Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Bundesministerium des Innern
Referat V II 4

Nachrichtlich: Ressorts lt. Verteiler

Nur per E-Mail

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

TELEFON (0228) 997799-110
TELEFAX (0228) 997799-550
E-MAIL referat11@bfdi.bund.de
BEARBEITET VON Sven Hermerschmidt
INTERNET www.datenschutz.bund.de

DATUM Bonn, 31.08.2016
GESCHÄFTSZ. **11-100/044#0115**

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

BETREFF **Entwurf eines Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU - DSAnpUG-EU**
HIER Stellungnahme der BfDI
BEZUG Schreiben des BMI vom 5. August 2016

Sehr geehrte Damen und Herren,

für die Zusendung des Gesetzentwurfs und die Gelegenheit zur Stellungnahme danke ich.

Zu dem o. g. Gesetzentwurf nimmt die BfDI wie folgt Stellung:

I. Zur Gesamtsystematik des Gesetzentwurfs

Der Entwurf ist als Artikelgesetz ausgestaltet. Artikel 1 enthält den Entwurf eines Allgemeinen Bundesdatenschutzgesetzes (ABDSG), das das allgemeine Datenschutzrecht des Bundes in Nachfolge des BDSG enthält. Die Artikel 2 bis 6 sehen Ände-

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

rungen einiger Gesetze aus dem Sicherheitsbereich vor, wobei bislang lediglich Entwürfe zu Art. 2 (Änderung des BVerfSchG) und Art. 6 (Änderung des G 10) vorliegen, während für Änderungen des MADG, des BNDG und des SÜG bislang nur Platzhalter vorgesehen sind. Art. 7 fungiert zunächst als Platzhalter für weitere bundesgesetzliche Änderungen, die von den Ressorts noch vorgeschlagen werden müssen. Mit Art. 8 wird das Inkrafttreten am 25.5.2018 und das gleichzeitige Außerkrafttreten des BDSG geregelt.

Gegen die systematische Struktur des Gesetzentwurfs insgesamt bestehen keine Einwände. Es bleibt abzuwarten, in welchem Umfang die Art. 3 bis 5 sowie 7 des Entwurfs mit Leben erfüllt werden. Die Stellungnahme bezieht sich naturgemäß auf die bislang vorliegenden Entwürfe zu den Art. 1, 2 und 6.

II. Zum Vorblatt, hier: D. Haushaltsausgaben ohne Erfüllungsaufwand

Es ist zu begrüßen, dass der Gesetzentwurf anerkennt, dass bei der BfDI für die Übernahme der Funktionen des gemeinsamen Vertreters und der zentralen Anlaufstelle der Bedarf für weitere 10 Planstellen besteht. Positiv ist insbesondere die Klarstellung, dass es sich um einen zusätzlichen Bedarf handele, der über die im Regierungsentwurf des Bundeshaushalts 2017 veranschlagten Mittel hinausgehe.

In den für den Bundeshaushalt 2017 vorgesehenen Planstellen für die Umsetzung der DSGVO und der JI-Richtlinie sind die Aufgaben des gemeinsamen Vertreters und der zentralen Anlaufstelle noch nicht berücksichtigt, weil noch nicht klar war, ob und in welchem Umfang diese Aufgaben der BfDI übertragen werden.

Den im Vorblatt enthaltenen Bedarf konkretisiere ich zum besseren Verständnis wie folgt:

1x B 3	Leitung der zentralen Anlaufstelle; Übernahme wichtiger Vertretungsfunktionen
2x A 15 2x A 14	Referententätigkeit zur Durchführung zentraler Funktionen der zentralen Anlaufstelle:

	• Koordinierung der Positionsbestimmung der deutschen Datenschutzbehörden • Inhaltliche Aufbereitung der Positionsbestimmungen • Bewertung und Weiterverarbeitung eingehender Stellungnahmen, Entscheidungsvorschläge und anderer Dokumente aus dem Europäischen Datenschutzausschuss, von anderen Aufsichtsbehörden und der Europäischen Kommission • Weiterleitung der vorgenannten Dokumente an die deutschen Aufsichtsbehörden • Ggf. Teilnahme an Sitzungen insbesondere von Arbeitsgremien des Europäischen Datenschutzausschusses • Teilnahme an Terminen mit Vertretern des Ausschusses, anderer Aufsichtsbehörden, der Europäischen Kommission oder anderen Gremien • Information und Beratung des gemeinsamen Vertreters
3x A 13 g	Sachbearbeiter zur Unterstützung der Referenten bei den o. g. Aufgaben, sowie insbesondere folgende Aufgaben: • Überwachung von Fristen und Terminen • Hinwirken auf die Einhaltung der Verfahren • Entwicklung standardisierter Formate für den Informationsaustausch • Informationsmanagement
2x A 8	Bürosachbearbeiter zur Unterstützung der o. g. Aufgaben der Kontaktstelle, Liegenschaftsverwaltung, Serviceangelegenheiten

Ob die vorgenannten Ansätze tatsächlich auskömmlich sind, um die neuen Aufgaben zu erfüllen, bedarf noch eingehenderer Prüfung. Insofern behalte ich mir vor, begründeten darüber hinaus gehenden Bedarf geltend zu machen.

III. Zu Art. 1 – Entwurf eines Allgemeinen Bundesdatenschutzgesetzes (ABDSG-E)

1. Zum ABDSG-E allgemein

a. Problembeschreibung

Der Entwurf hat sich zum Ziel gesetzt,

- die Regelungsaufträge und einen Teil der Regelungsoptionen aus der Datenschutz-Grundverordnung (DSGVO) umzusetzen,
- allgemeine Bestimmungen zur Umsetzung der Richtlinie (EU) 2016/680 (JI-Richtlinie) zu erlassen und
- allgemeine Regelungen für die Verarbeitung personenbezogener Daten durch solche öffentliche Stellen des Bundes zu schaffen, deren Tätigkeiten nicht im Anwendungsbereich des Unionsrechts liegen (d. h. vor allem die Nachrichtendienste des Bundes und im Zusammenhang mit dem SÜG).

Dieser gewählte Ansatz ist nicht nur ambitioniert, sondern er ist h. E verfehlt und weitgehend misslungen.

Der Regelungsansatz führt dazu, dass für den Rechtsanwender bei vielen Vorschriften deren Anwendungsbereich unklar ist. Einzelne Regelungen gelten nur im Anwendungsbereich der DSGVO, andere nur im Anwendungsbereich der JI-Richtlinie, weitere nur für die nicht unionsrechtlich geregelten Bereiche und wieder andere für mehrere der vorgenannten Bereiche zugleich. Dies macht den Gesetzentwurf unübersichtlich und kaum handhabbar. Diese unterschiedlichen Anwendungsbereiche finden sich zum Teil auch innerhalb einer einzigen Vorschrift wieder, wie z. B. in § 14 ABDSG-E, ohne dass dies kenntlich gemacht wird. Häufig verbleiben dadurch Unklarheiten, was genau der Inhalt einer Regelung eigentlich ist. Zum Teil lassen sich die Anwendungsbereiche der Vorschriften zwar mithilfe der Begründung ermitteln. Dies ist aber nicht ausreichend, denn dem Rechtsanwender steht die Begründung in der Regel nicht zur Verfügung und wesentliche Fragen wie der Anwendungsbereich einer Vorschrift müssen sich aus rechtsstaatlichen Gründen unmittelbar aus dem Gesetzestext ergeben.

Im Anwendungsbereich der JI-Richtlinie, vor allem aber bei den Bereichen außerhalb des Unionsrechts lässt der Gesetzentwurf die aktuelle Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Zweckbindung und zur datenschutzrechtlichen Kontrolle völlig unberücksichtigt. Dies gilt besonders für die Informationsverarbeitung im Bereich der Nachrichtendienste. Das ist ein erheblicher Mangel. Zu rechtfertigen ist dies nur, soweit für den Bereich der Fachgesetze eine Umsetzung angestrebt ist. Derzeit liegt insoweit nur ein Entwurf für den Bereich des BKAG vor, zu dem ich gesondert Stellung nehme. Der vorliegende Entwurf des BVerfSchG in Art. 2 wiederum berücksichtigt die aktuelle Rechtsprechung des Bundesverfassungsgerichts nicht. Änderungen des BNDG und des MADG liegen noch nicht vor.

Der Gesetzentwurf lässt entgegen den verfassungsrechtlichen Vorgaben im Bereich der Nachrichtendienste eine Verbesserung der unabhängigen Datenschutzkontrolle vermissen. Bei den Durchsetzungsmöglichkeiten der BfDI ist der Gesetzentwurf in diesem Bereich ein deutlicher Rückschritt.

Der Entwurf ist insoweit entschieden abzulehnen, als er die Kontrollbefugnisse der BfDI im Bereich der Nachrichtendienste erheblich einschränkt. Darüber hinaus streicht er in diesem Bereich Sanktionsmöglichkeiten. Auch erhebliche Datenschutzverstöße im Bereich der Nachrichtendienste sind künftig vollständig straflos gestellt und nicht mehr bußgeldbewehrt. Mit der angesprochenen Rechtsprechung des BVerfG ist dies nicht zu vereinbaren.

Auch werden die Rechte des Parlaments dadurch beschnitten, dass die BfDI im Bereich des BVerfSchG nicht mehr auf Aufforderung des Bundestages Gutachten erstellen oder Berichte erstatten soll oder auf Ersuchen des Bundestages, des Petitionsausschusses oder des Innenausschusses Hinweisen bei öffentlichen Stellen des Bundes nachgehen kann.

Die Bewertung steht insgesamt unter dem Vorbehalt, dass die Pläne für den Bereich der Fachgesetze im JI-Bereich hier nur teilweise bekannt sind Unbekannt sind die Vorstellungen insbesondere für die Bereiche Bundespolizei, Zollfahndungsdienst, Strafverfolgung, Strafvollzug und internationale Rechtshilfe. Die Regelungen lassen sich aber nur im Zusammenhang sinnvoll beurteilen.

Hinzukommt, dass an einigen Stellen keine Unterscheidung zwischen nicht-öffentlichen Stellen und öffentlichen Stellen des Bundes getroffen wird. Zwar erfasst die DSGVO beide Bereiche, enthält ihrerseits aber ebenfalls eine Binnendifferenzierung und eröffnet in unterschiedlichem Umfang Regelungsmöglichkeiten für die nationalen Gesetzgeber. Diese Binnendifferenzierung nimmt der Entwurf zum Teil nicht vor (siehe z. B. § 6) und kommt dadurch zu unausgewogenen Ergebnissen.

b. Schlussfolgerung

BfDI hält es dringend für erforderlich, die Gesamtsystematik des Gesetzentwurfs grundlegend zu überarbeiten und eine klare Trennung zwischen der Umsetzung der Regelungsaufträge und -optionen nach der DSGVO, der Umsetzung der JI-Richtlinie und der Regelung für die nicht unionsrechtlich erfassten Bereiche herzustellen.

2. Zur Umsetzung der JI-Richtlinie und zu den Vorschriften außerhalb des Unionsrechts (insbesondere zu den Nachrichtendiensten) im Allgemeinen

a. Problembeschreibung

Sowohl die JI-Richtlinie als auch zuletzt das Urteil des Bundesverfassungsgerichts vom 20.04.2016 zum BKAG enthalten grundsätzliche Aussagen, die über den Bereich der in diesem Entwurf erfassten Regelungen hinausgehen (BVerfG NJW 2016, 1781). Das Bundesverfassungsgericht hat eine ähnliche Umsetzungsfrist gesetzt, wie sie auch für die JI-Richtlinie gilt. Deshalb wäre es erforderlich, die jeweiligen Vorgaben in einem Gesetz gemeinsam umzusetzen. Der vorliegende Entwurf geht auf die verfassungsrechtlichen Vorgaben jedoch nicht ein.

Entgegen der Angabe in seinem Titel enthält der Entwurf weitgehend nur die notwendigen Anpassungen aus der DSGVO. Die JI-Richtlinie setzt er nur in rudimentären Ansätzen um. Die Begründung verweist zwar insoweit auf weiteren notwendigen Umsetzungsbedarf im Fachrecht (Allgemeiner Teil, I.). Wie dieser aber im Einzelnen aussehen soll, bleibt weitgehend unklar. Lediglich für den Bereich des Bundeskrimi-

nalamts liegt ein Entwurf für ein eigenes Umsetzungsgesetz vor. Dort sind Platzhalter für die betroffenen Fachgesetze im JI-Bereich, insb. BPolG, StPO vorgesehen. Die Regelungen des ABDSG lassen sich bezogen auf den JI-Bereich nur sinnvoll im Zusammenhang beurteilen. Da der Entwurf für das BKAG erst am 18.08.2016 hier eingegangen ist, können die Zusammenhänge in dieser Stellungnahme noch nicht berücksichtigt werden.

Die JI-Richtlinie enthält allgemeine Vorgaben, die zu berücksichtigen sind. So stellt sich etwa die Frage, ob wegen Art. 7 der JI-Richtlinie eine allgemeine Regelung zur Qualität der Daten und ihrer Dokumentation eingefügt werden sollte. Darüber hinaus sollte gesetzlich vorgesehen sein, besondere Verarbeitungsbeschränkungen gemäß Art. 9 Abs. 3 der JI-Richtlinie zu kennzeichnen.

Insgesamt müssen die sich aus der Richtlinie ergebenden zusätzlichen Anforderungen eingearbeitet werden. Dies gilt etwa für die Prüfung der Datenqualität in § 7 oder das Vertretungsrecht in Artikel 55 der JI-Richtlinie. Art. 19 und 20 der JI-Richtlinie bestimmen, dass Verantwortliche geeignete und angemessene technische und organisatorische Maßnahmen umsetzen müssen, um sicherzustellen, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt. Das Ziel solcher technischen und organisatorischen Maßnahmen ist damit lediglich abstrakt beschrieben. Da die gesamte Richtlinie in Bezug genommen wird, wird jedoch deutlich, dass sämtliche Aspekte des Datenschutzrechts durch technische und organisatorische Maßnahmen gewährleistet werden sollen. Der Entwurf geht hierauf nicht ein.

Von besonderer Bedeutung ist die Anpassung der Begrifflichkeiten in allen Vorschriften zum JI-Bereich. Dies betrifft u.a. den vielfach verwendeten Begriff „verarbeiten“ bzw. „Verarbeitung“. Nach Art. 3 Nr. 2 der JI-Richtlinie fällt hierunter eine Aufzählung verschiedenster Vorgänge bis hin zur „Verbreitung“ der Daten. Dadurch ändern sich bislang verwendete Begrifflichkeiten erheblich. So fällt etwa der Begriff „Nutzen“ weg. Die „Verwendung“ ist dem „Verarbeiten“ nicht mehr übergeordnet, sondern jetzt eine Teilmenge davon. Art. 3 Nr. 2 der JI-Richtlinie zwingt den nationalen Gesetzgeber dazu, hinsichtlich der einzelnen Verarbeitungstätigkeiten genau zu differenzieren. Zu pauschale und wenig differenzierte Ermächtigungen verstoßen gegen den Grundsatz der Verhältnismäßigkeit.

Insbesondere im Bereich der nicht vom Unionsrecht erfassten Regelungen für die Nachrichtendienste bedarf es im Hinblick auf die Verfahrenssicherungen deutlicher Verbesserungen.

Richtervorbehalte, Transparenz, Protokollierung und datenschutzrechtliche Kontrolle sollte der Gesetzgeber ebenfalls für das gesamte Sicherheitsrecht überarbeiten.

Das Bundesverfassungsgericht hat in zwei grundlegenden Urteilen der BfDI eine Kompensationsfunktion zum Schutz der Grundrechte der Betroffenen zugewiesen (Urt. v. 20. April 2016, Abs. Nr. 141; Urt. v. 24. April 2013, Abs. Nr. 217). Insbesondere im Bereich der heimlichen Datenverarbeitung ist der schwach ausgestaltete Individualrechtsschutz durch effiziente, wirksame und regelmäßige Datenschutzkontrollen zu kompensieren. Zunehmend operieren auch Polizeibehörden geheim. Zwar müssen sie grundsätzlich Daten offen erheben. Gerade im Bereich der Zentralstellenfunktion des Bundeskriminalamts kommt es jedoch zu zahlreichen Datenverarbeitungen, die den Betroffenen verborgen bleiben und mit denen dieser nicht rechnet. Mit polizeilichen Informationsverbünden, die im Hintergrund Zusammenhänge herstellen und Daten abgleichen, ist zu erwarten, dass derartig verborgene Datenflüsse in Zukunft weiter zunehmen.

