVO o. ä. erforderlich. Sollte der Gesetzgeber entgegen des Wortsinns („ist die Verarbeitung [...] zulässig“) davon ausgehen, dass § 27 BDSG-E keine Rechtsgrundlage für die Datenverarbeitung u. a. von Gesundheitsdaten darstellt, wäre dies sprachlich und systematisch klarzustellen. Die jedenfalls missverständliche Passage sollte anderenfalls aus der Begründung entfernt werden.

Wegen § 27 Abs. 1 S. 2 BDSG-E, der auf § 22 Abs. 2 S. 2 BDSG-E verweist, sind angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorgesehen. Dies dürfte die Anforderungen von Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DSGVO erfüllen: Durch die Verpflichtung der Verantwortlichen, z. B. Pseudonymisierungen der personenbezogenen Daten vorzunehmen, wird insbesondere dem Grundsatz der Datenminimierung entsprochen (Art. 89 Abs. 1 S. 1 DSGVO).

Die zusätzlichen Anforderungen gemäß § 27 Abs. 3 BDSG-E, die § 40 BDSG entsprechen, sind jedenfalls zulässige Beschränkungen i. S. d. Art. 9 Abs. 4 DSGVO und erscheinen sinnvoll, um grundlegende Datenschutzprinzipien (Datensparsamkeit) zu wahren und den Interessen der Betroffenen zu entsprechen. Zweifelhaft bleibt aber auch im Regierungsentwurf, ob eine Anonymisierung von genetischen Daten überhaupt möglich ist (vgl. dazu Arning et al., DÄBl. 2011, A-518; Pommerening, in: Anzinger et al., Schutz genetischer, medizinischer und sozialer Daten als multidisziplinäre Aufgabe, 2013, S. 24 ff.). Zu prüfen wäre, ob spezifische Anforderungen für die Forschung mit genetischen Daten, die – anders als der Regierungsentwurf es immer noch nahelegt (Begründung zum RegE, S. 103) – nicht im Gendiagnostikgesetz (GenDG) geregelt sind (s. ausdrücklich § 2 Abs. 2 Nr. 1

GenDG), zu treffen sind. Wegen der besonderen Schutzbedürftigkeit genetischer Daten bedarf es hierfür Sonderregelungen im neuen BDSG oder einem bereichsspezifischen Gesetz.

Die im Regierungsentwurf nunmehr aufgenommene Bestimmung des § 27 Abs. 4 BDSG-E entspricht § 40 Abs. 3 BDSG und ist sachgemäß. Die Norm könnte aber übersichtlicher gestaltet werden, indem die beiden Varianten, wie in § 40 Abs. 3 BDSG, in Nummern abgebildet werden. Das dürfte künftig auch eine Bezugnahme auf vorhandene Kommentierungen sowie die Rechtsprechung und damit die Rechtsanwendung erleichtern.

Erforderlich ist auch für diesen Bereich eine Abstimmung mit den Voraussetzungen des Geheimnisschutzrechts. § 203 Abs. 1 StGB steht insoweit vielfach einer Verarbeitung von Gesundheitsdaten zu Forschungszwecken auf Basis von § 27 BDSG-E entgegen.

c. Änderungsvorschlag der Bundesärztekammer

In Anlehnung an § 28 Abs. 6 Nr. 4 BDSG sollte in § 27 Abs. 1 BDSG-E nach den Worten „erforderlich ist“ eingefügt werden: *„und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an einem Ausschluss der Verarbeitung erheblich überwiegt.“*

Wegen der Übersichtlichkeit sollte § 27 Abs. 4 BDSG-E entsprechend § 40 Abs. 3 BDSG wie folgt gestaltet werden:

„Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn

- 1. die betroffene Person eingewilligt hat oder*
- 2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“*

3. Rechtsgrundlagen für die Weiterverarbeitung personenbezogener Daten, zu §§ 23, 24 BDSG-E

a. Beabsichtigte Neuregelung

§ 23 Abs. 1 BDSG-E sieht vor, dass die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung aus bestimmten Gründen zulässig sein kann. Gemäß § 23 Abs. 1 Nr. 7 BDSG-E kommt dies für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen in Betracht. § 24 Abs. 1 BDSG-E sieht vor, dass die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nicht-öffentliche Stellen aus bestimmten Gründen zulässig sein kann.

b. Stellungnahme der Bundesärztekammer

(1) Allgemeine Anmerkung

Ausweislich der Gesetzesbegründung orientieren sich §§ 23 und 24 BDSG-E an vorhandenen Regelungen des BDSG in der geltenden Fassung (s. die Aufzählung in der Begründung zum RegE, S. 98). Abweichend von den im Begründungstext angegebenen Normen erfolgt in § 24 Abs. 1 BDSG-E eine Orientierung lediglich an § 28 Abs. 2 Nr. 2 lit. b und Abs. 6 Nr. 3 BDSG. Insoweit werden die Gründe „Wahrung berechtigter Interessen der verantwortlichen Stelle“ (§ 28 Abs. 2 i.V.m. Abs. 1 Nr. 2 BDSG) oder „Schutz lebenswichtiger

Interessen des Betroffenen oder eines Dritten“ (§ 28 Abs. 8 i.V.m. Abs. 6 Nr. 1 BDSG) nicht mehr aufgeführt.

Ungeachtet unionsrechtlicher Vorbehalte gegen §§ 23, 24 BDSG-E und verfassungsrechtlicher Einwände gegen eine Relativierung des datenschutzrechtlichen Grundsatzes der Zweckbindung sowie gegen die Verwendung sehr allgemeiner (generalklauselartiger) Ermächtigungstatbestände ist zu begrüßen, dass jedenfalls Einschränkungen zur Berücksichtigung des schutzwürdigen Interesses des Betroffenen (vgl. § 28 Abs. 2 Nr. 1 i.V.m. Abs. 1 S. 1 Nr. 2 und Abs. 2 Nr. 2 BDSG) entsprechend der Anmerkung der Bundesärztekammer (Stellungnahme zum Referentenentwurf, S. 11) im Regierungsentwurf in § 24 BDSG-E nunmehr Eingang gefunden haben.

Dass eine Verarbeitung besonderer Kategorien personenbezogener Daten zu anderen Zwecken gemäß § 24 Abs. 2 i.V.m. Abs. 1 Nr. 1 BDSG-E abweichend von § 28 Abs. 8 i.V.m. Abs. 6 BDSG nunmehr auch zur „Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder **zur Verfolgung von Straftaten**“ zulässig sein soll, überrascht und ermöglicht damit eine Zweckänderung bei der Verarbeitung von Gesundheitsdaten unter deutlich erleichterten Voraussetzungen, als z. B. zum „Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten“ (§ 28 Abs. 8 i.V.m. Abs. 6 Nr. 1 BDSG). Allein die Berücksichtigung des schutzwürdigen Interesses des Betroffenen mildert diese Erweiterung ab. Die Bundesärztekammer sieht die Erweiterung, insbesondere die Weiterverarbeitung für Zwecke der Strafverfolgung, gleichwohl kritisch. Diese Aufgabe obliegt insbesondere den staatlichen (öffentlichen) Stellen und z. B. Ärzte sollten infolge der Regelung nicht in eine unauflösbare Konfliktlage gebracht werden, Daten zu diesen Zwecken weitergeben zu können. Denn hierbei treten **Friktionen mit** dem parallel zu berücksichtigenden **Geheimnisschutzrecht** für Berufsgeheimnisträger auf, wonach eine Offenbarung von Patientengeheimnissen zum Zwecke der Strafverfolgung grundsätzlich unzulässig ist und gegen § 203 Abs. 1 StGB verstößt. Insoweit wird eine Unterstützung bei der Strafverfolgung durch Ärzte im Interesse des Vertrauensverhältnisses zwischen Arzt und Patient richtigerweise ausgeschlossen.

Es ist daher vorzugsweise zwischen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten und den in Ansehung ihres spezifischen Schutzbedürfnisses jeweils unterschiedlichen Anforderungen zu differenzieren. Es empfiehlt sich, wie noch im Referentenentwurf (§ 24 Abs. 3 und 4 BDSG-E), eine separate Regelung für die Verarbeitung besonderer Kategorien personenbezogener Daten zu treffen. Auf die Anmerkungen der Bundesärztekammer zu § 23 Abs. 3 Nr. 6 und Abs. 4 Nr. 3 BDSG-E (i.d.F. des Referentenentwurfs) in ihrer Stellungnahme wird hier vorsorglich ergänzend Bezug genommen (S. 10 f.).

(2) Rechtsgrundlagen für die Weiterverarbeitung personenbezogener Daten durch länderübergreifende Arbeitsgemeinschaften der Landesärztekammern, zu § 23 Abs. 1 BDSG-E

Hinsichtlich der Erforderlichkeit von Rechtsgrundlagen für die Weiterverarbeitung personenbezogener Daten durch länderübergreifende Arbeitsgemeinschaften der Landesärztekammern wird auf die Stellungnahme der Bundesärztekammer zum Referentenentwurf Bezug genommen (S. 11 f.) Dementsprechend sollte in § 23 Abs. 1 Nr. 5 BDSG-E nach dem Wort „Ordnungswidrigkeiten“ nach dem Komma folgender Halbsatz eingefügt werden: „zur Aufsicht der Berufskammern über ihre Mitglieder und Berufsangehörigen, [...]“.

III. Befugnisse der Aufsichtsbehörden für den Datenschutz und Wahrung des Berufsgeheimnisses

1. Beschränkung der Befugnisse von Aufsichtsbehörden im Kontext von Wahrung von Berufsgeheimnissen, zu § 29 Abs. 3 BDSG-E

a. Beabsichtigte Neuregelung

Gemäß § 29 Abs. 3 S. 1 BDSG-E erfolgt eine Beschränkung datenschutzaufsichtsrechtlicher Befugnisse. Gegenüber insbesondere schweigepflichtigen Personen bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Art. 58 Abs.1 lit. e und f DSGVO nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Die Einschränkung betrifft die Befugnisse gemäß Art. 58 Abs. 1 lit. e und f DSGVO, mithin den Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte und den Zugang zu allen personenbezogenen Daten und Informationen. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer solchen Geheimhaltungspflicht unterliegen, soll die Geheimhaltungspflicht auch für die Aufsichtsbehörde gelten (§ 29 Abs. 3 S. 2 BDSG-E).

b. Stellungnahme der Bundesärztekammer

Die Beschränkung datenschutzaufsichtsrechtlicher Untersuchungs- und Kontrollbefugnisse gemäß § 29 Abs. 3 S. 1 BDSG-E ist grundsätzlich nachvollziehbar. Bei der Ausgestaltung der Befugnisse von Aufsichtsbehörden i. S. d. Art. 90 DSGVO ist nämlich darauf zu achten, dass die Pflicht zur Geheimhaltung in einem angemessenen Verhältnis zum Recht auf Schutz der personenbezogenen Daten stehen. Der Gesetzgeber geht zutreffend davon aus, dass es ansonsten zu einer Kollision mit Pflichten des Geheimnisträgers käme (Begründung zum RegE, S. 104).

Eine unabhängige und **effektive Datenschutzkontrolle** ist maßgeblich für die Durchsetzung des Datenschutzanliegens, insbesondere **für den Schutz besonders sensibler Gesundheitsdaten**. Trotz der Einschränkungen gem. § 29 Abs. 3 S. 1 BDSG-E dürfte der Schutz von personenbezogenen Daten besonderer Art, die zugleich einem Berufsgeheimnis unterfallen können, aber **weiterhin gewährleistet** sein, denn eine Datenschutzkontrolle bleibt weiterhin möglich:

- Die Befugnisse werden nach § 29 Abs. 3 S. 1 BDSG-E nur eingeschränkt, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Das ist z. B. der Fall, wenn ein Arzt anlässlich der aufsichtsrechtlichen Kontrolle vorsätzlich gegen die Vorschriften zum Schutz der ärztlichen Schweigepflicht (§ 203 StGB, vgl. § 9 MBO-Ä) verstoßen müsste. Liegt zuvor bereits ein solcher Verstoß z. B. durch einen Arzt vor, von dem die Aufsichtsbehörde z. B. von einem Patienten oder Dritten Kenntnis erlangt, können die datenschutzaufsichtsrechtlichen Untersuchungs- und Kontrollbefugnisse hinsichtlich eines möglicherweise zugleich vorliegenden Verstoßes gegen datenschutzrechtliche Bestimmungen gleichwohl weiterhin wahrgenommen werden.
- Auch § 29 Abs. 3 S. 2 BDSG-E geht davon aus, dass Untersuchungen durch eine Aufsichtsbehörde durchgeführt werden können, anlässlich derer sie Kenntnis von Daten erhalten könnten, wobei in der Gesetzesbegründung darauf abgestellt wird, dass die Aufsichtsbehörden die Kenntnis der Daten von z. B. durch Ärzte

herangezogene externe Dienstleister als Auftragsdatenverarbeiter erlangen könnten. Aus diesem Grund sei es erforderlich und von S. 2 vorgesehen, die Geheimhaltungspflicht auch auf diese Aufsichtsbehörde zu „verlängern“ (vgl. Begründung zum RegE, S. 104).

Einer darüber hinausgehenden Datenschutzaufsicht über die Einhaltung des Berufsgeheimnisses im ärztlichen Bereich bedarf es nicht. Die Überwachung der ärztlichen Schweigepflicht nach den Vorschriften des Berufsrechts ist eine originäre Aufgabe der Landesärztekammern.

Soweit aber zugleich personenbezogene Daten betroffen sind, müssen die Aufsichtsbehörden ihre Untersuchungs- und Kontrollbefugnisse ausüben können. Ansonsten wäre eine effektive Prüfung der Datenverarbeitung in dem Bereich, in dem Gesundheitsdaten z. B. im Krankenhaus verarbeitet werden, nicht möglich. Folgende Anforderungen sind zu beachten:

- Ein Zugriff auf Daten, die dem Patientengeheimnis unterliegen sollte nur ermöglicht werden, soweit dies zur Erfüllung der Aufgaben der Aufsichtsbehörden unbedingt notwendig ist und das Interesse des Patienten am Schutz seiner personenbezogenen Daten dies erfordert.
- Eine Verwertbarkeit der anlässlich einer Kontrolle erlangten Informationen im Strafverfahren muss ausgeschlossen sein.
- Kontrollbefugnisse sollten nur bestehen, soweit zugleich eine Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO (s. v. a. § 1 Abs. 1 S. 2 BDSG) stattfindet. Von einer Deckungsgleichheit von Geheimnisinhalt und personenbezogenen Datum kann per se aber ebenso wenig ausgegangen werden, wie von einer stets teilweise oder vollständig automatisiert erfolgenden Datenverarbeitung von Patientengeheimnissen. Aus diesem Grund muss die Kontrolle beschränkt sein.
- Zugriffsmöglichkeiten auf Patientengeheimnisse durch Stellen und Personen, die nicht zu dem Kreis der in das besondere Vertrauensverhältnis einbezogenen Personen gehören, sollten auf ein absolut notwendiges Maß beschränkt werden.

Der Schutz des Patientengeheimnisses kann zwar grundsätzlich auch in der Sphäre der Aufsichtsbehörden gewahrt bleiben, denn diese unterliegen de lege lata gemäß § 203 Abs. 2a StGB der strafbewehrten Schweigepflicht (vgl. zudem § 5 BDSG, § 5 NDSG) und § 29 Abs. 3 S. 2 BDSG-E ordnet an, dass die Geheimhaltungspflichten auch für die Aufsichtsbehörden gelten sollen. Diese Folgerung sowie § 29 Abs. 3 S. 2 BDSG-E stehen aber im Widerspruch zu der mit dem Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (Regierungsentwurf) vorgeschlagenen Regelung des § 203 Abs. 4 StGB-E, wonach nur noch die „bei den in den [§ 203] Abs. 1 [StGB] genannten Personen“ tätigen Beauftragten für den Datenschutz erfasst werden. Damit sollen de lege ferenda offenbar lediglich betriebliche Datenschutzbeauftragte erfasst sein und es entfällt die Strafbewehrung des Geheimnisschutzes für Landes- bzw. Bundesbeauftragte für den Datenschutz.

Soweit in der Gesetzesbegründung darauf abgestellt wird, dass externe Dienstleister als Auftragsdatenverarbeiter keiner Geheimhaltungspflicht unterliegen würden, und Aufsichtsbehörden über diesen „Umweg“ Kenntnis von Daten anlässlich einer Überwachungs- und Kontrolltätigkeit erlangen könnten (vgl. Begründung zum RegE, S. 104), sollte ebenfalls der Gesetzesentwurf zu § 203 Abs. 4 StGB-E Beachtung finden, wonach externe Dienstleister als „mitwirkende Personen“ künftig ebenfalls zu dem Kreis schweigepflichtiger Personen zählen sollen und insoweit die Kollisionslage i. S. d. § 29 Abs.

3 S. 1 BDSG-E auch bei diesen auftritt. Auch aus diesem Grund sollten die beiden Gesetzgebungsvorhaben miteinander abgestimmt werden.

2. *Aufsichtsbehörde für die Datenverarbeitung durch nicht-öffentliche Stellen, zu § 40 BDSG-E*

a. *Beabsichtigte Neuregelung*

§ 40 BDSG-E regelt die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften bei einer Datenverarbeitung durch nicht-öffentliche Stellen. Zuständig sind die nach Landesrecht zuständigen Behörden.

b. *Stellungnahme und Änderungsvorschlag der Bundesärztekammer*

Die Zulässigkeit einer Regelung im Bundesgesetz sollte vor dem Hintergrund der verfassungsrechtlich festgelegten Gesetzgebungskompetenzen geprüft werden.

Aus Gründen der Klarstellung in § 40 Abs. 4 BDSG-E sollte darauf verwiesen werden, dass § 29 Abs. 3 BDSG-E zu beachten ist.

IV. *Einschränkung von Betroffenen- bzw. Patientenrechten*

1. *Einschränkung von Betroffenenrechten im Rahmen der Forschung, zu § 27 Abs. 2 BDSG-E*

a. *Beabsichtigte Neuregelung*

Die Rechte des Betroffenen sind gem. § 27 Abs. 2 BDSG-E „insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft [...] besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.“ Die Einschränkungen der Betroffenenrechte erfolge aufgrund Art. 89 Abs. 2 und Art. 23 Abs. 1 lit. i DSGVO (Begründung zum RegE, S.102).

b. *Stellungnahme der Bundesärztekammer*

Die mit § 27 Abs. 2 S. 2 BDSG-E vorgenommene Einschränkung des Rechts des Betroffenen auf Auskunft und Erhalt einer Kopie gemäß Art. 15 DSGVO ist sehr weitgehend. Zweifelhaft dürfte sein, ob ein „unverhältnismäßiger Aufwand“ (§ 27 Abs. 2 S. 2 BDSG-E), der nach Auffassung des Gesetzgebers gegeben sein soll, wenn ein Forschungsvorhaben mit besonders großen Datenmengen arbeitet (Begründung zum RegE, S. 103) stets die Einschränkung des Auskunftsrechts rechtfertigt. Dies sollte insbesondere im Hinblick auf die gegenwärtig verfügbaren Möglichkeiten der elektronischen Datenverarbeitung und „smart data“ überdacht werden. Das zur Wahrnehmung informationeller Selbstbestimmung essentielle Recht auf Auskunft sollte nicht aus Gründen bloßer Arbeitserleichterung beschränkt werden. Fraglich ist auch, wie der Einschränkungsgrund des unverhältnismäßigen Aufwandes mit der vom Gesetzgeber zitierten Öffnungsklausel des Art. 23 Abs. 1 lit. i DSGVO, die den „Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“ in Bezug nimmt, in Einklang gebracht werden kann.

2. Einschränkung von Betroffenenrechten wegen Geheimhaltungspflichten, zu § 29 Abs. 1 S. 1-3 BDSG-E

a. Beabsichtigte Neuregelung

§ 29 Abs. 1 BDSG-E schränkt die Pflicht zur Information, Auskunft und Benachrichtigung der betroffenen Person ein, soweit dadurch Informationen offenbart würden, die (nach einer Rechtsvorschrift oder) ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Es handele sich ausweislich der Begründung des Regierungsentwurfes um eine Fortführung bestehender Regelungen des BDSG (Begründung zum RegE, S. 104: „wie bisher“), wobei von den Öffnungsklauseln des Art. 23 Abs. 1 lit. i und Art. 34 DSGVO Gebrauch gemacht werde.

b. Stellungnahme der Bundesärztekammer

Es wird begrüßt, dass entsprechend der Anregung der Bundesärztekammer zum Referentenentwurf, auf die hier ergänzend Bezug genommen wird (S. 12 ff.), im Normtext nunmehr die Klarstellung erfolgt, dass Auskünfte an den Betroffenen nicht schon deshalb verweigert werden können, weil die Daten dem (Patienten-)Geheimnis unterliegen, sondern allenfalls, soweit insbesondere Geheimhaltungsinteressen Dritter einschlägig sind.

Die Wendung „ihrem Wesen nach“ lässt indes weiterhin offen, warum eine Verweigerung z. B. des Auskunftsrechts erfolgen können soll. Auch die Formulierung „insbesondere“ suggeriert, dass es weitere Gründe gäbe, welche die essentiellen Rechte auf Information, Auskunft und Benachrichtigung einzuschränken vermögen. Hinsichtlich des Auskunftsrechts sollte Einklang mit § 630g BGB bestehen. Im Übrigen sollte in den Regelungen hinreichend zum Ausdruck gebracht werden, dass eine Einschränkung aufgrund überwiegender berechtigter Interessen Dritter möglich ist.

c. Änderungsvorschlag der Bundesärztekammer

Die Formulierungen „ihrem Wesen nach“ und „insbesondere“ in § 29 Abs. 1 S. 1-3 BDSG-E sind zu streichen. Stattdessen ist in § 29 Abs. 1 S. 1 BDSG-E nach den Worten „genannten Ausnahmen nicht“ zu formulieren:

„soweit durch ihre Erfüllung Informationen offenbart würden, die ~~ihrem Wesen nach, insbesondere~~ wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.“

Entsprechend ist in § 29 Abs. 1 S. 2 BDSG-E nach den Worten „besteht nicht“ zu formulieren:

„soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ~~ihrem Wesen nach, insbesondere~~ wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.“

Entsprechend ist in § 29 Abs. 1 S. 3 BDSG-E nach den Worten „genannten Ausnahmen nicht“ zu formulieren:

„soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ~~ihrem Wesen nach, insbesondere~~ wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.“

3. Keine pauschale Einschränkung von Betroffenen- bzw. Patientenrechten, insb. zu §§ 32 ff. BDSG-E

a. Beabsichtigte Neuregelung

Unter Berufung auf Art. 23 DSGVO sollen in Teil 2, Kapitel 2 (§§ 32 ff. BDSG-E) Einschränkungen der in Art. 12 bis 22 und 34 DSGVO kodifizierten Informationspflichten und Betroffenenrechte erfolgen. Bereits das bestehende nationale Recht sieht Einschränkungen vor (vgl. z. B. § 34 Abs. 7 i. V. m. § 33 Abs. 2 Nr. 2 BDSG), über die unter Rückgriff auf Art. 23 DSGVO hinausgegangen werden soll.

Den §§ 32 ff. BDSG-E soll zentrale Bedeutung für die Einschränkung von Betroffenenrechten im Datenschutzrecht zukommen. Ausweislich der Gesetzesbegründung sollen die „Beschränkungen der Betroffenenrechte in Kapitel 2 [...] auch Anwendung auf die [...] Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken“ finden (Begründung zum RegE, BT-Drs. S. 106). Die Bestimmungen gelten daher „ergänzend“ zu den in § 27 Abs. 2, § 28 Abs. 2 und § 29 Abs. 1 genannten Ausnahmen (vgl. z. B. § 34 BDSG-E).

b. Stellungnahme der Bundesärztekammer

Es ist zu begrüßen, dass der Gesetzgeber von den entsprechenden Möglichkeiten in Art. 23 DSGVO Gebrauch macht. Die in den nationalen Datenschutzgesetzen bereits vorgesehenen Bestimmungen zur Einschränkung von Betroffenenrechten sollten erhalten bleiben, um einen angemessenen Ausgleich zwischen den Interessen einer pflichtgemäßen Ausübung des ärztlichen Berufs einerseits und den Betroffenenrechten andererseits zu bewahren. Vorbehaltlich einer Vereinbarkeit mit Art. 23 DSGVO und den europäischen Grundrechten ist sicherzustellen, dass die Betroffenenrechte mit berufsrechtlichen Pflichten nicht in Konflikt geraten. Beispielsweise mit dem Recht auf Berichtigung (Art. 16 DSGVO) oder Löschung (Art. 17 DSGVO) könnten im Einzelfall z. B. die ärztlichen Dokumentations- und entsprechende Aufbewahrungspflichten kollidieren (vgl. die i. Erg. zu begrüßende Regelung in § 35 Abs. 3 BDSG-E). Auch für das neue Recht auf Datenportabilität gemäß Art. 20 DSGVO könnten Beschränkungen geboten sein (vgl. zum Auskunftsrecht § 34 Abs. 1 Nr. 2 BDSG-E). Einschränkungen des Patientenrechts auf Auskunft aus der ärztlich geführten Dokumentation müssen im Übrigen in Einklang mit § 630g BGB stehen.

Einer pauschalen Einschränkung von Betroffenenrechten bedarf es jedoch nicht. Die Einschränkungen sehen aber sehr weitestgehende Tatbestandsmerkmale vor. Ein allgemeiner Hinweis z. B. auf die „besondere Art der Speicherung“ sowie einen von den unionsrechtlichen Bestimmungen nicht vorgesehenen „unverhältnismäßig hohen Aufwand“ (vgl. § 35 Abs. 1 und § 34 Abs. 1 Nr. 2 BDSG-E), den z. B. eine Auskunft oder eine Löschung erzeugen würde, dürfte keinen hinreichend differenzierten Grund bieten, um essentielle Rechte der Patienten einzuschränken (Art. 8 Abs. 2 S. 2 GRCh). Der Gesetzgeber sollte hier nicht zuletzt im Interesse des verfassungsrechtlichen Gebots der Normklarheit die ihm obliegende Ausgestaltungs- und Konkretisierungsaufgabe wahrnehmen. Durch rechtsklare und verhältnismäßige Bestimmungen würde vermieden, dass Konflikte über die Reichweite des Auskunfts- oder Löschungsrechts z. B. das Arzt-Patienten-Verhältnis belasten.

BGA | Am Weidendamm 1A | 10117 Berlin

Ansgar Heveling MdB
Vorsitzender des Innenausschusses
des Deutschen Bundestags
Platz der Republik 1
11011 Berlin

Bundesverband
Großhandel, Außenhandel,
Dienstleistungen e.V.

Postanschrift:
BGA, 10873 Berlin

Hausanschrift:
Am Weidendamm 1A
10117 Berlin

Telefon 030 590099-50
Telefax 030 590099-519
info@bga.de
www.bga.de

Ansprechpartner Alexander Kolodzik

Telefon 030 590099 – 581

E-Mail alexander.kolodzik@bga.de

Datum 21. März 2017

Entwurf der Bundesregierung für ein Datenschutz-Anpassungs-
und -Umsetzungsgesetz EU (DSAnpUG-EU)

Sehr geehrter Herr Heveling,

der Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V. (BGA) ist die Spitzenorganisation des Groß- und Außenhandels sowie der unternehmensnahen Dienstleistungen. Ihm gehören 69 Bundesfachverbände sowie Landes- und Regionalverbände an. Der BGA vertritt die Interessen von 125.000 Handels- und Dienstleistungsunternehmen in Deutschland mit 1,9 Millionen Beschäftigten und 60.000 Auszubildenden.

Der BGA hat ein elementares Interesse an einem leistungsfähigen Auskunftswesen. Es ist uns ein wichtiges Anliegen, dass Wirtschaftsauskunfteien ihre für den Groß- und Außenhandel und die Gesamtwirtschaft bedeutende Arbeit auch ab Geltung der Vorschriften der EU-Datenschutzgrundverordnung im Mai 2018 rechtssicher und reibungslos fortführen können.

Die Vorschriften der § 28a und § 28 b BDSG-alt haben sich als Rechtsgrundlagen für die Datenübermittlung an Auskunftsteien und für das Scoring in der Praxis millionenfach bewährt. Wir begrüßen es deshalb ausdrücklich, dass diese Rechtsgrundlagen mit § 31 BDSG-neu (Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften) des Gesetzentwurfs für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU im Wesentlichen beibehalten werden sollen.

Wir weisen jedoch darauf hin, dass die Verwendung des Begriffs „Gläubiger“ in § 31 Abs. 2 Nr. 1 4 c) und Nr. 5 BDSG-E zu Unsicherheit im Rechtsverkehr führen könnte. So sind nach geltendem Recht auch Dritte wie Inkassounternehmen berechtigt, anstelle und im Auftrag des Gläubigers Informationen an Auskunftsteien zu übermitteln. Damit diese Praxis auch in Zukunft rechtssicher fortgeführt werden kann, empfehlen wir, auf den Begriff „Gläubiger“ zu verzichten oder eventuelle Zweifel jedenfalls durch eine Klarstellung in der Gesetzesbegründung auszuräumen.

Zum Aufbau neuer und zum Ausbau bestehender Geschäftsbeziehungen sind die Wirtschaft und gerade der Handel auf den Zugang zu verlässlichen Bonitätsauskünften angewiesen, den sie bei Handels- und Kreditauskunftsteien finden. Allein die Unternehmen des deutschen Großhandels beziehen pro Jahr etwa 2,4 Millionen Auskünfte von Wirtschaftsauskunftsteien,

auf die sie u.a. für das Kreditmanagement und zur Finanzierung angewiesen sind. Mit Bonitätsauskünften leisten Auskunftsteile einen unverzichtbaren Beitrag zur Ausweitung des Warenkreditvolumens durch den deutschen Groß- und Außenhandel, wirken einer Kreditklemme entgegen und wirken als Wachstumstreiber. So tragen sie dazu bei, dass der Großhandel seine Rolle als „Bank des Mittelstands“ erfolgreich ausüben kann.

Wir würden es sehr begrüßen, wenn Sie unsere Einschätzung bei den anstehenden Beratungen berücksichtigen würden. Für Rückfragen und zur Erläuterung unserer Position stehe ich Ihnen jederzeit sehr gern zur Verfügung.

Mit freundlichen Grüßen



Syndikusrechtsanwalt
Alexander Kolodzik

Geschäftsführer
Abteilungsleiter Arbeit, Recht und Dienstleistungen

Stellungnahme

**des Gesamtverbandes der Deutschen Versicherungswirtschaft
zum Regierungsentwurf für ein 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)**

**Gesamtverband der Deutschen
Versicherungswirtschaft e. V.**

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Dr. Martina Vomhof
Leiterin Datenschutz/Grundsatzfragen

E-Mail: m.vomhof@gdv.de

www.gdv.de



Zusammenfassung

Die Wirtschaft braucht möglichst schnell **Rechtssicherheit** über die endgültige Ausgestaltung des neuen Datenschutzrechts. Der vorgelegte Regierungsentwurf ist hierfür eine gute Grundlage, bedarf jedoch einiger Anpassungen.

Der Wunsch nach einer EU-weiten Rechtsvereinheitlichung darf nicht dazu führen, dass die **Nutzung vorgesehener Öffnungsklauseln** unterbleibt, obgleich sie zur praxisgerechten Anwendung des Datenschutzrechts erforderlich ist.

Zudem sollte die Anwendung von Öffnungsklauseln aktiv dazu genutzt werden, den Weg in die **Digitalisierung** gangbar zu machen.

Folgende Regelungen des Regierungsentwurfs sind von erheblicher Bedeutung für die Tätigkeit der Versicherungsunternehmen:

- **Zulässigkeit vollautomatisierter Einzelfallentscheidungen in weiteren Fallkonstellationen**, um die drängende Digitalisierung von Geschäftsprozessen zu ermöglichen, z. B. bei der Schadensregulierung (§ 37 RegE BDSG → dazu 2.1)
- **Rechtssichere Grundlage für die Verarbeitung von Gesundheitsdaten zum Zwecke von Versicherungsstatistiken** (§ 27 RegE BDSG → dazu 2.2)
- **Praxisgerechte Ausnahmen von den Informationspflichten** in besonderen Fällen (§ 29 und § 32 Abs. 1 RegE BDSG → dazu 2.3)
- **Einschränkung der Verarbeitung** statt Datenlöschung bei besonderer Art der Speicherung (§ 35 Abs. 1 RegE BDSG → dazu 2.4)

1. Grundsätzliche Anmerkungen / Wesentliche Anliegen

Die deutsche Versicherungswirtschaft begrüßt, dass die Bundesregierung den Gesetzentwurf zur Anpassung des deutschen Datenschutzrechts an die EU-Datenschutz-Grundverordnung (DSGVO) beschlossen hat und das Gesetzgebungsverfahren in dieser Legislaturperiode abschließen möchte. Es ist notwendig, dass die Unternehmen **möglichst bald Rechtsklarheit über die künftige Ausgestaltung des neuen Datenschutzrechts** erhalten. Sie müssen frühzeitig die Umsetzungsmaßnahmen planen, um ab 25. Mai 2018 das neue Recht anwenden zu können. Spätere Änderungen der Rechtslage können einen erheblichen organisatorischen und finanziellen Mehraufwand zur Folge haben.

Das Datenschutz-Anpassungs- und Umsetzungsgesetz sollte im Rahmen des EU-rechtlich Möglichen dazu beitragen, der deutschen Wirtschaft den **Weg in die Digitalisierung zu erleichtern**. Der von der Verordnung ausdrücklich eingeräumte Regelungsspielraum sollte genutzt werden, um eine zukunftsfähige, **medienbruchfreie Gestaltung von Geschäftsprozessen** zu ermöglichen. Dabei sollte das neue Recht nicht hinter den geltenden Bestimmungen des heutigen BDSG zurückbleiben. Für die Versicherungswirtschaft ist insbesondere eine maßvolle Ausfüllung der in Art. 22 Abs. 2 lit. b DSGVO enthaltenen Öffnungsklausel nach dem Vorbild des § 6a BDSG für **automatisierte Einzelfallentscheidungen** notwendig. Hier enthält § 37 RegE BDSG einen sinnvollen Ansatz, der jedoch ausgebaut werden muss (dazu im Einzelnen 2.1).

Ein **EU-einheitliches Datenschutzrecht** ist grundsätzlich wünschenswert. Das Ziel einer Rechtsvereinheitlichung sollte jedoch keinesfalls dazu führen, auf erforderliche ergänzende Regelungen für die Privatwirtschaft zu verzichten. Die **Nutzung einiger Öffnungsklauseln ist notwendig**, um eine praxisgerechte Anwendung der DSGVO zu gewährleisten. Für das Versicherungsgeschäft von besonderer Bedeutung ist vor allem eine **klare gesetzliche Grundlage für Statistiken mit Gesundheitsdaten** auf der Basis von Art. 9 Abs. 2 lit. j DSGVO (dazu im Einzelnen 2.2).

Transparenz ist zu Recht ein wichtiges Anliegen der EU-Datenschutz-Grundverordnung. Die Versicherungswirtschaft wird sich auf die erhöhten Anforderungen einstellen. Allerdings sind Einschränkungen der Informationspflichten dort erforderlich, wo sie andernfalls (etwa bei der Kriminalitätsbekämpfung) zu ungewollten Ergebnissen führen (dazu im Einzelnen 2.3).

