Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)788

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

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

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

Nachrichtlich:

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

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

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

INTERNET www.datenschutz.bund.de

DATUM Bonn, 03.03.2017
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), BT-Drs. 18/11325**
HIER Positionspapier der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

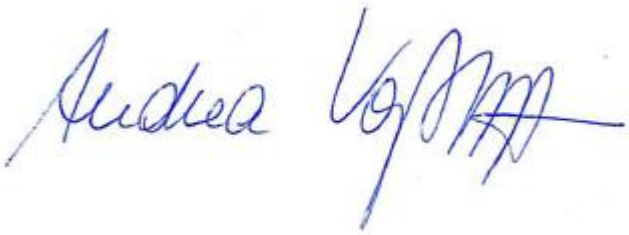
Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

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

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

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

Mit freundlichen Grüßen



Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

Bundestags-Drucksache 18/11325

Positionen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Bonn, den 3. März 2017

Vorbemerkung

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

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

I. Artikel 1 (Entwurf BDSG-neu)

1. Befugnisse der BfDI im Bereich der JI-Richtlinie

§ 16 Abs. 2 BDSG-neu-E lautet:

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

Vorschlag BfDI:

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

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

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

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

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

a) § 17 Abs. 2 BDSG-neu lautet:

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

b) § 18 Abs. 2 BDSG-neu-E lautet:

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

Vorschlag BfDI:

a) Zu § 17 Abs. 2:
Beibehaltung des Regierungsentwurfs

b) § 18 Abs. 2 wird wie folgt gefasst:
„(2) Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter ei-

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

Begründung:

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

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

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

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

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

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

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

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

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

§ 20 Abs. 7 BDSG-neu-E lautet:

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

Vorschlag BfDI: *Streichung*.

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

4. Verarbeitung zu anderen Zwecken durch öffentliche Stellen (§ 23 Abs. 1 BDSG-neu-E

§ 23 Abs. 1 BDSG-neu-E lautet:

„(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn
1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,
4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
5. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.“

Vorschlag BfDI:

§ 23 Abs. 1 wird wie folgt gefasst:
„(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu

demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn
1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, ~~es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,~~
4. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,
5. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
6. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, ~~soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen~~.

und sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. “

Begründung:

Wie auch bei der Verarbeitung zu anderen Zwecken durch nicht öffentliche Stellen (§ 24 BDSG-neu-E) sollte bei der zweckändernde Verarbeitung durch öffentliche Stellen in allen von den Nummern 1 bis 7 des § 23 Abs. 1 genannten Varianten als Korrektiv eine Interessenabwägung vorgesehen werden. Der Regierungsentwurf schreibt eine solche Interessenabwägung nur in § 23 Abs. 1 Nr. 3 und Nr. 7 BDSG-neu-E vor. Die Erforderlichkeit einer Interessenabwägung ergibt sich schon daraus, dass - wie in der Gesetzesbegründung ausgeführt- den Mitgliedstaaten durch die Verordnung Regelungsspielraum nur insoweit gewährt wird, als die nationale Rege-

lung eine „in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme“ zum Schutz der in Art. 23 genannten Ziele darstellt. Die Verhältnismäßigkeit gebietet es, neben den in § 23 Abs. 1 Nr. 1 bis 7 BDSG-neu-E genannten Rechtsgüter auch die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung einzubeziehen. Beispielsweise wäre sonst jede zweckändernde Datenverarbeitung durch öffentliche Stellen zulässig, wenn sie zur Sicherung des Steueraufkommens erforderlich ist (Nr. 5), unabhängig von der Höhe der Steuerschuld und der Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung der betroffenen Person.

5. Untersuchungsbefugnisse der Aufsichtsbehörden bei Geheimhaltungspflichten (§ 29 Abs. 3 BDSG-neu-E)

§ 29 Abs. 3 BDSG-neu-E lautet:

„(3) Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.“

Vorschlag BfDI:

§ 29 Abs. 3 wird wie folgt gefasst:

„(3) Die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 erstrecken sich auch auf Berufs- und besondere Amtsgeheimnisse. Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen diese Befugnisse nur insoweit, als ihre Inanspruchnahme zur Ausübung der Datenschutzaufsicht unabdingbar ist. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.“

Begründung:

Die im Entwurf der Bundesregierung vorgesehenen Einschränkungen der Befugnisse auf Zugang zu personenbezogenen Daten und den Geschäftsräumen und Datenverarbeitungsanlagen von Berufsgeheimnisträgern sind insgesamt zu unpräzise und lassen einen weiten Interpretationsspielraum zu. Auch die Gesetzesbegründung liefert keine präzisen Hinweise zur Auslegung der Norm. Es ist deshalb zweifelhaft, ob § 29 Abs. 3 BDSG-neu-E tatsächlich notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen und damit den Anforderungen der Öffnungsklausel des Art. 90 DSGVO gerecht wird. Vielmehr besteht die Gefahr, dass beispielsweise Ärzte oder Rechtsanwälte den Beschäftigten der Aufsichtsbehörden unter Berufung auf ihre Geheimhaltungspflicht und § 29 Abs. 3 BDSG-neu-E pauschal den Zugang zu ihren

Geschäftsräumen und Datenverarbeitungsanlagen verwehren könnten. Das würde im Ergebnis dazu führen, dass gar keine Datenschutzkontrolle mehr stattfinden würde, was einen Verstoß gegen die DSGVO darstellen würde und auch nicht von dem in der Gesetzesbegründung zitierten Urteil des Bundesverfassungsgerichts bezweckt ist.

Die vorgeschlagene alternative Formulierung würde hingegen in Satz 1 zunächst klarstellen, dass sich die Datenschutzkontrolle – wie im geltenden Recht – auch auf besondere Amtsgeheimnisse und Berufsgeheimnisse erstreckt. Hinsichtlich der Berufsgeheimnisse stellt Satz 2 einen Ausgleich zwischen den Geheimhaltungspflichten und der Datenschutzkontrolle her, indem der Zutritt zu den Geschäftsräumen und der Zugang zu den gespeicherten Daten auf das notwendige Maß beschränkt wird. Sollte die Aufsichtsbehörde dabei Kenntnis von Daten erlangen, die unter das Berufsgeheimnis fallen, ist durch § 29 Abs. 3 Satz 2 BDSG-neu-E gewährleistet, dass diese Daten von der Aufsichtsbehörde nicht weitergegeben oder offenbart werden.

6. Einschränkungen von Betroffenenrechten

Der Entwurf des BDSG-neu enthält in Kapitel 2 einige Paragrafen, die die in der DSGVO vorgesehenen Betroffenenrechte einschränken. Zwar lässt Art. 23 DSGVO Beschränkungen grundsätzlich zu, allerdings nur unter strengen Voraussetzungen, die im Entwurf des BDSG-neu nicht immer eingehalten werden. Dies gilt insbesondere für die folgenden Normen:

- **§ 32 Abs.1 Nr. 5 BDSG-neu-E**

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

…

5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.“

Vorschlag BfDI:

Streichung von § 32 Abs. 1 Nr. 5.

Begründung:

Die Norm eröffnet ihrem Wortlaut nach einen weiten Spielraum, in dem auf die Information der betroffenen Person verzichtet werden kann. Zwar stellt die Begründung klar, dass sich die Ausnahme nur auf spezifische Fälle im Kontext der öffentlichen Sicherheit bezieht. Dies ist aber bereits durch § 32 Absatz 1 Nummern 2 und 3 abgedeckt. „Vertraulichkeit“ als solche ist kein Schutzgut im Sinne von Artikel 23 DSGVO, vielmehr sind bestimmte Zwecke der Datenverarbeitung zu schützen, was – wie dargelegt – bereits durch die Nummern 2 und 3 sichergestellt wird.

- **§ 33 Abs. 1 Nr. 1 Buchstabe a) BDSG-neu-E**

§ 33 Abs. 1 Nr. 1 Buchstabe a) BDSG-neu-E lautet:

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Falle einer öffentlichen Stelle

a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679 gefährden würde.“

Vorschlag BfDI:

Streichung von § 33 Abs. 1 Nr. 1 Buchstabe a).

Begründung:
Der Tatbestand erfüllt nicht die Anforderungen an die Verhältnismäßigkeit, wie sie von Artikel 23 DSGVO gefordert werden. Das pauschale Abstellen auf eine Gefährdung der Aufgabenerfüllung in Verbindung mit dem Verweis auf Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung sind nicht ausreichend. Vielmehr müssten zumindest konkrete Fallgestaltungen in den Normtext aufgenommen werden. Andernfalls ist die Nummer zu streichen.

- **§ 33 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu-E**

§ 33 Abs. 1 Nr. 2 Buchstabe a) BDSG-neu-E lautet**:**

„Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahmen nicht, wenn die Erteilung der Information

1. im Falle einer nicht-öffentlichen Stelle
a) allgemein anerkannte Geschäftszwecke des Verantwortlichen erheblich gefährden würde, es sei denn dass das Interesse der betroffenen Person an der Informationserteilung überwiegt.“

Vorschlag BfDI**:**

Streichung von § 33 Abs. 1 Nr. 2 Buchstabe a).