Das Bundesverfassungsgericht hat zur Kompensationsfunktion hervorgehoben, es obliege dem Gesetzgeber und den Behörden gemeinsam, die verfassungsrechtlichen Anforderungen einer wirksamen Kontrolle sowohl „auf der Ebene des Gesetzes als auch in der Verwaltungspraxis“ zu gewährleisten (a.a.O., Abs. Nr. 214 und 218). Den Gesetzgeber treffe auch die Verpflichtung, die Kontrollbehörden zur Erfüllung dieser Aufgabe angemessen auszustatten (a.a.O., Abs. Nr. 217). Das Gericht hebt nicht nur die aus der Kompensationsfunktion resultierende Häufigkeit der Kontrollen hervor, sondern auch die „qualifizierten Anforderungen an die Kontrolle“ (a.a.O., Abs. Nr. 134)

Der Entwurf will die Kontrollbefugnisse der BfDI für die Nachrichtendienste erheblich einschränken, indem er die Berichtsmöglichkeiten gegenüber dem deutschen Bun-

destag abschaffen will (siehe dazu im Einzelnen zu den Vorschriften des BVerfSchG, zu Artikel 2). Das lehne ich entschieden ab.

Darüber hinaus kann die Kompensationsfunktion nur dann Wirkung entfalten, wenn die betroffenen Behörden auf Beanstandungen der BfDI in derselben Weise reagieren, wie auf verwaltungsgerichtliche Urteile. Gerade gegenüber den Verfassungsschutzbehörden hat BfDI jedoch keine Weisungsbefugnisse. Auch ein gerichtliches Verfahren kann BfDI nicht anstoßen. Künftig soll die BfDI nicht einmal mehr dem Parlament gegenüber berichten dürfen. Insofern hat BfDI gegenüber den Nachrichtendiensten weniger Durchsetzungsmöglichkeiten, obwohl hier die Kompensationsfunktion am stärksten gefordert ist. Das ist im Ergebnis ein Wertungswiderspruch und mit den verfassungsrechtlichen Vorgaben mitnichten vereinbar.

b. Schlussfolgerung

Die bislang vorliegenden Regelungen zur Umsetzung der JI-Richtlinie und vor allem zur Verarbeitung personenbezogener Daten durch die Nachrichtendienste des Bundes werden den verfassungsrechtlichen Anforderungen nicht gerecht und müssen daher geändert bzw. ergänzt werden.

Die Kompensationsfunktion der datenschutzrechtlichen Kontrolle der Nachrichtendienste durch die BfDI ist sachgerecht auszufüllen; insbesondere bedarf die BfDI auch in diesem Bereich wirksamer Eingriffsbefugnisse wie sie etwa in § 25 Abs. 2 Sätze 3 und 4 ABDSG-E im Bereich der JI-Richtlinie geschaffen worden sind.

Im ABDSG als auch in den Fachgesetzen (wie BKAG oder BVerfSchG) sollte eine ausdrückliche Regelung aufgenommen werden, wonach eine Sperrung bzw. eine Einschränkung der Verarbeitung von Daten anstelle einer Löschung vorzunehmen ist, wenn die BfDI eine Kontrolle zu dem Gegenstandsbereich ankündigt, von dem die Daten betroffen sind. Damit wird verhindert, dass solche Daten – die an sich zu löschen wären, von der BfDI nicht mehr überprüft werden können, weil die Kontrolle zeitlich kurz nach dem beabsichtigten Löschtermin stattfindet.

3. Zu § 1 ABDSG-E

§ 1 ist weitgehend überflüssig und im Übrigen schwer verständlich. Er beinhaltet größtenteils Aussagen, die richtigerweise Gegenstand der Gesetzesbegründung sind.

Zu den generellen systematischen Bedenken der Umsetzung verschiedener Rechtsakte in einem Gesetz wird auf die obigen Ausführungen (III.1) Bezug genommen. Die hier für notwendig gehaltenen Änderungen der Systematik würden notwendigerweise auch zu einer Änderung des § 1 ABDSG-E führen.

In Abs. 2 Nr. 1 wird der Begriff „Öffnungsklausel“ verwendet. Dies ist kein eingeführter Rechtsbegriff und er trifft auch sprachlich nicht vollständig zu. Ich rege daher an, die Worte „durch Öffnungsklauseln“ zu streichen. Der verbleibende Text wäre nach wie vor eindeutig.

4. Zu § 3 ABDSG-E

In den Absätzen 5 ff. sind Begriffsbestimmungen aus Art. 4 DSGVO und Art. 3 JI-Richtlinie übernommen worden. Offensichtlich handelt es um Definitionen, die zum Teil sowohl in der DSGVO als auch in der JI-Richtlinie wortgleich verwendet werden. Zum Teil handelt es sich um Begriffsbestimmungen, die es ausschließlich im Anwendungsbereich der DSGVO gibt (insbes. die Absätze 20 ff.). Schließlich wird eine Begriffsbestimmung aus der JI-Richtlinie nicht übernommen, die der zuständigen Behörde nach Art. 3(7) JI-Richtlinie. Ebenso fehlt aus der DSGVO die Begriffsbestimmung aus Art. 4(24) DSGVO.

Zwar bestehen gegen die aufgeführten Begriffsbestimmungen inhaltlich naturgemäß keine Einwände, da sie wortgleich dem Unionsrecht entnommen sind. Dennoch ist die Vorschrift insofern problematisch, als sie für die Anwendungsbereiche von DSGVO und JI-Richtlinie gleichermaßen gilt, ohne dass deutlich gemacht wird, welche Begriffsbestimmung in welchem Bereich anzuwenden ist. So hat der Begriff „Haupt-

niederlassung“ nur im Anwendungsbereich der DSGVO eine Bedeutung, nicht aber in dem der JI-Richtlinie.

Zudem besteht bei einer EU-Verordnung das grundsätzliche Verbot wiederholender Regelungen im nationalen Recht. Für die DSGVO sieht deren EG 8 hierfür Ausnahmen vor, worauf die Begründung auch Bezug nimmt. Allerdings erlaubt es EG 8 der DSGVO nicht, die Begriffsbestimmungen zu wiederholen. EG 8 erlaubt nämlich nur dann Wiederholungen, wenn in der Verordnung „Präzisierungen oder Einschränkungen … durch das Recht der Mitgliedstaaten“ vorgesehen sind. Eine Reihe von Begriffsbestimmungen der DSGVO steht jedoch in keinem Zusammenhang mit solchen Regelungsspielräumen. Das gilt namentlich für die in § 3 Absätze 20 bis 24 sowie 26 bis 28 ABDSG-E aufgeführten Begriffsbestimmungen.

In § 3 ABDSG-E sollten deshalb nur die aufgrund der JI-Richtlinie notwendigen Begriffsbestimmungen geregelt werden. Darüber hinaus gehende Begriffsbestimmungen aus der DSGVO sind zu streichen. Insgesamt zeigt § 3 ABDSG-E erneut, dass die gemeinsame Umsetzung von DSGVO und JI-Richtlinie in einem Gesetz hoch problematisch ist.

Zu Abs. 11 sei angemerkt, dass der Satz unvollständig ist.

5. Zu § 4 ABDSG-E

In der Überschrift rege ich an, am Ende die Worte „des Bundes“ anzufügen, um Unklarheiten zu vermeiden, da in § 3 Abs. 2 ABDSG-E auch öffentliche Stellen der Länder definiert werden.

Inhaltlich teile ich die Auffassung, dass es in Nachfolge der §§ 12 ff. BDSG nach wie vor allgemeiner Datenschutzvorschriften für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes bedarf, da letztlich nicht sämtliche Lebensbereiche durch bereichsspezifisches Recht erfasst werden können und dies auch nicht wünschenswert wäre. Auch im Anwendungsbereich der DSGVO können solche Rechtsgrundlagen gem. Art. 6(1)(e), Art. 6(3) DSGVO geschaffen werden.

Die Vorschrift ist jedoch insgesamt problematisch, zu undifferenziert und sie wahrt nicht das Prinzip der Verhältnismäßigkeit.

Absatz 1 übernimmt den Wortlaut der DSGVO, dies aber nur teilweise. So wird etwa dem Verordnungstext in der Version des § 4 Absatz 1 insbesondere hinzugefügt: *„Unbeschadet anderer Rechtsgrundlagen“*. Dieser Zusatz ist eher verwirrend, da nicht klar ist, auf welche anderen Rechtsvorschriften er sich alles bezieht. Er ist aber insbesondere auch überflüssig. § 2 Abs. 2 ABDSG-E stellt die Nachrangigkeit des ABDSG bereits klar, sodass im Falle des Vorhandenseins anderer Rechtsvorschriften dieses gar nicht anwendbar ist und damit auch § 4 ABDSG nicht zur Anwendung käme. Folgerichtig enthalten auch §§ 13, 14 BDSG einen solchen Zusatz nicht. Er ist daher zu streichen.

Zudem ist die in Absatz 1 vorgenommene reine Wiederholung von Art. 6(1)(e) DSGVO nicht sinnvoll und führt nicht weiter. Art. 6(3) DSGVO erlaubt eine Konkretisierung von 6(1)(e) DSGVO, die der Absatz 1 gerade nicht vornimmt. Er ist letztlich überflüssig.

Die vorgenannte Konkretisierung soll offensichtlich durch Absatz 2 vorgenommen werden. Die dort vorgenommene Aufzählung ist jedoch systematisch verfehlt und inhaltlich fragwürdig:

Sie lässt einen erheblichen Anwendungsspielraum zu durch eine erhöhte Aufzählung einzelner Zwecke, die unspezifisch für alle Behörden gelten. Nach der Vorschrift dürfen zum Beispiel alle Polizei- und Justizbehörden personenbezogene Daten zur Verhütung von Berufsstandsregeln für reglementierte Berufe speichern (präventiv!). Dies gilt unabhängig davon, ob eine konkrete (!) Gefahr für die öffentliche Sicherheit vorliegt, wie dies traditionell Voraussetzung für die Polizeibehörden ist. Umgekehrt darf beispielsweise ein Gesundheitsamt allgemein – auch präventiv ohne konkreten Anlass – Daten zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten speichern. Für Polizei-, Justiz- und Nachrichtendienstbehörden sollte der § 4 Absatz 2 für unanwendbar erklärt und die Voraussetzungen ausschließlich in den Fachgesetzen geregelt werden.

Genannt wird unter anderem die Abwehr einer Gefahr für die öffentliche Sicherheit (Nr. 2), die Verfolgung von Straftaten oder Ordnungswidrigkeiten (Nr. 5), die Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen (Nr. 6).

Wegen des etwaigen späteren Zugriffs der Ermittlungsbehörden und der Nachrichtendienste auf die gespeicherten Daten ist auch Nummer 8 problematisch. Diese Vorschrift bietet ein Einfallstor für die relativ undifferenzierte Speicherung einer Vielzahl von Daten auf Vorrat. „Netz-, Daten- und Informationssicherheit“ sind nur wenig bestimmt. Welche Daten davon erfasst sein sollen ist unklar. Die Speicherdauer bleibt ebenfalls offen.

Letztlich ergibt sich der Umfang der den öffentlichen Stellen des Bundes erlaubten Verarbeitung personenbezogener Daten aus der Grundrechtsbindung, dem Verhältnismäßigkeitsprinzip und dem Rechtsstaatsprinzip. Öffentliche Stellen dürfen Eingriffe in das Recht auf informationelle Selbstbestimmung nur vornehmen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Aus Art. 20 Abs. 3 GG ergibt sich, dass sich die Aufgaben der Exekutive aus Recht und Gesetz ergeben müssen. Aus der Bindung an die Grundrechte folgt letztlich das datenschutzrechtliche Erforderlichkeitsprinzip. Insofern ist Absatz 2 Nr. 1 völlig ausreichend. Alle weiteren Aufzählungen in den folgenden Ziffern sind im besten Fall wertlose – da undifferenziert nebeneinander stehende – Ausformungen dieser Grundprinzipien. Im schlechteren Falle vermitteln sie den Eindruck, öffentliche Stellen könnten sich über Grundrechts- und Gesetzesbindung hinwegsetzen. § 13 des geltenden BDSG beschränkt sich dementsprechend auf die Erforderlichkeit.

Die Konkretisierung der Erforderlichkeit im Einzelfall kann sich hingegen nur aus den gesetzlichen Aufgaben jeder einzelnen öffentlichen Stelle ergeben, die ihrerseits im jeweiligen Fachrecht geregelt sind. Dies schließt als Annex auch allgemeinere Aufgaben wie etwa die Wahrung des Hausrechts ein.

Die durch Art. 6(3)3 DSGVO möglichen Konkretisierungen von Eingriffsvoraussetzungen. der Arten von Daten, der betroffenen Personen, der Übermittlungsempfänger, der Zweckbindung, der Speicherfristen etc. können sinnvoll nur spezifisch im Fachrecht, nicht aber durch einen Rundumschlag im ABDSG vorgenommen werden.

Im Ergebnis plädiere ich für eine Speicherung des gesamten Kataloges in Absatz 2 mit Ausnahme der Nummer 1.

Ebenso ist Absatz 3 (fälschlicherweise als Absatz 2 bezeichnet) überflüssig. Selbstverständlich kann der Gesetzgeber unter den verfassungsrechtlichen Voraussetzungen im öffentlichen Interesse liegende Aufgaben festlegen.

6. Zu § 5 ABDSG-E

Die Regelung orientiert sich sehr stark am derzeitigen § 13 Absatz 2 BDSG, der Artikel 8 Absatz 2 EG-Datenschutzrichtlinie 95/46/EG umgesetzt hat. Datenschutzpolitisch war diese Umsetzung schon seinerzeit verbesserungsfähig. Das grundsätzliche Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten lässt sich ledig aus einem Umkehrschluss herleiten („ist nur zulässig, soweit“).

Deshalb sollte die Gelegenheit genutzt werden, das sowohl in Artikel 8 Absatz 1 EG-Datenschutzrichtlinie 95/46/EG als auch in Artikel 9 Absatz 1 EU-DSGVO normierte grundsätzliche Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten deutlich zu machen. Ich rege daher an, die Obersätze von Absatz 1 und Absatz 2 wie folgt zu fassen:

„Die Verarbeitung besonderer Kategorien personenbezogener Daten ist untersagt. Abweichend von Satz 1 ist die Verarbeitung besonderer Kategorien personenbezogener Daten (ggf. im Anwendungsbereich der…) nur zulässig, soweit dies erforderlich ist …“

Systematisch wirkt die Vorschrift so, als sei der Katalog in Absatz 1 abschließend, obwohl er sich ausschließlich auf die Regelungsspielräume in Art. 9 Abs. 2 lit. b), g),

h) und i) DSGVO stützt und die übrigen Tatbestände des Art. 9 Abs. 2 DSGVO unmittelbar anwendbar sind. Dies wird dem Rechtsanwender nicht klar und zeigt erneut die problematische Systematik bei der Umsetzung des Unionsrechts.

Die in Abs. 1 Satz 2 vorgesehenen Maßnahmen zur Wahrung der der Grundrechte der Betroffenen beschränken sich im Wesentlichen auf eine Wiederholung des Wortlauts der entsprechenden Normen aus der DSGVO. Dies ist nicht ausreichend.

7. Zu § 6 ABDSG-E

Die Vorschrift ist insgesamt zu weitgehend und missachtet das Gebot der Zweckbindung.

Problematisch ist zunächst, dass die Vorschriften undifferenziert in gleicher Weise für öffentliche wie für nicht-öffentliche Stellen gilt. Dies ist schon aus systematischen Gründen fragwürdig, weil die nach der DSGVO bestehenden unterschiedlichen Regelungsspielräume diese Differenzierung erfordern.

Ausweislich der Begründung wird § 6 ABDSG-E in Gänze auf Art. 6 Abs. 4 DSGVO (i. V. m. Art. 23 DSGVO) gestützt. Dies ist allerdings in dieser undifferenzierten Weise nicht möglich. Art. 6 Abs. 4 DSGVO enthält keine Ermächtigung, mitgliedstaatliches Recht zu schaffen. Er ermöglicht lediglich in den Bereichen, in denen bereits nach anderen Vorschriften der DSGVO Regelungsspielräume bestehen (namentlich Art. 6 Abs. 2 und 3 DSGVO) weitergehende Zweckänderungen. Anderenfalls würde das Ziel der Harmonisierung im nicht-öffentlichen Bereich über den Umweg der Zweckänderung nach Art. 6 Abs. 4 DSGVO ad absurdum geführt.

Zu kritisieren ist auch, dass die Vorschrift die gleichen Zweckänderungen für Daten i. S. v. Art. 9 DSGVO zulässt, was dessen enge Bindungen weitgehend entwertet.