2. Anmerkungen zu einzelnen Bestimmungen

2.1 Erweiterung des Erlaubnistatbestandes für automatisierte Einzelfallentscheidungen (§ 37 RegE BDSG)

Um den Weg in die **Digitalisierung von Geschäftsprozessen** gehen zu können, bedarf es eines nationalen Erlaubnistatbestandes für automatisierte Einzelfallentscheidungen, der nicht hinter § 6a BDSG zurückfällt.

Sowohl auf europäischer Ebene als auch in Deutschland steht das Thema **Digitalisierung** zu Recht weit oben auf der Agenda. Deutsche Unternehmen werden sich im internationalen Wettbewerb nur behaupten können, wenn die **Chance** zur Digitalisierung von datenverarbeitenden Geschäftsprozessen **nicht verpasst** wird. Dies gilt in besonderem Maße für die Versicherungswirtschaft, deren Kerngeschäft die Datenverarbeitung voraussetzt. Kommunikation und **Prozessabläufe** werden in Zukunft in der Versicherungsbranche weiter **automatisiert und medienbruchfrei** gestaltet werden. Vollautomatisierte Entscheidungen können so zu **Kosteneinsparungen** auf Seiten der Unternehmen und zu erheblich **schnelleren Bearbeitungszeiten** im Interesse der Anspruchsteller beitragen.

Beispiel:

Mit voranschreitender Digitalisierung werden Schadenmeldungen per E-Mail, App oder Messenger-Dienste an Bedeutung zunehmen. Versicherungsunternehmen werden in der Lage sein, ihre Verpflichtung zum Ersatz eines Schadens in einer Vielzahl von Fällen und vor allem im Massengeschäft vollautomatisiert abzuwickeln und die Ersatzleistung direkt und ohne weitere Prüfung zu überweisen, wenn der Kunde oder der Geschädigte ausreichende Angaben zum Schaden macht. Damit kann die Schadenabwicklung im Massengeschäft auch zum Wohle der Geschädigten erheblich beschleunigt werden.

2.1.1 Vollautomatisierte Entscheidungen in Drittkonstellationen

Ein wichtiger Schritt in die richtige Richtung ist § 37 Abs. 1 Nr. 1 RegE BDSG. Durch diese Nutzung der Öffnungsklausel des Art. 22 Abs. 2 b) DSGVO werden vollautomatisierte Entscheidungen gegenüber einem geschädigten Dritten, der nicht Vertragspartner des Unternehmens ist, rechtssicher möglich. Das gilt nach dem Regierungsentwurf allerdings nur dann, wenn dem Begehren der Betroffenen stattgegeben wird.

Nicht vollumfänglich stattgebende Entscheidungen

Nicht nachvollziehbar ist, warum der Regierungsentwurf – anders als in § 35 S. 2 des Referentenentwurfs – bis auf den Fall der Leistungsregulie-

rung in der Krankenversicherung **keine Ausnahme mehr für die Fälle** vorsieht, **in denen** mit der Entscheidung **dem Begehren des Betroffenen nicht vollumfänglich stattgegeben wird**.

Werden Ansprüche geltend gemacht, die in ihrer Reichweite vom Leistungsumfang des Versicherers nicht mehr abgedeckt sind, sollte eine vollautomatisierte Entscheidung unter Beachtung der Sicherungsmaßnahmen des Art. 22 Abs. 3 DSGVO ebenfalls möglich sein.

Beispiel:

Nach einem Kfz-Unfall mit einer Reparaturdauer von 2 Tagen werden die Kosten für einen Mietwagen von einer Woche geltend gemacht. In der vollautomatisierten Schadensabwicklung wird schnell gezahlt, jedoch diese Position gekürzt. Der Geschädigte kann sich direkt mit dem Versicherungsunternehmen in Verbindung setzen und eine manuelle Prüfung verlangen, wenn er der Ansicht ist, dass die weitergehenden Mietwagenkosten zu ersetzen sind.

Ist ein Betroffener Vertragspartner des Versicherers (etwa in der Vollkaskoversicherung), ist die Abwicklung eines Schadens im Rahmen des Vertragsverhältnisses nach Art. 22 Abs. 2 lit. a DSGVO vollautomatisiert auch dann zulässig, wenn dem Begehren des Betroffenen nicht vollumfänglich stattgegeben wird. Ist der Betroffene – wie im oben dargestellten Fall – demgegenüber **nicht selbst der Vertragspartner** (z. B. ein Geschädigter in der **Kfz-Haftpflichtversicherung**) greift die Ausnahme der DSGVO nicht ein. Die unterschiedliche Behandlung der Fälle ist nicht nachvollziehbar und sollte – wie in **§ 35 des Referentenentwurfs** geschehen – durch Nutzung der Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO verhindert werden.

Die Regelung würde nicht über das derzeit geltende Recht hinausgehen. Schon jetzt sind automatisierte Einzelfallentscheidungen unabhängig vom Vorliegen eines Vertragsverhältnisses gemäß Art. 15 Abs. 2 RL 95/46/EG und **§ 6a Abs. 2 Nr. 2 BDSG** auch dann **zulässig**, wenn dem Anspruch des Betroffenen nicht oder nicht in vollem Umfang stattgegeben wird. Voraussetzung ist, dass gleichzeitig Maßnahmen ergriffen werden, um die **Rechte der Betroffenen zu wahren**. Den Interessen der Betroffenen kann auch unter Geltung der DSGVO Rechnung getragen werden, indem die Anforderungen des **Art. 22 Abs. 3 DSGVO auf diese Fallgruppe ausgedehnt** werden.

Sonstige Drittkonstellationen

Bedauerlich ist auch, dass der Regierungsentwurf – anders als der Referentenentwurf – **keine Regelung mehr für andere Konstellationen** trifft,

in denen der Betroffene nicht selbst Vertragspartner des Unternehmens ist, und daher Art. 22 Abs. 2 lit. a DSGVO nicht eingreift. Das gilt z. B. für die Rückversicherung oder für die Regulierung von Schäden von mitversicherten Personen, die nicht Vertragspartner des Versicherungsunternehmens sind.

Beispiel:

Ein Rückversicherungsunternehmen entscheidet vollautomatisiert darüber, ob ein Vertrag rückversichert werden kann. Die Entscheidung hat zwar rechtliche Wirkung nur gegenüber dem Erstversicherer. Sie hat aber auch mittelbare Auswirkungen für den Betroffenen, wenn der Erstversicherer die Entscheidung des Rückversicherers zur Grundlage seiner Vertragsentscheidung gegenüber dem Kunden macht.

Für die vergleichbare Fallgruppe der **Regulierung von Ansprüchen mitversicherter Personen** geht die Gesetzesbegründung zwar nachvollziehbar davon aus, dass Art. 22 DSGVO gar nicht einschlägig ist. Um Rechtsunsicherheit zu vermeiden, sollten jedoch **derartige Drittkonstellationen klar im Gesetzestext geregelt** werden. Die Formulierung in **§ 35 des Referentenentwurfs**, die auf eine Entscheidung in einem „sonstigen Rechtsverhältnis“ abstellt, erfasste diese Fälle.

In den Konstellationen, in denen kein Vertrags- oder Rechtsverhältnis mit dem Betroffenen besteht, bliebe anderenfalls künftig als Rechtfertigungsgrund gemäß Art. 22 Abs. 2 lit. c DSGVO nur die **Einwilligung**. Die Einholung einer Einwilligung würde jedoch regelmäßig einen **zusätzlichen Kommunikationsprozess** erfordern, der die Schadenbearbeitung unnötig verkompliziert und die Regulierung verlangsamt. Für Rückversicherungsunternehmen, die keinen direkten Kundenkontakt haben, wäre dieser Weg kaum gangbar.

Die deutsche Versicherungswirtschaft fordert daher

§ 37 Abs 1 RegE BDSG nach dem Vorbild von § 35 S. 2 des Referentenentwurfs auszugestalten.

2.1.2 Maßvolle Regelung für vollautomatisierte Entscheidungen mit Gesundheitsdaten

Sehr zu begrüßen ist, dass mit **§ 37 Abs. 2 RegE BDSG** eine Regelung geschaffen wird, die **vollautomatisierte Entscheidungen, bei denen dem Begehren des Betroffenen stattgegeben wird, auch mit Gesundheitsdaten** ermöglicht. Die Regelung ist über die Krankenversicherung hinaus **auch für andere Sparten von Bedeutung**. Es wird auch in ande-

ren Versicherungszweigen, z. B. bei kleineren Personenschäden in der Haftpflichtversicherung, sowie in der Rückversicherung mit zunehmender Digitalisierung standardisierte automatisierte Entscheidungen geben können.

Beispiel:

Bei einem Unfall mit einem Kfz wird zusätzlich zu dem Sachschaden eine eingescannte Arztrechnung über eine ambulante Behandlung am Unfalltag sowie eine plausible Schilderung der Verletzung elektronisch übermittelt. Versicherer werden in Zukunft den Schaden vollautomatisiert prüfen und damit sehr zügig erstatten können.

In allen Fällen eines Vertragsschlusses oder einer Leistungsregulierung werden **Gesundheitsdaten zu einem klar umgrenzten Zweck verwendet**, etwa um einen Anspruch des Betroffenen zu erfüllen. Da es sich um massenhaft auftretende Fälle handelt, besteht erhebliches Einsparpotential, wenn keine manuelle Prüfung mehr erforderlich ist. Mittels der vollautomatisierten Prüfung kann eine **objektive Entscheidung** gewährleistet und dem **Begehren des Betroffenen schnell entsprochen** werden. Bei Entscheidungen, mit denen einem Antrag stattgegeben wird, sind deren Interessen nicht negativ betroffen. Hier gebietet es der Schutzzweck des Art. 22 DSGVO nicht, die Möglichkeiten des Unternehmens zur automatisierten Verarbeitung einzuschränken.

Der Bedarf für eine Regelung dürfte mit zunehmender Digitalisierung darüber hinaus auch dann bestehen, wenn nur ein Teil der geltend gemachten Leistung reguliert wird, weil der Betroffene etwa auch Ersatz solcher Aufwendungen verlangt, die mit dem eigentlichen Schaden nicht im Zusammenhang stehen.

Beispiel:

Im o. g. Fall enthält die Arztrechnung zusätzlich eine Untersuchung wegen einer Erkältung, die nach vollautomatisierter Prüfung nicht erstattet wird. Diese Position würde von der vollautomatisierten Regulierung ausgenommen. Der Betroffene müsste sich an den Kraftfahrzeug-Haftpflichtversicherer wenden, wenn er der Meinung ist, dass diese Kosten ebenfalls zu ersetzen seien. Dann würde eine manuelle Prüfung erfolgen.

Auch für diese Fälle – die nach der allgemeinen Bestimmung des § 6a BDSG nach aktuell geltendem Recht zulässig sind – wäre aus der Sicht der Versicherungswirtschaft eine Ausnahme vom Verbot der vollautomatisierten Einzelfallentscheidung sehr hilfreich, da die oben genannten Einsparpotentiale auch hier zum Tragen kommen. Die Ausführungen in der Begründung des Regierungsentwurfs gelten hier ebenfalls.

Die deutsche Versicherungswirtschaft

hält die Regelung des § 37 Abs. 2 RegE BDSG für erforderlich.

2.2 Erlaubnisgrundlage für die statistische Verarbeitung von Gesundheitsdaten (§ 27 RegE BDSG)

Die deutsche Versicherungswirtschaft begrüßt, dass der Regierungsentwurf in § 27 RegE BDSG von der in **Art. 9 Abs. 2 lit. j DSGVO** enthaltenen spezifischen Öffnungsklausel Gebrauch macht. Für das Funktionieren des Versicherungsgeschäfts ist eine **gesetzliche Erlaubnisgrundlage für die statistische Verarbeitung von Gesundheitsdaten erforderlich**. Um Rechtssicherheit zu erreichen, bedarf § 27 RegE BDSG jedoch noch einer Anpassung.

Das Versicherungsgeschäft beruht auf dem Erstellen und Auswerten von Statistiken. Die statistische Datenverarbeitung zieht sich durch den gesamten Betriebsablauf eines Versicherungsunternehmens.

Beispiele:

Statistiken werden benötigt, um überhaupt beurteilen zu können, ob bestimmte **Risiken versicherbar** sind und um entsprechende **Tarife zu entwickeln**. So ist es heute etwa möglich, dass mit dem HI-Virus infizierte Menschen eine Risikolebensversicherung abschließen können. Neben besseren Behandlungsmethoden ist dies auf ein besseres Verständnis der Krankheit durch die statistische Auswertung von Krankheitsverläufen zurückzuführen.

Versicherungsunternehmen sind nach den aufsichtsrechtlichen Regelungen der **Solvency-II-Rahmenrichtlinie** verpflichtet, die in ihrem Bestand gehaltenen Risiken zu bewerten und ein dem Risiko entsprechendes Solvenzkapital vorzuhalten. Um die gesetzlichen Vorgaben aus Solvency II zur Angemessenheit, Vollständigkeit und Exaktheit der verwendeten Daten zu erfüllen, ist die Verarbeitung personenbezogener Daten zu statistischen Zwecken notwendig.

Die Erstellung von Statistiken umfasst die Vorbereitung, Erhebung und Aufbereitung statistischen Datenmaterials, wobei in der gängigen Praxis (pseudonymisierte) personenbezogene Daten verwendet werden. Dabei müssen in der Lebens-, Kranken- und Unfallversicherung sowie im Hinblick auf Personenschäden in der Haftpflichtversicherung auch **Gesundheitsdaten** einfließen. Auf Grundlage dieses statistischen Datenmaterials werden in einem zweiten Schritt **statistische Ergebnisse** generiert, **die keinen Personenbezug mehr aufweisen**.

Die **Statistikgesetze des Bundes oder der Länder** können der Privatwirtschaft hier nicht weiterhelfen, weil sie nur die Erstellung von Statistiken erlauben, die Bundes- oder Landeszwecke verfolgen. Nicht-öffentlichen Stellen ist ein Rückgriff auf diese Erlaubnisgrundlagen verwehrt.

Eine **vollständige Anonymisierung der der Statistik** zugrundeliegenden Daten ist ebenfalls nicht möglich, da so Datensätze im weiteren Schadensverlauf nicht mehr ergänzt werden könnten. Zudem ist für die Qualitätssicherung der Statistik ein gezielter Rückgriff auf einzelne Datensätze erforderlich.

Schließlich stellt es keine Lösung dar, für die statistische Verarbeitung von Gesundheitsdaten jeweils die **Einwilligung** des Betroffenen einzuholen. Erfahrungsgemäß ist die Resonanz auf eine entsprechende Bitte um Einwilligung zur Datenerhebung und Verarbeitung äußerst gering, wenn mit der Einwilligung kein unmittelbarer Nutzen für Kunden oder Geschädigte erkennbar ist. Dies ist hier der Fall: Für den einzelnen Kunden bzw. Anspruchsberechtigten steht die Statistikarbeit der Versicherer naturgemäß nicht im Vordergrund. Die Versicherungsunternehmen stützen auf die statistischen Auswertungen jedoch Entscheidungen, die am Ende die Erfüllbarkeit aller Verträge betreffen können.

Im Gegensatz zu § 22 Abs. 1 Nr. 1 lit. d des Referentenentwurfs setzt § 27 Abs. 1 RegE BDSG für die Zulässigkeit der statistischen Verarbeitung ein **„erhebliches Überwiegen“ der Interessen des Verantwortlichen** voraus. Der unbestimmte Rechtsbegriff der „Erheblichkeit“ führt zu großer **Rechtsunsicherheit** bei der Frage, wann die Voraussetzungen dieses gesetzlichen Erlaubnistatbestandes vorliegen. Angesichts der **klaren Entscheidung der EU-Datenschutz-Grundverordnung für eine grundsätzliche Zulässigkeit der statistischen Datenverarbeitung**, z. B. in Art. 5 Abs. 1 lit. b und Art. 89 DSGVO, ist diese **Einschränkung nicht gerechtfertigt**. Entscheidend ist nach Art. 9 Abs. 2 lit. j DSGVO, dass der Wesensgehalt des Rechts auf Datenschutz gewahrt wird und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen werden. Derartige Maßnahmen schafft § 27 RegE BDSG bereits, indem er neben den hohen Anforderungen des Art. 89 DSGVO durch den Verweis auf § 22 Abs. 2 RegE BDSG weitere Schutzvorkehrungen trifft.

Daher regt die Versicherungswirtschaft an,

bei der Ausfüllung des Art. 9 Abs. 2 lit. j DSGVO in § 27 RegE BDSG nicht auf ein erhebliches, sondern auf ein einfaches Überwiegen der Interessen des Verantwortlichen abzustellen, da die Norm bereits angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und der Interessen der betroffenen Person trifft.

2.3 Praxisgerechte Einschränkungen der Informationspflichten des Art. 13 DSGVO (§ 29 und § 32 RegE BDSG)

Nötig sind praxisgerechte Regelungen, die die Informationspflichten nach Art. 13 DSGVO für bestimmte Situationen einschränken. § 29 und § 32 Abs. 1 RegE BDSG enthalten dazu einen richtigen Ansatz.

Die Versicherungswirtschaft **erkennt** an, dass die Herstellung einer **größeren Transparenz** für den Betroffenen ein Bedürfnis der europäischen Gesetzgeber war. Gleichwohl gibt es Situationen, in denen die Daten ihrem Wesen nach geheim gehalten werden müssen, sich der mit der Wahrung der Transparenz verbundene **Aufwand als unverhältnismäßig** erweist oder aber der mit der **Verarbeitung verbundene Zweck durch die Information vereitelt** würde.

Art. 14 Abs. 5 lit. b DSGVO regelt eine Ausnahme von den Informationspflichten nach Art. 14 DSGVO, wenn die Daten bei Dritten erhoben wurden. Für die Beurteilung der Geheimhaltungsbedürftigkeit oder eines unverhältnismäßigen Aufwands kann es aber keinen Unterschied machen, ob die Daten beim Betroffenen oder aber bei einem Dritten erhoben wurden. Dies trifft insbesondere auch auf die Fälle zu, in denen die personenbezogenen Daten zulässigerweise zweckändernd verarbeitet werden.

Beispiel:

Hat ein Versicherungsunternehmen eindeutige Hinweise darauf, dass ein Kunde **Versicherungsbetrug** begangen hat, gibt es die Kundendaten an die Polizei weiter. Die Übermittlung stellt eine (Weiter-)Verarbeitung i. S. d. Art. 13 Abs. 3 DSGVO dar. Daher müsste das Unternehmen den Betroffenen über die Weitergabe der Daten informieren, während die Polizei selbst von der Informationspflicht befreit wäre. Durch die Information des potentiellen Betrügers würden womöglich die Ermittlungen unterlaufen.

Die Versicherungswirtschaft

hält die in den §§ 29 und 32 RegE BDSG enthaltenen Einschränkungen der Informationspflichten für notwendig und angemessen.

2.4 Einschränkung der Verarbeitung statt Datenlöschung wegen der besonderen Art der Speicherung (§ 35 Abs. 1 RegE BDSG)

Sinnvoll erscheint die in § 35 Abs. 1 RegE BDSG vorgesehene Ausnahme von der in Art. 17 Abs. 1 DSGVO geregelten Löschverpflichtung. Wenn eine **Löschung wegen der besonderen Art der Speicherung nicht**

oder nur mit unverhältnismäßig hohem Aufwand möglich ist, sollte es ausreichen, die weitere Verarbeitung der Daten einzuschränken.

Macht ein Betroffener sein Recht auf Löschung geltend, kann es in der Praxis technische Hürden geben, die ein gezieltes Löschen einzelner personenbezogener Daten nicht erlauben.

Beispiele:

Bei der früher gebräuchlichen **Archivierung auf Mikrofiche**, die für langfristige Verträge (z. B. in der Lebensversicherung) immer noch praktische Bedeutung hat, ist es nicht möglich, einzelne Informationen vom Mikrofiche zu entfernen.

Es gibt **revisionssichere Speicher**, die ein physisches Löschen einzelner Datensätze verhindern, um so den Anforderungen an eine revisionssichere Archivierung gerecht zu werden. Hier kann nur der Zugriff auf einzelne Datensätze unterbunden werden.

Bei bestimmten Datenbankkonzepten ist es nicht möglich, einzelne Datensätze zu löschen, ohne dass die **Datenbankstruktur** aufgrund der darin enthaltenen Verweise zerstört wird. Hier könnten aber einzelne Datensätze so markiert werden, dass sie von der Verarbeitung zukünftig ausgeschlossen werden und für den Datenbanknutzer nicht mehr sichtbar sind.

Für die oben genannten Fälle ist eine Regelung erforderlich, die es nach dem **Vorbild von § 35 Abs. 3 Nr. 3 BDSG** genügen lässt, anstatt einer physischen Entfernung der Daten diese von der weiteren Verarbeitung auszuschließen. Werden die Daten für die weitere Verarbeitung gesperrt, stehen diese für die Zukunft dem operativen Geschäft nicht mehr zur Verfügung und sind nicht mehr einsehbar. Dem **Schutzbedürfnis des Betroffenen** wird damit entsprochen.

Die Versicherungswirtschaft

hält die in § 35 Abs. 1 RegE BDSG enthaltene Einschränkung der Löschpflicht für notwendig und angemessen.

Berlin, den 14. Februar 2017

**Stellungnahme
zu Artikel 1
des Entwurfs der Bundesregierung für ein Datenschutz-Anpassungs-
und -Umsetzungsgesetz EU (DSAnpUG-EU¹), BT-Drs. 18/11325
vom 24. Februar 2017**

(Stand: 22.03.2017)

I. Allgemein

1. Zur Vermeidung von Rechtsunsicherheit benötigen Wirtschaft und Verwaltung eine Verabschiedung der Begleitgesetzgebung noch in dieser Legislaturperiode.

Für die Umsetzung des neuen Datenschutzrechts ab dem 25. Mai 2018 durch die Unternehmen und die öffentliche Verwaltung ist es von sehr hoher Bedeutung, dass das vorliegende Gesetzesvorhaben bis zum Sommer 2017 abgeschlossen wird. Nur so erhalten die datenverarbeitenden Stellen rechtzeitig Rechtsklarheit und Rechtssicherheit, in welchen Bereichen von den Gestaltungsmöglichkeiten der EU-Datenschutz-Grundverordnung 2016/679 (DS-GVO) im nationalen Recht Gebrauch gemacht wird. Eine spätere Begleitgesetzgebung zur DS-GVO könnte von den datenverarbeitenden Stellen faktisch nicht mehr bis zum Mai 2018 berücksichtigt werden.

2. Die Begriffsbestimmung „anonymisieren“ sollte aufgenommen werden.

Die Verwendung eines Begriffes, der bislang weder in der DS-GVO noch im BDSG-E definiert wird, wird zu Interpretationsschwierigkeiten bei Wirtschaft und Verwaltung und damit zu Rechtsunsicherheiten führen. In den §§ 27 III, 28 I, § 50 und § 71 I BDSG-E wird der Begriff „anonymisieren“ erwähnt. Ausgehend von der Vorbildfunktion, die eine bundesdeutsche Gesetzgebung bei der Umsetzung in Europa haben wird, ist die Definition dieser Begrifflichkeit für die Umsetzung der DS-GVO wie auch für die RL 2016/680 zu empfehlen. Dabei kann auch auf die bestehende Begriffsbestimmung aus § 3 Abs. 6 BDSG zurückgegriffen werden.

¹ Voller Titel: „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“

Postanschrift

Düsseldorfer Str. 40
65760 Eschborn

Kommunikation

Tel: (0 61 96) 777 26-0

Fax: (0 61 96) 777 26-51

E-Mail: info@awv-net.de

Internet: <http://www.awv-net.de>

3. Der Regierungsentwurf führt Regelungen des heutigen BDSG im Rahmen des EU-rechtlich Möglichen fort und schließt in konkretisierender Weise Regelungslücken der DS-GVO.

Das Anliegen der Bundesregierung ist sehr zu unterstützen, mit den Regelungen in § 4 und §§ 22 bis 38 BDSG-E im Rahmen des EU-rechtlich Möglichen bewährte Vorschriften aus dem heutigen BDSG weiterzuführen. Damit wird die - auch von Herrn Prof. Roßnagel (jahrelanger Berater der Bundesregierung in IT- und Datenschutzfragen) festgestellte - „Unterkomplexität“ der DS-GVO unter Berücksichtigung der Betroffenenrechte in einem vernünftigen Maß ausgefüllt und Kontinuität im Datenschutzrecht erreicht. Beispielsweise gewährleistet eine möglichst weitgehende Fortführung der Ausnahmetatbestände bei den Informations- und Auskunftspflichten nach den heutigen §§ 33 Absatz 2 und 34 Absatz 7 BDSG, dass der Umstellungsaufwand für die datenverarbeitenden Stellen nicht höher ausfällt als wirklich notwendig. In der Gesamtbetrachtung aller zu berücksichtigenden Grundrechte der involvierten Parteien liegt ein angemessener Ausgleich zwischen dem informationellen Selbstbestimmungsrecht des Betroffenen einerseits und Schutzgütern von verfassungsrechtlichem Rang der datenverarbeitenden Stellen (z.B. Wahrung von Geschäftsgeheimnissen) andererseits. Der Grundsatz des Übermaßverbots hat auch im Lichte der DS-GVO weiterhin seine Berechtigung.

4. Der „one-stop-shop“-Ansatz der DS-GVO bei der Datenschutzaufsicht sollte auch bei rein innerstaatlichen Sachverhalten etabliert werden.

Wie auch vom Bundesrat in seinem Votum vom 10. März 2017 unter Ziffer 12 zu § 19 BDSG-E (vgl. BR-Drs.110/17) vorgeschlagen, sollte der „one-stop-shop“-Ansatz der DS-GVO auch bei innerstaatlichen Sachverhalten mit bundesweiter Bedeutung etabliert werden, da laut Regierungsentwurf die föderale Struktur der Datenschutzaufsicht beibehalten werden soll. Denn für grenzüberschreitende Sachverhalte innerhalb der Europäischen Union gelten spezielle Bestimmungen zur grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden (vgl. Artikel 56 und 60 ff. DS-GVO). Wählt ein EU-Mitgliedstaat - wie hier Deutschland - eine föderale Aufsichtsstruktur im Inland, so muss im Wege des Erstrechtsschlusses auch innerstaatlich das Gleiche gelten wie im EU-Kontext. Dementsprechend sollte § 19 BDSG-E wie vom Bundesrat vorgeschlagen ergänzt werden, um eine Regelung zur federführenden Zuständigkeit einer Datenschutzbehörde in den Fällen zu erhalten, in denen Aufsichtsfragen über die Grenzen eines Bundeslandes hinaus Bedeutung haben (z.B. bei bundesweit agierenden Unternehmen oder länderübergreifend einheitlich nutzbaren Produkten).

II. Zu einzelnen Vorschriften

1. § 20 BDSG-E: Der Rechtsweg im Bußgeldverfahren sollte die Komplexität des Datenschutzrechts und den hohen Bußgeldrahmen der DS-GVO berücksichtigen.

Angesichts des sehr hohen Bußgeldrahmens in Artikel 83 DS-GVO sollte die bislang im Regierungsentwurf vorgesehene Zuständigkeit von Amtsgerichten bei der Ahndung von Verstößen gegen das Datenschutzrecht überdacht werden. Die Bußgeldvorschriften der DS-GVO lehnen sich in der Höhe an entsprechende Regeln im EU-Kartellrecht an. Betrachtet man das Kartellrecht, so fällt auf, dass für dortige Bußgeldverfahren ein besonderer Rechtsweg geregelt ist, um bei den Gerichten Fachzuständigkeiten zu haben. So regeln die §§ 81 und 83 GWB in Bußgeldsachen

die Zuständigkeit des Oberlandesgerichts, in dessen Bezirk die zuständige Aufsichtsbehörde ihren Sitz hat. Angesichts des sehr hohen Bußgeldrahmens der DS-GVO und zur Gewährung eines effektiven Rechtsschutzes sollte der Rechtsweg zumindest ab einer bestimmten Bußgeldhöhe (z.B. 100.000 Euro) derart gestaltet werden, dass auf das Datenschutzrecht spezialisierte Spruchkörper bei einem Amtsgericht oder bei einer höheren Eingangsinstanz zuständig sind.

2. § 24 BDSG-E: Die Fortführung von Vorschriften zur Zweckänderung ist sinnvoll.

Die vorgesehenen Regeln in § 24 BDSG-E über zulässige Zweckänderungen sind im Lichte des Artikels 6 Absatz 4 DS-GVO zu begrüßen. Sie greifen zu Recht die bislang im BDSG enthaltenen Vorschriften auf und schaffen damit Kontinuität und Rechtssicherheit für die verarbeitenden Stellen, ohne das informationelle Selbstbestimmungsrecht des Betroffenen unverhältnismäßig zu beeinträchtigen. Doch sollte in der Vorschrift deutlicher werden, dass diese nicht abschließend sind, sondern die anderen Fälle der zulässigen Zweckänderung aus Artikel 6 Absatz 4 DS-GVO unberührt bleiben.

3. § 26 BDSG-E: Die „Kleine Lösung“ des BDSG für Regelung des Beschäftigungsdatenschutzes reicht zunächst.

Der Ansatz, den heutigen § 32 BDSG mit § 26 Absatz 1 BDSG-E fortzuführen, ist zu begrüßen, da damit rechtliche Kontinuität und Sicherheit geschaffen sowie der Anpassungsaufwand für Unternehmen und Verwaltung begrenzt wird. Aufgrund der kurzen Zeit in der aktuellen Legislaturperiode würde man das Gesetzesvorhaben ansonsten völlig überfrachten.

Zu den einzelnen Regelungen ist Folgendes anzumerken:

Einwilligungslösung erhalten

Mit § 26 Absatz 2 BDSG-E soll der Grundsatz der Freiwilligkeit von Einwilligungen im Kontext von Beschäftigungsverhältnissen geregelt werden. Zu unterstützen ist die damit verbundene Aussage, dass Einwilligungen auch im Beschäftigungsverhältnis weiter möglich bleiben. Jedoch sollte die Regelung zur Einwilligung im Sinne eines schlankeren Gesetzestextes auf das Notwendige beschränkt werden, damit auch die diesbezügliche Rechtsprechung der Arbeitsgerichte fortgelten kann.

Textform statt Schriftform der Einwilligung

Mit Blick auf die Digitalisierungsstrategie der Bundesregierung und der zunehmenden Bedeutung von digitalen Arbeitsabläufen erscheint die Anordnung der Schriftform nicht nur anachronistisch, sondern überzogen restriktiv, weil die DS-GVO gerade nicht die Schriftform für die Einwilligung verlangt. Auch sind die Beschäftigten im Datenschutzrecht durch das umfassende Widerrufsrecht zusätzlich geschützt, sodass für die Einwilligung die Textform als ausreichend anzusehen ist. Darüber hinaus ist der Verantwortliche schon im Interesse seiner Nachweispflicht gehalten, die Einwilligung in nachvollziehbarer Weise zu dokumentieren. Es wird folgende Formulierung von Absatz 2 vorgeschlagen:

„Die Verarbeitung personenbezogener Daten von Beschäftigten kann auch auf der Grundlage einer Einwilligung erfolgen. Die Einwilligung bedarf der Textform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.“

Steuerrechtliche Zwecke berücksichtigen

Die in § 26 Absatz 3 BDSG-E enthaltene Regelung ist sinnvoll, um eine im Beschäftigungsverhältnis häufig erforderliche Verarbeitung sensibler Daten weiter möglich zu machen. Zur Klarstellung sollte erwogen werden, auch den Zweck „Pflichten aus dem Steuerrecht“ als Rechtfertigungsgrund aufzunehmen, da z.B. die Verarbeitung von Daten über den Familienstand und die Religionszugehörigkeit im Rahmen des Beschäftigungsverhältnisses gewährleistet bleiben muss.

Kollektivvereinbarungen als Erlaubnistatbestand

Sehr zu unterstützen ist auch § 26 Absatz 4 BDSG-E, wonach die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch auf der Grundlage von Kollektivvereinbarungen zulässig bleibt (vgl. Erwägungsgrund 155 DS-GVO).

Erweiterung des Beschäftigtenbegriffs um Leiharbeitnehmer

Die im § 26 Absatz 8 Nr. 1 BDSG-E vorgesehene Klarstellung, dass Leiharbeitnehmer nicht nur im Verhältnis zum Verleiher, sondern auch im Verhältnis zum Entleiher als Beschäftigte gelten, sollte beibehalten werden. Mit der Begriffsbestimmung im BDSG erfolgt lediglich eine Klarstellung, dass für die Verarbeitung der Daten der Leiharbeitnehmer im Rahmen der Entleiherung auch beim Entleiher die gleichen Grundlagen und Maßstäbe anzuwenden sind, wie bei Arbeitnehmern des Entleihers. Eine Differenzierung wäre hier bürokratiefördernd, nicht interessensgerecht und führt zu rechtlichen Unsicherheiten. So wäre ohne Aufnahme der Leiharbeitnehmer in die Begriffsbestimmungen beispielsweise bei dem Vorgehen eines Arbeitgebers zur Aufdeckung einer Straftat die Regelung aus § 26 Abs. 1 Satz 2 bei Leiharbeitnehmern nicht anwendbar. Auch bliebe ohne diese Klarstellung offen, inwieweit die Regelung aus § 26 Abs. 3 über die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses dann auch auf Leiharbeitnehmer zulässig anzuwenden wäre. Rechtsunsicherheiten wären die Folge.

Die arbeitsrechtliche Stellung der Leiharbeitnehmer wird durch diese Klarstellung nicht tangiert: Auch bisher können beispielsweise Leiharbeitnehmer nach § 7 Satz 2 BetrVG auch aktiv an Betriebsratswahlen teilnehmen. Allein dadurch eröffnet sich bereits die Zuständigkeit eines Betriebsrates auch für diese Gruppe im Rahmen der mitbestimmungsrechtlichen Regelungen, deren Interessen wahrzunehmen. Die Aufnahme in die Begriffsbestimmungen der Beschäftigten führt lediglich zum erforderlichen rechtssicheren Umgang des Entleihers mit den Daten der Leiharbeitnehmer.

4. § 32 BDSG-E: Ein angemessener Interessenausgleich bei der Konkretisierung des Umfangs der Informationspflichten nach Artikel 13 DS-GVO ist zu unterstützen.

Der Ansatz der Gesetzesvorlage ist sehr zu unterstützen. Zutreffend wird erkannt, dass im Vergleich zur heutigen Rechtslage die Informationspflicht nach Artikel 13 DS-GVO zu einer höheren Formalisierung der Informationserteilung durch Unternehmen und Verwaltung gegenüber dem Betroffenen führen kann. Wie mit Absatz 1 zutreffend festgestellt wird, gibt es Sachverhalte, in denen eine Unterrichtung zum Zeitpunkt der Erhebung der Daten einen unverhältnismäßigen Aufwand darstellt oder die Geltendmachung rechtlicher Ansprüche beeinträchtigen würde.