Begründung:
Die erhebliche Gefährdung der Geschäftszwecke des Verantwortlichen rechtfertigt trotz der verankerten Interessenabwägung in dieser Allgemeinheit nicht die Einschränkung der Informationspflicht. Es bedarf vielmehr einer konkreten Bezugnahme auf die Tatbestände des Artikels 23 Abs. 1 der DSGVO und die Einschränkung muss

der Prüfung standhalten, ob es sich dabei um eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme handelt. Ob hiermit reine Privatinteressen überhaupt geschützt werden können, erscheint zweifelhaft. Auch die vorgesehene Interessenabwägung hilft letztlich zur Rechtfertigung der Beschränkung nicht weiter, da der Verantwortliche zunächst ohne Weiteres das Nicht-Überwiegen der Interessen der betroffenen Person behaupten kann.

7. § 48 BDSG-neu-E (Verarbeitung besonderer Kategorien personenbezogener Daten)

§ 48 BDSG-neu-E lautet:

„(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.
(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein
1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,
2. die Festlegung von besonderen Aussonderungsprüffristen,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,
5. die von anderen Daten getrennte Verarbeitung,
6. die Pseudonymisierung personenbezogener Daten,
7. die Verschlüsselung personenbezogener Daten.
8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.“

Vorschlag BfDI:

§ 48 wird wie folgt gefasst:

„Die Verarbeitung besonderer Kategorien von Daten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt.“

Begründung:
Der Inhalt des Vorschlags der Bundesregierung geht nicht über die Vorgaben der Richtlinie hinaus und stellt keine Konkretisierung dar. In welchen Fällen Polizei- und Strafverfolgungsbehörden sensitive Daten speichern dürfen, sollte ausschließlich in den Fachgesetzen geregelt werden.

8. § 49 BDSG-neu-E (Zweckbindung)

§ 49 BDSG-neu-E lautet:

„Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.“

Vorschlag BfDI:
§ 49 wird wie folgt gefasst:

„Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als demjenigen, zu dem sie erhoben wurden, ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt.

Begründung:
Diese Vorschrift betrifft die zentralen Aussagen zur Zweckbindung im Urteil des Bundesverfassungsgerichts zum BKAG (BVerfG NJW 2016, 1781). Die Vorschrift ist nicht mit den Aussagen des Urteils vereinbar. Die Zwecke der Gefahrenabwehr und der Strafverfolgung werden nicht hinreichend differenziert. Zudem bleiben die Aussagen sogar hinter § 481 StPO zurück, der seinerseits nicht mehr den verfassungsrechtlichen Anforderungen entspricht. Das BVerfG hält eine Übermittlung personenbezogener Daten aus eingriffsintensiven Ermittlungsmaßnahmen zum einen nur für zulässig, wenn ein gleichgewichtiger Rechtsgüterschutz besteht. Darüber hinaus muss sich aus einem hinreichend spezifischen Anlass ein konkreter Ermittlungsansatz ergeben. Ein lediglich potentieller Ermittlungsansatz oder gar eine allgemeine Nützlichkeit ist nicht ausreichend. Vor diesem Hintergrund sollten die Anforderungen an die Zulässigkeit von Zweckänderungen konkret im Fachrecht geregelt werden.

9. § 64 Absätze 2 und 3 BDSG-neu-E (Anforderungen an die Sicherheit der Datenverarbeitung)

§ 64 Absätze 2 und 3 BDSG-neu-E lauten:

„(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich ist. Die Maßnahmen nach Satz 1 sollen dazu führen, dass
1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt wird und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:
1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennbarkeit).
Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.“

Vorschlag BfDI:

Aufnahme eines neuen Absatzes 2 statt der bisherigen Absätze 2 und 3.
„(2) Dabei ist insbesondere zu gewährleisten, dass

1. *nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),*
2. *personenbezogene Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität),*
3. *personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden (Verfügbarkeit),*
4. *jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können und in das Verfahren eingegriffen werden kann (Authentizität und Intervention),*
5. *festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),*
6. *die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).“*

Begründung:
Die Norm beinhaltet Regelungen, die sich an den ersten Datenschutzgesetzen aus den 1970er und 1980er Jahren orientieren und die inzwischen fachlich als veraltet

anzusehen sind. So geht § 64 Abs. 3 Nr. 2 BDSG-neu-E beispielsweise an den technischen Möglichkeiten vorbei. Man kann zwar durch Verschlüsselung versuchen, einen Unbefugten vom Datenzugriff abzuhalten, wie man das Kopieren, Löschen, usw. verhindern will, bleibt aber offen. Es wird deshalb die oben dargestellte, zeitgemäße Alternativregelung vorgeschlagen.