Schließlich ist auch für öffentliche Stellen der Katalog in den Buchstaben a) bis j) zu weitgehend und zu undifferenziert und damit unverhältnismäßig. Er geht auch über

§ 14 Abs. 2 und 3 des geltenden BDSG hinaus. Es ist stärker zu berücksichtigen, dass Zweckänderungen eine Ausnahme und die Zweckvereinbarkeit die Regel sind.

Im Ergebnis ist in § 6 somit einerseits zwischen öffentlichen und nicht-öffentlichen Stellen zu differenzieren, wobei Zweckänderungen bei nicht-öffentlichen Stellen in deutlich weniger Fällen zulässig sein dürfen als bei öffentlichen Stellen. Zudem sind die Möglichkeiten von Zweckänderungen bei Daten i. S. v. Art. 9 DSGVO zu beschränken. Schließlich ist bei den erlaubten Zweckänderungen das Prinzip der Verhältnismäßigkeit und der Ausnahmecharakter von Art. 6 Abs. 4 DSGVO zu wahren.

8. Zu § 7 ABDSG-E

In Absatz 2 wird die Informationspflicht für den Fall des unverhältnismäßigen Aufwandes ausgeschlossen. Diese Einschränkung des Art. 13 DSGVO wird lt. Begründung auf Art. 23 DSGVO gestützt.

Art. 23 DSGVO gibt diese Beschränkung h. E. nicht her. Demnach sind solche Beschränkungen nur zulässig, wenn sie in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Dies vermag ich im Falle eines hohen Verwaltungsaufwandes nicht festzustellen. Die Begründung zu Absatz 2 stützt sich darüber hinaus auf Art. 23 Abs. 1 lit. i) DSGVO. Mir erschließt sich nicht, in welcher Weise der Schutz eines unverhältnismäßigen Aufwandes die Rechte und Freiheiten anderer Personen schützen soll. Art. 23 Abs. 1 lit. i) DSGVO schützt ja nicht den Verantwortlichen, sondern nur Dritte. Zudem lässt Absatz 2 jede ernsthafte Auseinandersetzung mit den Anforderungen des Art. 23 Abs. 2 DSGVO vermissen. Der bloße Verweis auf Art. 23 Abs. 2 lit. c) DSGVO ist in keiner Weise ausreichend. Es bedarf vielmehr einer Reihe weiterer spezifischer Regelungen i. S. v. Art. 23 Abs. 2 DSGVO.

Schließlich bestehen auch systematische Zweifel gegen Absatz 2. Der Verordnungsgeber hat bei der Schaffung des Art. 13 DSGVO nach intensiven Diskussionen im Rat und im Europäischen Parlament bewusst darauf verzichtet, eine Beschränkung wegen des unverhältnismäßigen Aufwandes vorzusehen. Diese Einschränkung pau-

schal durch den nationalen Gesetzgeber wieder einzuführen verstößt h. E. gegen die DSGVO und lässt sich auch auf der Grundlage von Art. 23 DSGVO nicht begründen.

Im Ergebnis kann Absatz 2 nicht beibehalten werden.

9. Zu § 8 ABDSG-E

Systematisch ist bei dieser Vorschrift erneut problematisch, dass sie völlig undifferenziert für öffentliche und nicht-öffentliche Stellen gilt. Sie vermengt gewissermaßen die bisherigen §§ 19a und 33 BDSG. Damit wird nicht immer klar, welche Stellen sich auf welche Ausnahmen des Absatzes 2 stützen können. So kann etwa lit. a) nur für öffentliche Stellen gelten, lit. e) bspw. nur für nicht-öffentliche Stellen. Es muss ausgeschlossen werden, dass öffentliche Stellen etwa die Interessenabwägung nach Absatz 2 lit. e) vornehmen.

Im Hinblick auf die Anforderungen des Art. 23 DSGVO begegnet der Katalog insgesamt Zweifeln. Insbesondere ist die Berücksichtigung der Vorgaben von Art. 23 DSGVO überwiegend fragwürdig. In aller Regel wird ausschließlich pauschal auf Art. 23 Abs. 2 lit. c) DSGVO Bezug genommen. Auch die Vorgaben des Abs. 2 Satz 2 sind zu pauschal und undifferenziert. Dies erscheint insgesamt nicht ausreichend, um den spezifischen Anforderungen des Art. 23 Abs. 2 DSGVO insgesamt gerecht zu werden. Im Übrigen wird auf die Ausführungen zu § 7 Bezug genommen.

Die in Absatz 2 Satz 1 lit. c) vorgesehene Ausnahme wird auf Art. 23 Abs. 1 lit. h) DSGVO gestützt. Dies ist nicht nachvollziehbar und passt nicht.

Die in Absatz 2 Satz 1 lit. h) vorgesehene Ausnahme verlagert die Verpflichtungen des Gesetzgebers nach Art. 23 Abs. 2 DSGVO auf den Verantwortlichen, der sich durch schriftliche Festlegung selbst seine Ausnahme schaffen soll. Dies ist nicht akzeptabel.

Die in Absatz 2 Satz 1 lit. i) vorgesehene Ausnahme gehört h. E. systematisch zu § 7 ABDSG-E, da die Daten beim Betroffenen erhoben werden.

Im Ergebnis muss § 8 Abs. 2 ABDSG-E im Lichte der vorangehenden Ausführungen überarbeitet werden.

10. Zu § 9 ABDSG-E

Ebenso wie bei § 8 ABDSG-E differenziert die Vorschrift nicht in ausreichender Weise zwischen dem öffentlichen und dem nicht-öffentlichen Bereich. Auf die dortigen Ausführungen wird Bezug genommen.

Der Unterschied der Ausnahmen des Abs. 2 lit. c) und g) wird nicht deutlich. Vermutlich gilt lit. c) für öffentliche Stellen und lit. g) für nicht-öffentliche Stellen. Dies macht noch einmal deutlich, dass die undifferenzierte Regelung für den Anwender problematisch ist.

Auf die Ausführungen zu § 8 wird mit Blick auf die Anforderungen des Art. 23 DSGVO Bezug genommen.

Die Absätze 3 und 4 können sich wiederum nur auf öffentliche Stellen des Bundes beziehen; dies wird aus der Norm jedoch nicht deutlich und bedarf der Klarstellung. Anderenfalls sehe ich die Gefahr, dass sich auch nicht-öffentliche Stellen auf die Ausnahme berufen und die – insoweit unzuständige – BfDI befasst wird.

Absatz 4 Satz 2 ist zu einschränkend ausgestaltet. Zur besseren Rechtssicherheit sollte eine ausdrückliche Befugnis der BfDI aufgenommen werden, dem Betroffenen bestimmte Mitteilungen zu machen. Insbesondere muss es dem Betroffenen erleichtert werden, einzuschätzen, ob eine etwaige gerichtliche Klage erfolgreich sein könnte. Zumindest ist daher eine Befugnis zu regeln, nach der die BfDI das wesentliche Ergebnis der datenschutzrechtlichen Kontrolle mitteilen kann. Stets zulässig sollte es ausdrücklich sein mitzuteilen, ob Datenschutzverstöße festgestellt worden sind oder nicht. Nach der derzeitigen Formulierung kann dies im Konflikt mit der Formulierung stehen, nach der sich aus der Mitteilung der BfDI kein Rückschluss auf den Erkenntnisstand ergeben darf. Das Geheimhaltungsinteresse der verantwortlichen Stelle hat

jedoch in der Regel zumindest dann zurückzustehen, wenn sie rechtswidrig Daten verarbeitet.

In Absatz 5 wird ein Ausschluss der Auskunftserteilung in bestimmten Fällen vorgesehen. Aufgrund der gewählten Nummerierung könnte davon ausgegangen werden, dass sich dieser Ausschluss auch auf die Mitteilung an BfDI nach Absatz 4 bezieht. Es sollte klargestellt werden, dass sich Absatz 5 nicht auf die Mitteilung nach Absatz 4 bezieht.

11. Zu § 10 ABDSG-E

In Absatz 2 wird das Recht auf Löschung auf der Grundlage von Art. 23 DSGVO eingeschränkt, sofern die Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Ausweislich der Begründung wird diese Einschränkung auf Art. 23 Abs. 1 lit. i) DSGVO gestützt, weil die Einschränkung dem Schutz der Rechte und Freiheiten anderer Personen diene.

Diese Begründung ist nicht nachvollziehbar. Es besteht überhaupt kein Zusammenhang zwischen dem Schutz Dritter und dem in Absatz 2 geregelten Tatbestand. Der in Absatz 2 geregelte Fall soll in erster Linie die technische Unmöglichkeit einer Löschung bzw. den Aufwand hierfür berücksichtigen. Dies würde allein den Verantwortlichen schützen, nicht aber „andere Personen“ i. S: v. Art. 23 Abs. 1 lit. i) DSGVO. Im Zeitalter der automatisierten Datenverarbeitung ist diese Einschränkung ohnehin überholt, denn die heutigen Systeme ermöglichen regelmäßig eine vollständige oder selektive Löschung von Daten.

Im Ergebnis ist Absatz 2 zu streichen, da es für diese Einschränkung weder eine Rechtfertigung in Art. 23 Abs. 1 DSGVO noch ein inhaltliches Bedürfnis gibt.

12. Zu § 11 ABDSG-E

In Absatz 2 wird das Widerspruchsrecht nach Art. 21 DSGVO für alle Fälle des § 4 Abs. 2 ABDSG-E beschränkt. Auf welchen Tatbestand des Art. 23 Abs. 1 DSGVO diese Einschränkung gestützt wird, wird aus der Begründung nicht hinreichend deutlich (dort werden die Buchstaben a bis 3 genannt, was keinen Sinn ergibt).

Ungeachtet dessen bestehen jedoch erhebliche Zweifel, ob eine derart pauschale, auf den gesamten Katalog des § 4 Abs. 2 ABDSG-E bezogene Einschränkung des Widerspruchs möglich ist. H. E. bedarf es spezifischer Beschränkungen, die für jeweils spezifische, in Art. 23 Abs. 1 DSGVO genannte, Zwecke in einer demokratischen Gesellschaft erforderlich sein müssen. Diese Beschränkungen müssen spezifisch und konkret in den jeweiligen Rechtsvorschriften vorgenommen werden. Sie können nicht pauschal in einem allgemeinen Gesetz geregelt werden und im Übrigen einer nicht weiter spezifizierten Abwägung durch den Verantwortlichen überlassen bleiben. Dies wird weder den Anforderungen an die Bestimmtheit der Rechtsvorschrift in Art. 23 Abs. 1 DSGVO noch den spezifischen Anforderungen des Art. 23 Abs. 2 DSGVO gerecht.

Absatz 2 ist daher zu streichen.

13. Zu Kapitel 4 allgemein

Es wird angeregt, die Überschrift des Kapitels im Singular zu fassen, sodass sie wie folgt lautet:
„Ergänzende Pflichten für den Verantwortlichen und für den Auftragsverarbeiter“

Damit soll der Verordnung und der Richtlinie entsprochen werden, die die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ stets im Singular verwenden, wie es im Übrigen in §§ 14, 15 ABDSG-E mit Ausnahme von Absatz 1 (dazu nachfolgend) schon derzeit der Fall ist.

In den §§ 14 bis 15 einschließlich der Überschriften wird angeregt, den Sprachgebrauch der Verordnung und der Richtlinie (jeweils deutsche Fassung) zu übernehmen und „Datenschutzbeauftragte(r)“ statt „Beauftragte(n) für den Datenschutz“ zu formulieren.

Entsprechend wird angeregt, die Überschrift zu § 14 ABDSG-E wie folgt zu fassen:
„Benennung einer Datenschutzbeauftragten oder eines Datenschutzbeauftragten“

14. Zu § 14 ABDSG-E

Es wird angeregt, den Sprachgebrauch der Verordnung und der Richtlinie (jeweils deutsche Fassung) zu übernehmen und zu formulieren, dass ein Datenschutzbeauftragter „zu benennen“ statt „zu bestellen“ ist. Dann bestünde auch eine Überstimmung zur bereits entsprechend gefassten Überschrift von § 14, wie sie auch in der Inhaltsübersicht wiedergegeben ist.

Zu Singular/Plural siehe die obige Anmerkung zur Überschrift des Kapitels 4. Eine Formulierung im Singular wird entsprechend für den Datenschutzbeauftragten angeregt. Insofern stimmen derzeit die Überschrift von § 14 und dessen Satz 1 nicht überein.

Satz 1 kann in der jetzigen Fassung so gelesen werden, als könnte es den Fall geben, dass ein Verantwortlicher oder ein Auftragsverarbeiter jeweils mehr als einen Datenschutzbeauftragten zu bestellen hätten. Dies ist aber nicht vorgesehen.
Für Satz 1 wird aus diesen Gründen – auch in Anlehnung an Artikel 37 vor a) – folgende Fassung vorgeschlagen:
„Nach Maßgabe des Artikels 37 Absatz 1 der Verordnung (EU) 2016/679 und des Artikels 32 Absatz 1 der Richtlinie (EU) 2016/680 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten.“

Aus den vorstehenden Gründen sollte auch Satz 2 im Singular formuliert werden.

Von der im Entwurf angesprochenen Möglichkeit des Art 32 Abs. 1 Satz 2 JI-Richtlinie sollte kein Gebrauch gemacht werden. Für die hier einzig in Betracht kommenden Bundesgerichte ist eine solche Ausnahme nicht sinnvoll. Der Datenschutzbeauftragte kann außerhalb der richterlichen Unabhängigkeit Datenschutzfragen klären. Dies betrifft beispielsweise auch die von Richterinnen und Richtern genutzte technische Infrastruktur. Die Prüfung der technischen Infrastruktur z. B. gegen unzulässige Nutzung beeinträchtigt als solche nicht die richterliche Unabhängigkeit (vgl. BGH BeckRS 2011, 26455). Sie kann vielmehr sogar geboten sein, um durch vom Datenschutzbeauftragten geprüfte Berechtigungsregelungen eine unzulässige Einflussnahme auf einzelne Richter zu vermeiden.

Bei den Absätzen 3 und 4 wird lediglich aus der Begründung klar, dass diese ausschließlich für den Anwendungsbereich der JI-Richtlinie gelten. Insofern wird auf die einleitenden Ausführungen zur Gesamtsystematik (s. o. unter 1.) Bezug genommen.

In der Begründung zu Absatz 5 wird auf Artikel 38 Absatz 5 DSGVO Bezug genommen. Dort sind aber nicht Fragen der Kündigung, sondern die Wahrung der Geheimhaltung oder der Vertraulichkeit angesprochen. Deshalb bedarf die Begründung hier einer Anpassung. Ich gehe davon aus, dass diese inhaltlich wünschenswerte Regelung als eine solche des Arbeitsrechts anzusehen ist und daher vom nationalen Gesetzgeber ohne weiteres getroffen werden kann. Im Übrigen gelten die Ausführungen zu Artikel 14 Absätze 3 und 4 entsprechend, hier darauf bezogen, dass eine Regelung ausschließlich zur Verordnung getroffen werden soll.

15. Zu § 15 ABDSG-E

Die Begründung führt aus, dass die Absätze 1 bis 5 (also der gesamte Paragraph) Artikel 33 der JI-Richtlinieumsetzen. In Absatz 4 Satz 1 wird aber ausdrücklich auf die DSGVO Bezug genommen. Für die sich daran anschließenden Regelungen in Absatz 4 Satz 2 wird zwar in der Begründung am Ende inhaltlich zutreffend für eine Regelungskompetenz auf Artikel 38 Absatz 5 der DSGVO Verordnung (EU) 2016/679) verwiesen. Gleichwohl ist damit aus § 15 selbst nicht ohne weiteres nach-

vollziehbar, welche Regelungen nur für die Verordnung, welche möglicherweise nur für die Richtlinie gelten sollen.

Diese unterschiedlichen Regelungszusammenhänge stellen die Nachvollziehbarkeit von Artikel 15 grundsätzlich in Frage. Ist es schon für die Frage, auf welchen Sachverhalt eine gesetzliche Regelung zur Anwendung kommt, auf jeden Fall erforderlich, die Gesetzesbegründung und hier auch die Verordnung beizuziehen, so spricht dies dafür, gesetzestechnisch eine andere Lösung zu suchen. Im Übrigen wird auf die Ausführungen zur Gesamtsystematik Bezug genommen.

16. Zu § 16 ABDSG-E

Die Vorschrift lässt in Umsetzung des Art. 43 Abs. 1 Satz 2 DSGVO den Antragstellern für Akkreditierungen ein Wahlrecht, ob sie die Akkreditierung durch die zuständige Aufsichtsbehörde oder durch die DAkks vornehmen lassen wollen.