5. § 33 BDSG-E: Die vorgesehene Übernahme weiterer Ausnahmen bei den Informationspflichten aus dem heutigen § 33 Absatz 2 BDSG ist sinnvoll.

Die Ausnahmen in § 33 Absatz 1 Nr. 2 BDSG-E sind sachgerecht und eine erforderliche Konkretisierung der DS-GVO. Jedoch fehlt die Übernahme der bisherigen Ausnahmeregelungen des § 33 Absatz 2 Nr. 2, Nr. 7a, und 7b, 8a und 8b BDSG zu gesetzlichen Aufbewahrungspflichten und zur Übernahme von Daten aus öffentlichen Quellen. Viele Unternehmen (z.B. Kreditinstitute) sind aufgrund der Vorgaben zur Compliance und zur Geldwäschebekämpfung gehalten, Daten auch aus öffentlichen Quellen zu erheben. Eine Unterrichtung der davon Betroffenen könnte im Spannungsfeld zu den Zwecken Compliance und Geldwäschebekämpfung stehen. Deshalb sollten diese bisherigen Ausnahmetatbestände fortgeführt werden, zumindest bei Verfolgung der genannten Zwecke.

6. § 34 BDSG-E: Es wird ein angemessener Interessenausgleich beim Auskunftsrecht der betroffenen Person erreicht.

Die in § 34 Absatz 1 BDSG-E vorgesehenen Ausnahmen knüpfen an den heutigen § 33 Absatz 2 BDSG an. Diese sind eine sehr sinnvolle Konkretisierung der DS-GVO und äußerst wichtig, um den Anpassungsaufwand für speichernde Stellen unter Berücksichtigung der Güterabwägung auf ein vernünftiges Maß zu begrenzen. Dazu Folgendes zur Verdeutlichung bezugnehmend auf § 34 Absatz 1 Nr. 2 BDSG-E: Solche Daten, die nur noch zur Erfüllung von gesetzlichen Aufbewahrungspflichten vorhanden sind, sind heute schon gesperrt und damit nicht im laufenden Geschäftsbetrieb eines Unternehmens relevant (= „nicht operativer Datenbestand“). Weder für die speichernde Stelle noch für den Betroffenen haben solche „nicht operativen Daten“ eine aktuelle Bedeutung. Somit macht es auch aus der Sicht des Betroffenen keinen Sinn, solche Daten – ggf. mit großem Aufwand auf Seiten der speichernden Stelle (z.B. nachträgliche Digitalisierung von Mikrofilmen [micro fiches]) – zu beauskunften. Dieser Bewertung trägt § 34 Absatz 1 Nr. 2 BDSG-E zutreffend Rechnung.

7. § 35 BDSG-E: Die Weiterführung der heutigen Sperrmöglichkeit im Rahmen der Löschungspflichten erleichtert die Umsetzung der DS-GVO in den Unternehmen.

Der § 35 Absatz 1 Satz 1 BDSG-E regelt zutreffend, dass eine Löschung auch dann nicht verlangt werden kann, wenn diese wegen der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich wäre. Die Vorschrift führt zur Rechtssicherheit und trägt dem allgemeinen Grundsatz Rechnung, dass das Recht nicht Unmögliches verlangen darf und hat klarstellende Wirkung. Satz 1 normiert insofern einen Fall der (wirtschaftlichen) Unmöglichkeit und erlaubt dort eine Sperre als Alternative, wo aus verarbeitungstechnischen Gründen eine Löschung nicht durchgeführt werden kann. Dies ist sachgerecht und trägt den Interessen des Betroffenen Rechnung. Denn gesperrte Daten sind für den laufenden Geschäftsbetrieb nicht mehr ohne weiteres zugänglich. Auch damit lässt sich der technische Umsetzungsaufwand bei den speichernden Stellen deutlich beschränken und unnötige Kosten vermeiden, ohne das informationelle Selbstbestimmungsrecht des Betroffenen zu beeinträchtigen.

8. § 37 BDSG-E: Erweiterung auch auf nicht vollumfänglich stattgebende Entscheidungen

Um den Weg in die Digitalisierung von Geschäftsprozessen gehen zu können, bedarf es eines nationalen Erlaubnistatbestandes für automatisierte Einzelfallentscheidungen, der nicht hinter § 6a BDSG zurückfällt. Ein wichtiger Schritt in die richtige Richtung ist § 37 Abs. 1 Nr. 1 BDSG-E. Durch diese Regelung werden vollautomatisierte Entscheidungen gegenüber geschädigten Dritten, die nicht selbst Vertragspartner eines Versicherungsunternehmens sind, rechtssicher möglich. Das gilt nach dem Regierungsentwurf allerdings nur dann, wenn mit der Entscheidung dem Begehren des Betroffenen stattgegeben wird.

Nicht nachvollziehbar ist, warum nicht auch Entscheidungen erlaubt werden, bei denen dem Begehren des Betroffenen nicht vollumfänglich stattgegeben wird. Während nach Art. 22 Abs. 2 lit. a DS-GVO die vollautomatisierte Abwicklung eines Schadens im Rahmen des Versicherungsvertragsverhältnisses auch dann zulässig ist, wenn dem Begehren des Betroffenen nicht vollumfänglich stattgegeben wird, ist dies gegenüber einem geschädigten Dritten nach § 37 Abs. 1 Nr. 1 BDSG-E nicht möglich, obwohl hier eine vergleichbare Interessenlage vorliegt. Die Rechte und Freiheiten der betroffenen Person werden offensichtlich durch den Verantwortlichen nicht tangiert, wenn dem Antrag der betroffenen Person in einem automatisierten Entscheidungsprozess stattgegeben wird.

Beim Einstieg in einen automatisierten Einzelfallentscheidungsprozess steht das Ergebnis der Entscheidung noch nicht fest. Stellt sich heraus, dass mit der Entscheidung dem Begehren des Betroffenen nicht vollumfänglich stattgegeben werden kann, müsste der gesamte automatisierte Ablauf gestoppt und die Angelegenheit einem Sachbearbeiter überwiesen werden. Es verzögert sich also die gesamte Schadenabwicklung. Für beide Seiten günstiger ist es hingegen, wenn die Entscheidung zunächst elektronisch fällt und der Betroffene sich, soweit er mit der gefällten Entscheidung nicht einverstanden ist, zur erneuten Überprüfung an den Versicherer wenden kann. Deshalb sollten vollautomatisierte Entscheidungen auch dann möglich sein, wenn vom Geschädigten Ansprüche geltend gemacht werden, die in ihrer Reichweite vom Leistungsumfang des Versicherers nicht mehr abgedeckt sind.

Die unterschiedliche Behandlung der Fälle trotz gleicher Interessenslage ist nicht nachvollziehbar und sollte durch Nutzung der Öffnungsklausel des Art. 22 Abs. 2 lit. b DS-GVO verhindert werden. Den Interessen der Betroffenen kann dabei Rechnung getragen werden, indem die Anforderungen des Art. 22 Abs. 3 DS-GVO auf diese Fallgruppe ausgedehnt werden.

Generell sollte überlegt werden, ob die Formulierung des § 37 Abs. 1 nicht enger an den Wortlaut des § 6a BDSG angelehnt werden kann, um über die Leistungserbringung in der Versicherungswirtschaft hinaus auch andere mögliche Drittkonstellationen zu erfassen.

9. § 41 BDSG-E: Aus dem Gesetz sollte deutlich werden, dass Mitarbeiter von Unternehmen nicht Sanktionsadressaten nach Artikel 83 DS-GVO sind.

Mit § 41 Absatz 1 BDSG-E werden die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß für anwendbar erklärt. Aus der gewählten Formulierung wird nicht hinreichend deutlich, dass die sehr hohen und am Wettbewerbsrecht orientierten Sanktionsmöglichkeiten der DS-GVO sich ausschließlich an Verantwortliche oder an Auftragsverarbeiter richten, nicht aber an die Mitarbeiter der jeweiligen Stellen. Eine Einbeziehung von Mitarbeitern in die Bußgeldregeln mit

gleich hohem Bußgeldrahmen wäre unangemessen. Denn würden die persönlichen Bußgeldrisiken von Mitarbeitern derart hoch angesetzt, dann könnte beispielsweise die Ausübung des Amtes des betrieblichen Datenschutzbeauftragten wegen möglicher Existenzgefährdung für Mitarbeiter unattraktiv werden. Insofern sollte in Anknüpfung an Artikel 83 DS-GVO der § 41 Absatz 1 Satz 1 BDSG-E auf Verantwortliche und Auftragsverarbeiter wie folgt begrenzt werden:

„Für Verstöße eines Verantwortlichen oder eines Auftragsverarbeiters nach Artikel 83 Absätze 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.“

10. Überprüfung der Begrifflichkeiten bei Umsetzung der RL 2016/680

In den §§ 64 Abs. 1, 65 Abs. 1 und 66 Abs.1 BDSG-E werden in Umsetzung der RL 2016/680 neue Begrifflichkeiten eingeführt: Dort ist nun von „erheblicher Gefahr für Rechtsgüter betroffener Personen“ statt „(hohe) Risiken für die Rechte und Freiheiten betroffener Personen“ wie in Art. 29-31 der RL 2016/680 bei den vergleichbaren Regelungen. Es wird angeregt zu prüfen, inwieweit hier ein redaktioneller Fehler vorliegt. Die Beibehaltung hätte Rechtsunsicherheiten für die Verantwortlichen, deren Auftragsverarbeiter, die zuständigen Aufsichtsbehörden und nicht zuletzt für die betroffenen Personen zur Folge.

Stellungnahme

der Deutschen Krankenhausgesellschaft

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)**

BR-Drucksache 110/17 (Beschluss)

vom 23. März 2017

Inhaltsverzeichnis

Allgemeiner Teil.....	3
Besonderer Teil	4
Artikel 1 - Bundesdatenschutzgesetz - BDSG	4
Zu Ziffer 19; Zu Artikel 1 (§ 22 Absatz 2 Satz 3 BDSG-E)	
Verarbeitung besonderer Kategorien personenbezogener Daten	4
Zu Ziffer 21 und Ziffer 23; Zu Artikel 1 (§ 24 Absatz 1 Nummer 2 BDSG-E)	
Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen	5
Zum Gesetzentwurf allgemein; Zu Artikel 1 (§ 24 Absatz 2 Nummer 2 BDSG-E)	
Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen	6
Zu Ziffer 32; Zu Artikel 1 (§ 29 Absatz 3 BDSG-E)	
Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten	7
Zu Ziffer 39; Zu Artikel 1 (§ 32 Abs. 1 Nr. 1 BDSG-E)	
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	8
Zum Gesetzentwurf allgemein; Zu Artikel 1 (§ 40 Abs. 4 BDSG-E)	
Aufsichtsbehörden der Länder	11
Weiterer gesetzlicher Handlungsbedarf	13

Allgemeiner Teil

Unmöglichkeit umfassender Bewertung

Die eindeutigen Worte des Bundesrates sind zu begrüßen, dass eine umfassende Bewertung der vorgeschlagenen Neufassung des BDSG zum aktuellen Zeitpunkt nicht möglich ist. Die notwendigen Anpassungen des vorrangigen Fachrechts sind noch in keiner Weise absehbar, weshalb der konkrete Anwendungsbereich des Gesetzentwurfs zu großen Teilen im Unklaren bleibt.

Die Unsicherheiten im Krankenhausbereich hinsichtlich der notwendigen Anpassungen sind dadurch zum aktuellen Zeitpunkt erheblich.

Besonderer Teil

Artikel 1

Bundesdatenschutzgesetz – BDSG

Zu Ziffer 19; Zu Artikel 1 (§ 22 Absatz 2 Satz 3 BDSG-E)

Verarbeitung besonderer Kategorien personenbezogener Daten

Beabsichtigte Neuregelung

Gemäß § 22 Absatz 2 BDSG-E sind bei der Verarbeitung besonderer Kategorien personenbezogener Daten angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen. Dazu können insbesondere auch die Pseudonymisierung und Verschlüsselung der personenbezogenen Daten gehören.

Von der Ergreifung derartiger Maßnahmen ist in § 22 Absatz 2 Satz 3 BDSG-E explizit ausgenommen die Verarbeitung personenbezogener Daten, die zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich oder aufgrund eines Vertrages der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist, und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

Nach der Stellungnahme des Bundesrates soll diese Ausnahmeregelung in § 22 Absatz 2 Satz 3 BDSG-E gestrichen werden.

Stellungnahme

Die in § 22 Absatz 2 Satz 3 BDSG-E vorgesehene Ausnahmeregelung für die Fälle des § 22 Absatz 1 Nummer 1 Buchstabe b BDSG-E ist insbesondere für den Bereich der Heilbehandlung in Krankenhäusern zu Recht erfolgt. Die im Rahmen der Krankenhausbehandlung notwendige Datenverarbeitung kann bereits aus Gründen der Patientensicherheit keinesfalls mit spezifischen Maßnahmen, wie einer Pseudonymisierung und Verschlüsselung der personenbezogenen Daten, belastet werden, da damit eine nicht hinnehmbare Verwechselungsgefahr einhergehen würde. Die Interessen der hiervon betroffenen Patienten werden ausreichend dadurch gewahrt, dass die personenbezogenen Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden. Die Ausnahmeregelung in § 22 Absatz 2 Satz 3 BDSG-E sollte daher nicht gestrichen, sondern beibehalten werden.

Änderungsvorschlag

§ 22 Absatz 2 Satz 3 BDSG-E verbleibt wie folgt:

Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 1 Buchstabe b keine Anwendung.

Zu Ziffer 21 und Ziffer 23; Zu Artikel 1 (§ 24 Absatz 1 Nummer 2 BDSG-E) **Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen**

Beabsichtigte Neuregelung

Nach § 24 Absatz 1 Nr. 2 BDSG-E ist die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen zu einem anderen Zweck als zu demjenigen zulässig, zu dem die Daten erhoben wurden, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

Nunmehr soll gemäß der Stellungnahme des Bundesrates das Wort „rechtlicher“ durch „zivilrechtlicher“ ersetzt und nach dem Wort „Ansprüche“ sollen die Wörter „gegenüber der betroffenen Person“ eingefügt werden.

Stellungnahme

Auch wenn die DSGVO nicht gesetzliche Zweckänderungsregelungen zur Durchsetzung „aller“ rechtlichen Ansprüche ermöglicht, sind die Formulierungen „zivilrechtlicher“ Ansprüche „gegenüber der betroffenen Person“ für den Krankenhausbereich in entscheidendem Maße zu eng.

Machen Krankenhausträger beispielsweise Ansprüche auf Übernahme der Behandlungskosten gesetzlich krankenversicherter Patienten gerichtlich geltend, tun sie dies nicht gegenüber dem betroffenen Patienten, sondern gegenüber der jeweiligen Krankenkasse. Nach dem im Recht der gesetzlichen Krankenversicherung geltenden Sachleistungsprinzip ist Kostenträger der medizinischen Leistungen die Krankenkasse. Dabei befindet sich das Krankenhaus im Regime des Sozialrechts. Nach der vorgeschlagenen Neu-Regelung der Zulässigkeit nur der Geltendmachung „zivilrechtlicher“ Ansprüche gegenüber der betroffenen Person“ wäre den Krankenhäusern die Datenübermittlung zum Zwecke der Geltendmachung ihrer Kostenrechnung nicht erlaubt, da es sich bei diesen Ansprüchen weder um zivilrechtliche Ansprüche handelt noch werden sie gegenüber der betroffenen Person geltend gemacht.

Da zum heutigen Zeitpunkt nicht ansatzweise erkennbar ist, ob sich die Krankenhäuser bei der Geltendmachung derartiger Ansprüche auf das Rechtsinstitut der „Wahrnehmung berechtigter Interessen“ bzw. „berechtigten Wahrnehmung eigener Interessen“ stützen können, liefen die Krankenhäuser Gefahr, – ohne die Offenbarungsmöglichkeit

– praktisch rechtlos gestellt zu werden, ihre Vermögensinteressen prozessual durchzusetzen.

Insofern sollte der Passus „gegenüber der betroffenen Person“ nicht in die Regelung aufgenommen werden und nach dem Wort „zivilrechtliche“ sollten die Wörter „und sozialrechtliche“ eingefügt oder aber die ursprüngliche Fassung „rechtliche“ Ansprüche sollte beibehalten werden.

Änderungsvorschlag

§ 24 Abs. 1 Nr. 2 BDSG-E verbleibt wie folgt:

- „(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nicht-öffentliche Stellen ist zulässig, wenn
2. sie zur Geltendmachung, Ausübung oder Verteidigung **rechtlicher Ansprüche** erforderlich ist,

sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

Zum Gesetzentwurf allgemein; Zu Artikel 1 (§ 24 Absatz 2 Nummer 2 BDSG-E) **Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen**

Beabsichtigte Neuregelung

In § 24 Abs. 2 BDSG–E wird für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Verordnung 2016/679 über die Bezugnahme auf § 24 Abs. 1 am Ende BDSG–E eine zusätzliche Interessenabwägung eingeführt.

Stellungnahme

Zwar ist dem nationalen Gesetzgeber in diesem Zusammenhang durch die Verordnung 2016/679 ein Regelungsspielraum eröffnet, allerdings ist nicht nachvollziehbar, aus welchem Grunde eine derartige Interessenabwägung für erforderlich erachtet wird. Bisher ist für die in § 24 Abs. 1 Nr. 1 und Nr. 2 BDSG–E angesprochenen Bereiche keine Interessenabwägung notwendig.

Insbesondere für den Bereich der Verfolgung von Straftaten ist bislang gesetzlich keine Interessenabwägung geregelt. So sieht § 32 Bundesmeldegesetz (BMG) „Besondere Meldepflicht in Krankenhäusern, Heimen und ähnlichen Einrichtungen“ gemäß Abs. 2 vor, dass der zuständigen Behörde Auskunft aus den Unterlagen der in § 32 Abs. 1 BMG genannten Einrichtungen zu erteilen ist, wenn dies nach Feststellung der Behörde

zur Abwehr einer erheblichen und gegenwärtigen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermissten und Unfallopfern im Einzelfall erforderlich ist.

Ebenso ist die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche z. B. von Krankenhausträgern gegenüber Patienten derzeit in Deutschland Gegenstand einiger landesrechtlicher Regelungen (Landeskrankenhausgesetze o.ä.), die ebenfalls keine Interessenabwägung erfordern.

Beispielhaft seien hier

- § 29 S.1 Nr. 2 BbgKHEG,
- § 24 Abs. 5 Nr. 5 LKHG Berlin,
- § 11 Abs. 1 Nr. 5 HmbKHG,
- § 12 Abs. 2 Nr. 1 Hess. KHG,
- § 36 Abs. 3 Nr. 5 LKG R-P

genannt.

Änderungsvorschlag

§ 24 Abs. 2 BDSG–E wird wie folgt geändert:

- „(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen. **Einer Interessenabwägung im Sinne des Absatzes 1 bedarf es nicht.**“

Zu Ziffer 32; Zu Artikel 1 (§ 29 Absatz 3 BDSG-E)

Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

Beabsichtigte Neuregelung

§ 29 Absatz 3 BDSG-E schränkt die Untersuchungsbefugnisse der Aufsichtsbehörden gegenüber den in § 203 Absatz 1, 2a und 3 StGB genannten Personen ein, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

Nach der Stellungnahme des Bundesrates sollten diese Regelungen zugunsten einer zeitnahen, rechtssicheren und umfassenderen Gesamtregelung zurückgestellt werden.

Stellungnahme

Eine solche Zurückstellung sollte nicht erfolgen, da die in § 29 Absatz 3 BDSG-E vorgenommene Einschränkung der Untersuchungsbefugnisse der Aufsichtsbehörden mit Blick auf Artikel 90 Abs. 1 der Verordnung (EU) 2016/679 bereits zum jetzigen Zeitpunkt zulässig und wichtig ist. Die Regelung in § 29 Absatz 3 BDSG-E ist auch keinesfalls unklar oder vollzugsuntauglich, da die Reichweite der Einschränkungen durch die im Strafgesetzbuch vorgesehenen Geheimhaltungspflichten des angesprochenen Personenkreises klar umrissen ist.

Die Regelung in § 29 Absatz 3 BDSG-E sollte daher unverändert beibehalten werden.

Änderungsvorschlag

§ 29 Absatz 3 BDSG-E verbleibt wie folgt:

„Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuches genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.“

Zu Ziffer 39; Zu Artikel 1 (§ 32 Abs. 1 Nr. 1 BDSG–E)

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Beabsichtigte Neuregelung

§ 32 Abs. 1 BDSG–E enthält Regelungen, in welchen Fällen auf eine Information der betroffenen Person gem. Artikel 13 Abs. 3 der Verordnung (EU) 2016/679 verzichtet werden kann. Diese Ausnahmeregelungen gelten nur in den Fällen, in denen der Verantwortliche die erhobenen personenbezogenen Daten für einen anderen Zweck weiterverarbeiten möchte als den, für den die personenbezogenen Daten erhoben worden sind.

Stellungnahme

Unabhängig von der Streichung der Möglichkeit der Beschränkung der Informationspflicht aufgrund des damit verbundenen Aufwands, ist dringend erforderlich, dass die Ausnahmeregelungen nicht nur die Informationspflichten nach Artikel 13 Abs. 3 der Verordnung (EU) 2016/679, sondern insbesondere die Informationspflichten nach Artikel 13 Abs. 1 und 2 der Verordnung (EU) 2016/679 erfassen.

Die in Artikel 13 Abs. 1 und 2 der Verordnung (EU) 2016/679 vorgesehenen Informationspflichten stellen einen immensen bürokratischen Aufwand für Krankenhäuser dar. Dies gilt insbesondere, wenn Krankenhäuser gesetzlich versicherte Patienten behandeln und im Rahmen dieser Behandlung personenbezogene Daten erheben und verarbeiten. Krankenhäuser unterliegen schon heute zahlreichen Informations-, Hinweis-, Unterrichts- sowie Aufklärungspflichten, so dass das Maß des Zumutbaren – ohne eine Einschränkung der Verordnung – deutlich überschritten würde. Die eigentliche Zielrichtung von Krankenhäusern, Patienten zu behandeln, tritt zulasten von Verwaltungsaufgaben zunehmend in den Hintergrund, was keinesfalls hinnehmbar ist.

Nach Artikel 13 Abs. 1 der Verordnung (EU) 2016/679 muss u.a. Folgendes mitgeteilt werden:

- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,
- die Rechtsgrundlage für die Verarbeitung und
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

Nach Artikel 13 Abs. 2 der Verordnung (EU) 2016/679 müssen u.a. folgende weitere Informationen bereitgestellt werden:

- die Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
- das Bestehen eines Rechts auf Auskunft sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit,
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.

Dies stellt sich insbesondere im System der gesetzlichen Krankenversicherung als äußerst komplex sowie kaum umsetzbar dar.

Hinsichtlich der „Zwecke“ lässt sich festhalten, dass die erhobenen Daten für eine derartige Vielzahl von Zwecken verarbeitet werden, deren „Rechtsgrundlagen“ ebenfalls von unterschiedlichster Natur sind, dass eine entsprechende Mitteilung gegenüber den Patienten diese überfordern dürfte und im Übrigen dessen Sinnhaftigkeit äußerst zweifelhaft erscheint.

Beispielhaft seien hier nur folgende Zwecke genannt: Krankenhausträger verarbeiten die erhobenen Daten nicht nur für die Zwecke der Behandlung, sondern auch zum Zwecke der Abrechnung, wobei hier weiter zu unterscheiden ist, gegenüber wem die Abrechnung erfolgt, einer Krankenkasse, einer Kassenärztlichen Vereinigung oder auch gegenüber dem Patienten selbst. Daneben erfolgen Datenverarbeitungen aufgrund von Qualitätssicherungsmaßnahmen und -prüfungen, Wirtschaftlichkeitsprüfungen, Über-

mittlungspflichtigen gegenüber speziellen Registern (z.B. dem Endoprothesenregister), gegenüber anderen Ärzten, Nachbehandlern, usw.

Ad absurdum geführt würde diese Informations- bzw. Mitteilungspflicht insbesondere, sofern Krankenhäuser Patienten die „Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer“ mitzuteilen haben. Als Standardwerk hinsichtlich der Frage von „Aufbewahrungspflichten und –fristen“ im Krankenhausbereich gilt ein 27-seitiger Leitfaden (DKG-Leitfaden Aufbewahrungspflichten und –fristen von Dokumenten im Krankenhaus, Stand: 2015), der die spezialgesetzlichen Aufbewahrungsfristen darstellt und dabei nicht einmal Anspruch auf Vollständigkeit erhebt. Müssten Krankenhausträger die Dauer der Aufbewahrung gegenüber dem Patienten mitteilen, müssten Sie ihm sämtliche dieser Daten mitteilen, was das Maß des Zumutbaren überschreiben dürfte. Exemplarisch genannt seien Aufbewahrungsfristen aus folgenden Gesetzen: BGB, RöV, StrlSchV, BtMVV, BtMBinHV, ApoBetrO, AMWHV, AMHV, TFG, TPG, IfSG, Verletzungsartenverfahren-VAV, GenDG, SGB I, usw. Hinzu kommt, dass die meisten dieser Gesetze nicht nur eine Aufbewahrungsfrist beinhalten, sondern in der Regel mehrere Fristen von Krankenhausrelevanz.

Daneben müssen Patienten schon heute – lediglich im Rahmen der administrativen Aufnahme – auf diverse behandlungsimmanente Sachverhalte hingewiesen und über Vieles unterrichtet werden sowie ergänzend zahlreiche Unterschriften leisten. Im Einzelnen sei nur exemplarisch Folgendes genannt:

- Der Patient unterschreibt einen Behandlungsvertrag,
- er erhält eine Ausfertigung Allgemeiner Vertragsbedingungen sowie
- des Pflegekostentarifs bzw. Krankenhausentgelt- oder PEPP-Entgelttarifs und der Unterrichtung des Patienten nach § 14 BPfIV a.F. bzw. § 8 KHEntgG und BPfIV n.F. ,
- bei Inanspruchnahme von Wahlleistungen unterschreibt der Patient eine Patienteninformation bei wahlärztlichen Leistungen sowie eine
- eine Wahlleistungsvereinbarung.
- Des Weiteren ist der Patient nach seinem Hausarzt zu befragen und unterschreibt die Einwilligung gem. § 73 Abs. 1b SGB V zur Datenübermittlung zwischen Hausarzt und Krankenhaus,
- ferner erhält er einen Hinweis auf die sog. Patientenquittung gem. § 305 SGB V sowie
- des Weiteren einen Hinweis auf Datenverarbeitung und unterschreibt diesen,
- usw.

Allein dies sprengt bereits die Aufnahmesituation im Krankenhausbereich, wobei die Behandlung noch nicht einmal begonnen hat. Kaum einem Patienten lässt sich mehr vermitteln, warum er sich eines derartigen Aufnahmeprozesses unterziehen muss. Würde nunmehr eine Ausweitung des bereits ohnehin Erforderlichen tatsächlich – aufgrund datenschutzrechtlicher – Vorgaben notwendig werden, dürften die Kranken-

häuser dazu kaum mehr in der Lage sein. Ganz zu schweigen von den Nachfragen, die dies bei den Patienten verursachen würde sowie deren Verunsicherung.

Eine weitere Eingrenzung der in Artikel 13 Abs. 1 und 2 der Verordnung (EU) 2016/679 genannten Informationspflichten, für den Fall, dass die Verarbeitung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist, sieht Erwägungsgrund 62 der Verordnung (EU) 2016/679 im Übrigen explizit vor. Eine entsprechende Klarstellung in § 32 Abs. 1 Nr. 1 BDSG-E sollte unbedingt aufgenommen werden.

Änderungsvorschlag

§ 32 Abs. 1 Nr. 1 BDSG–E wird wie folgt geändert:

- „(1) Die Pflicht zur Information der betroffenen Personen gemäß Artikel 13 Absatz **1 bis** 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung
1. **sich erübrigt, da die Datenverarbeitung in Rechtsvorschriften geregelt ist,**“

Zum Gesetzentwurf allgemein; Zu Artikel 1 (§ 40 Abs. 4 BDSG–E) **Aufsichtsbehörden der Länder**

Beabsichtigte Neuregelung

In § 40 Abs. 3 BDSG–E ist wie auch bisher schon in § 38 Abs. 3 Satz 2 BDSG vorgesehen, dass der Auskunftspflichtige die Auskunft gegenüber der zuständigen Aufsichtsbehörde auf solche Fragen verweigern kann, deren Beantwortung ihn der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Diese Regelung wird zusätzlich flankiert durch § 29 Abs. 3 Satz 1 BDSG–E, wonach gegenüber den in § 203 Abs. 1, 2a und 3 des StGB genannten Personen oder deren Auftragsverarbeitern die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Abs. 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht bestehen, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

Gleichzeitig ist jedoch in § 40 Abs. 4 BDSG–E vorgesehen, dass die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen befugt sind, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der der Aufsicht unterliegenden Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und –geräten zu erhalten und die der Aufsicht unterliegenden Stelle insoweit zur Duldung verpflichtet ist.

Stellungnahme

Das in § 40 Abs. 3 BDSG–E und § 38 Abs. 3 Satz 2 BDSG – alt – enthaltene Recht auf Auskunftsverweigerung gegenüber der zuständigen Aufsichtsbehörde wegen einer möglichen Verletzung des Berufsgeheimnisses resultiert aus dem besonders geschützten Vertrauensverhältnis zwischen Arzt und Patient. Auch nach der Rechtsprechung können sich Berufsgeheimnisträger in solchen Fällen auf Grundlage von § 38 Abs. 3 Satz 2 BDSG – alt – auf ihre Verschwiegenheitspflicht berufen (vgl. KG, Beschluss vom 20.08.2010, Ws (B) 51/07 – 2 Ss 23/07). Dieses Recht auf Auskunftsverweigerung wird jedoch unterwandert, wenn die von der Aufsichtsbehörde mit der Überwachung der Einhaltung der Datenschutzvorschriften beauftragten Personen berechtigt sind, die Räume des Auskunftspflichtigen zu betreten und Zugang zu allen Datenverarbeitungsanlagen und-geräten zu erhalten.

Die Regelung in § 40 Abs. 4 BDSG steht damit auch in Widerspruch zu § 29 Abs. 3 Satz 1 BDSG–E, der ausdrücklich klarstellt, dass die Untersuchungsbefugnisse der Aufsichtsbehörden nicht bestehen, wenn dies zu einem Verstoß gegen die Geheimhaltungspflichten des Auskunftspflichtigen führen würde. In § 40 Abs. 4 BDSG–E sollten daher unter Verweis auf § 29 Abs. 3 Satz 1 und § 40 Abs. 3 BDSG–E entsprechende Einschränkungen der Berechtigungen der Aufsichtsbehörden zur Wahrung der Auskunftsverweigerungsrechte betroffener Berufsgeheimnisträger vorgesehen werden.

Änderungsvorschlag

§ 40 Abs. 4 BDSG–E wird wie folgt geändert:

„(4) Die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Die Stelle ist insoweit zur Duldung verpflichtet. § 16 Absatz 4 gilt entsprechend. **§ 29 Absatz 3 und § 40 Absatz 3 bleiben hiervon unberührt.**“

Weiterer gesetzlicher Handlungsbedarf

Streichung landesrechtlicher Vorgaben zum Verarbeitungsort

Im Zuge der notwendigen Anpassungen des Datenschutzrechts auf der Bundesebene sollten auch bestehende datenschutzrechtliche Einschränkungen auf der Landesebene auf den Prüfstand gestellt und aufgehoben werden. So bestimmen beispielsweise drei Landeskrankenhausgesetze, dass Patientendaten nur im behandelnden Krankenhaus oder durch Auftrag des behandelnden Krankenhauses durch ein anderes Krankenhaus verarbeitet werden dürfen:

1. § 48 Abs. 1 Landeskrankenhausgesetz Baden-Württemberg:

Patientendaten sind in dem Krankenhaus selbst oder im Auftrag des Krankenhauses durch ein anderes Krankenhaus zu verarbeiten.

2. Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz:

Zur Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, darf sich das Krankenhaus jedoch nur anderer Krankenhäuser bedienen.

3. § 24 Abs. 7 Satz 1 Landeskrankenhausgesetz Berlin:

Patientendaten sind grundsätzlich im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus zu verarbeiten.

Die Verordnung (EU) 2016/679 sieht demgegenüber in Artikel 1 Abs. 3 vor, dass der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt, noch verboten werden darf. Dazu wird in Erwägungsgrund 9 der Verordnung (EU) 2016/679 erläutert, dass Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, den unionsweiten freien Verkehr solcher Daten behindern können. Diese Unterschiede im Schutzniveau könnten daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet sei und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, sei eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schaffe, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstatte und dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsehe (vgl. Erwägungsgrund 13 der Verordnung (EU) 2016/679).

Vor diesem Hintergrund sind landesrechtliche Vorgaben, die eine Verarbeitung von Patientendaten nur im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus erlauben, auf den Prüfstand zu stellen. Derartige Einschränkungen für die Datenverarbeitung bestehen für Krankenhäuser in Deutschland lediglich in drei von 16 Bundesländern. Der durch die Verordnung (EU) 2016/679 postulierten Einheitlichkeit des vorgegebenen Rechtsrahmens steht es jedoch entgegen, auf der Landesebene in drei Bundesländern datenschutzrechtliche Vorgaben vorzusehen, die von den Landesregelungen der übrigen Bundesländer abweichen. Aufgrund des in Deutschland vorherrschenden einheitlich hohen Datenschutzniveaus ist es zudem weder sinnvoll, noch erforderlich, Krankenhäuser in nur einigen wenigen Bundesländern derart strikten Vorgaben zu unterwerfen, zumal diese erheblichen Einschränkungen für Krankenhäuser in den betroffenen Bundesländern bei der Verarbeitung von Patientendaten zu kaum lösbaren Schwierigkeiten führen.

Änderungsvorschlag

Landesrechtliche Beschränkungen des Verarbeitungsortes sollten im Zuge der Anpassungen des deutschen Datenschutzrechts an die Verordnung (EU) 2016/679 gestrichen werden.

DGB Bundesvorstand | Henriette-Herz-Platz 2 | 10178 Berlin

An den Vorsitzenden des
Bundestags-Innenausschusses
Herrn Ansgar Heveling, MdB
Platz der Republik 1
11011 Berlin

Annelie Buntenbach
Mitglied des Geschäftsführenden
Bundesvorstandes

vorab per E-Mail: innenausschuss@bundestag.de

Stellungnahme des Deutschen Gewerkschaftsbundes zum DSAnpUG-EU

23. März 2017

Sehr geehrte Herr Vorsitzender,

wir möchten Sie bitten, dieses Anschreiben – nebst der beigefügten Stellungnahme des Deutschen Gewerkschaftsbundes – allen Abgeordneten des Innenausschusses für die Öffentliche Anhörung zuzuleiten, auf der Website des Innenausschusses zu veröffentlichen bzw. in die Ausschussdrucksache mit aufzunehmen:

**Für weitere Absprachen
wenden Sie sich bitte an:**

Helga Nielebock
Abteilungsleiterin
Abteilung Recht

helga.nielebock@dgb.de

Die am 25.05.2016 in Kraft getretene europäische Datenschutzgrundverordnung (DSGVO) wird am 25.05.2018 unmittelbar geltendes Recht in allen Mitgliedsstaaten der Europäischen Union. Aus ihren Öffnungsklauseln ergeben sich an die Mitgliedsstaaten gerichtete Regelungsaufträge (Regelungsgebote und Regelungsoptionen), deren Erfüllung für den nationalen Gesetzgeber einen (erheblichen) gesetzgeberischen Anpassungsbedarf im nationalen Datenschutzrecht zur Folge hat. Zu diesem Anpassungsbedarf hat die Bundesregierung am 01.02.2017 einen Gesetzentwurf beschlossen hat, der Gegenstand der Öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags am 27.03.2017 sein wird.