Dieses Wahlrecht wird abgelehnt. Einerseits mag es zwar zutreffen, dass die DAkks im Allgemeinen über eine hohe Kompetenz und Erfahrung bei Akkreditierungen verfügt. Sie verfügt allerdings über keinerlei Erfahrungen im Bereich des Datenschutzes. Es ist daher zu befürchten, dass Akkreditierungen, die durch die DAkks vorgenommen werden, nicht den Qualitätsanforderungen der Aufsichtsbehörden entsprechen. Die Aufsichtsbehörden verfügen andererseits nicht nur über das notwendige datenschutzrechtliche Knowhow, sondern zum Teil bereits auch über Erfahrungen in der Akkreditierung und Zertifizierung. Zudem ist sicherzustellen, dass alle Akkreditierungsstellen die Akkreditierung nach identischen Maßstäben und Kriterien vornehmen, was eine enge Abstimmung zwischen den Aufsichtsbehörden und der DAkks voraussetzen und einen nicht unerheblichen Aufwand verursachen würde.

Die Akkreditierung von Zertifizierungsstellen sollte aus den vorgenannten Gründen deshalb ausschließlich den Aufsichtsbehörden zugewiesen werden.

17. Zu § 17 ABDSG-E

Es wird vorgeschlagen, an die Vorschrift folgenden neuen Absatz 3 anzufügen:

> *„(3) Die oder der Bundesbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Bundes übertragen. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgabe erforderlich ist“.*

Begründung:
Die BfDI war bis zum 31.12.2015 beim BMI eingerichtet. Da die Beschäftigten der BfDI solche des BMI waren, wurden die Aufgaben der Personalverwaltung und Personalwirtschaft daher auch vom BMI erledigt. Das BMI seinerseits hat zahlreiche dieser Aufgaben auf das BVA übertragen. Da es sich insoweit um eine Behörde des eigenen Geschäftsbereiches handelte, war dies rechtlich unproblematisch.

Mit Errichtung der BfDI als eigenständiger oberster Bundesbehörde muss die BfDI grundsätzlich alle Aufgaben der Personalverwaltung und -wirtschaft selbst ausführen, soweit nicht gesetzlich eine Übertragung auf andere Behörden zugelassen ist, wie dies etwa gem. § 108 Abs. 5 Satz 1 BBG für die Beihilfe vorgesehen ist.

Im Übrigen ist eine Übertragung von Aufgaben i. S. einer Funktionsübertragung auf andere Behörden jedoch nicht möglich, da es hierfür an den notwendigen Rechtsgrundlagen fehlt. Da die BfDI auch keinen eigenen nachgeordneten Geschäftsbereich hat, müsste sie die Aufgaben selbst wahrnehmen.

Angesichts der begrenzten Kapazitäten im Referat ZA der BfDI besteht aber ein Bedürfnis – wie bisher – bestimmte Aufgaben als Dienstleistung durch andere Behörden (namentlich das BVA) ausführen zu lassen. Dies betrifft beispielsweise Aufgaben der Reisevorbereitung, Reisekostenabrechnung, Gewährung von Trennungsgeld und Umzugskostenerstattung, Geltendmachung von Schadensersatzansprüchen gegenüber Dritten oder die Unterstützung bei Stellenbesetzungsverfahren.

Da die vorgenannten Aufgaben überwiegend auch eine selbständige Aufgabenerledigung beinhalten, kommt auch das Instrument der Auftragsdatenverarbeitung in der Regel nicht in Betracht, das lediglich eine strikt weisungsgebundene Auslagerung reiner Datenverarbeitungsprozesse ermöglicht.

Es ist daher notwendig, eine Rechtsgrundlage zu schaffen, die einerseits die Aufgabenübertragung erlaubt und andererseits die notwendige Übermittlungsbefugnis für die Beschäftigtendaten beinhaltet. Als Vorbild für den hier vorgeschlagenen Absatz 3 diente § 108 Abs. 5 Satz 1 BBG.

Da die Situation für die BfDI als kleinste oberste Bundesbehörde ohne eigenen Geschäftsbereich sehr spezifisch ist, bedarf es keiner allgemeinen Regelung im BBG. Eine nur für die BfDI geltende Spezialregelung, die systematisch in der Regelung über die Errichtung der BfDI am besten verankert ist, wäre daher eine ebenso notwendige wie ausreichende Regelung.

18. Zu § 18 ABDSG-E

Im Gesetzentwurf findet sich keine Regelung, die der BfDI die datenschutzrechtliche Aufsichtszuständigkeit für den Telekommunikations- und Postbereich zuweist. Eine klare gesetzliche Regelung ist jedoch essentiell, um den Status Quo der Zuständigkeitsverteilung zwischen Bund und Ländern zu wahren. Zwar ist es nicht zwingend erforderlich, die Zuweisung im ABDSG selbst vorzunehmen, sondern – wie bisher – die Zuständigkeitszuweisungen im TKG und PostG vorzusehen (dann wohl unter Artikel 7 des Gesetzentwurfs). Dann muss allerdings darauf geachtet werden, dass die bestehenden Zuweisungen in § 42 PostG und § 115 TKG nicht im Rahmen aktueller Anpassungsvorschläge des federführenden BMWi ersatzlos gestrichen werden.

Sofern eine Regelung in den jeweiligen Fachgesetzen vorgesehen ist, sollten neben der Zuweisung der generellen aufsichtsrechtlichen Zuständigkeit über Verweisung auf die relevanten Regelungen im ABDSG (§ 25 ABDSG-E) und der DSGVO (Art. 58) auch die Befugnisse der BfDI thematisiert werden. Die Vorschriften zur Beanstandung müssten hingegen in beiden Gesetzen gestrichen werden. Zudem müsste

im TKG klargestellt werden, dass ausschließlich der BfDI die Funktion der Datenschutzaufsichtsbehörde zukommt. Eine Parallelzuständigkeit der BNetzA wie bisher wäre aufgrund deren fehlender Unabhängigkeit als nachgeordnete Behörde des BMWi nach den Vorgaben der DSGVO und des EuGH unzulässig.

Von der in der Frage an BMJV angesprochenen Möglichkeit des Art. 45 Abs. 2 Satz 2 JI-Richtlinie kann für den GBA kein Gebrauch gemacht werden. Die Staatsanwaltschaften sind keine unabhängigen Justizbehörden, nur die Richter sind unabhängig (Art. 97 Abs. 1 GG). Insofern kann die Zuständigkeit der BfDI für den GBA auf der Basis von Art. 45 Abs. 2 Satz 2 JI-Richtlinie durch nationales Gesetz gar nicht beschränkt werden. Das würde auch gegen die verfassungsrechtlichen Vorgaben verstoßen, wonach bei heimlichen Datenerhebungen eine unabhängige Kontrolle zur Kompensation der Eingriffe erforderlich ist.

19. Zu § 20 ABDSG-E

a. Wahlverfahren

Entsprechend dem geltenden § 22 Abs. 1 BDSG ist in Absatz 1 Satz 1 vorgesehen, dass die BfDI auf Vorschlag der Bundesregierung gewählt wird.

Diese Vorschrift ist mit der DSGVO vereinbar, da diese in Art. 53 Abs. 1 sogar die Ernennung durch die Regierung zuließe.. Die BfDI wird künftig im Vergleich zur geltenden Rechtslage sehr viel weiter reichende Befugnisse vor allem im öffentlichen Bereich erhalten. Dies bedeutet, dass sie auch und gerade gegenüber Bundesbehörden Anordnungs- und Untersagungsbefugnisse erhält, die ihr eine völlig andere Stellung einräumen als das bisherige Beanstandungsrecht. Es sollte daher erwogen werden, ob nicht auch ein Vorschlagsrecht des Parlaments in Frage kommt.

b. Qualifikationsanforderungen

In Absatz 1 Sätze 4 und 5 werden die Anforderungen an die Qualifikation der BfDI festgelegt. Diese Festlegungen muss der Gesetzgeber aufgrund des Auftrages in Art. 54 Abs. 1 lit. b) DSGVO treffen. Die in Satz 5 festgelegten Anforderungen er-

scheinen allerdings sehr überzogen. Dabei ist zu berücksichtigen, dass es sich beim Amt der BfDI auch um eine politische Funktion handelt und die Erfahrung und die fachlichen Kenntnisse des Datenschutzrechts wichtig, aber nicht allein entscheidend sind. Die vorgeschlagene Formulierung würde den in Frage kommenden Kreis potentieller Bundesbeauftragter sehr stark reduzieren.

Es wird daher vorgeschlagen, in Satz 5 zumindest die Worte „mindestens fünfjährige“ und „ausgezeichnete“ zu streichen. Der dann verbleibende Text würde h. E. den Vorgaben von Art. 54 Abs. 1 lit. b) DSGVO noch genügen und zugleich eine höhere Flexibilität bei der Auswahl des/der Bundesbeauftragten schaffen.

20. Zu § 21 ABDSG-E

In Absatz 3 wird um Prüfung gebeten, ob hier tatsächlich auf § 22 verwiesen werden soll oder ob nicht vielmehr § 19 gemeint ist. Es würde jedenfalls mehr Sinn ergeben, dem Leitenden Beamten die Unabhängigkeit bei der Vertretung zu garantieren als eine Regelung zu den Pflichten seiner Amtsführung zu treffen, zumal für ihn in dieser Hinsicht die beamtenrechtlichen Vorschriften gelten.

21. Zu § 23 ABDSG-E

In Absatz 1 muss es statt „Datenarbeitungen“ „Daten**ver**arbeitungen“ heißen. Zudem gehe ich davon aus, dass hier § 1 Absatz 3 (statt Absatz 2) in Bezug genommen werden soll. Dieser Verweisungsfehler findet sich auch an anderen Stellen des Gesetzentwurfs (z. B. in § 25 Abs. 3).

22. Zu § 24 ABDSG-E

Es sollte geprüft werden, ob künftig seitens BfDI ein einheitlicher Tätigkeitsbericht zum Datenschutz und zur Informationsfreiheit gewünscht wird und ob dies nach DSGVO zulässig wäre.

23. Zu § 25 ABDSG-E

a. Zutrittsrecht (Absatz 1 Satz 2)

In Absatz 1 Satz 2 ist die Befugnis der BfDI festgelegt, während der Dienstzeiten Grundstücke und Diensträume zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Damit wird Art. 58 Abs. 1 lit. f) DSGVO umgesetzt.

Die Beschränkung auf die Dienstzeiten ist im Vergleich zum geltenden § 24 Abs. 4 Nr. 2 BDSG deutlich eingeschränkt, da dieser ein „jederzeitiges" Betretungs- und Zugangsrecht vorsieht. Ein solches jederzeitiges Recht ist für die Aufgabenerfüllung der BfDI unabdingbar notwendig. Es ist zudem nicht nachvollziehbar, warum bei der Umsetzung der JI-Richtlinie in Absatz 2 Satz 1 Nr. 2 im Widerspruch dazu das jederzeitige Betretungsrecht vorgesehen ist. Es muss auch im Anwendungsbereich der DSGVO beispielsweise in Eilfällen oder bei besonderen Behörden möglich sein, auch außerhalb der üblichen Dienstzeiten Zugang zu Liegenschaften und Datenverarbeitungsanlagen zu erhalten.

Die Worte „während der Dienstzeiten" sind daher durch das Wort „jederzeit" zu ersetzen.

b. Befugnisse im Bereich der JI-Richtlinie (Absatz 2)

Der Entwurf kopiert weitgehend das bisherige Recht, ohne sich Gedanken zu machen, wie die datenschutzrechtliche Kontrolle gestärkt und verbessert werden kann. Gerade wegen der verfassungsrechtlichen Kompensationsfunktion der Datenschutzkontrolle wäre dies jedoch notwendig gewesen.

Parallel ist hier ein Gesetzentwurf zur Änderung des Bundeskriminalamtgesetzes eingegangen. Diese beiden Entwürfe sind offenbar nicht aufeinander abgestimmt. So enthält der Entwurf für das BKAG eine eigene – höchst unvollständige – Vorschrift

zur Datenschutzkontrolle. Die Verweise bzw. die Verknüpfungen zwischen beiden Entwürfen sind höchst unklar.

Nicht nachvollziehbar ist aber, weshalb der Entwurf zum BKAG in hohem Maße ambitioniert sehr ausführliche Vorschriften zum behördlichen Datenschutzbeauftragten enthält, nicht aber gleichzeitig mit dem vorliegenden Entwurf die Datenschutzaufsicht gestärkt wird. So sehr die Stärkung des behördlichen Datenschutzbeauftragten zu begrüßen ist, desto mehr stellt sich aber auch die Frage, aus welchen Gründen beide Entwürfe auf eine so ambitionierte Stärkung der Befugnisse der Bundesbeauftragten für den Datenschutz verzichten.

c. Gerichtliche Verfahren

Der Entwurf sieht insbesondere keine Möglichkeit der BfDI vor, ein gerichtliches Verfahren bei Verstößen gegen datenschutzrechtliche Vorschriften zu betreiben. Ebenfalls kann sie sich nicht in anderer Weise an gerichtlichen Verfahren beteiligen (z. B. amicus curiae). Artikel 47 Absatz 5 der JI-Richtlinie und Artikel 58 Absatz 5 der DSGVO werden also nicht umgesetzt. Im Übrigen wird auf die Ausführungen zu § 28 Bezug genommen.

d. Verhältnis zu Bundesregierung und Bundestag (Absatz 2 Sätze 5 bis 7)

Absatz 2 betrifft nach seinem Wortlaut ausschließlich die JI-Richtlinie. Dies ist mit Blick auf die Sätze 1 bis 4 nachvollziehbar. Für die Sätze 5 bis 7 gibt es hingegen keine Entsprechung im Anwendungsbereich der DSGVO. Dies würde bedeuten, dass sich die BfDI in diesem Bereich bspw. nicht an den Deutschen Bundestag wenden könnte. Diese Folge wäre nicht hinnehmbar und ist – falls sie möglicherweise gar nicht beabsichtigt ist – wiederum der unübersichtlichen Systematik des Entwurfs geschuldet. H. E. ist es im Rahmen von Art. 58 Abs. 6 DSGVO auch in diesem Bereich möglich.

Die Formulierung in Absatz 2 Satz 5 – dass die BfDI sich nur im Rahmen ihrer Zuständigkeit mit Stellungnahmen an den Bundestag richten kann – ist zu eng. Dies könnte man so interpretieren, dass die BfDI nicht zu allgemeinen datenschutzpolitisch bedeutsamen Themen Stellung nehmen kann, wenn und soweit die handelnden Akteure nicht ihrer Zuständigkeit unterfallen. Dies ist auch notwendig, um bei allen Themen bundespolitischer Bedeutung eine parlamentarische Befassung zu ermöglichen. § 26 Abs. 2 BDSG enthält eine solche Beschränkung auch nicht.

Nach Absatz 2 Satz 6 können die Bundesregierung und der Deutsche Bundestag die BfDI auffordern, Gutachten zu erstellen oder Berichte zu erstatten. Dies sollte hinsichtlich der Bundesregierung wegen des damit verbundenen Eingriffs in die Unabhängigkeit der BfDI künftig nicht mehr möglich sein.. Daher sollten die Worte „oder der Bundesregierung“ gestrichen werden.

e. Datenschutzrechtliche Befugnisse gegenüber den Nachrichtendienste (Absatz 3)

In Absatz 3 ist für Datenverarbeitungen außerhalb des unionsrechtlichen Anwendungsbereichs nach § 1 Abs. 3 (im Entwurf fälschlicherweise Absatz 2) weiterhin lediglich das Beanstandungsrecht vorgesehen.

Dies ist zur verfassungskonformen Ausgestaltung der Kompensationsfunktion der unabhängigen Datenschutzkontrolle nicht mehr ausreichend. Vielmehr muss die BfDI gerade im Bereich der Nachrichtendienste effektive Mittel zur Durchsetzung des Datenschutzrechts an der Hand haben. Insofern müssten ihr zumindest die in Absatz 2 Sätze 3 und 4 im Bereich der JI-Richtlinie bestehenden Möglichkeiten gegeben sein. Darüber hinaus bedarf es auch in diesem Bereich des Rechts, dass sich die BfDI jederzeit an den Deutschen Bundestag wenden kann.

Besonders bei den Nachrichtendiensten ist es verfassungsrechtlich geboten, eine Möglichkeit der BfDI gesetzlich vorzusehen, rechtswidrige Datenverarbeitungen notfalls auch zu unterbinden. Die Datenschutzkontrolle ersetzt hier in weiten Bereichen den fehlenden individuellen Rechtsschutz und hat deshalb eine Kompensationsfunk-

tion (BVerfG NJW 2016, 1781, Abs. Nr. 141; NJW 2013, 1499, Abs. Nr. 217). Es wäre ein erheblicher Wertungswiderspruch, wenn die Datenschutzkontrolle in anderen Bereichen stärker ausgestaltet wäre als hier. Genau ein solcher ist mit dem vorgelegten Gesetzentwurf aber offenbar beabsichtigt. Der BfDI soll mit dem neuen Entwurf sogar die Befugnis genommen werden, sich unaufgefordert an den Bundestag und seine Kontrollgremien zu wenden. Mangels einer Untersagungsbefugnis oder der ebenfalls nicht vorgesehenen Möglichkeit ein Gericht einzuschalten, kann dies jedoch die einzige Möglichkeit sein, die Ergebnisse der Datenschutzkontrolle durchzusetzen. Ein Bereich der Exekutive, der keinen hinreichend wirksamen Gegenpol durch eine unabhängige Stelle hat, ist nicht nur in grundrechtlicher Hinsicht problematisch, sondern auch im Hinblick auf den Grundsatz der Gewaltenteilung.