Telefon: 030 24060-274
Telefax: 030 24060-761

Rec-ni/hy

Henriette-Herz-Platz 2
10178 Berlin

www.dgb.de

Der Deutsche Gewerkschaftsbund und seine Mitgliedsgewerkschaften treten gegenüber diesem Entwurf eines Gesetzes zur Anpassung des Datenschutzes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU) dafür ein, dass sowohl der bislang geltende Datenschutzstandard des Bundesdatenschutzgesetzes (BDSG), als auch der teils hohe Datenschutzstandard in den bestehenden bereichsspezifischen Datenschutzregelungen des Bundes – soweit nach dem verfügbaren Teil sowie den zur Auslegung dieser heranziehbaren Erwägungsgründen der DSGVO möglich – gewahrt bleibt. Im Zuge des von der Bundesregierung geplanten Anpassungsgesetzes darf es kein Absinken des Datenschutzniveaus geben und der bisherige hohe deutsche Schutzstandard – für Konsumenten, Arbeitnehmer und Arbeitnehmerinnen und alle von personenbezogener Datenverarbeitung betroffener Bürger – muss fortgeführt werden. Ein Zurückfallen hinter heutige Schutzstandards hält der DGB für nicht hinnehmbar. Dies gilt

insbesondere für den Beschäftigtendatenschutz, dessen spezifischere Ausgestaltung durch die Mitgliedsstaaten nach Maßgabe des Art. 88 DSGVO vorgenommen werden kann.

Der Deutsche Gewerkschaftsbund hat zu dem Kabinettsbeschluss eine (aktualisierte) Stellungnahme verfasst, die wir Ihnen im Anhang beifügen. Dem DGB und seinen Mitgliedsgewerkschaften geht es bei den darin formulierten Änderungs- und Ergänzungsvorschlägen zum Gesetzentwurf des DSAnpUG-EU vor allem darum, dass

- in Bezug auf § 4 BDSG-E die Möglichkeit, etwa Einkaufspassagen mit Ladenlokalen permant und flächendeckend durch optisch-elektronische Einrichtungen zu überwachen und dabei auch Beschäftigte mit in den Fokus der Videoüberwachung zu nehmen, zumindest in der Vorschrift über die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG-E) spezifisch für diese besondere Verarbeitungssituation eingeschränkt wird;
- jegliche Videoüberwachung, auch wenn punktuell und in kleineren Bereichen durchgeführt, zumindest für den Beschäftigungskontext spezifischen Regelungen unterliegt, die etwa die Überwachung von Sozialräumen und eine verdeckte Videoüberwachung generell verbieten;
- die in § 24 BDSG-E – gegenüber der entsprechenden Vorschrift der EU-Datenschutzgrundverordnung – geregelten Möglichkeiten für eine Zweckänderung der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen zumindest im Beschäftigungskontext (wieder) eingeschränkt wird;
- die Annahme der Freiwilligkeit einer – eingeschränkten – Einwilligung in die Datenverarbeitung im Beschäftigungsverhältnis (§ 26 Abs. 2 BDSG) im Falle der Gewährung eines (einfachen) Vorteils nicht ausreicht, sondern der Vorteil für die jeweiligen Arbeitnehmerinnen ausschließlich bestehen oder gegenüber dem Interesse des Arbeitgebers zumindest überwiegen muss; insoweit sollte ein „überwiegender Vorteil“ als Indiz einer Freiwilligkeit der Einwilligung geregelt werden;
- für die Beteiligung der Interessenvertretungen der Beschäftigten ein (erweitertes) Initiativ- und Mitbestimmungsrecht bei der Verarbeitung personenbezogener Beschäftigtendaten ergänzt werden muss. Das bisherige Mitbestimmungsrecht zur Leistungs- und Verhaltensüberwachung von Beschäftigten durch technische Einrichtungen reicht nicht aus, da auch Daten von Bewerberinnen und Bewerbern sowie Arbeitnehmerinnen und Arbeitnehmern, die nicht-automatisiert erhoben und genutzt werden, wie etwa durch Ausübung des Fragerechts des Arbeitgebers oder infolge der Beauftragung von Detekteien, der Mitbestimmung des Betriebsrats generell unterworfen werden müssen.

Mit freundlichen Grüßen



Stellungnahme des Deutschen Gewerkschaftsbundes zum Gesetzentwurf
der Bundesregierung

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (DS-RL) – DSAnpUG-EU 27.02.2017

I. Grundsätzliche Positionsbestimmung

Die Digitalisierung der Wirtschaft und Gesellschaft ist eine große Herausforderung, gerade auch für Beschäftigte, Arbeitnehmervertreter und Gewerkschaften, da sie im Begriff ist, die Industrie, Dienstleistungen, Märkte, aber auch die Arbeitswelt im Allgemeinen (in der Privatwirtschaft, wie im öffentlichen Dienst, im Bildungswesen usw.) zu verändern. Es besteht die Gefahr, dass Digitalisierung nicht nur die sozialen Ungleichheiten weiter verschärft, sondern insbesondere den Persönlichkeitsschutz von Beschäftigten und ihren Vertretern in den Betrieben und Verwaltungen beeinträchtigen könnte. Auch aus diesem Grund wird der Persönlichkeits- und Datenschutz immer wichtiger. Um diesen Schutz transparent und vollständig zu gewährleisten, ist ein **eigenständiges Beschäftigtendatenschutzgesetz** überfällig. Die europäische Reform des Datenschutzrechts durch die Datenschutzgrundverordnung (DSGVO), deren Ziel – neben dem freien Verkehr personenbezogener Daten in der Union – der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist, ist eine erste Antwort auf die Sicherung der Grundrechte und Grundfreiheiten natürlicher Personen unter den fortgeschrittenen Bedingungen von Digitalisierung und Globalisierung, sie reicht aber im Beschäftigungskontext nicht aus. Seit dem 25.05.2016 läuft die zweijährige Phase der Anpassung der nationalen Rechtsvorschriften an die Vorgaben der DSGVO, da die DSGVO zahlreiche an die Mitgliedstaaten gerichtete Regelungsaufträge, aber auch – insbesondere für „besondere Verarbeitungssituationen“ (wie den Beschäftigungskontext) – viele Öffnungsklauseln enthält, aus denen sich ein gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht ergibt.

Nach Auffassung des DGB und seiner Mitgliedsgewerkschaften, aber auch der überwiegenden Auffassung in der Literatur, wird den Mitgliedstaaten durch die Öffnungsklausel des Art. 88 DSGVO bei der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext ein weiterer Anwendungsbereich für „spezifischere“ Regelungen (durch Rechtsvorschriften oder durch Kollektivvereinbarungen) eingeräumt, so dass grundsätzlich

Deutscher Gewerkschaftsbund
Bundesvorstand
Abteilung Recht

Ralf-Peter Hayen
Referatsleiter

ralf-peter.hayen@dgb.de

Telefon: 030/24060-272
Telefax: 030/24060-761
Mobil: 0160/7121758

Henriette-Herz-Platz 2
10178 Berlin

www.dgb.de

Abweichungen zugunsten eines höheren Schutzniveaus nationaler Regelungen zum Beschäftigtendatenschutz möglich sind, soweit sie sich mit den Besonderheiten des abhängigen Beschäftigungsverhältnisses gegenüber – inhaltlich regelungsfreien oder einschränken – allgemeinen bzw. grundsätzlichen Regelungen der DSGVO rechtfertigen lassen. Für diese spezifischeren Regelungen gibt die DSGVO sowohl die zweckbezogenen Regelungsbereiche (Art. 88 Abs. 1) als auch inhaltliche Anforderungen an die Persönlichkeitsschutz- und Grundrechtewahrung in Bezug auf das Schutzniveau von im Beschäftigtenkontext zu treffenden besonderen Maßnahmen (Art. 88 Abs. 2) vor.

Zur gesetzlichen Ausgestaltung der Regelungsaufträge und Öffnungsklauseln wurde der Entwurf eines Gesetzes zur Anpassung des Datenschutzes an die DSGVO (und zur Umsetzung der RL 2016/680) vorgelegt, der am 01.02.2017 durch das Bundeskabinett beschlossen wurde. Kernstück dieses Gesetzentwurfs ist ein neugefasstes Bundesdatenschutzgesetz, das sich spezifisch zur „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ (Beschäftigtendatenschutz) in nur einer Vorschrift (§ 26 BDSG-E neu) befasst. Gegenüber dem Referentenentwurf sieht der Kabinettsbeschluss Ergänzungen im § 26 BDSG-E (neu) i.S. spezifischerer Schutzvorschriften im Beschäftigtenkontext (Art. 88 Abs. 1 DSGVO) vor

- zur Beurteilung der Freiwilligkeit der Einwilligung (Abs. 2),
- zur Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten in Abweichung von Art. 9 Abs. 1 DSGVO (Abs. 3),
- zur Regelungsbefugnis durch Kollektivvereinbarungen nebst zu beachtenden Schutzmaßnahmen (Abs. 4),
- zur Maßnahmenergreifung des Verantwortlichen zur Sicherstellung der Einhaltung der Datenverarbeitungsgrundsätze nach Maßgabe des Art. 5 DSGVO (Abs. 5) und
- zur Erweiterung der Definition des Beschäftigtenbegriffs (Abs. 8).

Der DGB und seine Gewerkschaften vertreten die Auffassung, dass die vom Gesetzgeber vorliegend gewollte Ausgestaltung des Beschäftigtendatenschutzes nach Maßgabe des Art. 88 DSGVO durch die Schaffung eines **eigenständigen Beschäftigtendatenschutzgesetzes** vorgenommen werden sollte. Die Öffnungsklausel des Art. 88 DSGVO für die Datenverarbeitung im Beschäftigungskontext unterstreicht diese Sichtweise. Solange eine detaillierte – und dem entsprechend – umfangreiche eigenständige Regelung kurzfristig nicht realisierbar ist, muss jedenfalls im Zuge des Anpassungsgesetzes eine Absenkung des Schutzniveaus verhindert werden. Dort, wo auf Grundlage etwaig defizitärer Regelungen der DSGVO ein Absinken des Schutzniveaus möglich werden könnte, muss durch die Schaffung von nationalen Spezialregelungen dafür gesorgt werden, dass es im Zuge dieser geplanten Anpassung nicht zu Verschlechterungen des bestehenden Datenschutzniveaus kommt. Ein Zurückfallen hinter heutige Schutzstandards, insbesondere des bestehenden BDSG, aber auch hinter bereichsspezifische Datenschutzvorschriften und Rechtsprechung, die den benötigten Schutz von Beschäftigten auf der Grundlage des informationellen

Selbstbestimmungsrechts und auf dem Hintergrund ihrer persönlichen Abhängigkeit im Beschäftigungsverhältnis ausgestaltet hat, ist für den DGB und seine Mitgliedsgewerkschaften nicht hinnehmbar.

Zum Erhalt des bestehenden Schutzniveaus gehört u.a. die Fortführung und Konkretisierung der nachfolgenden Regelungen; inwieweit diese im Entwurf aufgegriffen werden, wird wie folgt bewertet:

- Richtig ist die Fortführung der Regelungen der Abs. 1 bis 3 des – noch geltenden – § 32 BDSG durch die Abs. 1, 6 und 7 des § 26 BDSG-E (neu), die der Entwurf zwar als Übernahme der spezialgesetzlichen „Rahmenregelung“ des geltenden BDSG (punktuell) einlöst, deren Ergänzung durch spezifischere Schutzvorschriften für den Beschäftigungskontext aber im Gesetzentwurf entweder unzureichend konkretisiert oder – gemessen am bisherigen Datenschutzstandard – zu Lasten der Beschäftigten geregelt ist, wie in Bezug auf die
 - Beurteilung der Freiwilligkeit der Einwilligung;
 - Verarbeitung besonderer Kategorien personenbezogener Daten;
 - Klarstellung der Regelungsmöglichkeit durch Kollektivvereinbarungen nebst zu beachtender Schutzmaßnahmen;
 - Maßnahmenergreifung des Verantwortlichen zur Sicherstellung der Einhaltung der Datenverarbeitungsgrundsätze;
 - Erweiterung des Beschäftigtenbegriffs.

Es fehlen jedoch andere erforderliche Konkretisierungen für eine personenbezogene Verarbeitung von Beschäftigtendaten im Beschäftigungskontext, wie

- die notwendige Erweiterung des Mitbestimmungsrechts für Betriebsräte bei der personenbezogenen Datenverarbeitung;
- die Konkretisierung und Einschränkung der Videoüberwachung im Beschäftigungsverhältnis;
- die Regelung über die Voraussetzungen einer Nutzung personenbezogener Speicher- und Verarbeitungsmedien zu Zwecken des Beschäftigungsverhältnisses sowie
- die Ausformung der spezifischen Zweckbindung und Zweckänderung im Beschäftigungskontext.

Darüber hinaus fehlt eine Klarstellung im Entwurf, dass es sich bei § 26 BDSG-E (neu) um eine abschließende Sonderregelung – etwa im Verhältnis zu Art. 6 Abs. 1 Satz 1 lit. f DSGVO – handelt.

- Richtig ist die Beibehaltung des Anwendungsbereichs auf Beschäftigte, Bewerber, arbeitnehmerähnliche Personen etc. gemäß – des noch geltenden – § 3 Nr. 11 BDSG, die der Entwurf erfreulicherweise übernimmt.

Der Beschäftigtenbegriff muss jedoch aktuell – über die Ergänzung des § 26 Abs. 8 Satz 1 Nr. 1 BDSG-E (neu) um „Leiharbeiterinnen und Leiharbeiter im Verhältnis zum Entleiher“ hinaus – weitergehend ggf. auch auf Werkvertragsbasis Tätige erweitert werden.

- Einschränkende Regelungen fehlen, wie in Bezug auf die Überwachung von Beschäftigten am Arbeitsplatz und im privaten Umfeld, einschließlich von Leistungs- und Verhaltenskontrollen; insoweit fehlt eine spezifische Regelung zur Frage der Zulässigkeit der Beobachtung öffentlich zugänglicher Räume durch optisch-elektronische Einrichtungen (Videoüberwachung) im Beschäftigungskontext (entsprechend § 6b BDSG). Die Besonderheiten der Videoüberwachung von Beschäftigten sind im Gesetzentwurf weder in § 4 BDSG-E (neu) hinreichend spezifiziert noch – durch konkretisierende Spezial- bzw. Sonderregelung – in § 26 BDSG-E (neu) ausgestaltet. Vielmehr verschlechtert im Rahmen der vorgesehenen Rechtsgrundlagen des allgemeinen Datenschutzrechts die nun vorgegebene Schutzgüterabwägung in § 4 Abs. 1 Satz 2 BDSG-E (neu) i.V.m. den weit gefassten Zulässigkeitsgründen für eine Videoüberwachung (etwa Wahrnehmung des „Hausrechts“ oder „berechtigter Interessen“).
- Des Weiteren fehlt eine Vorschrift, die die Frage der Unterrichts- und Auskunftsrechte bei der Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien im Beschäftigungskontext (entsprechend § 6c des – noch geltenden – BDSG) klar regelt, da diese Frage im Gesetzentwurf weder im allgemeinen Teil noch für die besondere Verarbeitungssituation des Beschäftigungsverhältnisses angesprochen wird; die Beantwortung dieser Frage – möglicherweise - aus der Systematik der DSGVO abzuleiten, widerspricht den Grundsätzen der Rechtsklarheit und -sicherheit. Schließlich fehlt (entsprechend § 31 des – noch geltenden – BDSG) die Regelung zur strengen Zweckbindung von personenbezogenen Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert sind im Gesetzentwurf ebenfalls vollständig, sodass für sie als im Beschäftigungskontext auszugestaltende „spezifischere Vorschrift“ Ergänzungsbedarf besteht.
- Durch das Anpassungsgesetz sollte außerdem entsprechend § 28 Abs. 1 Satz 2 des geltenden BDSG für den Beschäftigungskontext ausdrücklich vorgesehen werden, dass die Zwecke, für die die Beschäftigtendaten verarbeitet werden sollen, bereits bei der Erhebung dieser personenbezogenen Daten konkret vom Arbeitgeber festzulegen sind; Zweckänderungen sind nur bei einer grundsätzlich geänderten Sachlage zulässig. Der Gesetzentwurf enthält – obwohl spezialgesetzlich sowohl im Hinblick auf Zweckbindung, als auch Zweckänderungen möglich – hierzu keine Konkretisierungen für den Beschäftigungskontext.

- Begrüßt werden die Regelung zur Bestellpflicht eines Datenschutzbeauftragten (entsprechend § 4f Abs. 1 des – noch geltenden – BDSG) und zum besonderen Kündigungsschutz des Datenschutzbeauftragten (entsprechend § 4f Abs. 2 des – noch geltenden – BDSG); sie sind im Gesetzentwurf erfreulicherweise mit dem Ansatz einer weitreichenden Regelung enthalten (vgl. § 38 i.V.m. § 6 Abs. 4, Abs. 5 Satz 2 und Abs. 6 BDSG-E neu).
- Richtig ist auch die beabsichtigte Beibehaltung sektorspezifischer Spezialregelungen, wie die der Regelungen der §§ 19 – 21 Gendiagnostikgesetz, die im vorliegenden Entwurf jedoch nicht Regelungsgegenstand sind.

Die Forderung des DGB nach Fortführung – zumindest – des derzeit bestehenden Datenschutzniveaus gilt nicht nur für Regelungen zur Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, sondern – im Vergleich zum geltenden BDSG – insbesondere auch für die allgemeinen Bestimmungen, die Rechtsgrundlagen der Datenverarbeitung und die Betroffenenrechte im vorgelegten Entwurf eines neuen BDSG. Diese generelleren Regelungen stellen häufig die „Rückfallgrundlagen“ für spezifischere Regelungen im Beschäftigungskontext dar, wenn durch diese keine Verdrängung der allgemeinen Vorschriften stattfinden. Während die generelle Vorschrift zur Zweckänderung von Datenverarbeitungen durch nicht-öffentliche Stellen (§ 24 BDSG-E –neu) dem bislang geltenden Datenschutzstandard besser gerecht wird, als noch die Fassung dieser Regelung im Referentenentwurf des Bundesministeriums des Innern (insbesondere wegen des Wegfalls des Zulässigkeitstatbestandes „berechtigter Interessen des Verantwortlichen“), werden die Betroffenenrechte (§§ 30ff. BDSG-E-neu) durch den Gesetzentwurf (für den nicht-öffentlichen Bereich) immer noch zu weit eingeschränkt.

Der DGB und seine Mitgliedsgewerkschaften sind darüber besorgt, weil die Aufrechterhaltung des Datenschutzniveaus der allgemeinen Datenschutzregelungen den Beschäftigten wiederum in ihrer Rolle als von personenbezogener Datenverarbeitung betroffene Bürger und Konsumenten dient.

Der DGB sieht im vorliegenden Gesetzentwurf noch weiteren Regulierungs- und Ergänzungsbedarf und fordert eine Festlegung der Politik auf die **Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes**, um die genannten Detailanforderungen bei der Anpassung der Datenschutzgrundverordnung – insbesondere für den spezifischen Beschäftigungskontext – umfassend aufzunehmen.

II. Zu ausgewählten Regelungen des Artikel 1 (Bundesdatenschutzgesetz – BDSG)

Teil 1: Gemeinsame Bestimmungen

Anwendungsbereich und Begriffsbestimmungen (Kapitel 1)

Zu § 1: Anwendungsbereich

Bislang erfasst der Anwendungsbereich des geltenden BDSG auch die **nichtautomatisierte Datenverarbeitung** gemäß § 1 Abs. 2, während die DSGVO jene Datenverarbeitung gemäß Art. 2 Abs. 1 nur erfasst, soweit es um eine „nichtautomatisierte Verarbeitung personenbezogener Daten geht, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ Damit werden nichtautomatisierte Datenverarbeitungsprozesse, die auch nicht auf eine entsprechende Speicherung angelegt sind, nicht erfasst, was im Beschäftigungskontext etwa auf das Fragerecht des Arbeitgebers, die Überwachung von Arbeitnehmern durch Detekteien, das Abhören von Telefonaten und handschriftliche Notizen zutrifft, sofern hier jeweils keine Speicherung von Daten bzw. eine Überführung in ein Dateisystem erfolgt.

War der Anwendungsbereich des geltenden BDSG in Bezug auf die nichtautomatisierte Datenverarbeitung (generell) im Beschäftigungskontext noch im Referentenentwurf zum DSAnpUG-EU vom 23.11.2016 (durch die dort vorgeschlagene Regelung des § 24 Abs. 2 BDSG-E neu) übernommen und beibehalten worden, wurde dieser Anwendungsbereich – offenbar im Zuge der nachgefolgten Ressortabstimmungen – im vorliegenden Gesetzentwurf abgeändert: Zum einen wurde im vorliegenden – für alle Verarbeitungssituationen (generell) geltenden - § 1 Abs. 1 BDSG-E (neu) in Bezug auf die Anwendung des Gesetzes für nicht-öffentliche Stellen ergänzend zum Referentenentwurf ausgeführt, dass es „...für die nichtautomatisierte Verarbeitung personenbezogener Daten (gilt), die in einem Dateisystem gespeichert sind oder gespeichert werden sollen,...“. Zum anderen wurden – bereichsspezifisch für DV-Zwecke des Beschäftigungsverhältnisses - in § 26 Abs. 7 BDSG-E (neu) die Worte „automatisiert oder“ gestrichen. Dabei wurde zusätzlich die weiter gefasste „Verarbeitungsdynamik“ des geltenden BDSG („...**in** oder **aus** einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden“), die noch im Referentenentwurf vom 23.11.2016 redaktionell zusammengefasst erhalten geblieben war, im Gesetzentwurf auf eine bloße Speicherung in einer Datei bzw. einem Dateisystem reduziert. Der DGB und seine Mitgliedsgewerkschaften lehnen diese Einschränkung des allgemeinen Anwendungsbereichs des Gesetzentwurfs, wie auch - insbesondere - des (spezifischen) Anwendungsbereichs der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses im BDSG-E (neu) gegenüber dem geltenden BDSG als Verschlechterung des Datenschutzniveaus der Beschäftigten ab und fordern, dass § 32 Abs. 2 des geltenden BDSG in § 26 Abs. 7 BDSG (neu) mit dem bisherigen Inhalt übernommen wird. Dann sind die Absätze 1 bis 6 auch anzuwenden, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, **ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet oder für die Verarbeitung in einer solchen Datei erhoben werden**. Mit dieser Ergänzung des § 26 Abs. 7 des Gesetzentwurfs würde die bislang geltende Regelung des § 32 Abs. 2 BDSG für den Beschäftigungskontext als eine – gleichsam – „spezifischere“ Regelung i.S. des Art. 88 Abs. 1 DSGVO, nämlich für die Konkretisierung des Anwendungsbereichs des Gesetzes in der besonderen Verarbeitungssituation der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ausgeformt und beibehalten.

Zu § 2: Begriffsbestimmungen

Die Definition des geltenden § 3 Abs. 10 BDSG zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien wurde nicht übernommen. Dass sich aber **zu den Voraussetzungen der Zulässigkeit der Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien** (entsprechend § 6c des geltenden BDSG) in den allgemeinen Datenschutzregelungen der DSGVO keine diesbezügliche Regelung findet, darf nicht zu dem Schluss verleiten, dass insoweit auch keine Definition notwendig ist. Die Norm des bislang geltenden § 6c BDSG über die konkreten Unterrichtungspflichten des Verantwortlichen ist bedeutsam. Zu seinen Pflichten gehört die Unterrichtung a) über – etwa – die Funktionsweise des Mediums, einschließlich der Art der zu verarbeitenden personenbezogenen Daten, b) die Ausübung der Rechte des Betroffenen, insbesondere seines Auskunftsrechts, und c) die zu treffenden Maßnahmen bei Verlust der Zerstörung, sowie die eindeutige Erkennbarkeit der Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen. Diese Pflicht zur Unterrichtung kommt insbesondere zur Anwendung beim Einsatz von Ortungsdiensten für Beschäftigte (etwa im Rahmen der Routenkontrolle oder aus Sicherheitsgründen). Diese – spiegelbildlich zu den Pflichten des Verantwortlichen – detailliert im geltenden BDSG bestehenden Rechte des Betroffenen bei Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien werden durch die Betroffenenrechte nach Maßgabe des Kapitels III der DSGVO sowie derjenigen des vorliegenden Gesetzentwurfs (Kapitel 2) nicht aufgegriffen oder gar ersetzt. Der Entwurf macht vielmehr für die vorliegenden Gesetzgebungsmaßnahmen von der Öffnungsklausel für **Beschränkungen dieser Betroffenenrechte** (Art. 23 DSGVO) weitestgehend Gebrauch, Wenn – mangels Nachfolgeregelung – keine Verpflichtung mehr bestehen würde, etwa eine eindeutige Erkennbarkeit von Kommunikationsvorgängen, die auf dem Medium eine Datenverarbeitung auslösen, für den Betroffenen zu gewährleisten, würde sich das bisherige **Datenschutzniveau für Beschäftigte verschlechtern**. Da dieses Defizit in der DSGVO bezüglich der zulässigen Nutzung dieser Medien durch eine spezialgesetzliche Regelung für den Beschäftigungskontext analog des geltenden § 6c BDSG ausgeglichen werden muss [vgl. nachfolgende Erläuterung in der Stellungnahme zu § 26 BDSG (neu)], bedarf es auch weiterhin der Definition dieser Datenträger in der vorliegenden Norm oder (ergänzend) im Rahmen der spezifischeren Vorschrift über die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses.

Rechtsgrundlagen der Verarbeitung personenbezogener Daten (Kapitel 2)

Zu § 4 Videoüberwachung

Dem Regelungsansatz des geltenden BDSG folgend, erfasst die Vorschrift als Nachfolgeregelung in Abs. 1 Satz 1 Nr. 2 und 3, Satz 2 auch die Videoüberwachung durch nicht-öffentliche Stellen. Die Bestimmung legt für die Zulässigkeit der **Videoüberwachung** zum einen deren Erforderlichkeit in Bezug auf drei Voraussetzungen (im Folgenden: a-c) fest: a) zur Aufgabenerfüllung öffentlicher Stellen, b) zur Wahrnehmung des Hausrechts oder c) zur

Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke. Als weitere Voraussetzung für die Zulässigkeit der Videoüberwachung dürfen keine Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der Betroffenen bestehen. Allerdings werden diese „schutzwürdigen Interessen“ der Betroffenen in Abs. 1 Satz 2 durch die gesetzliche Fiktion eingeschränkt, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in öffentlich zugänglichen großflächigen Anlagen aufhalten (als ein „besonderes wichtiges Interesse“), gilt. Nach der Gesetzesbegründung wird durch diese gesetzliche Fiktion die Abwägungsentscheidung zugunsten der Zulässigkeit der Videoüberwachung geprägt. Das heißt im Klartext: Die Zulässigkeit der Videoüberwachung ist für den Betreiber öffentlich zugänglicher Einkaufszentren etwa unter der Bedingung der Wahrnehmung des Hausrechts oder der Geltendmachung „berechtigter Interessen“ bei Berufung auf diese Schutzgüter quasi vorgegeben. Auch ein Landesdatenschutzbeauftragter kann die Videoüberwachung mit Hinweis auf die schutzwürdigen Interessen der Beschäftigten in dem jeweiligen Einkaufszentrum nicht mehr untersagen. Dies stellt einen eklatanten Eingriff in die Persönlichkeitsrechte der dort beschäftigten Arbeitnehmerinnen und Arbeitnehmer dar.

Fazit/Bewertung:

Durch die Neufassung der Vorschrift zur Videoüberwachung öffentlich zugänglicher Räume wird die Videoüberwachung im Vergleich zur Regelung des geltenden § 6b BDSG in größerem Umfang und nach zum Teil deutlich weniger strengen Voraussetzungen zulässig sein. Zwar ist § 4 BDSG-E (neu) mit seinem Abs. 1 Satz 1 sowie den Abs. 2 bis 5 mit § 6b Abs. 1 bis 5 des geltenden BDSG weitgehend wortidentisch. Durch die Verknüpfung des **Satzes 1** mit dem neu eingefügten **Satz 2** des § 4 Abs. 1 BDSG-E (neu) und der damit - quasi - vorgegebenen Abwägungsentscheidung für die Zulässigkeit der Videoüberwachung, ist es einem Arbeitgeber als Betreiber einer Videoüberwachungsanlage unter Berufung auf die Verteidigung dieser besonderen Schutzgüter (letztlich zum Schutz vor Folgen terroristischer Angriffe) – etwa – in Einkaufszentren, Ladenlokalen usw. möglich, gleichzeitig seine Beschäftigten – dazu noch dauerhaft – zu überwachen.

Nach Maßgabe der Vorgaben der DSGVO (Art. 35 Abs. 1 DSGVO i.V.m. Art. 35 Abs. 3 lit. c) DSGVO sowie Art. 88 Abs. 2 DSGVO) ist der deutsche Gesetzgeber verpflichtet, die Regelungen für eine Ausweitung der Videoüberwachung in öffentlich zugänglichen Räumen, wie diese im Rahmen der allgemeinen datenschutzrechtlichen Vorschriften vorgesehen sind, für die besondere Situation der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses einschränkend zu konkretisieren:

Art. 35 Abs. 1 DSGVO i.V.m. Art. 35 Abs. 3 lit. c DSGVO (sowie Erwägungsgrund 91) erachtet nur die „systematische“ und „umfangreiche“ Videoüberwachung als eine Datenverarbeitung, die hohe Risiken für die Rechte und Freiheiten der Betroffenen in sich birgt. Damit erfasst diese Anforderung jedoch lediglich einen kleinen Ausschnitt des Arbeitslebens. Wichtige Bereiche von Produktion, Dienstleistung und Verwaltung, in denen die Videoüberwachung gerade auch zur Kontrolle von Leistung und Verhalten sowie der Privatsphäre von Beschäftigten eingesetzt wird bzw. eingesetzt werden kann, würden ohne eine spezifische

Sonderregelung für den Beschäftigtenkontext vom Schutzbereich dieser Norm ausgeblendet. Auch würde die häufig punktuelle und auf kleinere Bereiche bezogene Videoüberwachung in Betrieben, aber auch in öffentlich zugänglichen Ladenlokalen, der – gegenüber § 6b des geltenden BDSG – herabgesetzten Rechtfertigungsschwelle für Videoüberwachung nach der DSGVO und nach der allgemeinen Datenschutzvorschrift in § 4 Abs. 1 des BDSG-E (neu), unterfallen. **Die fehlende (Detaillierung der Datenschutzfolgeabschätzungs-) Vorschrift zur Videoüberwachung für „allgemeine Datenverarbeitungssituationen“ in der DSGVO, stellt ohne nationale Spezifizierung ihrer Voraussetzungen im Beschäftigungskontext ein „Schlupfloch“ für den Beschäftigtendatenschutz dar, das durch die für eine Zulässigkeit der Videoüberwachung vorgegebene bzw. „geprägte Abwägungsentscheidung“ nach Maßgabe des § 4 Abs. 1 BDSG-E (neu) noch vergrößert wird.** Dem gegenüber verpflichtet Art. 88 Abs. 2 DSGVO die Mitgliedstaaten jedoch zur Ergreifung „angemessener und besonderer Maßnahmen“ zu Schutzzwecken, soweit diese Mitgliedsstaaten in ihrer nationalen Rechtsordnung von spezifischen Vorschriften zur Verarbeitung personenbezogener Beschäftigten im Beschäftigungskontext Gebrauch machen (Art. 88 Abs. 1 DSGVO). Solche Schutzmaßnahmen werden von Art. 88 Abs. 2 DSGVO namentlich in Bezug auf „Überwachungssysteme am Arbeitsplatz“ beispielhaft gefordert.

Darüber hinaus haben nach bestehender Rechtslage die aus dem geltenden § 6b BDSG abgeleiteten Voraussetzungen einer zulässigen Videoüberwachung auch Rückwirkungen auf die Videoüberwachung in **nicht öffentlich zugänglichen Bereichen**, wie etwa Produktionsstätten, deren Zulässigkeit sich nach dem geltenden § 32 BDSG richtet. Auf der Grundlage der vorliegenden (defizitären) Regelung des Gesetzentwurfs erscheint es möglich, dass die Rechtsprechung zukünftig bei der Videoüberwachung in öffentlich zugänglichen Räumen auch im Beschäftigungskontext auf § 4 Abs. 1 BDSG-E (neu) und ergänzend auf Art. 6 Abs. 1 lit. f DSGVO zurückgreifen wird. Das aber würde eine deutliche Absenkung des Schutzstandards im Beschäftigungskontext bewirken, der nicht hinnehmbar ist. Da der Entwurf nach dem Wortlaut dieser Vorschrift (§ 4 BDSG-E neu) unter Berücksichtigung der Verknüpfung mit § 4 Abs. 1 Satz 2 BDSG-E (neu) eine Fortführung von § 6b BDSG für den Beschäftigungskontext und die Beibehaltung der bisherigen nationalen Maßstäbe tatsächlich nicht beinhaltet, muss die Videoüberwachung im Beschäftigungskontext auch aus diesem Grund spezifisch in § 26 BDSG-E (neu) geregelt werden. Schließlich erscheint angesichts der bekannten Datenskandale in Bezug auf die Überwachung von Beschäftigten sowie Vorsitzenden und Mitgliedern ihrer Interessenvertretungen Anfang der Jahre 2000 (allen voran das Beispiel des Inhabers der inzwischen insolventen Drogeriekette Schlecker, der alle Beschäftigten in den Filialen hat Videoüberwachen lassen) eine einschränkende konkretisierende Regelung zur Videoüberwachung im Beschäftigungskontext – auch durch diese Verstöße belegt – dringend erforderlich. Diese spezifischen Regelungen sollten Grundsätze für eine Videoüberwachung für Zwecke des Beschäftigungsverhältnisses ausformen (vgl. hierzu nachfolgende Ausführungen im Abschnitt „weitere Regelungserfordernisse“ im Rahmen einer Ergänzung des § 26 BDSG-E neu).