Im Übrigen wird auf die obigen Ausführungen zu den Verfahrenssicherungen (s. o. 2.) Bezug genommen.

f. Aufsichtsverfahren (Absatz 6)

In Absatz 6 Satz 1 wird festgelegt, dass die BfDI bei der Feststellung von Verstößen die in den Ziffern 1. bis 3. aufgeführten Stellen Gelegenheit zur Stellungnahme innerhalb einer von der BfDI festzusetzenden Frist gibt, bevor sie ihre Befugnisse nach Art. 58 Abs. 2 DSGVO bzw. nach Absatz 2 Sätze 3 und 4 ausüben kann.

Diese Verfahrensvorschrift ist in der vorliegenden Form nicht akzeptabel. Sie würde die Ausübung der Abhilfebefugnisse des Art. 58 Abs. 2 DSGVO bzw. nach Absatz 2 Sätze 3 und 4 an von der BfDI nicht beeinflussbare Faktoren knüpfen. Mit dieser Regelung wird die Ausübung der Befugnisse unter zeitlich schwer zu kalkulierende Voraussetzungen gestellt. Unklar wären auch die Rechtsfolgen einer nicht oder nicht fristgerecht eingegangenen Stellungnahme. Zudem sind in dem Vorschlag keine Möglichkeiten enthalten, in Eil- oder Wiederholungsfällen unmittelbar von den Abhilfebefugnissen des Art. 58 Abs. 2 DSGVO bzw. des Absatzes 2 Sätze 3 und 4 Gebrauch machen zu können.

Der Vorschlag verstößt h. E. auch gegen die DSGVO, da Art. 58 Abs. 2 DSGVO unmittelbar geltendes Recht ist und keine weiteren Voraussetzungen für die Ausübung der Befugnisse enthält. Die Verpflichtung, vor Ausübung der Befugnisse immer erst eine Stellungnahme einzuholen, geht auch deutlich über die in Art. 58 Abs. 4 DSGVO genannten ordnungsgemäßen Verfahren hinaus.

Nach der Begründung soll die Regelung lediglich sicherstellen, dass die öffentlichen Stellen des Bundes gerade wegen der sehr weitreichenden Befugnisse der BfDI ihre verfahrensmäßigen Rechte im Sinne eines rechtlichen Gehörs wahren können.

Diese berechtigten Verfahrensinteressen der der Aufsicht der BfDI unterliegenden Behörden sind h. E. grundsätzlich nachvollziehbar. Insbesondere würde für die Ausübung der Mehrzahl der Befugnisse durch die Aufsichtsbehörden im nichtöffentlichen Bereich unstreitig überwiegend § 28 VwVfG gelten, da es sich insoweit um Verwaltungsakte handeln dürfte.

Allerdings geht die hier vorgeschlagene Regelung zu Lasten der BfDI deutlich über § 28 VwVfG hinaus und ist zu undifferenziert:

- Die Gelegenheit zur Stellungnahme darf nur für diejenigen Befugnisse des Art. 58 Abs. 2 DSGVO vorgesehen werden, die den Charakter eines Verwaltungsaktes haben. Das sind die in Art. 58 Abs. 2 lit. c), d), e) f), g) und j) DSGVO genannten Befugnisse (die Befugnisse in Art. 58 Abs. 2 lit. h) und i) DSGVO nur insoweit, als sie für den öffentlichen Bereich überhaupt relevant sind). Hinsichtlich der Befugnisse des Art. 58 Abs. 2 lit. a) und b) DSGVO bedarf es hingegen keiner vorherigen Anhörung; sie entsprechen weitgehend dem bisherigen Beanstandungsrecht.
- Es muss zwingend dem § 28 Abs. 2 und 3 VwVfG vergleichbare Ausnahmen von der Anhörungspflicht geben, um insbesondere in Eilfällen oder bei zwingendem öffentlichen Interesse eine sofortige Anwendung der Befugnisse sicherzustellen (z. B. bei wiederholten Verstößen).

Es sollte schließlich klargestellt werden, dass die in Absatz 6 normierte Anhörungspflicht anzuhören, lediglich für die in diesem Absatz genannten Stellen gilt und deren Aufzählung damit als abschließend betrachtet werden kann. Andernfalls müsste zu-

mindest klargestellt werden, dass der Absatz nicht anwendbar ist, soweit die BfDI als Aufsichtsbehörde im nicht-öffentlichen Bereich entsprechend tätig wird. Hier bedarf es auch rein rechtlich eines derartigen Vorverfahrens nicht, da hoheitliche Maßnahmen in der Regel in der Form von Verwaltungsakten erlassen werden und somit die allgemeinen Voraussetzungen des VwVfG greifen (insb. § 28 VwVfG).

24. Zu § 27 ABDSG-E

In Absatz 1 wird angeregt, den Punkt durch ein Komma zu ersetzen und die Worte *„soweit nicht die oder der Bundesbeauftragte zuständig ist“* anzufügen. Dies sollte jedenfalls dann gelten, wenn die Zuständigkeit im Post- und TK-Bereich ebenfalls im BDSG-Ablösegesetz geregelt wird.

25. Zu § 28 ABDSG-E

Die Einrichtung des Klagerechtes für Datenschutzbehörden in § 28 ABDSG-E dient der Umsetzung der Vorgaben des EuGH im Schrems-Urteil in nationales Recht. Ich begrüße daher, dass den wiederholten Forderungen von mir und den Landesdatenschutzbeauftragten nach einem solchen Klagerecht nunmehr entsprochen wird.

Gleichwohl halte ich die Beschränkung des Anwendungsbereiches von § 28 ABDSG-E für zu eng gefasst. Die im Lichte von Artikel 58 Abs. 5 DSGVO und Art. 47 Abs. 5 JI-RL eingeräumte Möglichkeit einer weitergehenden Regelung sollte ausgeschöpft werden.

So sollten nicht nur Angemessenheitsentscheidungen nach Artikel 45 DSGVO, sondern auch andere Rechtsakte der Kommission wie bspw. Standardvertragsklauseln – ein Instrument nach Artikel 46 DS-GVO – von dem Klagerecht erfasst sein. Gleiches gilt für andere abstrakt-generelle Regelungen unabhängig davon, ob diese von der Europäischen Kommission oder vom nationalen Gesetzgeber erlassen werden.

Durch die Verwendung des allgemeinen Begriffes „Verstöße“ in den 58 Abs. 5 DS-GVO und Art. 47 Abs. 5 JI-RL kommt der Wunsch des europäischen Verordnungs- bzw. Richtliniengebers zum Ausdruck, für möglichst viele Maßnahmen den Rechtsweg zu eröffnen. Dies würde dem Ziel dienen, auch für andere Rechtsakte einen schnellen Weg zum EuGH zu eröffnen, der seinerseits zügig für eine unionsweit einheitliche Rechtsanwendung sorgen kann.

Von Vorteil wäre in diesem Zusammenhang auch, dass viele Rechtsfragen auf diesem Wege abstrakt geklärt werden könnten. In diesem Sinne rege ich den Verzicht auf das Vorliegen einer Beschwerde von Betroffenen an, um erst dadurch den Rechtsweg eröffnen zu können.

Die Datenschutzbehörden sollten also nicht auf das (zufällige) Vorliegen einer Beschwerde oder eines konkreten Sachverhaltes angewiesen sein, um dem EuGH über das BVerwG einen Rechtsakt zur Prüfung vorzulegen. Das Vorliegen einer Beschwerde oder das Bekanntwerden eines Sachverhaltes kann auf vollkommen zufällige Umstände zurückzuführen sein. Sofern die Datenschutzbehörden nur in diesen Fällen klageberechtigt wären, müssten sie das Klageverfahren mglw. zu Lasten des Betroffenen oder eines Unternehmens führen, obwohl eigentlich die abstrakt-generelle Regelung selbst überprüft werden soll und kein Fehlverhalten der beteiligten Stellen vorliegt. Dieses sachwidrige und zufallsgetriebene Verfahren sollte daher zugunsten einer rein abstrakten Überprüfungsmöglichkeit von Rechtsnormen aufgegeben werden.

26. Zu § 29 ABDSG-E

a. Aufgabenzuweisung (Absatz 1)

Die in Absatz 1 grundsätzlich festgelegte Zuweisung der Aufgabe des gemeinsamen Vertreters nach Art. 68 Abs. 4 DSGVO und der zentralen Anlaufstelle nach EG 119 der DSGVO an die BfDI ist zu begrüßen. Die in der Begründung dafür genannten Gründe werden ausdrücklich unterstützt.

Die Stellung des Landesvertreters als Stellvertreter i. S: v. Art. 68 Abs. 3 DSGVO begegnet ebenfalls keinen Einwänden. Allerdings müsste klargestellt werden, dass die Abwesenheitsvertretung (=Stellvertretung) für die BfDI durch Mitarbeiter der BfDI in Fällen außerhalb der ausschließlichen Länderzuständigkeit möglich ist. Dem Wortlaut nach könnte § 29 Abs. 1 so verstanden werden, als ob dieser Stellvertreter auch in Angelegenheiten, die nicht in der Federführung der Länder liegen, bei Verhinderung der BfDI die Verhandlungen im EDSA führen soll, was nicht sachgerecht erscheint. Die Verhandlungsführung für Angelegenheiten, die nicht in den ausschließlichen Zuständigkeitsbereich der Länder fallen, sollte bei Verhinderung der BfDI bei deren Leitenden Beamten oder einem sonstigen Vertreter aus der Dienststelle der BfDI liegen. Die notwendige Klarstellung könnte in der Gesetzesbegründung erfolgen.

Absatz 1 Satz 2 würde eine Wiederwahl des gemeinsamen Vertreters bzw. des Stellvertreters erforderlich machen, wenn deren verbleibende nationale Amtszeit kürzer ist als 5 Jahre, die Amtszeit der BfDI oder des Landesvertreters während der fünfjährigen Vertreterfunktion im Europäischen Datenschutzausschuss (EDSA) jedoch verlängert wird. Vorzuziehen wäre h. E. eine Formulierung, die die Funktion im EDSA an die tatsächliche Beendigung des nationalen Amtes knüpft, z.B.
"Die Wahl erfolgt für fünf Jahre. Mit einem früheren Ausscheiden aus dem Amt als Leiterin der Leiter der nationalen Aufsichtsbehörde endet auch die Funktion als Gemeinsamer Vertreter bzw. Stellvertreter im EDSA."

b. Zuständigkeitsübertragung auf den Landesvertreter (Absatz 2)

Der Absatz regelt drei Fallvarianten, in denen die BfDI dem Landesvertreter die Verhandlungsführung und das Stimmrecht im EDSA übertragen muss. Dies ist neben der ausschließlichen Gesetzgebungszuständigkeit der Länder und der Einrichtung von Landesbehörden auch „das Verfahren von Landesbehörden".

Hier ist nicht hinreichend klar, was mit „Verfahren" in diesem Sinne gemeint ist. Die Begründung (S. 64) führt hier leider nicht zu mehr Klarheit. Sie spricht hier von der „sachlichen Alleinzuständigkeit der Länderaufsichtsbehörden". Der Gesetzeswortlaut

in Absatz 2 spricht weder von den Aufsichtsbehörden i. S. v. § 27 ABDSG-E noch von deren Zuständigkeit, sondern vom Verfahren von Landesbehörden. BfDI legt der Formulierung des Gesetzestextes das Verständnis zugrunde, dass mit „Verfahren von Landesbehörden“ nicht dasjenige vor den Aufsichtsbehörden i. S: v. § 27 ABDSG-E gemeint ist, sondern allgemein das Verfahren von (anderen) Landesbehörden, d. h. der öffentliche Bereich der Länder. Um dies deutlich zu machen und jeden Zweifel auszuschließen, sollte die Begründung eindeutig und präzise klarstellen, dass sich „Verfahren von Landesbehörden“ ausschließlich auf solche außerhalb der Datenschutzaufsichtsbehörden bezieht und deren Verfahren (d. h. der nicht-öffentliche Bereich) hier nicht gemeint sind.

27. Zu § 30 ABDSG-E

a. Absatz 1

Es ist unklar, in welchen Fällen es eines "gemeinsamen Standpunktes" von BfDI und LfD bedarf. Der Terminus wird in der DSGVO selbst nicht verwandt. Die DSGVO bestimmt in Art. 51 Absatz 3 lediglich, dass auf nationaler Ebene ein Verfahren einzuführen ist, mit dem sichergestellt wird, dass "die Regeln für das Kohärenzverfahren" von allen nationalen DS-Behörden eingehalten werden.

Mit anderen Worten verlangt die DSGVO eine abgestimmte Vorgehensweise der Datenschutzbehörden für Sachverhalte, die dem Kohärenz- und dem ihm vorgeschalteten Verfahren der Zusammenarbeit unterfallen. Eine darüber hinausgehende, generelle Verpflichtung der Datenschutzbehörden von Bund und Ländern zur Festlegung "gemeinsamer Standpunkte" auch in anderen Fällen verlangt die DSGVO expressis verbis nicht.

Bei den übrigen eher informellen Aufgaben des EDSA bedarf es h. E. auch keines derart formalisierten Verfahrens für die gemeinsame Positionierung der Datenschutzbehörden. Der Entwurf erscheint in diesem Punkt präzisierungsbedürftig, da anderenfalls eine Pflicht zur Herstellung eines "gemeinsamen Standpunktes" zwischen BfDI und LfD zu allen erdenklichen Themen und Sachverhalten mit Bezug zur DSGVO auch außerhalb des Zusammenarbeits- und des Kohärenzverfahrens abge-

leitet werden könnte, der in der Praxis zu einem massiven Koordinierungsaufwand für die zentrale Anlaufstelle führen kann. Die Vorbereitung der Zusammenkünfte des EDSA wäre äußerst aufwändig und würde dem gemeinsamen Vertreter und dem anwesenden Landesvertreter die notwendige Flexibilität erheblich beschneiden. Gerade in diesen Angelegenheiten – die denen der heutigen Art-29-Gruppe sehr ähneln – hat sich die bislang geübte Praxis einer eher informellen Meinungsbildung innerhalb der deutschen Datenschutzbehörden bewährt.

Das Verfahren zur Festlegung eines gemeinsamen Standpunktes sollte deshalb auf die unabdingbar notwendigen Fälle, d. h. das Kohärenz- und das vorgeschaltete Kooperationsverfahren beschränkt werden.

b. Zum Verfahren (Absatz 2)

In Absatz 2 Satz 4 ist festgelegt, dass die Aufsichtsbehörden mit einfacher Mehrheit einen gemeinsamen Standpunkt beschließen können. Diese Möglichkeit besteht nach dem Wortlaut offensichtlich für alle Fallkonstellationen, in denen ein gemeinsamer Standpunkt herzustellen ist. Es würde also auch dann eine Mehrheitsentscheidung möglich sein, wenn eine ausschließliche Kompetenz der BfDI – etwa im Post- oder Telekommunikationsbereich – besteht. Dies erscheint in keiner Weise sachgerecht.

Die BfDI könnte daher auch in solchen Angelegenheiten regelmäßig überstimmt werden, in denen sie die alleinige Zuständigkeit hat. Die in der Begründung angesprochene Möglichkeit, dass sich die LfD in diesen Fällen der Stimme enthalten können ist weltfremd.

Es ist daher in Absatz 2 zusätzlich zu regeln, dass in den Fällen der Alleinzuständigkeit der BfDI der gemeinsame Standpunkt auch allein von dieser festgelegt wird.

Wie unter a) dargestellt, hält BfDI im Übrigen ein Verfahren der Abstimmung mit einfacher Mehrheit nur dann für akzeptabel, wenn die Fälle, für welche ein gemeinsamer Standpunkt erforderlich ist, auf das Kooperations- und Kohärenzverfahren be-

schränkt werden, insbesondere dann, wenn eine Landesdatenschutzbehörde als federführende Behörde i. S. d. DSGVO zu betrachten ist oder es sich im Übrigen um einen Sachverhalt handelt, der die ausschließliche Gesetzgebungskompetenz der Länder betrifft.

28. Zu § 31 ABDSG-E

In Absatz 1 Satz 2 muss es Artikel 4 Nummer 16 (nicht Artikel 16 Nummer 16) heißen.

In Absatz 1 Satz 3 muss – wie auch in der Begründung dargestellt – der Verweis richtigerweise auf § 30 Abs. 2 gehen.

29. Zu § 32 ABDSG-E

Die Formulierung "diese Verordnung" in Absatz 4 Buchst. b ist zu Ändern in „die Verordnung (EU) 2016/679“.

30. Zu § 34 ABDSG-E

§ 34 Absatz 1 ABDSG-E regelt die Rechtmäßigkeit der Verarbeitung und Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken auch ohne Einwilligung des Betroffenen. Nach gegenwärtiger nationaler Rechtslage wird diese Fallgestaltung in § 13 Absatz 2 Nummer 8 BDSG und in § 14 Absatz 5 Nummer 2 BDSG geregelt. Laut Gesetzesbegründung ist die Vorschrift an den Vorgaben von Artikel 9 Absatz 2 Buchstabe j) DSGVO zu messen. Außerdem unterliegt die Verarbeitung zu Forschungszwecken den in Artikel 89 Absatz 1 DSGVO vorgesehenen „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person“.

a. Interessenabwägung (Absatz 1)

Abweichend von § 14 Absatz 5 Nummer 2 BDSG lässt § 34 Absatz 1 ABDSG-E für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken bereits das erheblich überwiegende "wissenschaftliche" Interesse genügen, wie es u. a. für die Weiterverarbeitung nicht sensibler personenbezogener Daten nach § 14 Absatz 2 Nummer 9 BDSG vorausgesetzt wird. Ein Grund für eine solche Abschwächung ist nicht zu erkennen. Daher sollte entsprechend § 14 Absatz 5 Nummer 2 BDSG auch in § 34 Absatz 1 ABDSG-E ein (insoweit gesteigertes) "öffentliches" Interesse für die Verarbeitung der besonderen Kategorien personenbezogener Daten vorausgesetzt werden.

b. Sicherungsmaßnahmen

Nach Artikel 9 Absatz 2 Buchstabe j) DSGVO muss die Verarbeitung und Weiterverarbeitung zu Forschungszwecken durch „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ z. B. auf der Grundlage des Rechts des Mitgliedsstaats abgesichert sein. Entsprechende Regelungen enthalten nach gegenwärtiger Rechtslage § 40 Absätze 2 und 3 BDSG. Die Vorgaben nach § 40 Absatz 2 BDSG, wonach die frühestmögliche Anonymisierung der Einzelangaben über persönliche oder sachliche Verhältnisse gefordert wird, werden im ABDSG nicht aufgegriffen. Auch fehlt in § 34 ABDSG-E eine den Vorgaben von § 40 Absatz 3 BDSG entsprechende Regelung für eine Veröffentlichung von Forschungsergebnissen. Diese ist nach § 40 Absatz 3 BDSG nur zulässig mit Einwilligung des Betroffenen bzw. mit Feststellung der Unerlässlichkeit (der Veröffentlichung) für den Fall der Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte. Auf eine Aufnahme der in § 40 Absätze 2 und 3 BDSG geregelten Vorgaben in § 34 ABDSG-E als Voraussetzungen für eine zulässige Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken kann aus datenschutzrechtlicher Sicht nicht verzichtet werden. § 34 ABDSG-E ist entsprechend zu ergänzen.

c. Technische und organisatorische Maßnahmen

§ 34 Absatz 1 ABDSG-E greift ebenfalls nicht die nach Artikel 89 Absatz 1 DS-GVO vorgeschriebenen "Garantien für Rechte und Freiheiten der betroffenen Person" in Gestalt „technischer und organisatorischer Maßnahmen" auf, mit denen insbesondere die Beachtung des Grundsatzes der Datenminimierung gewährleistet wird. So fehlt etwa die in Artikel 89 Absatz 1 DSGVO als Beispiel angesprochene Pseudonymisierung von personenbezogenen Daten. Auch die in § 40 Absätze 2 und 3 BDSG vorgesehenen Maßnahmen stellen nach hiesiger Auffassung „geeignete Garantien“ zur Wahrung der Betroffenenrechte im Sinne des Artikel 89 Absatz 1 DSGVO dar, die im ABDSG zu berücksichtigen sind. Da diese Garantien nicht nur für die Verarbeitung besonderer Kategorien personenbezogener Daten, sondern auch in Bezug auf nicht sensible personenbezogene Daten vorliegen müssen, ist das ABDSG hinsichtlich dieser Datenkategorie zu ergänzen.

d. Statistische Zwecke

a) § 34 Absatz 1 ABDSG-E regelt auch die Rechtmäßigkeit der Verarbeitung und Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu „statistischen Zwecken“. Die Datenerhebungen und -verarbeitungen zu statistischen Zwecken sind in Deutschland im Bundesstatistikgesetz (BStatG) und den Statistikgesetzen der Länder mit Rücksicht auf verfassungsrechtliche Vorgaben (Geheimhaltung statistischer Einzelangaben, Gebot der Abschottung der Datenverarbeitung zu statistischen Zwecken von Verwaltungsaufgaben) spezialgesetzlich geregelt. Darin sind besondere Vorkehrungen zum Schutz personenbezogener Daten (Anonymisierung, besondere Löschfristen, freiwillige und verpflichtende Befragungen, Trennungsgebot) festgeschrieben, die über die nach § 34 ABDSG-E vorgesehenen Vorgaben deutlich hinausgehen. Eine parallele Regelung der Verarbeitung personenbezogener Daten zu statistischen Zwecken im ABDSG und den Statistikgesetzen würde das in den letztgenannten verankerte und bewährte Schutzniveau zu Lasten der Betroffenen aufweichen. Nach Artikel 5 Absatz 1 und Artikel 6 Absatz 1 Buchstabe e) i. V. m. Absatz 2 und Absatz 3 DSGVO können bestehende spezifischere Bestimmungen in den Mitgliedsstaaten beibehalten werden, mit denen "eine rechtmäßig und nach Treu

und Glauben erfolgende Verarbeitung (personenbezogener Daten)" gewährleistet werden kann. Dies ist mit den Statistikgesetzen von Bund und Ländern der Fall.

Die Worte "oder zu statistischen Zwecken", "oder statistische Interesse" und "oder Statistikzweck" in der Überschrift und in Absatz 1 von § 34 ABDSG sollten daher gestrichen und ein aus der Umsetzung der DSGVO in nationales Recht folgender Regelungsbedarf in den Statistikgesetzen berücksichtigt werden.

e. Genetische, biometrische und Gesundheitsdaten

Die Möglichkeit von Artikel 9 Absatz 4 DSGVO, dass ein Mitgliedstaat zur Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten Regelungen treffen kann, wird bisher nicht genutzt. Deshalb sollte § 34 Absatz 1 ABDSG-E folgender Satz angefügt werden: *„Die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten ist nur zulässig, soweit der Betroffene eingewilligt hat oder soweit eine Rechtsvorschrift dies erlaubt.“* Systematisch wäre es auch denkbar, diese Regelung in § 5 ABDSG-E aufzunehmen.

f. Betroffenenrechte bei statistischen Zwecken (Absatz 2)

§ 34 Absatz 2 ABDSG-E regelt einen Anpassungsbedarf für die individuellen Rechte auf Auskunft und Berichtigung nach Artikel 15 und 16 DSGVO für die Durchführung von Bundesstatistiken. In Konsequenz zu den oben unter d) angeführten Argumenten sollte diese Regelung der entsprechenden bereichsspezifischen Vorschrift des BStatG vorbehalten bleiben. § 34 Absatz 2 ABDSG-E ist daher zu streichen.

31. Zu § 36 ABDSG-E

Der Arbeitshinweis, es handele sich um „ex § 39 BDSG“ ist irreführend, weil die Regelung einen neuen Gehalt aufweist. Während § 39 BDSG eine besondere Zweckbindung regelt, schränkt § 36 ABDSG-E die Rechte der Betroffenen ein.

Die geplante Regelung ist zu unbestimmt, weil sie die Betroffenenrechte insoweit einschränkt, „als dies erforderlich und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen“. Nach welchen Kriterien aber diese Abwägung zu treffen ist, wann welches Recht überwiegt, „regelt“ der Entwurf aber nicht. Damit lässt er die nach Artikel 23 DSGVO zu regelnden Fragen offen.

Artikel 90 EU-DSGVO sieht zudem keine Berechtigung vor, die Kontrollbefugnisse der Datenschutzaufsichtsbehörden in der vorgesehenen Weise zu beschränken, sondern lediglich ein Recht, Regelungen zu treffen, „soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen“. Die vorgesehene Regelung fällt weit hinter die seit Jahrzehnten bewährte Regelung des § 24 Absatz 2 Nr. 2 BDSG zurück. Der Kontrolle der BfDI (und auch der Aufsichtsbehörden) könnte zukünftig stets entgegen gehalten werden, dass die Daten einem Berufsgeheimnis unterliegen, obwohl dies nur in wenigen Fällen in der Vergangenheit problematisch war und gerechtfertigt erschien. Eine von der EU-DSGVO gewollte und vorgeschriebene Kontrolle gegenüber öffentlichen Stellen oder im Gesundheitsbereich oder bei anderen Berufsgeheimnisträgern wäre demnach unmöglich.

Hinzukommt, dass durch den Verweis auf Art. 58 Abs. 1 lit. f) DSGVO davon auszugehen ist, dass den Aufsichtsbehörden bereits der Zutritt zu den Räumen verwehrt wird und ihnen daher nicht einmal eine Kontrolle etwa der technischen und organisatorischen Maßnahmen ermöglicht wird.

Artikel 90 EU-DSGVO dürfte allenfalls dazu führen, etwa strafrechtliche Normen einzuführen, wie sie in Deutschland bereits durch § 203 Absatz 2a StGB vorhanden ist. Es ist geradezu widersinnig, das Vorhandensein von Berufsgeheimnissen zu Lasten der betroffenen Bürger dazu zu nutzen, eine effektive Kontrolle durch die Datenschutzaufsichtsbehörden auszuhebeln.

Zweifelhaft ist auch, ob das „Berufsgeheimnis“ hinreichend konkret eingegrenzt ist. Begriffliche Unschärfen sind bei § 39 BDSG insoweit unschädlich, weil dieser mit der Verschärfung der Zweckbindung die Rechtsstellung des Betroffenen verbessert. Die

geplante Regelung verschlechtert dessen Rechtsstellung hingegen. Deshalb ist das Berufsgeheimnis genauer zu umschreiben, z.B. durch ein Zitat des § 203 Absatz 1 StGB. Es kann zwar gerechtfertigt sein, die Betroffenenrechte gerade im Hinblick auf das Berufsgeheimnis einzuschränken. Dies kann zum Beispiel der Fall sein bei einem Facharzt der Psychiatrie, der auch Daten zu Angehörigen des Patienten in die Patientenakte aufgenommen hat. Hingegen wird dies in der Regel nicht der Fall sein bei einer Datenverarbeitung für wissenschaftliche Zwecke, wenn der davon Betroffene Auskunft über die zu ihm gespeicherten Daten erhalten möchte.

Insgesamt ist § 36 daher dringend zu überarbeiten. Die Betroffenenrechte müssen ebenso effektiv gewährleistet sein wie auch eine wirksame Kontrolle durch die BfDI und die Aufsichtsbehörden. Der notwendige Ausgleich zwischen den Geheimhaltungsbestimmungen und den Betroffenenrechten bzw. den Kontrollrechten kann nicht den Berufsgeheimnisträgern überlassen bleiben, sondern sowohl Art. 23 als auch Art. 90 DSGVO verlangen, dass der nationale Gesetzgeber diese Abwägung konkret und spezifisch vornimmt.

32. Zu § 37 ABDSG-E

In Absatz 1 wird die Verarbeitung durch Videoüberwachung erhobener personenbezogener Daten durch öffentliche Stellen (zu ergänzen: des Bundes) geregelt. Die Voraussetzungen entsprechen insoweit § 6b Abs. 1 und Abs. 3 Satz 1 BDSG.

Nicht geregelt wird allerdings die Erhebung der Daten, was insbesondere auch dann relevant wird, wenn eine Beobachtung ohne Speicherung erfolgt. Auch dies ist ein Eingriff in das Recht auf informationelle Selbstbestimmung und sollte geregelt werden, wie dies in § 6b Abs. 1 BDSG der Fall ist.

Darüber hinaus fehlen Regelungen zur Weiterverarbeitung gespeicherter Daten zu anderen Zwecken nach dem Vorbild des § 6b Abs. 3 Satz 2 BDSG. Solche einschränkenden Regelungen sind jedoch notwendig, da anderenfalls die (zu) weit gefassten Bestimmungen des § 6 ABDSG-E gelten würden. Eine dem § 6b Abs. 3 Satz 2 BDSG entsprechende Regelung ist daher aufzunehmen.

33. Zu den §§ 38, 39 ABDSG-E

Die Übernahme der Vorschriften der §§ 28a, 28b BDSG entspricht einem mehrheitlichen Wunsch der AG Auskunfteien des Düsseldorfer Kreises, dem sich die BfDI nicht entgegengestellt hat.

Es bestehen jedoch erhebliche Zweifel, ob die DSGVO überhaupt einen Regelungsspielraum bietet, diese Vorschriften weiterhin national zu regeln. Die Begründung hebt insoweit auf Art. 6 Abs. 4 DSGVO ab. Dieser enthält jedoch keine Befugnis für den nationalen Gesetzgeber, eigene Rechtsvorschriften zur Änderung zu nicht vereinbaren Zwecken zu erlassen. Auf die Ausführungen zu § 6 (o., Ziff. 7.) wird insoweit Bezug genommen.

Inhaltlich sollten die bisherigen §§ 28a, 28b BDSG jedoch auch nicht wortgleich übernommen, sondern die Erfahrungen der letzten 7 Jahre seit Schaffung der Vorschriften berücksichtigt werden. Dies betrifft in erster Linie das Scoring, bei dem erhebliche datenschutzrechtliche Defizite, wie beispielsweise bei der zu weitgehenden Nutzung des Geoscoring bestehen. Zudem fehlt es in der DSGVO und im ABDSG-E auch an adäquaten Auskunftsregelungen, wobei insoweit die geltenden Regelungen in § 34 Abs. 2 BDSG nicht ausreichen.

Im Ergebnis erscheint die vorgeschlagene partielle Übernahme der §§ 28a, 28b BDSG nicht als Ideallösung. BfDI hält es für notwendig, angesichts der sehr fragwürdigen Regelungsbefugnis und der inhaltlichen Defizite entweder auf spezifische Regelungen derzeit zu verzichten oder eine datenschutzrechtlich zufriedenstellende Lösung unter Berücksichtigung der Erfahrungen der Aufsichtsbehörden zu finden.

34. Zu § 41 ABDSG-E

Die Regelungen zum gerichtlichen Rechtsschutz gegen Maßnahmen der Aufsichtsbehörden – auch im öffentlichen Bereich – sind aus hiesiger Sicht im Wesentlichen zufriedenstellend.

In Absatz 7 wird jedoch 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 bspw. die Beseitigung einer Sicherheitslücke in einem IT-System einer Behörde an, darf eine Klage der Behörde nicht dazu führen, dass wegen der aufschiebenden Wirkung dieser Zustand zwei oder mehr Jahre nicht beseitigt wird.

Zwar ist es richtig, dass sich BfDI und Behörden nicht in einem Subordinationsverhältnis gegenüberstehen. Dies gilt aber für das gesamte Klageverfahren und kann deshalb bei der sofortigen Vollziehung auch nicht als Argument herangezogen werden, zumal sich der Zusammenhang nicht erschließt.

Würde eine sofortige Vollziehung angeordnet werden können, würden den Behörden hier auch keine Rechte genommen. Wie jeder andere Adressat der aufsichtsbehördlichen Maßnahmen hätten sie die Möglichkeit, gem. § 80 Abs. 5 VwGO die Wiederherstellung der aufschiebenden Wirkung zu beantragen.

Ob der in der Begründung als Alternative angesprochene Antrag auf einstweilige Anordnung statthaft wäre, ist fraglich. Dieser ist ein Rechtsschutzinstrument gegen (drohende) Maßnahmen von Behörden, ermöglicht es aber den Behörden nicht, ihrerseits Aufsichtsbefugnisse im Eilfall mit Hilfe des Gerichts durchzusetzen.

Vor diesem Hintergrund sollte Absatz 7 gestrichen werden.

35. Zu § 60 ABDSG-E

Die Regelung ist dringend überarbeitungsbedürftig.