Als Ausnahmetatbestand für eine solche (vermeintlich) „zulässige Videoüberwachung“ kann sich dieser Arbeitgeber auf die „Wahrnehmung seines Hausrechts“ oder die „Wahrnehmung berechtigter Interessen“ beziehen, womit ihm ein weiter Spielraum eingeräumt wird, Arbeitnehmer/innen permanent und flächendeckend zu überwachen. Während § 4 Abs. 1 Nr. 2 BDSG-E (neu) nach diesseitiger Auffassung und der Ansicht von Datenschutzexperten für europarechtswidrig gehalten wird, da es einen solchen – zudem „privaten“ – Rechtfertigungstatbestand nach der DSGVO (insbesondere seines Art. 6 Abs. 1) nicht gibt, ist die Zulässigkeit der Videoüberwachung/Datenverarbeitung „zur Wahrnehmung berechtigter Interessen“ nach der DSGVO grundsätzlich möglich (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Dies allerdings nur, „...sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen...“, was mit der (oben ausgeführten) Vorgabe der Interessenabwägung für eine Zulässigkeit der Videoüberwachung in § 4 Abs. 1 Satz 2 BDSG-E (neu) jedenfalls speziell in Bezug auf die Beschäftigten in den Einkaufszentren, Ladenlokalen etc. konfliktiert. Diese Beschäftigten in „öffentlich zugänglichen Räumen“ sind aber angesichts der „Zwangssituation“ bzw. ihrer existenziellen Abhängigkeit von Arbeitgebern, die ständige und anlasslos Videoüberwachung (z. B. in Ladenlokalen) betreiben und dabei „zufällig“ (als „unbeabsichtigtes“ Nebenprodukt) ihre Verkäufer/innen mit aufnehmen, besonders schutzwürdig. Schon seitens des europäischen Ordnungsgebers gibt es daher – wie vorstehend bereits skizziert – die Möglichkeit, solchen oder ähnlich weiten Interpretationen des Art. 4 Abs. 1 DSGVO im Beschäftigungskontext zu begegnen: Der nationale Gesetzgeber oder die Kollektivparteien können für die Datenverarbeitung im Beschäftigungskontext (Art. 88 Abs. 1 DSGVO) „spezifischere Vorschriften“ schaffen, die diesen Besonderheiten – ähnlich wie in Bezug auf die Einwilligung nach § 26 Abs. 2 BDSG-E (neu) – Rechnung tragen. Deshalb sollte der deutsche Gesetzgeber dem jetzt nachkommen und nicht noch die Videoüberwachung im Beschäftigungskontext erleichtern!

Zu begrüßen ist, dass der Gesetzentwurf die Absätze 2 bis 5 des geltenden § 6b BDSG durch die Regelungen des § 4 Abs. 2 bis 5 BDSG-E (neu) weitestgehend übernommen hat. Jedoch sollte in der vorliegenden Vorschrift (§ 4 BDSG-E –neu) – zur Beilegung des bislang insoweit bestehenden und zur Vermeidung zukünftigen dogmatischen Streits – klargestellt werden, dass für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext im Hinblick auf Videoüberwachung die Spezialnorm des § 26 BDSG-E (neu) ergänzend hinzutritt.

Zudem muss in der Gesetzesbegründung klar herausgestellt werden, dass mit der Fortführung der Regelung des geltenden § 32 Abs. 1 BDSG in § 26 Abs. 1 BDSG-E in Bezug auf die Videoüberwachung in nicht öffentlich zugänglichen Räumen die bisherige Rechtslage fortgeführt und nicht verschlechtert werden soll.

Teil 2: Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

Rechtsgrundlagen der Verarbeitung personenbezogener Daten (Kapitel 1)

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken (Abschnitt 1)

Zu § 22: Verarbeitung besonderer Kategorien personenbezogener Daten

Soweit ersichtlich, sind Verschärfungen der Einwilligung bei der Verarbeitung personenbezogener Daten – etwa das Erfordernis der Ausdrücklichkeit in § 4a Abs. 3 BDSG – in der vorliegenden Vorschrift nicht vorgesehen. Dies ist angesichts der besonderen Sensibilität dieser Daten auch nach Maßgabe der DSGVO nicht hinnehmbar. Art. 9 Abs. 2 lit. a DSGVO deckt als Öffnungsklausel für den Ausschluss einer Einwilligung bei der Verarbeitung die Überführung von § 4a Abs. 3 BDSG in die vorliegende Vorschrift. Die Einwilligung **der/des Beschäftigten** in die Verarbeitung ihrer/seiner personenbezogenen Daten bedarf insgesamt dringend einer **spezifischen Regelung**. Diese Regelung muss gewährleisten, dass die Grundsätze der Freiwilligkeit und der Informiertheit sichergestellt werden. Dabei können und sollten auch die besonderen Umstände, die in Bezug auf sensitive Daten zu beachten sind, Berücksichtigung finden. Diesen – einschränkenden - Prämissen kommt auch die im Gesetzentwurf gegenüber dem Referentenentwurf ergänzte spezifische Regelung der Verarbeitung „besonderer Kategorien“ personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses nach Maßgabe des § 26 Abs. 3 BDSG-E (neu) nur unzureichend nach (vgl. nachfolgende Stellungnahme zu Teil 2 Kapitel 1 Abschnitt 2 des Gesetzentwurfs).

Zu § 24: Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen

Zwar stellt die im Gesetzentwurf gegenüber dem Referentenentwurf vorgenommene (systematische) Differenzierung der Verarbeitung zu anderen Zwecken zum einen durch öffentliche Stellen, zum anderen durch nicht-öffentliche Stellen, durch (zwei) gesonderte Normen sowie die (inhaltliche) Beschränkung in der Vorschrift des § 24 Abs. 1 BDSG-E (neu) auf nur noch zwei Fallgruppen eine Verbesserung dar. Insbesondere ist die weit gefasste und einseitig auf wirtschaftliche Interessen bezogene Normierung von „zulässigen“ Zweckänderungsgründen, die gegen den Wortlaut von Art. 6 Abs. 4 und Art. 23 Abs. 1 DSGVO verstoßen hätten, größtenteils beseitigt worden (etwa der Zulässigkeitstatbestand „zur Wahrung berechtigter Interessen des Verantwortlichen“). Allerdings ist § 23 Abs. 1 **Nr. 2** BDSG-E (neu) des Gesetzentwurfs gegenüber den Anforderungen der DSGVO immer noch zu weit gefasst: Zwar ermöglicht Art. 6 Abs. 4 DSGVO den Mitgliedsstaaten für die Rechtmäßigkeit der Verarbeitung (inzidenter) den Erlass von Rechtsvorschriften, die Zweckänderungen erlauben. Diese Erlaubnis soll nach Art. 23 Abs. 1 lit. j DSGVO jedoch lediglich „die Durchsetzung zivilrechtlicher Ansprüche“ sicherstellen. Gesetzliche Zweckänderungsregelungen zur Durchsetzung aller „rechtlichen“ Ansprüche (§ 24 Abs. 1 Nr. 2 BDSG-E neu) sieht die DSGVO jedoch nicht vor. Insoweit ist diese Erweiterung im Gesetzentwurf – etwa auf Ansprüche verwaltungsrechtlicher Art – unverhältnismäßig und europarechtswidrig; der Begriff „rechtlicher“ (Ansprüche) in Abs. 1 Nr. 2 sollte daher im BDSG-E (neu) durch „zivilrechtlicher“ abgeändert und ersetzt werden.

Darüber hinaus bedarf es – nach Maßgabe der hierzu ermächtigenden Öffnungsklausel des Art. 88 Abs. 1 DSGVO – einer spezialgesetzlichen Einschränkung zulässiger Zweckänderungen für Zwecke des Beschäftigungsverhältnisses in § 26 BDSG-E (neu), um einer etwaig möglichen Interpretation weiter (als bislang nach Maßgabe des geltenden § 32 BDSG) reichender Zweckänderungen durch Art. 6 Abs. 4 DSGVO und damit einer Verschlechterung der datenschutzrechtlichen Position von Arbeitnehmerinnen und Arbeitnehmern vorzubeugen. Gleiches gilt für eine erforderliche gesetzliche Klarstellung im Rahmen des § 26 BDSG-E (neu), dass die allgemeine Interessenabwägung nach Maßgabe des Art. 6 Abs. 1 lit. f DSGVO im Beschäftigungskontext nicht greift, da § 26 BDSG-E (neu) insoweit als abschließende Sonderregelung zu betrachten ist, wonach der Begriff der „Durchführung“ des Arbeitsverhältnisses (§ 26 Abs. 1 BDSG-E neu) weit zu verstehen ist und bereits eine spezielle Interessenabwägung beinhaltet.

Besondere Verarbeitungssituationen (Abschnitt 2)

Zu § 26 (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses)

Der überwiegende Erhalt und die grundsätzliche Weitergeltung des § 32 Abs. 1 bis 3 und des § 3 Abs. 11 des geltenden BDSG in Gestalt des § 26 Abs. 1 bis 8 BDSG-E (neu) werden vom DGB und seinen Mitgliedsgewerkschaften begrüßt, soweit nicht die bestehende Reichweite des Beschäftigtendatenschutzes durch die Herausnahme des nichtautomatisierten Anwendungsbereichs aus Abs. 2 des geltenden § 32 BDSG eine Einschränkung erfährt.) Mit dieser Streichung im neuen § 26 Abs. 7 geht eine Verschlechterung des Beschäftigtendatenschutz-Niveaus des BDSG-E (neu) gegenüber dem geltenden BDSG einher. Angesichts des Wegfalls (etwa von § 4 des geltenden BDSG) oder der Modifizierung von weiteren Bestimmungen des geltenden BDSG durch die DSGVO sowie deren Eröffnung einer Konkretisierung der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext durch Rechtsvorschriften oder Kollektivvereinbarungen nach Maßgabe des Art. 88 Abs. 1 DSGVO, bedarf es jedoch weiterer ergänzender Regelungen im BDSG-E (neu).

Hierzu im Einzelnen wie folgt:

Zu Abs. 1 (Zulässigkeit der Beschäftigten-DV - Erhalt des Inhalts von § 32 Abs. 1 BDSG):

Die Übernahme der bisher geltenden Vorschrift des § 32 Abs. 1 BDSG durch den vorliegenden Abs. 1 des Gesetzentwurfs ist grundsätzlich zu begrüßen. Positiv ist hervorzuheben, dass die Ergänzung in Satz 1 des Abs. 1 [„...oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag oder einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten...“] erstmalig die Datenverarbeitung auch für Zwecke der Interessenvertretungen regelt. Allerdings erscheint eine Angleichung der Begrifflichkeit „schutzwürdiges Interesse“ (*der oder des Beschäftigten an dem Ausschluss der Verarbeitung* in Satz 2 des Abs. 1) an die Terminologie der DSGVO im Hinblick auf schutzwahrende Maßnahmen bei der Regelung spezifischerer Vorschriften für den Beschäftigungskontext nach Maßgabe des Art. 88 Abs. 2) DSGVO zweckmäßig und geboten („...und die berechtigten Interessen oder

Grundrechte und Grundfreiheiten der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegen,...“).

Zu Abs. 2 (Verarbeitung von Beschäftigtendaten auf der Grundlage einer **Einwilligung**)

Grundsätzlich zu begrüßen ist, dass in den Gesetzentwurf gegenüber dem Referentenentwurf eine Einschränkung der Einwilligung in die Verarbeitung personenbezogener Daten nach Maßgabe der allgemeinen Grundsätze der DSGVO (Art. 6 Abs. 1 lit. a) für die besondere Verarbeitungssituation einer Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses i.S. einer spezifischeren Vorschrift (Art. 88 Abs. 1 DSGVO) aufgenommen wurde. Nach Auffassung des DGB und seiner Mitgliedsgewerkschaften darf wegen der Besonderheit des Ungleichgewichts (Abhängigkeit) zwischen dem/der Beschäftigten und dem Arbeitgeber als Datenverarbeitendem die Einwilligung des/der Beschäftigten in die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis nur unter engen Voraussetzungen eine Rechtsgrundlage für die Erhebung und Verarbeitung von personenbezogenen Daten darstellen. Soweit die Einwilligung im Beschäftigungsverhältnis – gegenüber Art. 6 und Art. 9 DSGVO – ausnahmsweise als Rechtfertigung möglich sein soll, muss sie an strenge Voraussetzungen (vgl. auch Art. 7 DSGVO, Erwägungsgründe 42, 43, 155) geknüpft werden. Zutreffend soll nach Abs. 2 Satz 3 grundsätzlich das in der DSGVO fehlende (im geltenden BDSG aber enthaltene) **Schriftformerfordernis** fortgeführt werden. Denn mit einem Wegfall des Schriftformerfordernisses würde auch die damit bislang einhergehende Warnfunktion, mit der der Betroffene - durch die Notwendigkeit einer eigenhändigen Unterschrift - vor einer unüberlegten und vorschnellen Entscheidung abgehalten wurde, entfallen. Zum anderen kommt es ohne Schriftformerfordernis auch zu Einbußen an Rechtssicherheit hinsichtlich des Bestehens einer Einwilligung als Erlaubnistatbestand im konkreten Fall, die bislang durch das Schriftformerfordernis gewährleistet werden konnte. Dies ist auch für die datenverarbeitende Stelle nach Art. 7 Abs. 1 DSGVO von großer Bedeutung, da sie die Beweislast dafür trägt, dass der Betroffene seine Einwilligung zu der Verarbeitung seiner personenbezogenen Daten erteilt hat. Im Falle einer bloß mündlich oder konkludent erteilten Einwilligung wird dieser Nachweis regelmäßig nicht zu führen sein (auf die Nachweispflicht des Arbeitgebers als einer der Gründe für die gesetzlich grundsätzlich angeordnete Schriftform als formelle Voraussetzung einer Einwilligung weist auch die Begründung des Gesetzentwurfs hin). Allerdings ermöglicht die Vorschrift in Satz 4 „wegen besonderer Umstände“ (ausnahmsweise) auch eine andere „angemessene“ Form anstelle der Schriftform für die Einwilligung. Um insoweit Missbrauch auszuschließen und in solchen Fällen einem verminderten Schutz der betroffenen Beschäftigten vorzubeugen, bedarf es einer ausgleichenden und flankierenden Regelung, die im Anschluss an Abs. 2 Satz 4 wie folgt ergänzt werden sollte: „Wird die Einwilligung nach § 4a Absatz 1 Satz 3 BDSG [*beziehungsweise nach § 26 Abs. 2 DSGVO-E als Nachfolgenorm*] in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen [...] kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.“ Diese Regelung entspricht § 28 Abs. 3a des geltenden BDSG

und würde insofern als spezifische Vorschrift für den Beschäftigungskontext das bisherige Datenschutzniveau erhalten.

Ergänzend bedarf es jedoch einer ausdrücklichen Regelung, dass die Einwilligung nur bezogen auf einen genau umschriebenen **Verwendungsvorgang** unter Benennung der gebilligten Verbreitungsziele und Verbreitungsphasen erteilt werden kann. Durch den Verweis in Abs. 2 Satz 4 auf Art. 7 Abs. 3 DSGVO ist zwar klargestellt, dass die Einwilligung **jederzeit widerrufen** werden kann. Ergänzungsbedarf besteht jedoch an einem klarstellenden (besonderen) Maßregelungsverbot, wonach sich der Widerruf oder die Ablehnung der Einwilligung **nicht zum Nachteil** des oder der Beschäftigten auswirken darf. Schließlich muss in diesem Zusammenhang ausdrücklich ergänzend normiert werden, dass der Arbeitgeber im Fall des Widerrufs der Einwilligung durch die Beschäftigte bzw. den Beschäftigten die aufgrund der Einwilligung erhobenen Daten unverzüglich zu löschen hat. Es muss zudem sichergestellt werden, dass der oder die Beschäftigte vor der Erteilung der Einwilligung ausführlich über den Zweck oder die Zwecke der Datenverarbeitung, die strenge Zweckbindung, die Freiwilligkeit der Einwilligung, das Benachteiligungsverbot im Weigerungsfalle, das jederzeitige Widerrufsrecht und die daraus resultierende Löschungsverpflichtung unterrichtet wird. Insoweit bedauern der DGB und seine Mitgliedsgewerkschaften, dass die Bundesregierung der von den Gewerkschaften geforderten umfassenden Aufklärungspflicht des Arbeitgebers nur unzureichend durch eine Normierung in Satz 4 des Abs. 2 des vorliegenden Gesetzentwurfs in Bezug auf die Angabe des Zwecks der Datenverarbeitung und auf das bestehende Widerrufsrecht nachgekommen ist.

Soweit man dem Ansatz des Gesetzentwurfs zur (definitiven) Möglichkeit des Vorliegens einer „Freiwilligkeit“ für die Beurteilung der Einwilligung in Satz 2 des Abs. 1 folgt, ist dieser Hinweis auf den Maßstab für die Beurteilung der Freiwilligkeit einer Einwilligung jedenfalls unzureichend: Zunächst ist darauf hinzuweisen, dass eine Einwilligung für die Verarbeitung von Beschäftigtendaten im Beschäftigungskontext nach Auffassung des DGB und seiner Mitgliedsgewerkschaften - entgegen der nach Satz 1 des Abs. 2 vorausgesetzten Einzelfallprüfung - generell und ohne Prüfung in jedem Einzelfall nur **ausnahmsweise** als Rechtsgrundlage angesehen werden kann. Sie kann in Bezug auf die Durchführung und Beendigung des Arbeitsverhältnisses - ausnahmsweise - dann als rechtmäßig angesehen werden, wenn die daraus resultierenden rechtlichen oder wirtschaftlichen Folgen für den abhängig Beschäftigten **überwiegend** vorteilhaft sind. Eine „irgendwie“ geartete Vorteilhaftigkeit, wie jedoch Satz 2 ausreichen lässt, kann als Hinweis auf die Freiwilligkeit der Einwilligung nicht ausreichen. Die Vorteilhaftigkeit der Folgen einer Einwilligung müssen für den Beschäftigten gegenüber den Vorteilen, die der Arbeitgeber aus der Einwilligung zieht, zumindest überwiegen (mehr als 50%). So fehlt es auch nach der Rechtsprechung des BGH grundsätzlich an der Freiwilligkeit einer Einwilligung, wenn diese „in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird“ (vgl. BGH Urte. v. 16.7.2008 – VIII ZR 348/06, DuD 2008, 818 (820) – Payback; Urte. v. 11.11.2009 – VIII ZR 12/08, DuD 2010, 493 (495) – Happy Digits). Im Bewerbungsverfahren ist das Kriterium einer – auch überwiegenden – Vorteilhaftigkeit für den – angehenden – Beschäftigten hingehend untauglich, da (auch) nach weit überwiegender Auffassung in der Literatur (vgl. für viele: Taeger/Rose, BB 2016, 819FF., 822; Wybitul/Pötters, RdA 2016, 10ff., 12f.;

Stelljes, DuD 2016, 1ff., 2, mit Hinweis auf BVerfG vom 23.11.2006 – 1 BvR 1909/06, NJW 2007, 286.) in dieser Situation eine Freiwilligkeit der Einwilligung kaum denkbar ist, weil der Bewerber das Verlangen des Arbeitgebers nach einer Einwilligung immer als Einstellungsvoraussetzung für den Arbeitsplatz verstehen wird, der er zur Erlangung dieser Existenzgrundlage zustimmen muss. Daher muss für diese Situation (im Bewerbungsverfahren) die Einwilligung als Rechtfertigungsmöglichkeit generell ausgeschlossen werden, um das bestehende Datenschutzniveau zu erhalten. Auch eine solche Differenzierung lässt die Regelung des Abs. 2 Satz 2 leider vermissen.

Schließlich muss – sowohl im Zuge eines Bewerbungsverfahrens, als auch in Bezug auf Durchführung und Beendigung des Arbeitsverhältnisses - ausgeschlossen sein, dass der Erhalt oder die Erhaltung des Arbeitsplatzes als vorteilhaft gilt oder sich der Arbeitgeber die Einwilligung durch finanzielle Zuwendungen an den/die Arbeitnehmer/in „erkauft“; darauf ist zumindest in der Gesetzesbegründung ergänzend hinzuweisen. Denn insbesondere wirtschaftliche Vorteile, wie beispielsweise Prämien oder Zulagen, haben für die allermeisten Beschäftigten teilweise existentielle Bedeutung. Insoweit haben sie keine freie Wahl, die Einwilligung zu verweigern oder zurückzuziehen, soweit ihnen dadurch der wirtschaftliche Vorteil wieder entzogen wird. Zudem bestehen Bedenken, ob die in Abs.2 Satz 2 vorgesehene Regelung nicht gegen das Koppelungsverbot nach Art. 7 Abs. 4 DSGVO verstößt. Als bessere Alternative sollte für die Beurteilung der Freiwilligkeit der Einwilligung anstelle des Erreichens eines (überwiegenden) rechtlichen oder wirtschaftlichen Vorteils für die beschäftigte Person – unter Berücksichtigung der Erwägungsgründe 43 und 44 der DSGVO – im Gesetz definiert werden: „Freiwilligkeit liegt vor, wenn die betroffene Person eine echte und freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.“

Zu Abs. 3 (Verarbeitung besonderer Kategorien personenbezogener Daten)

Nach Art. 9 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt und nur unter den in Abs. 2 des Art. 9 DSGVO genannten Ausnahmen (lit. a bis j) zulässig. Durch Umfang und Konkretisierungsgrad der beschriebenen Ausnahmebestimmungen ist diese Verordnungsvorschrift umfassend und abschließend. Der deutsche Gesetzgeber verstößt daher mit seiner Regelung in Abs. 3 des § 26 BDSG-E (neu) gegen das europarechtliche „Wiederholungsverbot“, zumal diese Regelung keine Einschränkung der DSGVO-Ausnahmen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses (zugunsten des Beschäftigten-datenschutzes) darstellt. Jedenfalls erschließt sich die Spezifizierung dieser Sonderregelung für den Beschäftigungskontext nicht i.S. einer Ausnahmegesetzvorschrift. Sie erscheint (etwa im Hinblick auf die Zulassung einer Einwilligung der betroffenen Person nach Satz 2 in die Verarbeitung besonderer Kategorien personenbezogener Daten zur Aufhebung der Untersagung nach Art. 9 Abs. 1 DSGVO sowie den Verweis in Satz 3 auf § 22 Abs. 2 BDSG-E neu, ohne spezifisch geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person zu formulieren) zu Lasten des Datenschutzniveaus der Beschäftigten weiter gehender, als dies die DSGVO zulässt (etwa durch ein nach Art. 9 Abs. 2 lit. a DSGVO mögliches

nationales Verbot der – ausdrücklichen – Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext, durch das die Untersagung nach Art. 9 Abs. 1 DSGVO nicht aufgehoben würde).

Anstelle dieser zweifelhaften Ausformung der Vorschrift für die Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext erscheint stattdessen ein Verweis auf Art. 9 DSGVO als ausreichend, sofern dieser überhaupt nötig ist.

Zu Abs. 4 (Beschäftigten-DV auf der Grundlage von Kollektivvereinbarungen)

Die Regelung, dass eine Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig ist, ist grundsätzlich ebenso zu begrüßen, wie der – insbesondere für die Betriebsparteien wichtige – rechtliche Verweis und Hinweis auf die (neben den nationalen Schutzregelungen, etwa des – geltenden – BDSG sowie der §§ 75, 80 Abs. 1 BetrVG bzw. der einschlägigen Vorschriften des Personalvertretungsrechts) dabei zu beachtenden Schutzmaßnahmen nach Maßgabe des Art. 88 Abs. 2 DSGVO.

Anders als durch den wegfallenden § 4 BDSG, der Kollektivvereinbarungen (Tarif- und Betriebsvereinbarungen) i.S. einer „anderen Rechtsvorschrift“ (vgl. § 4 Abs. 1 des geltenden BDSG) als Erlaubnistatbestand für die Zulässigkeit von personenbezogenen Datenverarbeitungen angesehen hat, werden Kollektivvereinbarungen mangels Nachfolgenorm für § 4 des geltenden BDSG und in der vorliegenden Vorschrift nicht explizit als Legitimationstatbestand genannt. Allerdings räumt die DSGVO in Art. 88 Abs. 1 den Mitgliedstaaten ausdrücklich die Befugnis ein, durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Beschäftigtendatenschutzes vorzusehen, die unionsrechtlich dann den gleichen materiellen Anforderungen unterliegen wie eigene Rechtsvorschriften der Mitgliedsstaaten, insbesondere dem Abs. 2 des Art. 88 DSGVO und den allgemeinen Grundsätzen aus Art. 5 DSGVO. Erwägungsgrund 155 nennt dabei Betriebsvereinbarungen explizit als Beispiel. Zwar lässt sich auf diesem Hintergrund vertreten, dass der Status quo insoweit erhalten bleibt, weil bereits nach geltendem Recht eine entsprechende Legitimation als „andere Rechtsvorschrift“ im Sinne des geltenden § 4 Abs. 1 BDSG anerkannt ist, und gegenwärtig unmittelbar aus dem Unionsrecht abgeleitet wird. Da dies aber nicht eindeutig ist und in Frage gestellt wird, ist die vorliegende ausdrückliche gesetzliche Regelung notwendig, dass die Ausgestaltung des Beschäftigtendatenschutzes durch Tarifverträge und Betriebsvereinbarungen im Sinne des § 87 Abs. 1 Eingangssatz BetrVG (sowie von Dienstvereinbarungen nach Maßgabe der einschlägigen personalvertretungsrechtlichen Regelungen) zusätzlich weiterhin national möglich ist. Damit wird zugleich eine rechtssichere Datenverarbeitung auf der Grundlage von (auch allgemeinverbindlichen) Tarifverträgen sichergestellt. Bei spezifischer Regelung der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses durch tarifliche oder betriebliche Vereinbarungen müssen diese mindestens dem gesetzlichen Niveau entsprechen.

Diese Bestimmung der kollektiven Regelungsbefugnis reicht nach Auffassung des DGB und seiner Mitgliedsgewerkschaften in Bezug auf die Regelungsinstrumente der Kollektivpartei

„Betriebsrat“ zur Wahrnehmung seiner Aufgaben i.S. des Art. 88 DSGVO aber nicht aus: Damit bei Betriebsvereinbarungen beide Vertragsparteien an deren Ausgestaltung und den Verhandlungen nach Maßgabe des Abs. 4 auf Augenhöhe mitwirken können, bedarf es weiter einer gesetzlichen Verankerung eines – über den Anwendungsbereich des geltenden Mitbestimmungsrechtes (§ 87 Abs. 1 Nr. 6 BetrVG) hinaus gehenden – erzwingbaren und einigungsstellenbewährten Mitbestimmungsrechts, das generell die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext umfasst. Dies gilt auch für den Anwendungsbereich des Bundespersonalvertretungsrechts, da die §§ 68 Abs. 1 Nr. 2, 75 Abs. 3 Nr. 17, 76 Abs. 2 Nr. 2, 5 und 7 BPersVG die Mitbestimmung des Personalrats bei sämtlichen Vorgängen, die die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses beinhalten, nicht hinreichend und umfassend sicherstellen. Daher muss § 26 BDSG-E (neu) oder (bereichsspezifisch) § 87 Abs. 1 BetrVG um ein solches Mitbestimmungs- und Initiativrecht ergänzt werden.

Zu Abs. 5 (Beachtung von DV-Grundsätzen im Beschäftigungskontext)

Der Verweis in Abs. 5 auf die Verpflichtung des Verantwortlichen „geeignete Maßnahmen“ zu ergreifen und sicherzustellen, dass „insbesondere die in Art. 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden“, ist europarechtlich unzureichend (und wäre ohne Spezifizierung entbehrlich). Abs. 5 erfüllt damit in keiner Weise die Anforderungen des Art. 88 Abs. 2 DSGVO. Vielmehr ist der Gesetzgeber für die spezifische Ausgestaltung der Öffnungsklausel der DSGVO für den Beschäftigungskontext insoweit gehalten, Vorschriften zu erlassen, die angemessene und besondere Maßnahmen zur Wahrung der Persönlichkeitsrechte der Beschäftigten umfassen. Durch konkrete Vorschriften zum „Datenschutz durch Technik“ wäre es beispielsweise möglich, Löschroutinen oder Verfalltermine für gespeicherte Beschäftigtendaten genau vorzugeben. Satz 1 sollte daher durch folgenden Satz ergänzt werden: „Dazu gehören technische und organisatorische Maßnahmen zur Vermeidung von Beschäftigten-Profilings. Dazu gehört insbesondere auch, dass zu unterschiedlichen Zwecken verarbeitete Beschäftigtendaten klar voneinander getrennt, frühzeitig gelöscht oder anonymisiert und dem Trennungsgebot entsprechende Zugriffsrechte eingerichtet werden.“

Zu Abs. 6 (Klarstellungshinweis):

Die Beibehaltung des klarstellenden Hinweises nach Maßgabe des § 32 Abs. 3 des geltenden BDSG auf die gesonderte **Geltung der Beteiligungsrechte der Interessenvertretungen** der Beschäftigten durch Abs. 6 wird begrüßt.

Zu Abs. 7 (Analoge Anwendung § 32 Abs. 1 BDSG a.F. auf nicht-automatisierte DV):

Der DGB und seine Mitgliedgewerkschaften begrüßen, dass auch § 32 Abs. 2 des geltenden BDSG als Abs. 7 in die vorliegende Norm des § 26 BDSG-E (neu) übernommen wird. Sie lehnen jedoch ab, dass diese Regelung – entgegen noch der Formulierung in § 24 BDSG-E des Referentenentwurfs – nunmehr von der Beschreibung des Anwendungsbereichs in Art. 2 Abs. 1 der DSGVO ausgeht. Dieser Anwendungsbereich erfasst die nichtautomatisierte Datenverarbeitung nicht vollständig. § 32 Abs. 2 des geltenden BDSG ist aber

(gleichsam) für den Beschäftigungskontext als eine „spezifischere“ Regelung i.S. des Art. 88 Abs. 1 DSGVO für eine Erweiterung dieses Anwendungsbereichs der DSGVO beizubehalten. Ansonsten ist die **nichtautomatisierte Verarbeitung personenbezogener Daten, die auch nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen**, durch diese Regelung nicht mehr erfasst. Die Erfassung der nichtautomatisierten Datenverarbeitung in den Schutzbereich des Abs. 1 ist von besonderer praktischer Bedeutung in der Arbeitswelt etwa hinsichtlich des Fragerechts des Arbeitgebers, der Überwachung von Arbeitnehmern durch Detekteien oder des Abhörens von Telefonaten, sofern hier jeweils keine Speicherung erfolgt. Durch die Streichung der nichtautomatisierten Datenverarbeitung aus dem Anwendungsbereich sind darüber hinaus aber auch handschriftliche Notizen, etwa in Bewerbungsgesprächen oder von Beschäftigten ausgefüllte Arbeitsbögen (etwa Erhebungen vor Umstrukturierungen etc.), die nicht in ein Dateisystem überführt werden sollen, nicht mehr erfasst. Hierdurch ergibt sich eine datenschutzrechtliche Verschlechterung für die Beschäftigten, die nicht hingenommen werden kann.

Darüber hinaus greifen in diesen Fällen auch die Betroffenenrechte nicht, da diese ebenfalls im BDSG-E (neu) auf die Anwendung der DSGVO verweisen, die wiederum für das Eröffnen ihres Anwendungsbereichs – anders als § 1 Abs. 2 des geltenden BDSG – zumindest eine (beabsichtigte) Speicherung in einem Dateisystem voraussetzt (vgl. Art. 2 Abs. 1 DSGVO). Dies gilt beispielhaft für das Auskunftsrecht in Art. 15 DSGVO in Bezug auf die von der DSGVO nicht erfassten handschriftlichen Notizen, die nicht in einem Dateisystem erfasst werden. Auch insoweit bedarf es für die Datenverarbeitung im Beschäftigungskontext einer entsprechenden Klarstellung, damit die Reduktion des Anwendungsbereichs der DSGVO nicht zu einer Verschlechterung des Status quo des datenschutzrechtlichen Niveaus für die Beschäftigten führt.

Zu Abs. 8 (Definition des Beschäftigtenbegriffs) Der DGB und seine Mitgliedsgewerkschaften begrüßen die in Abs. 8 erfolgte – lediglich redaktionell überarbeitete und aktualisierte – Übernahme der geltenden Begriffsbestimmungen aus § 3 Abs. 11 des geltenden BDSG und ihre Integration in die vorliegende Norm mit der Ergänzung, dass der Beschäftigtenbegriff auch Leiharbeitnehmer im Verhältnis zum Entleiher erfasst. Diese sind in den Betrieb des Entleihers eingegliedert und seinen Weisungen unterworfen, so dass sie bezüglich ihrer Schutzbedürftigkeit zutreffend auch in datenschutzrechtlicher Hinsicht den Stammbeschäftigten gleichgestellt werden. Richtigerweise werden Leiharbeitnehmer auch schon nach geltender Rechtslage den eigenen Beschäftigten des Entleihers gleichgestellt (vgl. Simitis, § 3 BDSG, 8. Aufl., § 3 Rn. 283 m.w.N.). Durch das aktuelle Gesetzgebungsverfahren wurde somit die Gelegenheit ergriffen, durch eine ausdrückliche gesetzliche Klarstellung die Rechtsanwendung durch höhere Klarheit des Gesetzestextes zu vereinfachen.

Zu erwägen ist jedoch weiter, auch andere im Betrieb tätige Personen, die keinen Arbeitsvertrag mit dem Betriebsinhaber geschlossen haben (etwa Beschäftigte eines beauftragten Unternehmens oder auf Werkvertragsbasis), in Bezug auf die Daten, die aufgrund ihrer Tätigkeit vom Betriebsinhaber verarbeitet werden, dem gleichen Datenschutzregime wie Stammbeschäftigte zu unterstellen, zumal aus dieser Datenverarbeitung unter bestimmten

Konstellationen auch Rückschlüsse möglich sind auf Leistung und Verhalten der Stammbeschäftigten.

Weitere Regelungserfordernisse für die Datenverarbeitung im Beschäftigungskontext:

Um den Besonderheiten des abhängigen Beschäftigungsverhältnisses gegenüber allgemeinen Datenverarbeitungssituationen gerecht zu werden, für die den Mitgliedsstaaten die Option der Regelung „spezifischerer Vorschriften“ zur Gewährleistung des Schutzes der Rechte und Freiheiten der Betroffenen vom Ordnungsgeber eingeräumt wurde, sind **weitere ergänzende bzw. konkretisierende Regelungen**, vorzugsweise durch Integration in die vorliegende Vorschrift (§ 26 BDSG-E – neu), erforderlich. In ihrer Notwendigkeit unabweisbar sollten – neben der für Zwecke des Beschäftigungsverhältnisses erforderlichen Konkretisierung einer Einwilligung (Abs. 2), der (klarstellenden) Ermächtigung einer Verarbeitung personenbezogener Daten auf der Grundlage von Kollektivvereinbarungen (Abs. 4), das die Schaffung eines ergänzenden Initiativ- und Mitbestimmungsrechts für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext (generell) voraussetzt, sowie von zu beachtenden Datenschutzgrundsätzen (Abs. 5) – durch spezialgesetzliche Vorschriften im Beschäftigungskontext die **Einschränkung zulässiger Zweckänderungen**, die **Einschränkung der Videoüberwachung im Beschäftigungskontext** und die **Grenzen der Zulässigkeit der Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien** geregelt werden.

Hierzu im Einzelnen wie folgt:

Zweckänderungen unter den besonderen Bedingungen der abhängigen Beschäftigung:

Nach Auffassung des DGB und seiner Mitgliedsgewerkschaften bedarf es im Rahmen dieser Vorschrift (§ 26 BDSG-E neu) – nach Maßgabe der hierzu ermächtigenden Öffnungsklausel des Art. 88 Abs. 1 DSGVO – einer spezialgesetzlichen **Einschränkung zulässiger Zweckänderungen** (nach Maßgabe der allgemeinen Vorschrift des § 24 BDSG-E – neu) für den Beschäftigungskontext, um einer etwaig möglichen Interpretation von weiter – als bislang nach dem geltenden § 32 BDSG – reichenden Zweckänderungen durch Art. 6 Abs. 4 DSGVO und damit einer Verschlechterung der datenschutzrechtlichen Position von Arbeitnehmerinnen und Arbeitnehmern vorzubeugen. Dies könnte beispielsweise – in Sektor spezifischer Weiterführung des geltenden § 31 BDSG – auch eine **besondere Zweckbindung** für solche personenbezogenen Beschäftigtendaten beinhalten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden (zur Ergänzung einer entsprechenden Vorschrift des § 31 BDSG in dieser Norm: vgl. nachfolgende Ausführungen).

Um einer Verschlechterung der datenschutzrechtlichen Position von Arbeitnehmerinnen und Arbeitnehmern vorzubeugen, ist gleichsam auch eine gesetzliche Klarstellung im Rahmen der Norm zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (§ 26 BDSG-E neu) (oder – ersatzweise – in § 24 BDSG-E neu mit Hinweis auf die Besonderhei-

ten einer „Verarbeitung personenbezogener Daten zu anderen Zwecken durch nicht-öffentliche Stellen“ im Beschäftigungskontext) mit dem Inhalt erforderlich, dass die allgemeine Interessenabwägung nach Maßgabe des Art. 6 Abs. 1 lit. f DSGVO im Beschäftigungskontext nicht greift, da die vorliegende Norm des § 26 BDSG-E (neu) insoweit als abschließende Sonderregelung zu betrachten ist, wonach der Begriff der „Durchführung“ des Arbeitsverhältnisses (Abs. 1) weit zu verstehen ist und bereits eine spezielle Interessenabwägung beinhaltet.

Videoüberwachung unter den besonderen Bedingungen der abhängigen Beschäftigung:

Der Entwurf stellt nach seinem Wortlaut in § 4 BDSG-E (neu) – entgegen der Begründung des Gesetzentwurfs (die insoweit auf einen nicht existenten Satz 2 des Abs. 1 des geltenden BDSG verweist) – keine gleichartige Fortführung von § 6b BDSG für den Beschäftigungskontext – unter Beibehaltung der bisherigen nationalen Maßstäbe – dar. Durch die Verknüpfung des (neuen) Satzes 2 des § 4 Abs. 1 BDSG-E (neu), der aus dem Gesetzentwurf der Bundesregierung eines der Terrorismusbekämpfung dienenden „Videoüberwachungsverbesserungsgesetzes“ (BuRats-Drs. 791/16 vom 30.12.2016) übernommen wurde, mit Satz 1 des Abs. 1 dieser Norm (der den Voraussetzungen des geltenden BDSG entspricht), beeinträchtigt die Abwägungsentscheidung für die Zulässigkeit der Videoüberwachung generell die „schutzwürdigen Interessen der Betroffenen“, da diese Entscheidung zugunsten der Zulässigkeit einer Videoüberwachung und ihrer Betreiber, etwa von Einkaufszentren, quasi vorgegeben ist (vgl. vorstehende Ausführungen zu § 4 BDSG-E neu). Damit ist es aber auch einem Arbeitgeber als Betreiber einer solchen Videoüberwachungsanlage unter Berufung auf die Wahrung der besonderen Schutzgüter Leben, Gesundheit oder Freiheit jederzeit gleichsam möglich, in solchen Einkaufszentren mit Ladenlokalen seine Beschäftigten – noch dazu dauerhaft – zu überwachen. Daher muss zur Wahrung der Persönlichkeitsrechte der Beschäftigten die Videoüberwachung im Beschäftigungskontext spezifisch in § 26 BDSG-E (neu) geregelt werden. Insoweit ist in dieser Vorschrift – zur Beilegung des bislang insoweit bestehenden und zur Vermeidung zukünftigen dogmatischen Streits – klarzustellen, dass für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext im Hinblick auf Videoüberwachung die vorliegende spezifische Norm (§ 26 BDSG-E neu) ergänzend hinzutritt. Dazu sind Regeln zur Videoüberwachung und Kontrolle von Beschäftigten in nicht allgemein zugänglichen Bereichen sowie Regeln zur Videoüberwachung in allgemein zugänglichen Bereichen in der Folge) zu formulieren. Diese spezifischen Regelungen sollten Grundsätze für eine Videoüberwachung für Zwecke des Beschäftigungsverhältnisses wie folgt ausformen:

- Offene optisch-elektronische Überwachung der nicht öffentlich zugänglichen Teile des Betriebs, die überwiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, insbesondere in Sanitär-, Umkleide-, Pausen- und Schlafräumen, sind unzulässig.
- Offene optisch-elektronische Überwachung der öffentlich zugänglichen Teile des Betriebs oder der nicht öffentlich zugänglichen Teile des Betriebs, die nicht über-

wiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, wie Eingangsbereiche, Foyers, Werkhallen o. ä., sind nur zulässig aus Gründen der Sicherheit der Arbeitnehmer und des Betriebs. Soweit nicht unumgänglich, sollte die Überwachung öffentlich zugänglicher Teile des Betriebs den Arbeitnehmer an seinem Arbeitsplatz nicht mit erfassen.

- Vor der Durchführung der Überwachung ist der Arbeitnehmer darüber zu unterrichten, wann und wie lange die Überwachungsinstrumente in Betrieb genommen werden.
- Aufzeichnungen der Überwachung sind zeitnah, spätestens innerhalb eines Monats nach Vornahme der Überwachung, zu löschen. Die ordnungsgemäße Löschung unterliegt der vierteljährlichen Kontrolle des betrieblichen Datenschutzbeauftragten oder der zuständigen Aufsichtsbehörde.
- Offene akustisch-elektronische Überwachung ist nur aus zwingenden Gründen der öffentlichen Sicherheit zulässig, etwa im Cockpit von Flugzeugen.
- Die heimliche Überwachung ist in jedem Fall unzulässig.

Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien:

Ergänzungsbedarf für eine Aufrechterhaltung des bisherigen Datenschutzniveaus besteht weiter gegenüber den – insoweit defizitären – Vorschriften des Entwurfs auch in Bezug auf bislang fehlende **Regelungen zur Zulässigkeit der Nutzung mobiler personenbezogener Speicher- und Verarbeitungsmedien** entsprechend § 6 c des geltenden BDSG (vgl. hierzu auch die vorstehenden Ausführungen zu § 2 Begriffsbestimmungen). Zwar finden sich hierzu in den allgemeinen Datenschutzregelungen der DSGVO gleichsam keinerlei Regelungen. Die Verwendung von Chipkarten (bspw. zur Zugangskontrolle), SIM-Karten im Mobilfunkbereich, Systeme der Radio Frequency Identification (RFID), spielt in der betrieblichen Realität jedoch eine große Rolle. Daher haben Regelungen über die Zulässigkeit und Voraussetzungen ihrer Nutzung, auch wegen des insoweit bestehenden Überwachungspotenzials im Beschäftigungskontext, eine große Bedeutung. Ein (ersatzloser) Fortfall der bisherigen Regelung des § 6c BDSG würde den derzeit bestehenden rechtlich vorgegebenen Datenschutzstandard für abhängig Beschäftigte senken, weshalb dieses Defizit durch eine spezialgesetzliche Regelung für den Beschäftigungskontext ausgeglichen werden muss.

Besondere Zweckbindung unter den Bedingungen der abhängigen Beschäftigung:

Ergänzungsbedarf besteht schließlich in der besonderen Datenverarbeitungssituation für Zwecke des Beschäftigungsverhältnisses in Bezug auf die **Fortführung der Regelungen zur strengen Zweckbindung von personenbezogenen Daten**, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert sind. Ein vergleichbarer strenger spezieller Zweckbindungsgrundsatz, wie dieser im geltenden § 31 BDSG normiert ist, findet sich zwar in der DSGVO nicht. Der dort in Art. 5 Abs. 1 lit. b DS-GVO allgemein geregelte

Grundsatz der Zweckbindung wird zudem durch die ausnahmsweise zulässige Zweckänderung (Art. 6 Abs. 4 DS-GVO) relativiert. Aber gerade im Beschäftigungskontext gilt es, die insoweit bestehenden Möglichkeiten des Arbeitgebers zum Schutz der abhängig Beschäftigten zu beschränken, auf große Datenbestände zum Nachteil der Arbeitnehmerinnen und Arbeitnehmer zurückgreifen zu können. Insoweit bedarf es einer spezialgesetzlichen Regelung.

Fortführung bereichsspezifischer Regelungen (z. B. §§ 19-21 Gendiagnostikgesetz)

Für den Beschäftigungskontext spielt der Umgang mit genetischen Beschäftigtendaten eine große Rolle. Für die datenschutzrechtliche Regelung sind die §§ 19 ff. GenDG als sektorspezifische Spezialvorschriften einschlägig. Demnach sind genetische Untersuchungen und Analysen (einschließlich des Einforderns und Verwertens von Ergebnissen bereits vorgenommener Untersuchungen oder Analysen) grundsätzlich unzulässig und bußgeldbewehrt. Hinsichtlich biometrischer Beschäftigtendaten greift mangels spezieller Regelung die „Generalklausel“ des geltenden § 32 BDSG. Da die DSGVO hier keine Änderungen bringt, weil sie in Art. 9 Abs. 4 für die Verarbeitung von genetischen, biometrischen und Gesundheitsdaten zusätzliche Bedingungen einschließlich Beschränkungen zulässt, sind entsprechende Sonderregelungen auf der Grundlage und im Rahmen der Öffnungsklausel des Art. 88 DSGVO ausdrücklich erlaubt. Soweit bislang § 32 BDSG einschlägig ist, greift künftig der normativ identische § 26 BDSG (neu). Daher bleiben diese Regelungen des GenDG unberührt (vgl. hierzu § 1 Abs. 2 Satz 1 BDSG-E –neu).

Dies gilt gleichsam für Eignungstests, deren Zulässigkeit primär am Allgemeinen Persönlichkeitsrecht aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG zu messen ist. Datenschutzrechtlich müssen Eignungstests im Sinne des § 32 Abs. 1 Satz 1 des geltenden BDSG „erforderlich“ sein, also nach wissenschaftlich anerkannten Methoden Auskunft über die gesuchte Eignung geben und von einem berechtigten und billigenswerten schutzwürdigen Interesse des Arbeitgebers an der Durchführung getragen sein; außerdem muss die Einwilligung des Beschäftigten in die Teilnahme am Test und dessen Durchführung vorliegen.

Zu § 31: Scoring

Während § 28b des geltenden BDSG eine Sondervorschrift für das Scoring zur Verfügung stellt, besteht hierzu in der DSGVO keine spezielle Vorschrift. Anknüpfungspunkte lassen sich jedoch aus Art. 6 Abs. 1 U Abs. 1 lit. f, Art. 23 Abs. 1 lit. i Alt. 2, und Art. 22 sowie Erwägungsgrund 71 der DSGVO entnehmen. Der vorliegende Entwurf übernimmt fast wortidentisch die Regelungen des § 28b BDSG. Die weite Fassung dieser Anpassungsvorschrift, wie sie noch in einem Vorentwurf (§ 39 Abs. 2 und 3 ABDSG-E) enthalten war und die dem bislang geltenden Datenschutzstandard nach dem BDSG nicht gerecht wurde, ist – soweit ersichtlich – (jedenfalls in diesem unmittelbaren Zusammenhang) beseitigt. Damit bleibt es bei der bestehenden Rechtslage nach dem geltenden BDSG, was von Seiten des DGB und seiner Mitgliedsgewerkschaften begrüßt wird.

Rechte der betroffenen Person (Kapitel 2)

Die Kritik des DGB und seiner Mitgliedsgewerkschaften richtet sich gegen eine starke Einschränkung der Informations-, Auskunfts-, Löschungs- und Widerspruchsrechte der betroffenen Personen im nicht-öffentlichen Bereich durch den Gesetzentwurf. Insoweit dürfen keine Regelungen aus dem BDSG übernommen werden, die hinter den Vorgaben der DSGVO zurück bleiben. Die Betroffenenrechte in der DSGVO (insbesondere Art. 13 DSGVO) sind tendenziell gar – schutzbezogen – umfassender ausgestaltet, als die des geltenden BDSG (vgl. insoweit §§ 19-21 und §§ 33-35 BDSG). Nach der DSGVO bestehen lediglich beschränkte Öffnungsklauseln (vgl. Anforderungen des Art. 23 DSGVO), die die im Entwurf vorgesehenen Einschränkungen der Betroffenenrechte nicht abdecken. Hierzu beispielhaft im Einzelnen wie folgt:

Zu § 32: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Die Kritik gilt im Bereich der Regelungen zu den Betroffenenrechten für die zu weit gehende Beschränkung der Informations- und Benachrichtigungspflicht, insbesondere durch Abs. 1 Nr. 1 der vorliegenden Vorschrift wegen eines „unverhältnismäßigen Aufwandes“. Dieses Kriterium wird auch nicht durch eine Interessenabwägung flankiert, da eine Abwägung mit den Interessen der betroffenen Person nicht vorgesehen ist. Eine solche das Unterrichtsrecht einschränkende Ausnahme kennt das BDSG in diesem Kontext nicht, und sie wird auch nicht durch die Vorgaben der DSGVO gestützt (vgl. die Anforderungen in Art. 23 DSGVO), zumal das (offensichtliche) Ziel, die verantwortliche Stelle vor hohem Aufwand zu bewahren, nicht als Ausdruck des Schutzes der Rechte und Freiheiten anderer Personen i.S. des Art. 23 Abs. 1 lit. i) angesehen werden kann. Zielrichtung dieser Norm der DSGVO ist der Schutz Dritter, nicht der Schutz des Verantwortlichen selbst. Zudem hat es der Verantwortliche selbst in der Hand, durch die Organisation seiner Datenverarbeitung zu bestimmen, wie groß der jeweilige Aufwand ausfällt. Art. 14 Absatz 5 lit. b DSGVO, auf den sich der in der Begründung genannte Erwägungsgrund 62 bezieht, erhält nur für die Fälle, in denen die Datenverarbeitung nicht bei der betroffenen Person erfolgt, eine Ausnahmemöglichkeit.

Daher sollte diese Ausnahme der Nr. 1 des Abs. 1 ersatzlos gestrichen werden, während der Begriff „rechtlicher“ (Ansprüche) in Nr. 4 des Abs. 1 – entsprechend der Vorschrift des Art. 23 Abs. 1 lit. j DSGVO, die nicht die Einschränkung der Informationspflicht zur Durchsetzung aller „rechtlichen“ Ansprüche ermöglicht - durch den Begriff „zivilrechtlicher“ ersetzt werden sollte.

Zu § 33: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

Die Kritik richtet sich gegen die Einschränkung der Informationspflicht gemäß Art. 14 Abs. 1 und 2 DSGVO, insbesondere durch Abs. 1 Nr. 2 lit. a der vorliegenden Vorschrift, soweit (im Falle einer nicht-öffentlichen Stelle) die Information die Geschäftszwecke des Verantwortlichen erheblich gefährdet. Nach Auffassung des DGB und seiner Mitgliedsgewerkschaften ist eine solche rein privatnützige Einschränkung nicht von der DSGVO gedeckt. Die

DSGVO kennt keinen Ausnahmetatbestand der „allgemein anerkannten Geschäftszwecke des Verantwortlichen“, sondern erlaubt in diesem Zusammenhang nur Einschränkungen zugunsten der in Art. 23 Abs. 1 lit. i und j genannten Ziele. Daher sollte Nr. 2 lit. a) dieser Vorschrift ersatzlos gestrichen werden.

Zu § 34: Auskunftsrecht der betroffenen Person

Die Kritik richtet sich – entsprechend den Ausführungen zu § 33 BDSG-E (neu) – insbesondere gegen die Einschränkung des Auskunftsrechts der betroffenen Person gemäß Art. 15 DSGVO durch Abs. 1 Nr. 1 (zumal Art. 23 DSGVO nicht die vorliegenden Abweichungen rechtfertigt). Zu begrüßen ist die gegenüber dem Referentenentwurf gestrichene Ausnahme, wonach eine nicht-öffentliche Stelle die Auskunft über die in Art. 15 Abs. 1 lit. c und g sowie Abs. 2 der DSGVO genannten Informationen verweigern kann, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse der betroffenen Person überwiegt. Ein rein privatnütziges Interesse kann nicht Ausgangspunkt einer Interessenabwägung sein.

Daher sollte die Vorschrift des Abs. 1 Nr. 1 nach Maßgabe der Anforderungen des Art. 23 DSGVO überarbeitet und sollten die darüber hinaus gehenden Einschränkungen – wie die über § 34 Abs. 1 Nr. 1 BDSG-E (neu) in Bezug genommene Ausnahme des § 33 Abs. 1 Nr. 2 lit. a) – gestrichen werden.

Zu § 35: Recht auf Löschung

Auch insoweit richtet sich die Kritik – entsprechend der vorstehenden Ausführungen zu § 32 BDSG-E (neu) – insbesondere gegen eine Negierung des Rechts der betroffenen Person zur Löschung personenbezogener Daten gemäß Art. 17 Abs. 1 DSGVO im Falle eines „unverhältnismäßigen Aufwandes“ (Abs. 1), ohne dass auch nur eine Abwägung mit den Interessen der betroffenen Person vorgesehen ist. Art. 23 Abs. 1 DSGVO rechtfertigt die vom Gesetzentwurf in Abs. 1 erlaubte Beschränkung des Löschanpruchs nicht, da dort kein Ausnahmetatbestand der Vermeidung eines unverhältnismäßig hohen Aufwandes normiert ist, sondern in diesem Zusammenhang nur die in Art. 23 Abs. 1 lit. i und j DSGVO genannten Tatbestände Einschränkungen der Betroffenenrechte rechtfertigen können. Auch bestünde bei der vorgeschlagenen Entbindung von der Löschpflicht aufgrund der besonderen Art der Speicherung die Gefahr, dass das Recht auf Löschung dadurch umgangen würde, dass entsprechende Speicherungsarten gewählt würden, um die Lösungsverpflichtung zu verhindern.

Da diese Einschränkung des Abs. 1 gegen die europarechtlichen Vorgaben der DSGVO verstößt, sollte sie ebenso ersatzlos gestrichen werden wie Abs. 3, der auf diese durch die DSGVO nicht gestützte Beschränkung Bezug nimmt.

Zu § 36: Widerspruchsrecht

Diese vom Gesetzentwurf vorgesehene Norm erweitert den Ausschluss des Widerspruchsrechts über Art. 21 Abs. 1 der DSGVO hinaus in einem Maße, das durch Art. 23 Abs. 1 DSGVO nicht gerechtfertigt ist. Nach Art. 21 Abs. 1 Satz 2 DSGVO ist es dem Verantwortlichen möglich, die personenbezogenen Daten trotz Widerspruchs zu verarbeiten, wenn er zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. In diesen Fällen nicht nur die durch den Widerspruch angegriffene Verarbeitung ausnahmsweise zu erlauben, sondern das Recht auf Widerspruch sogar ganz auszuschließen, kann nicht als dem Wesensgehalt des Grundrechts achtende und in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Art. 23 DSGVO angesehen werden.

Diese gegen die europarechtlichen Vorgaben der DSGVO verstoßende Vorschrift sollte ersatzlos gestrichen werden.

Zu § 37: Automatisierte Entscheidung im Einzelfall einschließlich Profiling

Diese vom Gesetzentwurf vorgesehene Regelung in Abs. 1 **Nr.1** würde eine Schlechterstellung der betroffenen Person im Versicherungsvertragsverhältnis im Vergleich zu allen anderen Vertragsverhältnissen darstellen, die nicht mit dem Gemeinwohlinteresse begründet werden kann (vgl. Art. 22 Abs. 2 lit. b in Verbindung mit Art. 23 Abs. 1 lit. e DSGVO). Sie würde zu einer anwenderunfreundlichen weiteren Zersplitterung der Anwendung der DSGVO beitragen und damit eine wirksame Wahrnehmung der Rechte durch die Betroffenen verkürzen. Die weiter in Abs. 2 **Nr. 2** vorgesehene Regelung ist darüber hinaus nicht erforderlich, weil die Datenverarbeitung – einschließlich der darauf beruhenden automatisierten Einzelfallentscheidungen – für die Leistungserbringung durch Versicherungen bereits nach Art. 22 Abs. 2 lit. a DSGVO zulässig ist.

Da die Regelungen dieser Vorschrift gegen die europarechtlichen Vorgaben der DSGVO verstößt, sollte die Vorschrift insgesamt ersatzlos gestrichen werden.

Pflichten der Verantwortlichen und Auftragsverarbeiter (Kapitel 3)

Zu § 38: Datenschutzbeauftragte nicht-öffentlicher Stellen

Der DGB und seine Mitgliedsgewerkschaften begrüßen den Ansatz einer weitreichenden Regelung auf der Basis der Art. 37 bis 38 DSGVO mit der vorliegenden Vorschrift. Die Reichweite der Bestellpflicht, die sich nach dem Gesetzentwurf aus den §§ 5 Abs. 1, 38 Abs. 1 BDSG-E (neu) ergibt, entspricht im Wesentlichen den Vorgaben des geltenden § 4f Abs. 1 BDSG. Hinzu kommen über den Verweis in § 38 Abs. 1 Satz 1 BDSG-E (neu) auf Art. 37 Abs. 1 lit. b und c DSGVO noch die dort spezifisch hervorgehobenen Fallgruppen. Jenseits der genannten Fallgruppen wird die Bestellpflicht für Verantwortliche und Auftragsverarbeiter auch weiterhin greifen, soweit sie „in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen“ (§ 38 Abs. 1 Satz 1 BDSG-E neu). Das ist im Ergebnis identisch zur bisherigen Regelung, die spiegelbildlich die Bestellpflicht bei höchstens neun entsprechend Beschäftigten entfallen ließ.

§ 38 Abs. 2 i.V.m. § 6 Abs. 3 Satz 1 BDSG-E (neu) enthält zwar eine Regelung zur Weisungsfreiheit nur für öffentliche Stellen; ergänzend ergibt sich eine umfassende Weisungsfreiheit jedoch aus Art. 38 Abs. 3 DSGVO. Das Benachteiligungsverbot wurde ebenso beibehalten (§ 38 Abs. 2 i.V.m. § 6 Abs. 3 S. 2 BDSG-E neu entspricht § 4f Abs. 3 S. 3 des geltenden BDSG), wie der Kündigungsschutz des Datenschutzbeauftragten, da § 5 Abs. 6 BDSG-E neu (für nicht-öffentliche Stellen i.V.m. § 38 Abs. 2 BDSG-RefE) § 4f Abs. 3 Sätze 4 - 6 des geltenden BDSG entspricht.

Sanktionen (Kapitel 5)

Zu § 41: Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

Durch Abs. 1 Satz 1 (Anwendung des Gesetzes über Ordnungswidrigkeiten) werden grundsätzlich auch Verstöße nach Art. 83 Abs. 4 bis 6 DSGVO erfasst. Nach der Begründung des Gesetzentwurfs geht die vorliegende Regelung des AnpUG (EU) davon aus, dass von den in Art. 83 Abs. 4 und 5 DSGVO genannten „Verstößen gegen die folgenden Bestimmungen“ auch dann gesprochen werden kann, wenn die Mitgliedsstaaten bzgl. der in den Abs. 4 und 5 des Art. 83 der DSGVO genannten Bestimmungen nationale Regelungen aufgrund von Öffnungsklauseln erlassen haben. Dies ist aufgrund der ausdrücklichen Regelung in Art. 83 Abs. 5 lit. d) DSGVO nachzuvollziehen, die **alle Pflichten gemäß den Rechtsvorschriften der Mitgliedsstaaten, die im Rahmen des Kapitels IX erlassen wurden** (zu diesen gehören auch diejenigen nach Art. 88 über die - spezifischere Vorschriften zur - Datenverarbeitung im Beschäftigungskontext, mithin auch die Pflichten nach § 26 BDSG-E neu) als eine dieser „folgenden Bestimmungen“ der dort geregelten Haftung bei entsprechenden Verstößen unterstellt.

Zweifel bestehen jedoch, ob diese unmittelbare Anwendung der DSGVO-Haftungsvorschriften für Pflichtverstöße auch für die Vorschrift des Art. 82 DSGVO (Haftung und Recht auf Schadensersatz), in Frage kommt, die in Abs. 1 einen Anspruch auf Schadensersatz wegen eines materiellen, aber auch immateriellen Schadens aufgrund eines Verstoßes **gegen diese Verordnung** regelt. Nach der Begründung des Gesetzentwurfs ergibt sich diese Folge einer Erfassung auch solcher nationalen Bestimmungen über Pflichtverstöße aus Erwägungsgrund 146 Satz 5 der DSGVO, der einen „vollständigen und wirksamen Schadensersatz“ für erlittene Schäden auch aufgrund einer Verarbeitung folgert, „die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsakten und Rechtsvorschriften der Mitgliedsstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht.“

Diese Erläuterung scheint zwar die Aussage in der Begründung des Gesetzentwurfs zu bestätigen. Da Erwägungsgründe jedoch keinen normativ-verpflichtenden Charakter haben, sondern lediglich als „Auslegungsgrundsätze“ für den Verpflichtungsteil der Verordnung fungieren, sollte – um jegliche Zweifel an der unmittelbaren Anwendbarkeit der DSGVO-Haftungsvorschriften zu beseitigen – angesichts der Bedeutung von (gerade auch immateriellen) Schadensersatzansprüchen von Beschäftigten in der besonderen Verarbeitungssitua-

tion von Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses eine solche Haftung gegenüber Verstößen und das Bestehen eines entsprechenden Rechts durch eine **ausdrückliche Klarstellung im Rahmen der vorliegenden Gesetzesnorm** (oder hilfsweise im Rahmen der spezifischen Vorschriften für den Beschäftigungskontext in § 26 BDSG-E neu,) erfolgen.

Nicht einschlägig ist dagegen § 83 BDSG-E (neu), da diese Vorschrift Regelungen zu Schadensersatz und Entschädigung im dritten Teil des BDSG-E (neu) nach Maßgabe des § 45 BDSG-E (neu) ausschließlich in Umsetzung von Art. 56 der Richtlinie (EU) 2016/680 trifft.

Ausblick

Der Handlungsspielraum für den deutschen Gesetzgeber ist durch Art. 88 DSGVO weit eröffnet. Das mit diesem Entwurf vorgelegte Gesetz zur Anpassung des nationalen Datenschutzrechts an die DSGVO kann daher für die personenbezogene Verarbeitung von Beschäftigtendaten im Beschäftigungskontext nur einen ersten Schritt zur umfassenden Regelung des Beschäftigtendatenschutzes darstellen, die in einem eigenständigen Beschäftigtendatenschutzgesetz vorzunehmen ist. Insbesondere in folgenden weiteren Themenbereichen, die nach dem Entwurf und den voranstehenden Ausführungen dazu offen bleiben, ist ein wirksamer Schutz bei Erhebung und Verarbeitung personenbezogener Daten erforderlich und einer mitgliedstaatlichen Ausgestaltung gem. Art. 88 Abs. 1 und Abs. 2 zugänglich:

- Zugriff auf personenbezogene oder beziehbare Daten bei der **Verwendung moderner Kommunikationsmittel**;
- Umfang des **Fragerechts des Arbeitgebers** sowie **Regeln zur Zulässigkeit ärztlicher Untersuchungen und Eignungstests**;
- **Verwertung und Aufbewahrung von Daten** vor, während und nach der Beendigung des Beschäftigungsverhältnisses;
- Umgang mit **Daten aus sozialen Medien**;
- Datenschutz bei **Bring Your Own Device**;
- **Beweisverwertungsverbot** von unrechtmäßig erhobenen Daten.

Zur effektiven Durchsetzung des Beschäftigtendatenschutzes sind die allgemeinen Vorgaben des Kapitel VIII (Art. 77 ff.) der DSGVO entsprechend den Anforderungen des Beschäftigungskontextes mitgliedstaatlich auszuformen:

Es müssen an den Beschäftigungskontext angepasste **Schadensersatz- und Sanktionsregelungen** sowie individuelle und kollektive **Rechtsdurchsetzungsmechanismen** – hier insbesondere ein umfassendes **Verbandsklagerecht** – eingeführt werden.

Schließlich müssen einer eigenständigen gesetzlichen Regelung die **Grundsätze der Datenvermeidung und der Datensparsamkeit** sowie – unter Bezugnahme auf die Transparenzanforderungen der DSGVO – der Grundsatz der Direkterhebung beim Beschäftigten zugrunde liegen.

Stellungnahme

zu Artikel 1
des Entwurfs der Bundesregierung für ein Daten-
schutz-Anpassungs- und -Umsetzungsgesetz EU
(DSAnPUG-EU¹),
BR-Drs. 110/17 vom 2. Februar 2017

Kontakt:

Dr. Christian Koch / Jan Schmidt-Seidl

Telefon: +49 30 2021-2321 / 2319

E-Mail: c.koch@bvr.de / j.schmidt-seidl@bvr.de

Berlin, 20. Februar 2017

Federführer:

Bundesverband der Deutschen
Volksbanken und Raiffeisenbanken e. V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

¹ Voller Titel: „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“

Inhalt

Stellungnahme	1
I. Allgemein	4
1. Rechtzeitige Begleitgesetzgebung ist erforderlich	4
2. Fortführung von BDSG-Vorschriften im Rahmen des EU-rechtlich Möglichen ist wichtig, um den Umsetzungsaufwand bei datenverarbeitenden Stellen in Grenzen zu halten und Kontinuität zu erreichen	4
3. Rolle des betrieblichen Datenschutzbeauftragten im nicht öffentlichen Bereich ist zu wahren	4
4. Zuständigkeit von Datenschutzbehörden auch bei innerstaatlichen Sachverhalten mit bundesweiter Bedeutung klären	5
5. Verständlichkeit für den Rechtsanwender verbessern	5
II. Zu den für Kreditinstitute relevanten Vorschriften in Artikel 1 DSAnpUG-EU (BDSG-E)	5
1. Überblick	5
2. § 4 Videoüberwachung: Informationspflicht praktikabel halten	6
3. § 20 Gerichtlicher Rechtsschutz: Rechtsweg im Bußgeldverfahren	6
4. § 24 Verarbeitung zu anderen Zwecken durch nicht öffentliche Stellen: Fortführung von Vorschriften zur Zweckänderung ist sinnvoll	7
5. § 26 Datenverarbeitung im Beschäftigungskontext: „Kleine Lösung“ des BDSG reicht zunächst, Einwilligungslösung erhalten	7
6. § 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften: Übermittlung und Nutzung von Daten über fällige Forderungen muss besser geregelt werden	8
7. § 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person: Angemessenen Interessenausgleich herstellen	10
8. § 33 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden: Weitere Ausnahmen aus dem heutigen § 33 Absatz 2 BDSG berücksichtigen	11
9. § 34 Auskunftsrecht der betroffenen Person: Angemessenen Interessenausgleich wahren	11
10. § 35 Recht auf Löschung: Weiterführung der heutigen Sperrmöglichkeit	12
11. § 37 Automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling: Rahmen der DS-GVO beachten	12
12. § 38 Datenschutzbeauftragte nicht öffentlicher Stellen: Rolle erhalten	13
13. § 40 Aufsichtsbehörden der Länder für nicht öffentliche Stellen: Zuständigkeitsfragen klären	14
14. § 41 Bußgeldverfahren: Differenzierung zwischen der verantwortlichen Stelle und deren Mitarbeitern	14

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

- 15. § 43 Bußgeldvorschriften: Systematik verbesserungsbedürftig 15**
- 16. Klarstellung in Bezug auf die Reichweite der Datenportabilität nach Artikel 20 DS-GVO bei der Kontowechselhilfe nach §§ 20 ff. ZKG 15**

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

I. Allgemein

1. Rechtzeitige Begleitgesetzgebung ist erforderlich

Die EU-Datenschutz-Grundverordnung 2016/679 (DS-GVO) gilt ab dem 25. Mai 2018 u. a. in Deutschland unmittelbar. Damit wird das bislang geltende Bundesdatenschutzgesetz (BDSG) zu weiten Teilen hinfällig. Gleichwohl räumt die DS-GVO dem nationalen Gesetzgeber in bestimmten Fällen noch Gestaltungsspielräume ein. Es ist daher sehr zu begrüßen, dass noch in dieser Legislaturperiode ein Begleitgesetz zur DS-GVO geschaffen werden soll, um von diesen Gestaltungsmöglichkeiten rechtzeitig Gebrauch zu machen. Für die Umsetzung des neuen Datenschutzrechts ab Mai 2018 durch die Unternehmen ist es von sehr hoher Bedeutung, dass das Gesetzesvorhaben bis zum Sommer 2017 abgeschlossen wird. Nur so erhalten die datenverarbeitenden Stellen Rechtsklarheit und -sicherheit. Eine spätere Begleitgesetzgebung könnte faktisch nicht mehr bis zum Mai 2018 berücksichtigt werden.

2. Fortführung von BDSG-Vorschriften im Rahmen des EU-rechtlich Möglichen ist wichtig, um den Umsetzungsaufwand bei datenverarbeitenden Stellen in Grenzen zu halten und Kontinuität zu erreichen

Bei den Regelungen in § 4 und §§ 22 bis 38 BDSG-E ist das Anliegen der Bundesregierung zu unterstützen, im Rahmen des EU-rechtlich Möglichen bewährte Vorschriften aus dem heutigen BDSG weiterzuführen. Damit wird der aus der DS-GVO resultierende erhebliche Umsetzungsaufwand auf ein vernünftiges Maß begrenzt und Kontinuität wird erreicht. Denn beispielsweise eine möglichst weitgehende Fortführung der Ausnahmetatbestände bei den Informations- und Auskunftspflichten nach den heutigen §§ 33 Absatz 2 und 34 Absatz 7 BDSG gewährleistet, dass der Umstellungsaufwand für die datenverarbeitenden Stellen nicht noch höher ausfällt als wirklich notwendig.

Unseres Erachtens sind die mit der bisherigen EU-Datenschutzrichtlinie kompatiblen Ausnahmegründe in der Gesamtbetrachtung aller zu berücksichtigenden Grundrechte der involvierten Parteien nach wie vor ein angemessener Ausgleich zwischen dem informationellen Selbstbestimmungsrecht des Betroffenen einerseits und Schutzgütern von verfassungsrechtlichem Rang der datenverarbeitenden Stellen (z. B. Wahrung von Geschäftsgeheimnissen) andererseits. Der Grundsatz des Übermaßverbots hat auch im Lichte der DS-GVO weiterhin seine Berechtigung.