- *Nachrichtendienste:* Die Regelung beschränkt sich auf den Anwendungsbereich der JI-Richtlinie. Gleichzeitig beschränkt sich § 42 auf den Bereich der DS-GVO. Damit sind rechtswidrige Datenverarbeitungen der Nachrichtendienste nicht mehr bußgeldbewehrt!

  Dies wird den verfassungsrechtlichen Vorgaben nicht gerecht. Eine verhältnismäßige Ausgestaltung der Vorschriften zur Datenverarbeitung setzt wirksame Sanktionen bei Rechtsverletzungen voraus (BVerfG NJW 2016, 1781, 1789, Abs. Nr. 139). „Würden auch schwere Verletzungen der Eingriffsvoraussetzungen im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, die Entfaltung der Persönlichkeit wirksam zu schützen."

  Bislang sind die §§ 43, 44 BDSG gemäß § 27 BVerfSchG anwendbar. Dass sollte so bleiben.

- Des Weiteren sollte die Verarbeitung *allgemein zugänglicher Daten* nicht vom Bußgeldtatbestand ausgeschlossen sein. Sie kann gerade im Bereich der Sicherheitsbehörden und der Nachrichtendienste als erheblicher Eingriff zu werten sein. Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann namentlich dann gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt (BVerfGE 120, 274, 345). Gerade im Bereich der Nachrichtendienste kann es dazu kommen, dass diese über mehrere Jahrzehnte Daten zu einer Person zusammentragen und dadurch ein umfassendes Persönlichkeitsdossier zur Verfügung haben. Das kann den Betroffenen auch dann erheblich belasten, wenn sich dies auf allgemein zugängliche Informationen beschränkt. Er muss dann da-

mit rechnen, dass alles von ihm geschriebene in nachrichtendienstlichen Datenbanken gespeichert und mit anderen – auch geheimen – Dateien abgeglichen und mit Analysesystemen ausgewertet wird. Das kann insbesondere beim Publizieren zu einer „Schere im Kopf“ führen (vgl. VG Köln, Urteil vom 20.01.2011 - 20 K 2331/08) und damit die Presse-, Rundfunk- und Meinungsfreiheit nachhaltig beeinflussen.

- Die *sachliche Zuständigkeit* ist zu hinterfragen. So müsste bei einem Verstoß gegen Absatz 1 Nummer 1 die betroffene Behördenleitung ein Bußgeldverfahren gegen sich selbst einleiten. Die Zuständigkeit sollte deshalb bei der BfDI liegen.

36. Zu § 61 ABDSG-E

Die Strafbarkeit wird gegenüber der jetzt geltenden Fassung des § 44 BDSG deutlich eingeschränkt.

Im Bereich der Nachrichtendienste existieren überhaupt keine datenschutzrechtlichen Strafvorschriften mehr.

Auch für den Bereich der Polizei- und Justizbehörden wird die rechtswidrige Verarbeitung in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, im Bereich der JI-Richtlinie nicht mehr strafbar sein. Die Vorschrift verweist nur auf § 60 Absatz 1 Nummer 3 und 4 ABDSG-E. Damit sind nur wenige Handlungen im Zusammenhang mit automatisierten Abrufverfahren strafbewehrt.

Der bisherige § 44 BDSG betrifft in ganz besonderer Weise die vom Bundesverfassungsgericht angesprochenen „schweren Verletzungen der Eingriffsvoraussetzungen“ polizeirechtlicher und nachrichtendienstlicher Vorschriften (BVerfG NJW 2016, 1781, 1789, Abs. Nr. 139, siehe oben). Dies betrifft darüber hinaus im Bereich der Nachrichtendienste einen Bereich, in dem die Betroffenen ohnehin eingeschränkte Rechtsschutzmöglichkeiten haben.

Zwar hat der Gesetzgeber einen weiten Gestaltungsspielraum. Die geplante überaus starke Einschränkung – bzw. bezogen auf die Nachrichtendienste: vollständige Aufhebung – der strafrechtlichen Sanktionsmöglichkeiten kann zur Unverhältnismäßigkeit der Vorschriften zur Datenverarbeitung als solcher führen. Sie kann damit die Verfassungsmäßigkeit weiter Teile der Polizei- und Nachrichtendienstgesetze in Frage stellen. Ein derartiges Risiko sollte der Gesetzgeber nicht in Kauf nehmen.

IV. Zu Artikel 2 – Änderung des Bundesverfassungsschutzgesetzes

1. Fehlende Regelung

Auslandsübermittlungen

Das Bundesverfassungsgericht hat die Voraussetzungen, unter denen eine Übermittlung von Daten aus heimlichen Überwachungseingriffen verfassungsrechtlich zulässig ist, umfangreich dargelegt (BVerfG NJW 2016, 1781, 1805, Abs. Nr. 323 ff.). Das betrifft ausnahmslos die mit nachrichtendienstlichen Mitteln erhobenen Daten des BfV.

Neben den bereits beschriebenen erheblichen allgemeinen Mängeln fordert die Vorschrift – anders als § 14 BKAG – keinerlei Schutzniveau des ausländischen Staates (vgl. dazu Bergemann, LD Kap. H Rn. 128). Die Übermittlung von Daten an das Ausland setzt danach eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen, sowie die Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland voraus (BVerfG NJW 2016, 1781, 1805, Abs. Nr. 329). Die regelmäßige datenschutzrechtliche Kontrolle ist gesetzlich festzuschreiben (Abs. Nr. 354).

All dies fehlt der derzeitigen gesetzlichen Regelung, die der Entwurf insoweit offenbar nicht ändern will.

2. Allgemein zum Begriff „Verarbeitung personenbezogener Daten“

Zur Ausweitung der Befugnisse durch die Verwendung des Begriffs „Verarbeitung“ anstatt „Erhebung, Verarbeitung und Nutzung“ wird zunächst auf das oben Gesagte verwiesen.

Wenn bspw. in § 8 Abs. 1 Satz 1 BVerfSchG die Befugnis zum Erheben, Verarbeitung und Nutzen durch die Befugnis zum Verarbeiten ersetzt wird, umfasst diese Befugnis nach § 3 Abs. 6 ABDSG nicht nur das Erheben oder die Verwendung, sondern u.a. auch das Verändern, die Offenlegung und Übermittlung, Verbreitung oder eine andere Form der Bereitstellung sowie den Abgleich oder die Verknüpfung. Zwar werden im weiteren Verlauf des Gesetzes spezielle Regelungen z.B. zur Übermittlung getroffen. Mit der weiten Begriffsdefinition signalisiert § 8 aber deutlich weitere Befugnisse als sie dem Bundesamt offenbar tatsächlich zustehen. Daher erscheint eine **Überarbeitung notwendig**. Sollte die Ausweitung der Befugnisse dagegen bewusst erfolgt sein, so ist sie aus Gründen der Verhältnismäßigkeit entschieden abzulehnen.

Im Übrigen erscheint die Überarbeitung auch notwendig hinsichtlich bislang nicht geänderter Paragrafen des BVerfSchG, wie bspw. solche Vorschriften, die den Begriff „nutzen“ beinhalten (z.B. § 11 oder § 14). Der Begriff des Nutzens findet in der JI-Richtlinie wie auch in § 3 ABDSG keine Grundlage mehr.

3. Änderungsbefehl Nr. 3.b) (§ 8b Abs. 8 Satz 2 Nr. 2 BVerfSchG)

Auch hier fehlt eine spezifische Gesetzesbegründung. Der Einschub des Wortes „erhobenen“ nach dem Wort „übermittelnden“ ist aber ebenfalls nicht mit den geänderten Begriffsdefinitionen erklärbar. Möglicherweise soll mit dem Einschub eine Klarstellung herbeigeführt werden, dies ist aber mangels Gesetzesbegründung nicht nachvollziehbar. Es versteht sich von selbst, dass man nur solche Daten übermitteln kann, die zuvor erhoben wurden. Korrekterweise müsste es dann wohl „erhobenen und gespeicherten“ heißen, denn die erhobenen Daten werden wohl immer auch gespeichert, jedenfalls dann, wenn sie später Gegenstand einer Anfrage nach § 8a sein können. Das BMI sollte um entsprechende Erläuterung gebeten werden.

4. Anpassungsbedarf in § 10 Abs. 1 Nr. 2 BVerfSchG

Nach Auffassung der BfDI muss bei dieser Gelegenheit auch eine **Anpassung des § 10 Abs. 1 Nr. 2 BVerfSchG erfolgen**. Da Nr. 2 im Gegensatz zu Nr. 1 nicht „tatsächliche Anhaltspunkte“ als Voraussetzung zur Verarbeitung personenbezogener Daten hat, schließt das Bundesamt daraus, dass solche für den Tatbestand von § 10 Abs. 1 Nr. 2 auch nicht erforderlich seien. Allerdings ist diese Vorschrift zwingend im Sinne von § 4 Abs. 1 Satz 3 zu lesen, wonach Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 das Vorliegen tatsächlicher Anhaltspunkte ist. Dies sollte in § 10 Abs. 1 Nr. 2 klargestellt werden.

5. Änderungsbefehl N. 5.b) (§ 13 Abs. 3 Sätze 5 und 6)

Auch diese Änderung betrifft nicht nur eine reine Folgeänderung aufgrund der Begriffsdefinitionen. Offenbar soll hier auch eine Klarstellung hinsichtlich des Umfangs einer Sperrung bzw. Einschränkung der Verarbeitung erfolgen. Dies wird **begrüßt**, da eine Sperrung/Einschränkung der Verarbeitung sich nur auf die entsprechenden personenbezogenen Daten beziehen kann und muss und nicht auf die gesamte Akte, wie der bisherige Wortlaut des § 13 Abs. 2 BVerfSchG vermuten ließ.

6. Änderungsbefehl Nr. 6 (§ 14a)

Mit dem neuen § 14a BVerfSchG bleibt der alte § 9 BDSG im Grundsatz erhalten, der der verantwortlichen Stelle die Pflicht zu entsprechenden technischen und organisatorischen Sicherungsmaßnahmen auferlegt. Dies wird begrüßt. Laut Begründung soll die bisherige Anlage zum BDSG für § 14a BVerfSchG auslegungs- und anwendungsrelevant sein. Nicht begründet wird allerdings, warum die Anlage nicht in der bisherigen oder in abgewandelter Form mit in das BVerfSchG übernommen wurde.

Die BfDI plädiert dafür, den Inhalt des bisherigen **Anlage zu § 9 BDSG** als Regelbeispiele in § 14a mitaufzunehmen. Außerdem sollte in Satz 1 nach den Worten „tech-

nischen und organisatorischen Maßnahmen“ die Worte **„nach dem jeweiligen Stand der Technik“** eingefügt werden.

Im Übrigen könnte man aufgrund der jetzigen Formulierung den Eindruck gewinnen, dass wirtschaftliche oder finanzielle Interessen im Zweifel den Vorrang vor den Grundrechten der Betroffenen haben. Gerade im Bereich der Nachrichtendienste spielt aber die Eingriffsintensität der Maßnahme und die Möglichkeit, entsprechende Maßnahmen durch die BfDI auch überprüfen zu können, eine elementare Rolle. Daher sollte über eine entsprechende Änderung des Gesetzeswortlaauts nachgedacht werden. Zumindest sollte aber in der Gesetzesbegründung klargestellt werden, dass eine Vollprotokollierung keine unverhältnismäßige Maßnahme darstellt, da sie nach den Vorgaben des Bundesverfassungsgerichts für eine effektive Datenschutzkontrolle notwendig ist (vgl. dazu auch 9.d))..

7. Zu Änderungsbefehl Nr. 8 (§ 22b Abs. 7 Sätze 1 und 2)

In § 22b Abs. 7 Sätze 1 und 2 BVerfSchG-neu wird klargestellt, dass das Bundesamt die Verantwortung für den Erlass von technischen und organisatorischen Maßnahmen im Sinne des § 14a in gemeinsamen Dateien mit ausländischen Nachrichtendiensten nur für die von ihm eigegebenen Daten und seine eigenen Abrufe hat.

Die BfDI wiederholt ihre **Bedenken** gegen den Inhalt dieser Norm, die ihre jetzige Gestalt durch das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 27.6.2016 (BGBl. I. S. 1786) erhalten hat. § 22b Abs. 7 gewährleistet die vom Bundesverfassungsgericht geforderte Datenschutzkontrolle nicht im ausreichenden Maße, da die **Kontrollkompetenz der BfDI** auf die vom BfV eingegebenen Daten sowie dessen Abrufe **beschränkt**. Die Kontrollkompetenz erstreckt sich nur auf Eingaben und Abrufe. Die analytische Nutzung der Daten, die ein deutlich höheres Eingriffsgewicht in Bezug auf das Grundrecht der informationellen Selbstbestimmung besitzt, ist dagegen von der Kontrolle ausgeschlossen. Um Wiederholungen zu vermeiden, wird auf die Stellungnahme der BfDI im Rahmen der Sachverständigen-Anhörung des Bundestags-Innenausschusses am 20.6.2016 verwiesen.

8. Änderungsbefehl Nr. 10 (§§ 26a, 26b)

Mit Nr. 10 wird § 26a in das BVerfSchG eingefügt, der § 21 und 24 Abs.1, 2 Satz 3 und Abs. 4 BDSG ersetzen und die Kontrollkompetenz der BfDI gegenüber dem Bundesamt festlegen soll.

Die Vorschrift **schränkt** geradezu erdrutschartig die bisherigen **Befugnisse und Sanktionsmöglichkeiten der BfDI ein**. Angesichts der Rechtsprechung des Bundesverfassungsgerichts zur Kompensationsfunktion der datenschutzrechtlichen Kontrolle ist dies nicht hinnehmbar und **verfassungswidrig**. Derartige Einschränkungen der Kontrollbefugnis wirken sich auf die Verhältnismäßigkeit der Befugnisse der Datenverarbeitung insgesamt aus.

a) Gemäß § 26 a Absatz 4 Satz 2 BVerfSchG-E soll die Anwendung des **§ 25 Absatz 2 ABDSG-E ausgeschlossen** werden. **Ausgeschlossen** wird damit die Möglichkeit der BfDI von sich aus **Stellungnahmen an den Deutschen Bundestag**, die **Bundesregierung**, sonstige Einrichtungen und Stellen sowie an die **Öffentlichkeit** richten. Sie **nimmt dem Deutschen Bundestag** die Möglichkeit, die **BfDI** mit Gutachten und Berichten **zu beauftragen** und sie zu ersuchen, Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nachzugehen. Damit werden nicht nur die Möglichkeiten der BfDI, sondern **auch die Rechte des Parlamentes eingeschränkt**. Im Übrigen wird auf die obigen Ausführungen zu § 25 ABDSG verwiesen.

   Die Betroffenen haben gegenüber Nachrichtendiensten nur höchst eingeschränkte Rechtsschutzmöglichkeiten. Dies ist insbesondere dadurch bedingt, dass die Auskunftsrechte der Betroffenen stärker eingeschränkt sind als in anderen Bereichen. Gleichzeitig verlangt das Bundesverwaltungsgericht vom Betroffenen, bei Feststellungsklagen gemäß § 43 Absatz 1 VwGO die konkrete Betroffenheit darzulegen. Das ist aber ohne die durch Auskunftsanträge zu erlangenden Informationen nicht möglich. Deshalb müssen die Kontroll- und Sanktionsmöglichkeiten der BfDI ausreichend ausgestaltet sein (BVerfG NJW 2013, 1499, 1515, Abs. Nr. 204 ff.; BVerfG NJW 2016, 1781, 1789, Abs. Nr. 140 f.).

Der Gesetzentwurf verzichtet auf Anordnungsbefugnisse der BfDI. Diese sind zwar auch bislang nicht vorgesehen. Dies wird jedoch – zumindest zum Teil – dadurch ausgeglichen, als sich die BfDI an die parlamentarischen Gremien wenden kann. Darüber hinaus kann sie im äußersten Fall in allgemeiner und abstrakter Form die Öffentlichkeit über Missstände informieren. Diese Möglichkeiten werden der BfDI genommen. Erhält das Parlament – z.B. über den Petitionsausschuss – derartige Hinweise, hat es keine Möglichkeit mehr, die BfDI in der Weise einzubeziehen, dass es mit einer Rückmeldung durch diese rechnen kann.

b) Anordnungsbefugnisse der BfDI und die Möglichkeit, diese gerichtliche anzustoßen, sind für den Bereich der Nachrichtendienste zwar nicht durch die JI-Richtlinie vorgegeben, da diese nicht unmittelbar anwendbar ist. Das Bundesverfassungsgericht hat allerdings gerade für diesen Bereich die Kompensationsfunktion der datenschutzrechtlichen Kontrolle hervorgehoben. Daher wäre es ein Wertungswiderspruch, wenn die BfDI gerade in dem Bereich, in dem ihre Kontrolle verfassungsrechtlich am stärksten gefordert ist, die schwächsten Befugnisse hätte.

c) § 26a Abs. 1 entspricht grds. § 21 BDSG. § 26a Abs. 2 Satz 1 entspricht § 24 Abs. 1 BDSG. § 26a Abs. 2 Satz 2 entspricht § 24 Abs. 2 Satz 3 BDSG. Damit fällt offenbar der Inhalt von § 24 Abs. 2 Sätze 1, 2 und 4 BDSG weg. Mit der jetzigen Formulierung **sollen** ausweislich der Begründung zum einen überlappende Kontrollzuständigkeiten von BfDI und G 10-Kommission und zum anderen **Kontrolllücken ausgeschlossen werden**.

Diesem Ziel wird die Regelung im Ergebnis **nicht gerecht**. Es ist richtig, dass divergierende Auffassungen über den Kontrollumfang der BfDI bei G 10-Maßnahmen bestehen, und dass es eine Doppelzuständigkeit nicht geben kann und sollte. Dies liegt auch in der Tat an der bisherigen Formulierung des § 24 Abs. 2 BDSG sowie § 15 Abs. 5 G 10. Die Kontrollbefugnis der G 10-Kommission erstreckt sich nach § 15 Abs. 5 Satz 2 G 10 auf die *gesamte Erhebung, Verarbeitung und Nutzung* (Erhebung und Nutzung sollen durch die Änderung wegfallen, vgl. dazu oben) der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes einschließlich der Entscheidung über die

Mitteilung an Betroffene. Diese Daten können dem Bundesamt als Grundlage beispielsweise für eine Ausschreibung im Schengener Informationssystem (SIS II) nach § 17 Abs. 3 BVerfSchG dienen. Ob die Voraussetzungen für eine Ausschreibung vorliegen, wird also mit einem G 10-Datum legitimiert. Maßnahmen nach § 17 Abs. 3 BVerfSchG unterliegen unzweifelhaft der Kontrollkompetenz der BfDI. Ob tatsächlich eine G 10-Erkenntnislage vorliegt (und ein Datum rechtlich zulässig als G 10-Datum gekennzeichnet wurde), kann die BfDI nach dieser Lesart des Gesetzes aber nicht prüfen, weil die Nutzung von G 10-Daten ausschließlich der G 10-Kommission unterliegt. Die G 10-Kommission wiederum ist aber als solches nicht kontrollbefugt für Maßnahmen nach § 17 Abs. 3 BVerfSchG. Würde die Formulierung so bleiben, wie sie bislang in § 24 BDSG, § 15 Abs. 5 G 10 besteht bzw. neu in § 26a BVerfSchG geregelt wird, würde sich an dem Bestehen einer Kontrolllücke nichts ändern.

Die Regelung in **§ 26a muss daher sinngemäß lauten**, dass die BfDI Daten aus G 10-Maßnahmen *insoweit* sehen und verwenden darf, wie sie für ihre Prüfung relevant sind. Eine Kenntnisnahme, Verifikation sowie Verwendung muss im Rahmen der Kontrollkompetenz der BfDI möglich sein. Diese ausdrückliche Regelung ist auch deshalb dringend erforderlich, weil sich bisherige Absprachen zur – teilweisen – Lösung des Problems nicht als hinreichend belastbar erwiesen haben.

d) Anders als im allgemeinen Datenschutzrecht können sich eine Betroffene oder ein Betroffener nur dann an die BfDI wenden, wenn er oder sie „der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch das Bundesamt für Verfassungsschutz in seinen Rechten verletzt worden zu sein.“ § 26 ABDSG verweist auf den entsprechenden Artikel der Richtlinie bzw. der Verordnung, welche beide eine Darlegung verlangen, dass „die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt“. Das Erfordernis, gegenüber dem Bundesamt eine potentielle Rechtsverletzung darzulegen, erscheint als eine größere Hürde zur Wahrnehmung der eigenen Rechte als im allgemeinen Datenschutzrecht. Gerade im Bereich der Nachrichtendienste haben die Betroffenen wie dargelegt die geringsten Kenntnisse darüber, ob sie überhaupt betroffen sind oder nicht. Das

ist ein erheblicher Wertungswiderspruch. Denn der aufgrund dieses fehlenden Wissens geringer ausgestaltete Rechtsschutz soll durch die Datenschutzkontrolle gerade kompensiert werden.

e) Nach § 26a Abs. 2 Satz 1 kontrolliert die BfDI beim BfV die Einhaltung des Datenschutzes. Das Wort „beim“ könnte einschränkend dahingehend verstanden werden, dass gemeinsame Dateien mit anderen ausländischen Nachrichtendiensten davon ausgeschlossen sind. Um einer solchen Auslegung entgegenzuwirken, sollte es stattdessen sinngemäß heißen, dass die BfDI die Einhaltung des Datenschutzes im Hinblick auf alle in der Verantwortung des Bundesamtes stehenden personenbezogenen Daten kontrolliert.

f) Nach § 26a Abs. 3 Satz 2 Nr. 1 BVerfSchG muss das Bundesamt der BfDI Einsicht in alle Unterlagen gewähren, die im Zusammenhang mit der Kontrolle stehen. Diese Formulierung birgt die Gefahr einer Einschränkung der Kontrollmöglichkeiten der BfDI. Zum einen ist die Gewährung der Einsichtnahme weniger als die Gewährung des Zugangs, so wie § 24 Abs. 4 BDSG bzw. § 25 Abs. 2 ABDSG die Rechte der BfDI formuliert. Daher sollte es auch hier „Zugang zu“ heißen. Zum anderen darf sich die Gewährung nicht nur auf den Zugang zu Unterlagen „im Zusammenhang mit der Kontrolle“ beschränken. Ansonsten besteht die Gefahr, dass der Zugang zu Unterlagen, die zwar ggf. nicht im Zusammenhang mit einer aktuellen Kontrolle stehen, die aber ebenfalls der Kontrollkompetenz der BfDI unterliegen und die z.B. zur Vorbereitung oder Nachbereitung einer Kontrolle erforderlich sind, verweigert wird. Daher sollte dieser Zusatz gestrichen werden.

g) Auch § 26 Abs. 4 BDSG bzw. § 25 Abs. 7 ABDSG sollen für den Bereich des Bundesamtes keine Anwendung finden. Nach dieser Vorschrift wirkt die BfDI auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhalten der Datenschutzvorschriften der Länder zuständig sind, sowie mit den Aufsichtsbehörden im nichtöffentlichen Bereich hin. Gerade im Bereich der Nachrichtendienste ist eine verpflichtende **Zusammenarbeit mit allen Kontrollgremien** (Landesdatenschutzaufsichtsbehörden, G 10-Kommission, Parlamentarisches Kontrollgremium) **dringend erforderlich**. Dies kann in entsprechender

Anwendung auch dem Urteil des **Bundesverfassungsgerichts** zur Antiterrordatei entnommen werden, in dem das Gericht die gemeinsame Verantwortung einer wirksamen aufsichtlichen Kontrolle Gesetzgeber und Behörden gemeinsam auferlegt (Urt. v. 24.4.2013, 1 BvR 1215/07, Rdnr. 218). Bei der Erarbeitung einer entsprechenden Norm für den Bereich des Bundesamtes sollte allerdings darauf geachtet werden, dass alle beteiligten Stellen zur Zusammenarbeit verpflichtet sind und werden (und nicht – wie die bisherige Formulierung nahelegt – nur die BfDI in die Verantwortung genommen wird).

h) Es wird darauf hingewiesen, dass die Formulierung des § 26a Abs. 3 Satz 3 (ex § 24 Abs. 4 Satz 4 BDSG – sog. Staatswohlklausel) aufgrund der Vorgaben des Bundesverfassungsgerichts sehr restriktiv ausgelegt werden muss (BVerfG, Urt. v. 24.3.2013, 1BvR 1215/07, Rdnr. 219: Verweigerung der Auskunft oder Einsichtnahme nur in strikt zu handhabenden Ausnahmefällen). Um dies sicherzustellen, sollte zumindest in der Gesetzesbegründung hervorgehoben werden, dass die Verwehrung der Auskunft und des Zutritts die ultima ratio bleiben muss und insbesondere allgemeine Hinweise auf eine Gefährdung der Zusammenarbeit mit ausländischen Nachrichtendiensten nicht ausreichen.

9. Weiterer Anpassungsbedarf

a) Anpassung der Begrifflichkeiten „Akte“ bzw. „Datei“

Wiederholt wurde seitens der BfDI darauf hingewiesen, dass mit Inkrafttreten der BDSG-Änderung von 2001 zwar in § 46 Abs. 1 BDSG eine Weitergeltung von Begriffsbestimmungen (Abs. 1: Datei) vorgesehen ist, aber eine Anpassung im BVerfSchG erforderlich erscheint. Dieser Anforderung ist der Gesetzgeber mit Einführung des § 13 Abs. 4 BVerfSchG nur teilweise gerecht geworden. Nach § 13 Abs. 4 können Akten auch in elektronischer Form geführt werden. Elektronische Akten sind aber nach Auffassung des Bundesamtes keine Dateien. Es wird dringend angeregt, bei der jetzigen Novellierung des BVerfSchG nicht nur Begrifflichkeiten an die Datenschutz-Grundverordnung anzupassen, sondern auch endlich den Begriff der „Akte“ zu bereinigen.

b) Verarbeitungsbefugnisse für die Beobachtung von „Randpersonen“

§ 4 enthält Begriffsbestimmungen, die u.a. für § 10 i.V.m. § 3 BVerfSchG relevant sind, nämlich Informationen über Bestrebungen von Einzelpersonen oder von Personenzusammenschlüssen zu sammeln und auszuwerten und dafür auch personenbezogene Daten zu verarbeiten. Verfassungsrechtlich bislang nicht hinreichend im Gesetz konkretisiert ist die Frage, welche Einzelpersonen in die Beobachtung einbezogen werden dürfen. Das Gesetz selbst sollte zwischen verschiedenen Personenkreisen differenzieren, wie „Zielpersonen“, „Hinweisgebern“ oder „Kontakt- oder Begleitpersonen“, und an die Befugnis zur Datenverarbeitung unterschiedliche Anforderungen stellen. Insbesondere Kontakt- und Begleitpersonen dürfen mangels einer hinreichend klaren und bestimmten Ermächtigung im Gesetz nicht in die Beobachtung einbezogen werden bzw. nur in dem verfassungsgerichtlich zuerkannten Umfang. Der Gesetzgeber ist gehalten, für die jeweils unterschiedlich eingriffsintensiven Maßnahmen unterschiedliche eingriffsschwellen festzulegen. Dies hat das Bundesverfassungsgericht für Polizeibehörden entschieden (vgl. BVerfGE 120, 274, 329f.), nichts anderes kann aber für Nachrichtendienste gelten. Für sie gelten die Grundsätze der Verhältnismäßigkeit und der Normenklarheit und Bestimmtheit ebenfalls uneingeschränkt. Besonders schwerwiegende Eingriffe sind etwa der Einsatz von Vertrauenspersonen oder das Abhören des nichtöffentlich gesprochenen Wortes auch außerhalb von Wohnungen. Dies hat das Bundesverfassungsgericht deutlich hervorgehoben (BVerfG NJW 2016, 1781).

c) Übermittlungsregelungen

Die Übermittlungsregelungen der §§ 18 ff. BVerfSchG entsprechen nicht den verfassungsrechtlichen Vorgaben. Sie verstoßen gegen das informationelle Trennungsprinzip und den Grundsatz der Zweckbindung. Dies hatte ich mehrfach nach der Entscheidung des Bundesverfassungsgerichts zum ATDG dargelegt und daran halte ich fest. Wie das Bundesverfassungsgericht in seiner Entscheidung zum BKAG bestätigt, sind nicht nur die Regelungen zur Übermittlung der Dienste an Polizeibehörden zu überarbeiten. Es sind auch in der umgekehrten Richtung die Regelungen zur

Übermittlung der Polizeibehörden an die Nachrichtendienste zu weit gefasst (BVerfG NJW 2016, 1781, 1805, Abs. Nr. 319). Deshalb sind nicht nur §§ 19, 20, sondern auch § 18 BVerfSchG grundlegend zu überarbeiten.

d) Erfordernis der Vollprotokollierung

Die BfDI wiederholt ihre Auffassung, dass insbesondere auch im Bereich der Nachrichtendienste eine Inhalts- und Transaktionsvollprotokollierung eine erforderliche und angemessene technische Maßnahme ist, um den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. In Anlehnung an das Urteil des Bundesverfassungsgerichts zum ATDG ist bei den Dateien der Sicherheitsbehörden die Gewährleistung der Transparenz bedingt durch Zweck und Funktionsweise hinsichtlich des Informationsaustauschs nur in begrenztem Umfang möglich. Damit werden den Betroffenen auch nur eingeschränkte Rechtsschutzmöglichkeiten eröffnet. Die Kontrolle über die rechtmäßige Anwendung der Sicherheitsgesetze liegt damit im Wesentlichen bei der Aufsicht durch die Datenschutzbeauftragten. Damit diese ihre Aufgaben angemessen wahrnehmen können, ist es erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden (BVerfG, 1 BvR 1215/07 Rdnr. 204, 207). Daher sollte dieses verfassungsrechtliche Erfordernis bei dieser Gelegenheit mit ins BVerfSchG aufgenommen werden.

e) „Gender“-gerechte Formulierung

Es wird angeregt, in § 14 Abs. 1 Satz 2 vor den Worten „Der Bundesbeauftragte“ die Worte „Die oder“ einzufügen. Dies würde der Formulierung im BDSG und im ABDSG entsprechen.

V. Zu Artikel 6 – Änderung des Artikel-10-Gesetzes

1.Änderungsbefehl Nr. 1.b)bb) (§ 4 Abs. 4 Satz 2)

Mit dem neu eingefügten Worten in Abs. 4 Satz 1 und dem neuen Satz 2 des § 4 Abs. 4 werden § 19 Abs. 3 Sätze 2 und 4 BVerfSchG für Übermittlung von Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen für anwendbar erklärt. Ich verweise hier insofern auf meine Ausführungen zu Artikel 2 (III.1.c)), wonach § 19 Abs. 3 BVerfSchG verfassungswidrig ist, sodass eine Bezugnahme dieser Vorschrift schon aus diesem Grund nicht in Betracht kommt.

Die Gesetzesbegründung lässt vermuten, dass der Verweis auf § 19 Abs. 3 BVerfSchG lediglich eine Klarstellung von Befugnissen des Bundesamtes im Bereich der Übermittlung ins Ausland darstellt. Das würde voraussetzen, dass das Bundesamt schon bisher Übermittlungen ins Ausland vornehmen durfte und nur der Umfang unklar war.

Dieser Auslegung wird widersprochen. § 4 Abs. 4 G 10 ist lex specialis zu den §§ 19-21 BVerfSchG für Übermittlungen des Bundesamtes in Bezug auf G 10-Daten. Von einer Übermittlung ins Ausland ist in § 4 nicht die Rede. Im Gegenteil wird dagegen die Übermittlung ins Ausland durch den BND in § 7a G 10 ausdrücklich erwähnt. Der Gesetzgeber hat die Norm des § 7 G 10 für Übermittlungen ins Ausland als verfassungsrechtlich nicht ausreichend klar und bestimmt genug angesehen und daher eine eigene Befugnisnorm mit § 7a geschaffen. Im Zuge dieser Gesetzesänderung hat der Gesetzgeber bewusst auf Schaffung eines entsprechenden §4a für das Bundesamt verzichtet. Daher stellt die jetzige Regelung eine neue, allerdings in dieser Form nicht verfassungsrechtlich hinreichend deutliche, neue Befugnisnorm dar und ist daher **abzulehnen**.

Wenn überhaupt, dann sollte eine Übermittlungsbefugnis des Bundesamtes an ausländische öffentliche Stellen direkt in § 4 G 10 geregelt und nicht auf (verfassungsrechtlich fragwürdige) Normen des BVerfSchG verwiesen werden.

2. Änderungsbefehl Nr. 3 und 4 (§ 15 Abs. 5 Satz 2; § 16 Satz 2)

Zur Ausweitung der Befugnisse durch die Verwendung des Begriffs „Verarbeitung“ anstatt „Verarbeitung und Nutzung“ wird auf das oben Gesagte verwiesen.

3. weiterer Anpassungsbedarf

Es wird angeregt, in § 15 Abs. 5 Satz 4 vor dem Wort „Bundesbeauftragten“ die Worte „oder der“ und danach die Worte „und für die Informationsfreiheit“ einzufügen. Dies würde der Formulierung im BDSG und im ABDSG entsprechen.

Mit freundlichen Grüßen
Im Auftrag

Hermerschmidt