3. Rolle des betrieblichen Datenschutzbeauftragten im nicht öffentlichen Bereich ist zu wahren

Die in § 38 BDSG-E vorgesehene Fortführung der Institution des betrieblichen Datenschutzbeauftragten im nicht öffentlichen Bereich ist zu begrüßen. Jedoch sollten die diesbezüglichen Vorschriften in §§ 4f und 4g BDSG zu den Eigenschaften und den Aufgaben des betrieblichen Datenschutzbeauftragten so weit wie im Lichte der DS-GVO möglich, erhalten bleiben, damit die Ausübung dieses Amtes in gleicher Qualität fortgesetzt werden kann und Kontinuität erreicht wird. So ist beispielsweise die im heutigen § 4f Absatz 3 Satz 1 BDSG geregelte unmittelbare Unterstellung des Datenschutzbeauftragten unter die Geschäftsleitung des Unternehmens wichtig, damit dieser seiner Aufgabe in gleicher Weise und Qualität gerecht wer-

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

den kann. Für den Datenschutzbeauftragten im öffentlichen Bereich wird mit § 6 BDSG-E bereits dieser Weg beschritten.

4. Zuständigkeit von Datenschutzbehörden auch bei innerstaatlichen Sachverhalten mit bundesweiter Bedeutung klären

Mit § 40 BDSG-E soll die Zuständigkeit der Aufsichtsbehörden der Länder für nicht öffentliche Stellen fortgesetzt werden. Da die DS-GVO bei grenzüberschreitenden Sachverhalten besondere Regeln zur Zuständigkeit von Aufsichtsbehörden in den einzelnen EU-Mitgliedstaaten und zur Abstimmung deren Aufsichtshandelns enthält, müssen diese Leitlinien zur Kooperation erst recht bei einer föderalen Aufsichtsstruktur innerhalb eines EU-Mitgliedstaats gelten. Ansonsten könnte das Harmonisierungsziel der DS-GVO innerstaatlich verfehlt werden. Sollte dieses Thema in der nur noch kurzen Legislaturperiode nicht mehr geklärt werden können, sollte es gleich zu Beginn der neuen Legislaturperiode aufgegriffen werden.

5. Verständlichkeit für den Rechtsanwender verbessern

Im Unterschied zur heutigen Rechtslage, wird der Rechtsanwender im Datenschutz zukünftig mehrere Rechtsquellen – DS-GVO, BDSG und bereichsspezifische Vorschriften im europäischen und nationalen Recht – parallel im Blick haben müssen (vgl. auch § 1 Absätze 2 und 5 BDSG-E). Dies ist aufgrund der Konstruktion der DS-GVO und des sonstigen EU-Rechts kaum vermeidbar, aber für die Umsetzung und Auslegung der Vorschriften eine deutliche Erhöhung der Komplexität. Für die Anwendungspraxis wäre es hilfreich, die Rangfolge und das Ineinandergreifen der maßgeblichen Rechtsquellen in § 1 BDSG-E sowie in den relevanten Vorschriften noch verständlicher zu beschreiben. Dazu folgendes Beispiel: § 24 BDSG-E regelt zwei Fälle von zulässigen Zweckänderungen. Daraus könnte der Leser den voreiligen Schluss ziehen, dass es nur diese beiden Fälle gibt, obwohl Artikel 6 Absatz 4 DS-GVO weitere Fälle der zulässigen Zweckänderung beschreibt. § 24 BDSG-E wäre aus sich heraus verständlicher, wenn dort in geeigneter Weise zum Ausdruck käme, dass die übrigen Fallgestaltungen aus § 6 Absatz 4 DS-GVO daneben gelten.

II. Zu den für Kreditinstitute relevanten Vorschriften in Artikel 1 DSAnpUG-EU (BDSG-E)

1. Überblick

Wie oben bereits unter Abschnitt I.2 ausgeführt, begrüßen wir sehr den Ansatz, heutige BDSG-Vorschriften im Rahmen des EU-rechtlich Möglichen fortzuführen, um den Umsetzungsaufwand bei datenverarbeitenden Stellen in Grenzen zu halten und Kontinuität zu wahren. Deshalb unterstützen wir insbesondere die vorgesehenen Vorschriften in §§ 4 Absatz 1, 22, 24, 26, 30, 31 Absatz 1, 32, 33 und 34 BDSG-E.

Dagegen sehen wir insbesondere bei folgenden Regelungen Verbesserungsbedarf, der im Nachfolgenden im Einzelnen begründet wird:

- § 4 Absatz 2 – Videoüberwachung

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

- § 31 – Scoring
- § 35 – Löschung
- § 37 – Automatisierte Einzelentscheidung
- § 38 – betrieblicher Datenschutzbeauftragter
- § 40 – Aufsichtsbehörden
- § 41 – Sanktionen.

2. § 4 Videoüberwachung: Informationspflicht praktikabel halten

Die Videoüberwachung in „öffentlich zugänglichen Räumen“ hat in der Kreditwirtschaft erhebliche Bedeutung. Beispiele sind die Kameraüberwachung in den Geschäftsstellen der Institute und an Serviceterminals, wie insbesondere Geldausgabeautomaten. Daher ist es sehr zu begrüßen, dass § 4 Absatz 1 Satz 1 BDSG-E nunmehr den Wortlaut von § 6b Absatz 1 BDSG a. F. übernimmt.

Zu begrüßen ist auch das Anliegen der Bundesregierung, die Informationspflichten bei der Videoüberwachung in § 4 Absatz 2 BDSG-E praktikabel zu halten. Doch sind im Vergleich zu § 6b Absatz 2 BDSG a. F. nicht nur der Umstand der Beobachtung und die verantwortliche Stelle, sondern konkret der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Eine solche Ausdehnung ist nicht praxistauglich, wenn wie bisher und allgemein akzeptiert mit einem Videoaufzeichnungspiktogramm oder einem anderen Kurzhinweis der Betroffene schnell informiert werden soll. Insbesondere die Angabe von Kontaktdaten (= Adresse, Telefonnummer und E-Mail-Adresse) sprengt den umsetzbaren Rahmen. Kreditinstitute als eingetragene Kaufleute, Personenhandelsgesellschaften oder juristische Personen sind bereits durch ihre Firma (vgl. auch § 17 Absatz 1 HGB) eindeutig bestimmbar und eine Angabe von Kontaktdaten ist wegen der jedermann zugänglichen Registerdaten (vgl. Handelsregister und Unternehmensregister der BaFin) überflüssig. Es ist daher vorzuzugswürdig, § 4 Absatz 2 BDSG-E wie § 6b Absatz 2 a. F. zu fassen:

„Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.“

3. § 20 Gerichtlicher Rechtsschutz: Rechtsweg im Bußgeldverfahren

Die Bußgeldvorschriften der DS-GVO lehnen sich insbesondere in der Höhe an entsprechende Regeln im EU-Kartellrecht an. Betrachtet man das Kartellrecht, so fällt auf, dass für dortige Bußgeldverfahren ein besonderer Rechtsweg geregelt ist, um bei den Gerichten Fachzuständigkeiten zu haben. So regeln die §§ 81 und 83 GWB in Bußgeldsachen die Zuständigkeit des Oberlandesgerichts, in dessen Bezirk die zuständige Aufsichtsbehörde ihren Sitz hat. Angesichts des sehr hohen Bußgeldrahmens der DS-GVO und zur Gewährung eines effektiven Rechtsschutzes sollte überlegt werden, den Rechtsweg zumindest ab einer bestimmten Bußgeldhöhe (z. B. 100.000 Euro) so zu gestalten, dass auf das Datenschutzrecht spezialisierte Spruchkörper bei einem Amtsgericht oder bei einer höheren Eingangsinstanz zuständig sind.

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

4. § 24 Verarbeitung zu anderen Zwecken durch nicht öffentliche Stellen: Fortführung von Vorschriften zur Zweckänderung ist sinnvoll

Die vorgesehenen Regeln in § 24 BDSG-E über im Lichte des Artikel 6 Absatz 4 DS-GVO zulässige Zweckänderungen sind zu begrüßen. Sie greifen zu Recht die bislang im BDSG enthaltenen Vorschriften auf und schaffen damit Kontinuität und Rechtssicherheit für die verarbeitenden Stellen. Doch sollte in der Vorschrift deutlicher werden, dass sie nicht abschließend ist, sondern die anderen Fälle der zulässigen Zweckänderung aus Artikel 6 Absatz 4 DS-GVO unberührt bleiben. Ferner ist die Übernahme des bisherigen § 28 Absatz 8 BDSG mit § 24 Absatz 2 BDSG-E sachgerecht.

5. § 26 Datenverarbeitung im Beschäftigungskontext: „Kleine Lösung“ des BDSG reicht zunächst, Einwilligungslösung erhalten

Der Ansatz, den heutigen § 32 BDSG mit § 26 Absatz 1 BDSG-E fortzuführen, ist zu begrüßen, da damit rechtliche Kontinuität und Sicherheit geschaffen sowie der Anpassungsaufwand für Unternehmen begrenzt wird. Aufgrund der kurzen Zeit in der aktuellen Legislaturperiode würde man das Gesetzesvorhaben völlig überfrachten, sogleich weitere Aspekte des Beschäftigtendatenschutzes regeln zu wollen.

Mit § 26 Absatz 2 BDSG-E soll der Grundsatz der Freiwilligkeit von Einwilligungen im Kontext von Beschäftigungsverhältnissen geregelt werden. Zu unterstützen ist die damit verbundene Aussage, dass Einwilligungen auch weiter im Beschäftigungsverhältnis möglich bleiben. Jedoch sollte die Regelung zur Einwilligung im Sinne eines schlankeren Gesetzestextes auf das Notwendige beschränkt werden, damit auch die diesbezügliche Rechtsprechung der Arbeitsgerichte fortgelten kann. Mit Blick auf die Digitalisierungsstrategie der Bundesregierung („digitale Wirtschaft und digitales Arbeiten“) und der zunehmenden Bedeutung von digitalen Arbeitsabläufen erscheint die Anordnung der Schriftform nicht zielführend. Auch sind die Beschäftigten im Datenschutzrecht durch das umfassende Widerrufsrecht zusätzlich geschützt, sodass für die Einwilligung die Textform als ausreichend anzusehen ist. Es wird folgende Formulierung von Absatz 2 vorgeschlagen:

„Die Verarbeitung personenbezogener Daten von Beschäftigten kann auf der Grundlage einer Einwilligung erfolgen. Die Einwilligung bedarf der Textform. Der Arbeitgeber hat die beschäftigte Person [...]“

Die in § 26 Absatz 3 BDSG-E enthaltene Regelung ist sinnvoll, um eine im Beschäftigungsverhältnis häufig erforderliche Verarbeitung sensibler Daten weiter möglich zu machen. Zur Klarstellung sollte erwogen werden, auch den Zweck „Pflichten aus dem Steuerrecht“ als Rechtfertigungsgrund aufzunehmen, da z. B. die Verarbeitung von Daten über den Familienstand und die Religionszugehörigkeit gewährleistet bleiben muss.

Sehr zu unterstützen ist auch § 26 Absatz 4 BDSG-E, wonach die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch auf der Grundlage von Kollektivvereinbarungen zulässig bleibt (vgl. Erwägungsgrund 155 DS-GVO).

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

6. § 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften: Übermittlung und Nutzung von Daten über fällige Forderungen muss besser geregelt werden

Absatz 1 - Rahmenbedingungen für das Scoring

Die Beibehaltung der Vorschrift des heutigen § 28b BDSG mit § 31 Absatz 1 BDSG-E ist aus Gründen der Kontinuität und der Rechtssicherheit sinnvoll. Wie auch in der Gesetzesbegründung zutreffend ausgeführt, wird damit die Bedeutung des (Kredit-)Scorings für die sachgerechte, objektive und effektive Beurteilung der Kreditwürdigkeit von Verbrauchern unterstrichen und insgesamt die Relevanz der Datenverarbeitung bei der Kreditvergabe gewürdigt. Auch hier gilt, dass die Regelung schon aus EU-rechtlichen Gründen nur konkretisierenden Charakter haben und nicht den Erlaubnistatbestand in Artikel 6 und ggf. Artikel 22 DS-GVO einschränken kann. Ferner sollte in den Gesetzesmaterialien auch § 10 KWG berücksichtigt werden, der ähnliche Parameter im Bankaufsichtsrecht für das wesensverwandte Rating definiert².

Absatz 2 - Nutzung von Bonitätsdaten durch Auskunftsteien

Entgegen der Aussage in der Gesetzesbegründung enthält der § 31 Absatz 2 BDSG-E nur noch ein Teilstück des heutigen § 28a BDSG. Deshalb müssen folgende Punkte bedacht werden:

- Der § 28a Absatz 2 BDSG a. F. soll augenscheinlich nicht mehr fortgeführt werden. Folge ist, dass für die Übermittlung von Kundendaten vonseiten des Kreditinstituts an eine Auskunftstei die allgemeinen Erlaubnistatbestände in Artikel 6 DS-GVO gelten, dort insbesondere Artikel 6 Absatz 1a (Einwilligung) und Artikel 6 Absatz 1f (Interessenabwägung) DS-GVO. Es ist daher sehr hilfreich für die praktische Umsetzung, dass mit § 31 Absatz 2 Satz 2 BDSG-E auch gewährleistet werden soll, dass die Datenübermittlung an die Auskunftstei gleichermaßen aufgrund einer Einwilligung des Betroffenen oder einer Interessenabwägung möglich bleibt. Dies erhält der Kreditwirtschaft Gestaltungsspielräume unter Berücksichtigung der DS-GVO.
- Der § 28a Absatz 1 BDSG a. F. soll laut Gesetzesbegründung zwar fortgeführt werden, doch wird mit dem neuen § 31 Absatz 1 Satz 1 BDSG-E die Vorschrift vom Anwendungsbereich bzw. Anknüpfungspunkt deutlich verändert – sprichwörtlich wird das „Pferd von hinten aufgezäumt“. Während bislang die Datenübermittlung von der einmeldenden Stelle (z. B. Kreditinstitut) an die Auskunftstei geregelt wird, soll nunmehr die Verwendung eines von der Auskunftstei ermittelten Wahrscheinlichkeitswertes durch den Datenempfänger (z. B. Kreditinstitut) geregelt werden, wobei auf die bisherigen Einmeldevoraussetzungen in § 28a Absatz 1 Nr. 1 bis 5 BDSG a. F. aufgesetzt wird. Diese Anknüpfung verkennet, dass die etablierten Einmeldevoraussetzungen außerhalb des Kenntniskreises der Auskunftstei und insbesondere des Datenempfängers liegen, die den Wahrscheinlichkeitswert verwenden. Ob eine fällige Forderung besteht, kann nur das an die Auskunftstei übermittelnde Unternehmen beurteilen. Deshalb sollte besser der § 28a Absatz 1 BDSG a. F. fortgeführt werden und in eine eigene Norm im Anschluss an § 31 BDSG-E Eingang finden. Dabei

² Vgl. auch Begründung im Regierungsentwurf von 2008 in BT-Drs. 16/10529 vom 10. Oktober 2008, S. 16: „(...) Die Regelungen des Kreditwesengesetzes, insbesondere die über die Ausgestaltung der internen Risikomessverfahren, und die Regelungen des Versicherungsaufsichtsgesetzes bleiben durch die vorgeschlagenen Regelungen im BDSG unberührt.“

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

könnte der oben positiv bewertete § 31 Absatz 2 Satz 2 BDSG-E dort auch Eingang finden. Die Vorschrift würde somit lauten:

„§ 31a Datenübermittlung an Auskunftsteilen

Die Übermittlung personenbezogener Daten über eine Forderung an Auskunftsteilen ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und (...)

Die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.“

Sollte die im Regierungsentwurf vorgesehene Lösung gleichwohl weiterverfolgt werden, so ist der Wortlaut des § 31 Absatz 2 Satz 1 BDSG-E unbedingt verbesserungsbedürftig. Denn aus der Formulierung könnte gefolgert werden, dass die Auskunftsteil für ihr Scoring nur noch sogenannte Negativdaten nutzen kann. Ein solches Verständnis wäre äußerst problematisch, da Auskunftsteil-Scores in erheblicher Weise durch sogenannte Positivdaten gespeist werden und dies auch im hohen Interesse von Kreditnehmern ist. Denn die Positivdaten (z. B. vertragstreues Verhalten durch rechtzeitige Bedienung von Kreditraten und -zinsen) beeinflussen die Scorewerte zugunsten des Betroffenen. Daher müsste der Satz 1 eingangs wie folgt lauten:

„(2) Die Verwendung eines von Auskunftsteilen ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, nur zulässig, soweit die Voraussetzungen nach Absatz 1 vorliegen und nur solche Forderungen ~~über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist~~, berücksichtigt werden,

1. die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt, (...)

Die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.“

- Was § 31 Absatz 2 Satz 1 Nr. 4c) und Nr. 5 angeht, sollte die Formulierung des § 28a Absatz 1 BDSG a. F. in der Weise beibehalten werden, als dass auf den Begriff „Gläubiger“ verzichtet wird („... der Schuldner zuvor (...) über (...) unterrichtet worden ist“). Andernfalls könnte in Frage gestellt werden, ob auch Inkassounternehmen, die eine Forderung im Namen des Gläubigers geltend machen, weiterhin berechtigt sein sollen, Informationen an Auskunftsteilen zu übermitteln. Dies soll aber der Begründung zufolge ausdrücklich der Fall sein, da die geltende Rechtslage abgebildet werden soll. Hilfsweise sollte eine entsprechende Klarstellung in den Gesetzesmaterialien erfolgen.

Verbesserungsbedürftig erscheint auch die Überschrift zu § 31 BDSG-E. Diese sollte wie § 28b BDSG a. F. auf den Begriff „Scoring“ beschränkt werden, da der Regelungsgehalt der Norm letztlich nur die Zulässigkeit der Verwendung von Wahrscheinlichkeitswerten umfasst.

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

7. § 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person: Angemessenen Interessenausgleich herstellen

a. Absatz 1 – Einschränkung der Informationspflicht wegen unverhältnismäßigem Aufwand und Beeinträchtigung der Geltendmachung von Ansprüchen

Der Ansatz der Gesetzesvorlage ist sehr zu unterstützen:

Zutreffend wird wahrgenommen, dass im Vergleich zur heutigen Rechtslage die Informationspflicht nach Artikel 13 DS-GVO zu einer höheren Formalisierung der Informationserteilung gegenüber dem Verbraucher führen kann. Wie mit Absatz 1 richtig festgestellt wird, gibt es Situationen, in denen eine Unterrichtung zum Zeitpunkt der Erhebung der Daten einen unverhältnismäßigen Aufwand darstellt oder die Geltendmachung rechtlicher Ansprüche beeinträchtigen würde.

§ 32 Absatz 1 BDSG-E sollte jedoch nicht bloß auf den Anwendungsbereich des Artikel 13 Absatz 3 DS-GVO beschränkt bleiben, sondern auch Artikel 13 Absätze 1 und 2 DS-GVO erfassen. Am deutlichsten wird dies bei der Videoüberwachung z. B. in öffentlichen Verkehrsmitteln oder am Geldausgabeautomaten, bei der – wie in § 6b BDSG a. F. anerkannt – nur eine Schnellinformation des Betroffenen per Kurzhinweis bzw. Piktogramm möglich ist. Ein solcher Kurzhinweis muss weiterhin ausreichen, zumal es für Videoaufzeichnungen die Regel ist, dass diese nach wenigen Wochen bereits gelöscht werden, wenn mangels eines Zwischenfalls im beobachteten Feld keine Notwendigkeit zur weiteren Speicherung mehr besteht.

Ein weiteres Beispiel für die Notwendigkeit der Einschränkung sind telefonische Vorgänge (z. B. Kunde ruft wegen Vertragsschluss Call-Center der Bank an), bei denen die Eigenschaften des Mediums Telefonie es nicht zulassen, sofort alle erforderlichen Informationen dem Betroffenen mitzuteilen. Wie auch sonst im Fernabsatzrecht anerkannt, muss es ausreichen, dass die vollständige Information nachgeholt werden kann, wie es Absatz 3 auch vorsieht.

b. Absatz 3 – Nachholung von Informationen

Eine Nachholung von Informationen sollte entbehrlich sein, wenn die Daten – wie z. B. bei der Videoaufzeichnung – zeitnah gelöscht werden. Auch sollte eine Nachholungspflicht nicht dazu führen, weitere Nachforschungen anstellen zu müssen, um den hinreichenden Personenbezug herzustellen, um überhaupt in der Lage zu sein, den Betroffenen unterrichten zu können. So sind viele Videoaufzeichnungen aus sich heraus ohne weitere Nachforschungen nicht auf eine bestimmte Person beziehbar. Im Übrigen ist die Fristvorgabe verbesserungsbedürftig und sollte besser lauten:

„... kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist, spätestens jedoch innerhalb von zwei Wochen, nach Fortfall des Hinderungsgrundes, nach.“

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

8. § 33 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden: Weitere Ausnahmen aus dem heutigen § 33 Absatz 2 BDSG berücksichtigen

Die Ausnahmen in § 33 Absatz 1 Nr. 2 BDSG-E sind sachgerecht. Jedoch fehlt die Übernahme der bisherigen Ausnahmeregelungen des § 33 Absatz 2 Nr. 2, Nr. 7a und 7b BDSG zu gesetzlichen Aufbewahrungspflichten und zur Übernahme von Daten aus öffentlichen Quellen. Gerade Kreditinstitute sind aufgrund der Vorgaben zur Compliance und zur Geldwäschebekämpfung gehalten, Daten auch aus öffentlichen Quellen zu erheben. Eine Unterrichtung der davon Betroffenen könnte im Spannungsfeld zu den Zwecken Compliance und Geldwäschebekämpfung stehen. Deshalb sollten diese bisherigen Ausnahmetatbestände fortgeführt werden, zumindest bei Verfolgung der genannten Zwecke.

9. § 34 Auskunftsrecht der betroffenen Person: Angemessenen Interessenausgleich wahren

Die in Absatz 1 vorgesehenen Ausnahmen knüpfen an den heutigen § 33 Absatz 2 BDSG an. Diese sind sehr sinnvoll und äußerst wichtig, um den Anpassungsaufwand für speichernde Stellen auf ein vernünftiges Maß zu begrenzen. Dazu Folgendes zur Verdeutlichung:

- § 34 Absatz 1 Nr. 1 i. V. m. § 33 Absatz 1 Nr. 2a – Die aus dem bisherigen § 34 Absatz 1 Satz 4 BDSG resultierende Beschränkung des Auskunftsrechts ist sinnvoll und überdies verfassungsrechtlich geboten. Denn nicht nur der Betroffene ist ein Grundrechtsträger, sondern auch die speichernde Stelle. Sie muss das verfassungsrechtlich geschützte Gut in Gestalt von Geschäftsgeheimnissen weiter in Anspruch nehmen können (vgl. auch Erwägungsgrund 63 DS-GVO). Der gewählte Ansatz führt zu einem geeigneten Ausgleich dieser unterschiedlichen Interessen.
- § 34 Absatz 1 Nr. 2 – Solche Daten, die nur noch zur Erfüllung von gesetzlichen Aufbewahrungspflichten vorhanden sind, sind heute schon gesperrt und damit nicht im laufenden Geschäftsbetrieb eines Unternehmens relevant (= „nicht operativer Datenbestand“). Weder für die speichernde Stelle noch für den Betroffenen haben solche „nicht operativen Daten“ eine aktuelle Bedeutung. Somit macht es auch aus der Sicht des Betroffenen keinen Sinn, solche Daten – ggf. mit großem Aufwand aufseiten der speichernden Stelle (z. B. nachträgliche Digitalisierung von Mikrofilmen [micro fiches]) – zu beauskunften. Dieser Bewertung trägt § 34 Absatz 1 Nr. 2 BDSG-E zutreffend Rechnung.

Darüber hinaus sollte an der noch im Referentenentwurf vorgesehenen Klarstellung auf Grundlage von Erwägungsgrund 63 letzter Satz DS-GVO festgehalten werden, wonach der Auskunftersuchende die Beauskunftung durch ein zielgerichtetes Auskunftersuchen unterstützen muss, um die Auskunftspflicht der speichernden Stelle erfüllbar zu halten. § 34 sollte daher durch folgenden Absatz 5 wie folgt ergänzt werden:

„(5) Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so kann er verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftersuchen bezieht.“

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

10. § 35 Recht auf Löschung: Weiterführung der heutigen Sperrmöglichkeit

§ 35 Absatz 1 Satz 1 BDSG-E regelt zu Recht, dass eine Löschung auch dann nicht verlangt werden kann, wenn diese wegen der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich wäre. Die Vorschrift trägt dem allgemeinen Grundsatz Rechnung, dass das Recht nicht Unmögliches verlangen darf und hat klarstellende Wirkung. Satz 1 normiert insofern einen Fall der (wirtschaftlichen) Unmöglichkeit und erlaubt dort eine Sperre als Alternative, wo aus verarbeitungstechnischen Gründen eine Löschung nicht durchgeführt werden kann. Dies ist sachgerecht und trägt den Interessen des Betroffenen Rechnung. Denn gesperrte Daten sind für den laufenden Geschäftsbetrieb nicht mehr ohne Weiteres zugänglich. Auch damit lässt sich der technische Umsetzungsaufwand bei den speichernden Stellen deutlich beschränken und unnötige Kosten vermeiden.

Unmögliches darf allerdings auch dann nicht von der verantwortlichen Stelle verlangt werden, wenn der zu löschende Datensatz ursprünglich zu Unrecht erhoben wurde. Genau dies sieht aber Satz 3 gerade nicht vor. Vielmehr soll in diesem Fall die verantwortliche Stelle auch dann zu unverhältnismäßigen Löschungshandlungen verpflichtet bleiben. Die Vorschrift pönalisiert damit eine Handlung, ohne den Verschuldensgrad oder gar fehlendes Verschulden zu berücksichtigen. Die Bebußung unrechtmäßiger Handlungen ist abschließend in Artikel 86 geregelt. § 35 Absatz 1 Satz 3 BDSG-E sollte gestrichen werden.

11. § 37 Automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling: Rahmen der DS-GVO beachten

Die in § 37 Absatz 1 Nr. 1 BDSG-E vorgesehene Klarstellung im Hinblick auf die Leistungserbringung nach einem Versicherungsvertrag sollte auch auf andere Vertragsarten ausgedehnt werden, da damit an die Rechtslage des heutigen § 6a BDSG angeknüpft werden würde. Bei einer positiven automatisierten Einzelentscheidung ist nicht ersichtlich, warum eine solche eingeschränkt sein sollte. Auch aus dem Erwägungsgrund 71 der DS-GVO wird deutlich, dass sich die Frage der Zulässigkeit der Datenverarbeitung in den Fällen, in denen dem Begehren der betroffenen Person stattgegeben wird, nicht nach Artikel 22 DS-GVO richten soll. Denn in diesen Fällen liegt regelmäßig keine Beeinträchtigung der betroffenen Person vor. Darüber hinaus ist davon auszugehen, dass die betroffene Person von ihrem Recht, nicht einer voll-automatisierten Entscheidung unterworfen zu werden, angesichts der ihn begünstigenden Entscheidung keinen Gebrauch machen wird. § 37 BDSG-E sollte daher wie folgt gefasst werden (Änderungen sind hervorgehoben):

„§ 37

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen des Abschlusses

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

oder der Erfüllung eines Vertrags- oder sonstigen Rechtsverhältnisses oder der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde oder
2. die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag auf der Anwendung (...).

(2) Entscheidungen im Rahmen der Leistungserbringung nach einem Versicherungsvertrag nach Absatz 1 dürfen auf der (...).“

12. § 38 Datenschutzbeauftragte nicht öffentlicher Stellen: Rolle erhalten

Die Fortführung des bewährten Modells des betrieblichen Datenschutzbeauftragten ist sehr zu begrüßen. Allerdings besteht noch folgender Verbesserungsbedarf:

- Anders als in der Gesetzesbegründung angedeutet, erfolgt eine Änderung im Hinblick auf die Schwelle zur Bestellungspflicht. Künftig soll generell ein Schwellenwert von 10 Personen gelten für solche Verantwortliche oder Auftragsverarbeiter, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind (bislang 20 Personen bzw. 10 Personen bei automatisierter Verarbeitung, § 4f Absatz 1 BDSG). Im Interesse der Kontinuität plädieren wir dafür, die bisherigen Regelungen zur Schwelle der Bestellungspflicht fortzuführen.
- Anders als bei § 6 BDSG-E zum Datenschutzbeauftragten von öffentlichen Stellen werden in § 38 Absatz 2 BDSG-E nicht alle Vorschriften zu den Aufgaben des betrieblichen Datenschutzbeauftragten aus dem heutigen BDSG übernommen (vgl. § 4g und § 4f BDSG a. F.). Es ist nicht nachvollziehbar, warum der Verweis in § 38 Absatz 2 BDSG-E die Regelungen in § 6 Absätze 1 bis 3 BDSG-E ausspart. So stellt der § 38 BDSG-E eine Verschlechterung der Stellung des Datenschutzbeauftragten zum aktuellen § 4f BDSG a. F. dar. Denn es fehlt die für die Praxis sehr relevante Aussage der unmittelbaren Unterstellung des betrieblichen Datenschutzbeauftragten unter die Unternehmensleitung nicht öffentlicher Stellen (vgl. § 4f Absatz 3 Satz 1 BDSG a. F. und nunmehr § 6 Absatz 3 Satz 2 BDSG-E für öffentliche Stellen). Auch die rechtzeitige Einbindung des Datenschutzbeauftragten bei Vorhaben der automatisierten Verarbeitung personenbezogener Daten im Unternehmen (vgl. § 4g Absatz 1 Nr. 1 BDSG und nunmehr § 6 Absatz 1 BDSG-E für öffentliche Stellen) muss stärker zum Ausdruck kommen, damit der Datenschutzbeauftragte weiterhin seine Aufgaben effektiv wahrnehmen kann. Deshalb sollte § 38 Absatz 2 BDSG-E wie folgt lauten:

„(2) § 6 Absatz 1, Absatz 2, Absatz 3 Sätze 2 und 3, Absatz 4, Absatz 5 Satz 2 und Absatz 6 finden sinngemäß Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.“

- **In den Gesetzesmaterialien sollte klargestellt werden, dass nach dem BDSG bereits bestellte Datenschutzbeauftragte mit dem Inkrafttreten der neuen Regelungen nicht erneut bestellt werden müssen.**

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

- Schließlich ist nicht nachvollziehbar, warum insbesondere dann unabhängig von der Anzahl der Verarbeitungen ein Datenschutzbeauftragter bestellt werden muss, wenn die Verarbeitung gerade der anonymisierten Übermittlung dient. Ein solcher Verarbeitungsvorgang liegt außerhalb des Anwendungsbereichs von DS-GVO und BDSG. Diese Anforderung sollte gestrichen werden.

13. § 40 Aufsichtsbehörden der Länder für nicht öffentliche Stellen: Zuständigkeitsfragen klären

Die Gesetzesvorlage sieht vor, die bestehende Struktur der Datenschutzaufsicht durch die Länder im nicht öffentlichen Bereich fortzuführen. Es fehlt allerdings an einer Regelung zur federführenden Zuständigkeit in den Fällen, in denen Aufsichtsfragen über die Grenzen eines Bundeslandes hinaus Bedeutung haben (z. B. bundesweit agierende Unternehmen oder länderübergreifend einheitlich nutzbare Produkte). Denn für grenzüberschreitende Sachverhalte innerhalb der Europäischen Union gelten spezielle Bestimmungen zur grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden (vgl. Artikel 56 und 60 ff. DS-GVO). Wählt ein EU-Mitgliedstaat eine föderale Aufsichtsstruktur im Inland, so muss im Wege des Erstrechtsschlusses auch innerstaatlich das Gleiche gelten wie im EU-Kontext. Dementsprechend sollte § 40 Absatz 1 BDSG-E wie folgt ergänzt werden:

„(1) Die nach Landesrecht zuständigen Behörden überwachen im Anwendungsbereich der Verordnung (EU) 2016/679 bei den nicht öffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz. Ist eine nicht öffentliche Stelle nicht nur im Anwendungsbereich des jeweiligen Bundeslandes tätig, ist die Behörde am Hauptsitz der nicht öffentlichen Stelle federführende Aufsichtsbehörde im Sinne des Artikel 56 der Verordnung (EU) 2016/679. Die Zusammenarbeit der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden richtet sich nach Artikel 60 bis 63 der Verordnung (EU) 2016/679.“

Zudem sollten nach § 40 Absatz 5 BDSG-E die Aufsichtsbehörden, wie auch schon heute, nicht nur die Datenschutzbeauftragten beraten und unterstützen müssen, sondern auch den verantwortlichen Stellen als Ansprechpartner zur Verfügung stehen. Wir schlagen daher vor, an der aktuellen Formulierung des § 38 Absatz 5 Satz 1 BDSG festzuhalten.

14. § 41 Bußgeldverfahren: Differenzierung zwischen der verantwortlichen Stelle und deren Mitarbeitern

Mit § 41 Absatz 1 BDSG-E werden die Vorschriften des Ordnungswidrigkeitengesetzes sinngemäß für anwendbar erklärt. Aus der gewählten Formulierung wird nicht hinreichend deutlich, dass die sehr hohen und am Wettbewerbsrecht orientierten Sanktionsmöglichkeiten der DS-GVO sich ausschließlich an die speichernde Stelle oder an Auftragsverarbeiter richten, nicht aber an die Mitarbeiter der jeweiligen Stellen. Eine Einbeziehung von Mitarbeitern in die Bußgeldregeln mit gleich hohem Bußgeldrahmen wäre unangemessen. Denn würden die persönlichen Bußgeldrisiken von Mitarbeitern derart hoch angesetzt, dann könnte beispielsweise die Ausübung des Amtes des betrieblichen Datenschutzbeauftragten wegen möglicher Existenzgefährdung für Mitarbeiter unattraktiv werden. Insofern sollte in Anknüpfung an Artikel 83 DS-GVO der § 41 Absatz 1 Satz 1 BDSG-E auf Verantwortliche und Auftragsverarbeiter wie folgt begrenzt werden:

Stellungnahme zu Artikel 1 im Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (BR-Drs. 110/17 vom 2. Februar 2017)

„Für Verstöße eines Verantwortlichen oder eines Auftragsverarbeiters nach Artikel 83 Absätze 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.“

15. § 43 Bußgeldvorschriften: Systematik verbesserungsbedürftig

Die völlige Freistellung von öffentlichen Stellen von Bußgeldpflichten in § 43 Absatz 3 BDSG-E mag zwar EU-rechtlich möglich sein, führt aber wegen der damit verbundenen Signalwirkung aus der Perspektive von betroffenen Bürgern und nicht öffentlichen Stellen zu Irritationen.

16. Klarstellung in Bezug auf die Reichweite der Datenportabilität nach Artikel 20 DS-GVO bei der Kontowechselhilfe nach §§ 20 ff. ZKG

Artikel 20 DS-GVO regelt ein Recht des Betroffenen auf Datenübertragung. Damit soll dem Betroffenen vor allem ein Anbieterwechsel erleichtert werden. Aufgrund der im September 2016 in Kraft getretenen Vorschriften zur Kontowechselhilfe in den §§ 20 ff. des Zahlungskontengesetzes (ZKG), das auf der EU-Bankkontenrichtlinie beruht, dürfte im Bereich der Kreditwirtschaft der Regelungsbereich des Artikel 20 DS-GVO zu einem erheblichen Teil durch das ZKG abgedeckt sein. Deshalb wäre im nationalen Recht eine Norm begrüßenswert, die der spezifischen Rechtslage in der Kreditwirtschaft Rechnung trägt. Eine solche – auch an die Gestaltungsmöglichkeiten in Artikel 23 Absatz 1i) in Verbindung mit Artikel 23 Absatz 2c) DS-GVO anknüpfende – Vorschrift könnte beispielsweise lauten:

§ ... Recht auf Datenübertragbarkeit

Der betroffenen Person steht das Recht auf Datenübertragbarkeit gemäß Artikel 20 der Verordnung (EU) 2016/679 zu. Soweit in bereichsspezifischen Gesetzen der Anbieterwechsel mit einer konkreten Vorgabe für die Datenübermittlung von einem Verantwortlichen zu einem anderen Verantwortlichen ausdrücklich geregelt ist, und dem Begehren der betroffenen Person insoweit stattgegeben werden kann, gilt das Recht der betroffenen Person auf Datenübertragbarkeit gemäß Artikel 20 der Verordnung (EU) 2016/679 insoweit als erfüllt.



Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Bundessteuerberaterkammer, KdöR, Postfach 02 88 55, 10131 Berlin

Herrn
Ansgar Heveling, MdB
Vorsitzender des Innenausschusses
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

E-Mail: innenausschuss@bundestag.de

**Abt. Steuerrecht und
Rechnungslegung**

Unser Zeichen: Be/Ze
Tel.: +49 30 240087-61
Fax: +49 30 240087-99
E-Mail: steuerrecht@bstbk.de

24. März 2017

Gesetzentwurf zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (EU-DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (DS-RL)

Sehr geehrter Herr Heveling,

im Vorfeld zur öffentlichen Anhörung möchten wir zum o. g. Gesetzentwurf Stellung nehmen.

Aus unserer Sicht ist darauf zu achten, dass die Umsetzung der Datenschutz-Grundverordnung der EU (EU-DSGVO) im Bundesdatenschutzgesetz (BDSG) nicht dazu führt, dass die Geheimhaltungspflichten von Berufsgeheimnisträgern ausgehebelt werden.

Wir begrüßen daher nachdrücklich, dass in der nun vorliegenden Fassung des § 29 BDSG-E eine überarbeitete Ausnahmeregelung für die der Geheimhaltungspflicht unterliegenden Daten geschaffen wurde. Dies ist gesetztes- und regelungstechnisch eine wesentliche Verbesserung gegenüber dem ursprünglichen Referentenentwurf.

Dennoch ist es u. E. für den Berufstand der Steuerberater wichtig, dass weitere Ausnahmeregelungen geschaffen werden. In der derzeitigen Gesetzesfassung besteht weiterhin eine Kollision der Betroffenenrechte (insbesondere Art. 13, Art 18, Art. 19, Art 21, Art. 34 EU-DSGVO) mit der Geheimhaltungspflicht. In der Anlage finden Sie daher weitere Anmerkungen zu dem Aspekt der Verarbeitung von der Geheimhaltungspflicht unterliegenden Daten.

Mit freundlichen Grüßen

i. V. Claudia Kalina-Kerschbaum
Geschäftsführerin

i. A. Inga Bethke
Referatsleiterin

Anlage

Anlage

Stellungnahme
der Bundessteuerberaterkammer
zum
Gesetzentwurf eines Gesetzes
zur Anpassung des Datenschutzrechts an die
Verordnung (EU) 2016/679 (EU-DSGVO) und
zur Umsetzung der Richtlinie (EU) 2016/680 (DS-RL)

**Abt. Steuerrecht und
Rechnungslegung**

Telefon: 030 24 00 87-61
Telefax: 030 24 00 87-99
E-Mail: steuerrecht@bstbk.de

24. März 2017

1. Zu Abschnitt 2 – § 29 BSDG-E

Im Vergleich zum Referentenentwurf ist die Regelung in Bezug auf die Einschränkung der Rechte der betroffenen Personen im Fall von Geheimhaltungspflichten grundlegend überarbeitet worden und einige unserer Kritikpunkte wurden bereits umgesetzt. Daher begrüßen wir Teile des Regierungsentwurfes. Wir empfehlen jedoch ergänzend zu dem Verweis auf Art. 14 Abs. 5 EU-DSGVO in § 29 BSDG-E auch auf Art. 23 Abs. 1 Buchst. g EU-DSGVO zu verweisen. Dies würde den Schutz der Verschwiegenheitsverpflichtung ausweiten und verdeutlichen.

Im Weiteren sehen wir in folgenden Punkten Nachbesserungsbedarf:

- Zu § 29 Abs. 1 BSDG-E – Ausnahmen von der Informationspflicht

Paragraf 29 Abs. 1 BSDG-E legt ergänzend zu den in Art. 14 Abs. 5 EU-DSGVO genannten Ausnahmen fest, dass eine Pflicht zur Information nach Art. 14 Abs. 1 bis 4 EU-DSGVO nicht besteht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Nähere Angaben dazu, wann dies der Fall ist, finden sich im Wortlaut des Gesetzes nicht. Wir regen an, zumindest in der Gesetzesbegründung beispielhaft aufzuführen, welche Daten hiermit gemeint sein können. Aus unserer Sicht sollte klargestellt werden, dass davon auch solche Daten umfasst werden, für die eine Geheimhaltung vertraglich vereinbart worden ist. Wir gehen davon aus, dass auch das Vertragsrecht neben Berufs- und Strafrecht zum Schutz des Geheimbereichs der Mandanten herangezogen werden kann.

- Ausnahmen vom Auskunftsrecht § 29 Abs. 1 Satz 2 BSDG-E

Nach dem Gesetzestext wird das Recht auf Auskunft ausgeschlossen, wenn durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Wir gehen davon aus, dass diese Ausführung dahingehend zu verstehen ist, dass damit eine gesetzliche und eine vertragliche Geheimhaltungspflicht gemeint ist. Dennoch ist eine Klärung wünschenswert.

- Ausnahmen von der Pflicht zur Benachrichtigung § 29 Abs. 1 Satz 3 und 4 BSDG-E

Die Benachrichtigungspflicht des Verantwortlichen nach Art. 34 EU-DSGVO bei einer Verletzung des Schutzes personenbezogener Daten (mit der Folge eines hohen Risikos für die persönlichen Rechte und Freiheiten der betroffenen Person) entfällt unter den in Art. 34 Abs. 3 EU-DSGVO genannten Ausnahmen.

Es ist zu begrüßen, dass im Rahmen des BDSG-E – neben den schon bestehenden Ausnahmen des Art. 34 Abs. 3 EU-DSGVO – folgende weitere Ausnahme geschaffen wurde: Die Benachrichtigungspflicht entfällt hiernach, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Im Gegenzug enthält Satz 4 eine Formulierung, wonach jedoch eine Benachrichtigungspflicht besteht, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

Wir weisen darauf hin, dass es in der Praxis für den Steuerberater schwierig sein wird, abzuwägen, welches Interesse überwiegt. Diese Regelung ist unklar und führt zu Rechtsunsicherheit. Die Gesetzesbegründung enthält zu diesem Punkt keine Ausführungen. Wir gehen davon aus, dass eine Feststellung, ob das Interesse der betroffenen Person (insbesondere unter Berücksichtigung drohender Schäden) oder das Geheimhaltungsinteresse überwiegt, in der Praxis kaum möglich sein wird. Hier besteht Klarstellungsbedarf

2. Kollision der Betroffenenrechte mit der Verschwiegenheitsverpflichtung beseitigen

Die EU-DSGVO enthält in Art. 12 bis 22 und 34 verschiedene Rechte der betroffenen Personen hinsichtlich der über sie erhobenen Daten. Insbesondere haben sie ein Recht auf Information und Auskunft, ggf. auch auf Berichtigung und Löschung ihrer Daten. Diese Rechte sind im Sinne der auch vom BVerfG betonten informationellen Selbstbestimmung richtig und wichtig.

In einigen Fällen kollidieren diese Rechte jedoch mit der Verschwiegenheitsverpflichtung des Steuerberaters nach § 57 Abs. 1 StBerG. Wir sehen daher einige weitere Ausnahmeregelungen als erforderlich an. Zur besseren Übersichtlichkeit regen wir an, die weiteren – nachfolgend aufgeführten – Ausnahmen der Betroffenenrechte in § 29 Abs. 1 BDSG-E aufzunehmen.

• Informationspflicht nach Art. 13 EU-DSGVO

Erhebt ein Berufsgeheimnisträger im Rahmen einer Auftragsdurchführung personenbezogene Daten eines Dritten bei diesem, so können die Informationspflichten der Verschwiegenheitsverpflichtung des Berufsgeheimnisträgers gegenüber seinem Mandanten widersprechen.

Dies ist beispielsweise der Fall, wenn personenbezogene Daten eines Arbeitnehmers eines Mandanten im Rahmen der Lohnbuchhaltung erhoben werden.

Das gleiche gilt, wenn der Steuerberater für einen Mandanten eine Einkommensteuererklärung fertigt und im Rahmen dieser Einkommensteuererklärung Unterhaltsaufwendungen als Sonderausgaben geltend macht. Die Finanzverwaltung fordert in diesem Fall verschiedene persönliche Daten des Unterhaltsempfängers (Anlage U der Einkommensteuererklärung). In diesem Fall ist es erforderlich, verschiedene Daten des Unterhaltsempfängers abzufragen.

Daraus folgend müsste der Steuerberater verschiedene Informationspflichten an den Unterhaltsempfänger erfüllen. Dies verstößt nach unserer Auffassung gegen die Geheimhaltungspflicht. Eine Ausnahmeregelung ist erforderlich.

- Recht auf Einschränkung der Verarbeitung nach Art. 18 EU-DSGVO

Unter bestimmten Voraussetzungen kann die betroffene Person gem. Art. 18 Abs. 1 EU-DSGVO vom Verantwortlichen eine Einschränkung der Verarbeitung ihrer Daten verlangen. Dies betrifft zunächst zwar nicht die Verschwiegenheitsverpflichtung des Steuerberaters gegenüber seinem Mandanten. Nicht ausgeschlossen ist aber, dass der Steuerberater aufgrund des Verlangens eines Dritten (z. B. Gesellschafter einer GmbH) bei der Auftragsdurchführung gegenüber seinem Mandanten behindert wird.

Nach Art. 18 Abs. 2 EU-DSGVO ist geregelt, dass personenbezogene Daten auch bei Einschränkung der Verarbeitung nach Abs. 1 verarbeitet werden können, wenn dies aus Gründen eines wichtigen öffentlichen Interesses geschieht. Dies liegt u. E. im Hinblick auf die steuerberatende Tätigkeit vor, da der Steuerberater als Organ der Steuerrechtspflege tätig ist und wesentlich zur Funktionsfähigkeit der Steuererhebung und der Wahrung des Steueraufkommens beiträgt. Es wäre wünschenswert, wenn ein entsprechender Hinweis aus Gründen der Rechtssicherheit klarstellend in den Text des BDSG aufgenommen würde.

- Mitteilungspflicht nach Art. 19 EU-DSGVO

Empfängern (z. B. Finanzbehörde), denen personenbezogene Daten offengelegt wurden, soll jede Berichtigung oder Löschung dieser Daten oder eine Einschränkung der Verarbeitung mitgeteilt werden. Im Zusammenhang mit dem Besteuerungsverfahren führt diese Mitteilungspflicht zu einem unverhältnismäßiger Aufwand für den Steuerberater, insbesondere wenn es sich um Datenänderungen handelt, die für das Besteuerungsverfahren irrelevant sind. Dies sollte im BDSG-E klargestellt werden.

- Widerspruchsrecht des Betroffenen nach Art. 21 EU-DSGVO

Für eine Verarbeitung von personenbezogenen Daten, trotz eines Widerspruchs der betroffenen Person, muss der Verantwortliche zwingende schutzwürdige Gründe nachweisen. Es ist möglich, dass ein entsprechender Nachweis nur geführt werden könnte, indem gegen die Verschwiegenheitspflicht eines Berufsgeheimnisträgers verstoßen würde. Lösbar wäre diese Situation, wenn im BDSG klargestellt würde, dass ein solcher Nachweis nicht gegenüber der widersprechenden Person, sondern lediglich gegenüber der berufsaufsichtsführenden Stelle zu führen wäre.

- Benachrichtigung nach Art. 34 EU-DSGVO

Der Verantwortliche hat die betroffene Person von einer Verletzung des Schutzes ihrer Daten zu benachrichtigen. Wenn bei einer Auftragsdurchführung die personenbezogenen Daten eines Dritten verarbeitet wurden und die Daten nicht bei diesem Dritten selbst erhoben wurden, kann die Benachrichtigung gegen die Verschwiegenheitsverpflichtung des Verantwortlichen verstoßen.

3. Weiterer Regelungsbedarf in Spezialgesetzen

Im Weiteren möchten wir auf wichtige Regelungsbereiche in der Abgabenordnung und des Steuerberatungsgesetzes hinweisen:

- Auskunftsansprüche in der Abgabenordnung regeln

Wir möchten darauf hinweisen, dass mit dem Anwendungserlass des BMF vom 17. Dezember 2008 das datenschutzrechtliche Auskunftsrecht des Steuerpflichtigen im Besteuerungsverfahren eingeschränkt wurde. Unseres Erachtens steht dieses BMF-Schreiben im Widerspruch zur EU-DSGVO. Eine gesetzliche Regelung in der AO zum Auskunftsanspruch und sonstigen Betroffenenrechten ist dringend erforderlich.

- Klarstellung der weisungsfreien Aufgabenerfüllung bei Steuerberatern

Die Bundessteuerberaterkammer regt an, in Ergänzung zu den bisher vorgesehenen Regelungen in das Steuerberatungsgesetz eine klarstellende Regelung aufzunehmen, dass bei Ausübung beruflicher Tätigkeiten i. S. d. §§ 33, 57 Abs. 3 StBerG aufgrund der nach § 57 Abs. 1 StBerG geregelten Unabhängigkeit und fachlichen Weisungsfreiheit des Steuerberaters keine weisungsabhängige Tätigkeit nach § 46 Nr. 8, § 62 BDSG-E bzw. Art. 28 der Datenschutzgrundverordnung vorliegt, mit der Folge, dass es sich z. B. bei steuerlichen Beratungsleistungen oder der Erstellung der Lohn- und Finanzbuchhaltung um keine Auftragsdatenverarbeitung handelt.

Die Unabhängigkeit der Berufsausübung gehört zu den statusbildenden Grundpflichten des Steuerberaters als unabhängiges Organ der Steuerrechtspflege. Die Unabhängigkeit ist aber nur dann gewährleistet, wenn der Steuerberater bei der Mandatserfüllung auch hinsichtlich der Verwendung der personenbezogenen Daten weisungsfrei handeln kann und nicht durch Vorgaben des Mandanten eingeschränkt wird.

Die Mandanteninteressen werden durch die (strafbewehrte) Verschwiegenheitspflicht hinreichend geschützt, sodass eine Vereinbarung zur Auftragsdatenverarbeitung in diesen Fällen nicht erforderlich ist.

Eine Klarstellung ist wichtig, um in diesem Bereich Rechtssicherheit zu erhalten.

4. Regelungsbedarf der Aufsichtsbehörden

Artikel 40 EU-DSGVO ermöglicht die Ausarbeitung von Verhaltensregeln, die für einzelne Gruppen von Auftragsverarbeitern sowie Gruppen von Verantwortlichen (z. B. Steuerberater) zur ordnungsgemäßen Anwendung der Vorschriften der EU-DSGVO beitragen sollen. Im BSDG-E werden die Verhaltensregeln gem. Art. 40 EU-DSGVO nur an wenigen Stellen erwähnt.

Der Gesetzesentwurf enthält keine Ausführungen über das Verfahren zur Ausgestaltung und Genehmigung von Verhaltensregeln. Wir vermuten, dass man davon ausgeht, dass ausführliche Regelungen bereits in Art. 40,41 EU-DSGVO enthalten sind. Die Bundessteuerberaterkammer begrüßt diese Möglichkeit und unterstützt die Ausarbeitung solcher Verhaltensregeln für Steuerberater und Steuerberatungskanzleien.

Dennoch regen wir an, dass die Aufsichtsbehörden klare und eindeutige Regelungen über das Verfahren der Genehmigung von Verhaltensregeln treffen. Besonders die Funktionen der Aufsichtsbehörden sollten klar geregelt werden. Dies betrifft sowohl zeitliche und organisatorische Vorgaben, als auch die Anerkennung bereits genehmigter Verhaltensregeln durch weitere Aufsichtsbehörden. Auch sollte geregelt werden, wie das Verfahren der Akkreditierung einer Stelle zur Überwachung der genehmigten Verhaltensregeln ausgestaltet ist.



Dr. Philipp Kramer
Chefredakteur Datenschutz-Berater

Handelsblatt Fachmedien GmbH | Redaktion HH
Süllbergstrasse 1 | 22587 Hamburg

Vorsitzender des Innenausschusses
des Deutschen Bundestags
Herrn Ansgar Heveling
Platz der Republik 1
11011 Berlin

innenausschuss@bundestag.de

Hamburg, 27. März 2017

**Datenschutz-Anpassungs- und -Umsetzungsgesetz
EU-DSAnpUG-EU
Stellungnahme**

Sehr geehrter Herr Vorsitzender,

in der Anlage überreiche ich dem Innenausschuss zur weiteren Verwendung meine Stellungnahme zum geplanten § 26 BDSG-neu. Er ist Teil des Datenschutz-Anpassungs- und -Umsetzungsgesetzes (EU-DSAnpUG-EU), das am 27.03.2017 im Innenausschuss auf der Tagesordnung stand.

Nach meiner Stellungnahme ist im Interesse der Praxis dringend eine klärende Regelung aufzunehmen, die zeigt, dass die Datenverarbeitungserlaubnis aus überwiegendem Interesse weiterhin auch für das Beschäftigungsverhältnis gilt. Möglich ist eine Formulierung wie „Art. 6 Absatz 1 Satz 1 Buchstabe f der Verordnung (EU) 2016/679 bleibt unberührt“.

Weitere Formulierungsvorschläge und eine Darstellung der Notwendigkeit im Detail finden Sie in meiner beigefügten Stellungnahme.

Mit freundlichen Grüßen

Philipp Kramer

Dr. Philipp Kramer
Redaktion Datenschutz-Berater

Dr. Philipp Kramer
Rechtsanwalt, Hamburg
Vorstand der Hamburger Datenschutzgesellschaft
Lehrbeauftragter Universität Hamburg
Lehrbeauftragter Hochschule Ulm

Stellungnahme zu

- BT-Drucksache 18/11325

betreffend
Entwurf eines
Gesetzes zur Anpassung des Datenschutzrechts
an die Verordnung (EU) 2016/679 und zur Um-
setzung der Richtlinie (EU) 2016/680
(Datenschutz-Anpassungs- und
-Umsetzungsgesetz EU- DSAnpUG-EU)

aus Anlass der Anhörung in der 110. Sitzung
des Innenausschusses des Bundestags

27. März 2017/as

Übersicht

A. Ausgangspunkt

B. Problemstellung und Lösung

C. Im Einzelnen

1. Allgemeine Erlaubnisregelung des Art. 6 DSGVO von § 26 BDSG-neu nicht erwähnt
2. Es fehlt die Güterabwägung in § 26 BDSG-neu
3. Es bedarf der Güterabwägung in § 26 BDSG-neu
4. Verweis in § 26 BDSG-neu auf Art. 6 Abs. 1 Satz 1 Buchstabe f EU-DSGVO fehlt

D. Formulierungsvorschläge für die Berücksichtigung der Güterabwägung

1. Ergänzung eines Satzes 2 in § 26 Abs. 5 BDSG-neu des DSAnpUG-EU
2. Ergänzung des Satzes 1 in § 26 Abs. 1 BDSG-neu des DSAnpUG-EU um einen Erlaubnistatbestand
3. Erweiterung des Satzes 1 in § 26 Abs. 1 BDSG-neu des DSAnpUG-EU mit Rücksicht auf die Formulierungen des Art. 88 Abs. 1 DSGVO

A. Ausgangspunkt

Der Bundestag ist im Begriff, ein neues Bundesdatenschutzgesetz (**BDSG-neu**) zu verabschieden. Es soll (1) Vorschriften schaffen, die nach der neuen unmittelbar wirksamen EU-Datenschutz-Grundverordnung (**DSGVO**) vom Mitgliedstaatengesetzgeber zu schaffen sind und (2) vor allem auch Spielräume der DSGVO, gerade auch im Beschäftigtendatenschutz und bei Informationspflichten, ausschöpfen.

B. Problemstellung und Lösung

Der vor dem Bundestag zur Verhandlung stehende Regierungsentwurf des BDSG-neu hat verschiedene Kritik, auch aus dem Bundesrat, nach sich gezogen. Die Anhörung der Sachverständigen am 27.03.2017 wird hier sicher mehr Klarheit gebracht haben.

Eine wichtige Antwort aus Praktiker-Sicht sollte das BDSG-neu in jedem Fall noch auf folgende Frage geben: Wann dürfen Beschäftigtendaten vom Arbeitgeber verarbeitet werden?

Anders als zu vermuten wäre, wird diese Frage vom BDSG-neu-Entwurf bisher nicht abschließend beantwortet. Insbesondere ist fraglich, ob Datenverarbeitungserlaubnis „überwiegendes Interesse des Arbeitgebers“ (Güterabwägung) aus Art. 6 Abs. 1 Satz 1 Buchstabe f DSGVO auch unter dem BDSG-neu im Beschäftigungsverhältnis fort gilt.

Bis zum 25.05.2018 sieht der Beschäftigtendatenschutzparagraph 32 BDSG in seiner Begründung vor, dass die Erla

-

bar ist (siehe unten Abschnitt C,4).

Solche Hinweise fehlen dem neuen Entwurf eines BDSG-neu. Es droht eine Auslegung, bei dem viele anerkannte Nebendatenverarbeitungen (siehe unten Abschnitt C, 3) datenschutzrechtlich ab dem 25.05.2018 nicht mehr erlaubt sind oder nur noch mit Betriebsvereinbarung oder schwer erzielbarer Einwilligungen möglich sind.

Es bedarf daher einer Anpassung des Gesetzesentwurfs des § 26 BDSG-neu (zu den Vorschlägen siehe unten Abschnitt D, Formulierungsvorschläge für die Berücksichtigung der Güterabwägung).

C. Im Einzelnen

1. *Allgemeine Erlaubnisregelung des Art. 6 DSGVO von § 26 BDSG-neu nicht erwähnt*

Für die **vielen Datenverarbeitungen in Unternehmen, die nicht Mitarbeiter betreffen**, hält die DSGVO mit ihrem Artikel 5 (Grundsätze) und mit ihrem Artikel 6 (Erlaubnistatbestände) kla

Für den **speziellen Bereich der Verarbeitung von Beschäftigtendaten schafft der vorgeschlagene § 26 BDSG-neu eigene Erlaubnisse**. Für die Beschäftigtendaten gilt danach erstmal nicht der Artikel 6 der DSGVO (Erlaubnistatbestände). Erlaubt ist nach dem Regierungsentwurf des § 26 BDSG-neu die Beschäftigtendatenverarbeitung **für den Arbeitsvertrag** (Begründung, Durchführung, Beendigung), **für die Rechte und Pflichten von Betriebs- und Personalrat** und **bei Vorliegen einer Kollektivvereinbarung** und **bei einer wirksamen Einwilligung**. Sonderregeln gelten für die Verarbeitung sensibler Daten, insbesondere von Gesundheitsdaten.

2. *Es fehlt die Güterabwägung in § 26 BDSG-neu*

Werden Spezialvorschriften – hier mit § 26 BDSG im Verhältnis zur DSGVO – geschaffen, muss für den Praktiker klar sein, wann die Spezialvorschriften greifen und wann es bei den allgemeinen Vorschriften der DSGVO bleibt.

Der Regierungsentwurf des § 26 BDSG-neu wie auch dessen Begründung lassen jedoch offen, ob im Beschäftigungsverhältnis eine Verarbeitung von Beschäftigtendaten – a

- und
Personalrat, mit Inhalten einer Kollektivvereinbarung und mit Einwilligung – a

(Güterabwägung),

wie es die DSGVO mit Art. 6 Abs. 1 Satz 1 Buchstabe f vorsieht.

Art. 6 Abs. 1 DSGVO
Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[...]

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

[...]

Weder der Entwurf des § 26 BDSG-neu noch die Begründung des Regierungsentwurfs treffen dazu eine Aussage. Wohl gibt es Formulierungen, die für einen Ausschluss der Erlaubnis aus überwiegendem Verarbeitungsinteresse des Arbeitgebers sprechen.

3. *Es bedarf der Güterabwägung in § 26 BDSG-neu*

Der Arbeitsvertrag rechtfertigt die typischen Verarbeitungen von Beschäftigtendaten im Arbeitsverhältnis wie die Erhebung von Bewerbungsdaten für die Entscheidung über die Begründung eines Arbeitsverhältnisses und die Erhebung von Kontodaten für die unbare Zahlung des Lohns/Gehalts.

Doch schon Datenverarbeitungen für interne Revisionszwecke sind nicht mehr unmittelbar aus dem Arbeitsverhältnis zu rechtfertigen. Einwilligungen sind zwar als Alternative denkbar. Doch sie müssen wirklich freiwillig sein und werden sich häufig nicht erreichen lassen. Wer würde schon einer internen Revisionsmaßnahme zustimmen, es sei denn, er will mithilfe der Ergebnisse der durchgeführten Revisionsmaßnahme zeigen, dass er doch ordnungsgemäß gehandelt.

Im Rahmen der Unternehmensführung werden Beschäftigten-
daten – a – für vielfältige organisatorische,
soziale und personelle Zwecke verwendet, die nur mittelbar mit
dem Beschäftigungsverhältnis verbunden sind (**Nebendaten-
verarbeitungen im Beschäftigungsverhältnis**). Dazu gehören
neben den oben genannten Revisionsmaßnahmen die Verwen-
dung von Beschäftigtendaten für

- Personalplanungsmaßnahmen, die aus der Perspektive
des Unternehmens durchgeführt werden,
- gezielte Aus- und Fortbildungsmaßnahmen,
- unternehmens-/gruppeninterne Arbeitsprofile zur Projekt-
teambildung,
- Bescheinigungen, die nicht gesetzlich geregelt, sondern
vom Beschäftigten gewünscht werden, beispielsweise für
ausländische Gerichte,
- statistische Analysezwecke, denen der Zugriff auf perso-
nenbezogene, noch nicht anonymisierte Beschäftigtenda-
ten vorausgeht,
- Zutritts- und Zugangsberechtigungssysteme,
- Geburtstagsgrüße,
- Weiterbildungsangebote,
- Rabattierung beim Personaleinkauf,
- Essenszuschüsse,
- rabattierte Kantinennutzung,
- Firmenwagen mit Fuhrparkmanagement (einschließlich
Ordnungswidrigkeitenverwaltung),
- Fahrtkostenzuschuss,
- Busdienste,
- Zur-Verfügung-Stellung eines Parkpla
- firmenorganisierte Gesundheitsmanagementsysteme,
- Zuschüsse für die Mitgliedschaft in Sporteinrichtungen,
- freiwillige betriebliche Altersversorgungssysteme,
- Firmenkreditkarte für Firmen- und Privatnutzung,
- Betriebskindergarten,
- sonstige Betreuung von Kindern der Beschäftigten,
- Arbeitgeberdarlehen,
- Sterbekasse für Hinterbliebene des Beschäftigten.

All diese Maßnahmen müssten sich künftig auf eine Einwilli-
gung stützen, wobei die Wirksamkeit der Einwilligung im Ar-

beitsverhältnis schnell an der Darlegung der Freiwilligkeit der Einwilligung scheitern kann. Alternativ müsste der Arbeitgeber die Arbeitsverträge anpassen, was jedoch ebenfalls der Zustimmung des Mitarbeiters bedarf.

Ein weiterer Fall, bei dem eine abschließende Auslegung des neuen § 26 BDSG-neu zur Notwendigkeit der Einwilligung führen würde, wäre der Versand der Wirtschaftszeitung AKTIV. Die Zeitung wird von einem Dienstleister im Auftrag des jeweiligen Arbeitgebers an die Mitarbeiter nach Hause versendet, sofern der Mitarbeiter dem nicht widerspricht. Der Arbeitgeber nutzt dafür die ihm über den Arbeitsvertrag bekannten Privatadressen der Mitarbeiter. Diese Datenverarbeitung kann über das überwiegende Interesse des Arbeitgebers gerechtfertigt werden, soweit dem Beschäftigten ein Widerspruchsrecht eingeräumt ist. Über das Widerspruchsrecht ist er zu informieren. Eine Einwilligung hingegen ließe sich in der Mehrzahl der Fälle praktisch kaum realisieren. Einwilligungen werden vom Betroffenen häufig nur dann gegeben, wenn er einen Vorteil aus der Einwilligung erhält. Solche Vorteile können in einem Newsletter, in einer Gewinnspielteilnahme oder sonstigen Dingen, wie einer Mailingmöglichkeit, bestehen. Diese Vorteile können allerdings später auch für die Unfreiwilligkeit sprechen. Denn wer im Hinblick auf einen für ihn hohen Gewinn, wie ein Luxusauto, eine Einwilligung erklärt, wird von der Rechtsprechung teilweise als „unfreiwillig handelnd“ eingeordnet.

Will man die vielen, bisher anerkannten **Nebendatenverarbeitungen im Beschäftigungsverhältnis** faktisch nicht untersagen, sondern weiterhin zulassen und keine Pflicht zur Erhebung im Zweifel unwirksamer Einwilligungen der Mitarbeiter begründen, muss die Datenverarbeitungserlaubnis „überwiegendes Interesse des Arbeitgebers“ (Güterabwägung) nach Art. 6 Abs. 1 Satz 1 Buchstabe f DSGVO ausdrücklich erhalten bleiben.

4. Verweis in § 26 BDSG-neu auf Art. 6 Abs. 1 Satz 1 Buchstabe f DSGVO fehlt

Nun kann man vertreten, dass sich die Fortgeltung der Datenverarbeitungserlaubnis „überwiegendes Interesse des Arbeitge-

bers“ (Güterabwägung) aus Art. 6 Abs. 1 Satz 1 Buchstabe f DSGVO doch gewissermaßen von selbst aus den Vorschriften ergeben würde. Doch schon bei der Novelle des BDSG 2009 war umstritten, ob die Erlaubnis der Güterabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG neben dem neuen Beschäftigtendatenschutzparagrafen § 32 BDSG fortgelten würde. Immerhin half damals die Klarstellung in der Begründung:

<p>BT-Drs. 16/13657 Bericht der Abgeordneten Beatrix Philipp, Dr. Michael Bürsch, Gisela Piltz, Jan Korte und Silke Stokar von Neuforn Zu Artikel 1 Nummer 12 - neu - (§ 32 - neu)</p> <p>Werden personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt, findet § 28 Absatz 1 keine Anwendung mehr. Für andere Zwecke können auch im Verhältnis von Arbeitgeber und Beschäftigten die Vorschriften des Bundesdatenschutzgesetzes und anderer Gesetze, die eine Datenerhebung, -verarbeitung und -nutzung erlauben oder anordnen, weiterhin Anwendung finden. Dazu gehören die Regelungen über die Datenerhebung, -verarbeitung und -nutzung zur Wahrung berechtigter Interessen des Arbeitgebers (§ 28 Absatz 1 Satz 1 Nummer 2) [...].</p>
--

Nunmehr fehlt jede Äußerung zu dieser Berücksichtigung der Güterabwägung. Eine Ergänzung ist daher zwingend geboten, will man der Praxis nicht eine Vielzahl unnötiger neuer Abgrenzungsdiskussionen zumuten.

D. Formulierungsvorschläge für die Berücksichtigung der Güterabwägung

Es gibt mehrere Möglichkeiten, klarzustellen, dass das „überwiegende Interesse“ als Erlaubnistatbestand des noch geltenden BDSG auch beim Beschäftigtendatenschutz nach § 26 BDSG neu berücksichtigt wird.

1. Ergänzung eines Satzes 2 in § 26 Abs. 5 BDSG-neu des DSAnpUG-EU

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. **Art. 6 Absatz 1 Satz 1 Buchstabe f der Verordnung (EU) 2016/679 bleibt unberührt.**

Das wäre eine übliche Formulierung, die nach dem BMJV-Handbuch der Rechtsförmigkeit, 3. Auflage, Rdz. 87, vorzusehen ist, wenn „beide Regelungen nebeneinander anwendbar“ sein sollen.

2. Ergänzung des Satzes 1 in § 26 Abs. 1 BDSG-neu des DSAnpUG-EU um einen Erlaubnistatbestand

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist **oder die Verarbeitung zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Beschäftigten, die den Schutz personenbezogener Daten erfordern, überwiegen.**

3. Erweiterung des Satzes 1 in § 26 Abs. 1 BDSG-neu des DSAnpUG-EU mit Rücksicht auf die Formulierungen des Art. 88 Abs. 1 DSGVO

Nicht gleichermaßen geeignet, jedoch immer noch mehr Rechtssicherheit, gerade auch für die Maßnahmen der Internen Revision, wäre folgende Ergänzung.

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung, eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten **oder für Zwecke des Managements, der Planung und der Organisation der Arbeit** erforderlich ist.

Es handelt sich hierbei um Verarbeitungszwecke, die schon von der Datenschutz-Grundverordnung in Art. 88 Abs. 1 ausdrücklich genannt sind.

Dr. Philipp Kramer
Rechtsanwalt



Gutachtliche Stellungnahme/Prüfbitte

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)

Bundestags-Drucksache 18/11325
Bundesrats-Drucksache 110/17

Im Rahmen seines Auftrags zur Überprüfung von Gesetzentwürfen und Verordnungen der Bundesregierung auf Vereinbarkeit mit der nationalen Nachhaltigkeitsstrategie hat sich der Parlamentarische Beirat für nachhaltige Entwicklung gemäß Einsetzungsantrag (BT-Drs. 18/559) in seiner 59. Sitzung am 8. März 2017 mit 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) (BT-Drs. 18/11325) befasst.

Folgende Aussage zur Nachhaltigkeit wurde in der Begründung des Gesetzentwurfes getroffen:
„Die Managementregeln und Indikatoren der Nationalen Nachhaltigkeitsstrategie wurden geprüft und, soweit einschlägig, beachtet.“

Formale Bewertung durch den Parlamentarischen Beirat für nachhaltige Entwicklung:

Eine Nachhaltigkeitsrelevanz des Gesetzentwurfes ist bedingt gegeben.

Die Aussagen zur Nachhaltigkeitsprüfung sind nicht ausreichend. Es ergibt sich aus den Ausführungen nicht, ob ein Bezug zur Nachhaltigkeitsstrategie vorliegt und falls ja, in welcher Weise.

Prüfbitte:

Der Parlamentarische Beirat für nachhaltige Entwicklung bittet deshalb den federführenden Innenausschuss, bei der Bundesregierung nachzufragen, warum der Bezug zur nationalen Nachhaltigkeitsstrategie nicht hinreichend deutlich hergestellt wurde und welche konkreten Auswirkungen auf die Ziele der nationalen Nachhaltigkeitsstrategie zu erwarten sind sowie die Ergebnisse in Kurzform in den Bericht des Ausschusses aufzunehmen.

Berlin, 8. März 2017

Dr./Lars Castellucci, MdB
Berichterstatte

Dr. Valerie Wilms, MdB
Berichterstatte