10. § 76 Abs. 3 BDSG-neu-E (Verwendung von Protokolldaten)

§ 76 Abs. 3 BDSG-neu-E lautet:

„ (3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.“

Vorschlag BfDI:

Abs. 3 wird wie folgt gefasst:
„(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die oder den Bundesbeauftragten und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten verwendet werden.“

Begründung:
Protokollierung ist eine Verfahrenssicherung, die den Grundrechtseingriff der Datenverarbeitung abmildern soll. Sie darf deshalb nicht ihrerseits zu zusätzlichen Grundrechtseingriffen führen. Dies schließt die allgemeine Verwertung für die Strafverfolgung aus. Art. 25 Abs. 2 DS-RL, der erst im Trilog um die Möglichkeit der Nutzung von Protokolldaten für Strafverfahren ergänzt wurde, kann nicht dahingehend ausgelegt werden, dass eine Verwendung für jegliches Strafverfahren zulässig sein soll. Dies wäre mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Für die Verfolgung von Straftaten, die durch die Verwendung der personenbezogenen Daten begangen wurden, ist eine solche Regelung nicht erforderlich. Denn dieser Zweck ist bereits von der Zweckbestimmung „ Überprüfung der Rechtmäßigkeit der Datenverarbeitung“ erfasst. Die Richtlinie soll die nationale Verarbeitung begrenzen, nicht zu einer Erweiterung der Datenverarbeitung führen. Insofern sollte die Verwendung für Strafverfahren gestrichen werden.

II. Artikel 4 (Änderung des BND-Gesetzes)

1. § 32 BNDG-E (Unabhängige Datenschutzkontrolle)

In der Begründung zu § 32 BNDG-E (S. 69) wird Folgendes ausgeführt:

„Das in § 26a Absatz 3 Nr. 2 Bundesverfassungsschutzgesetz geregelte Zutrittsrecht zu allen Diensträumen bezieht sich nur auf die vom Bundesnachrichtendienst genutzten Räume. Räume, welche beispielsweise bei gemeinsam genutzten Dienststellen ausschließlich durch andere Einrichtungen genutzt werden, sind keine Diensträume des Bundesnachrichtendienstes. Insoweit besteht folglich auch kein Betretungsrecht nach dieser Vorschrift."

Vorschlag BfDI:

Streichung der vorgenannten Sätze

Begründung:
Die Entwurfsbegründung lässt sich aus dem Wortlaut des in Bezug genommenen § 26 a Abs. 3 Nr. 2 BVerfSchG nicht herleiten und steht in Widerspruch zum geltenden Recht (vgl. §§ 24 Abs. 4 Satz 1 Nr. 2 BDSG i.V.m. § 1 Abs. 5 Satz 2 BDSG). Nach § 1 Abs. 5 Satz 2 i.V.m. Satz 4 BDSG gilt das BDSG – und damit auch das Zutrittsrecht der BfDI –, wenn eine verantwortliche Stelle, die außerhalb der EU (d.h. in einem Drittstaat) „belegen ist" (§ 1 Abs. 5 Satz 2 BDSG), im Inland personenbezogene Daten erhebt, verarbeitet oder nutzt und nicht nur Datenträger zum Zweck des Transits durch das Inland einsetzt. Befinden sich demnach in einer Liegenschaft des BND im vorgenannten Sinne Räume, die z.B. ausschließlich von einem Nachrichtendienst eines Drittstaates genutzt werden, sind dies nach geltendem Recht Räume, zu denen die BfDI zutrittsberechtigt ist.

Die Entwurfsbegründung widerspricht den verfassungsrechtlichen Vorgaben zur Gewährleistung einer umfassenden und effizienten Kontrolle durch die BfDI und der der BfDI vom Bundesverfassungsgericht zugewiesenen Kompensationsfunktion zum Schutz der Grundrechte der Betroffenen. Die BfDI muss die Befugnis haben, eine behauptete Unzuständigkeit bezüglich des Zutrittsrechts überprüfen zu dürfen.

Zugunsten des BfV und des MAD existieren keine vergleichbaren Begründungen**.**

2. § 32a BNDG-E (Anwendung des Bundesdatenschutzgesetzes)

§ 32a Abs. 1 Nr. 1 lit. b) BNDG-E lautet:

„b) findet § 14 Absatz 2 mit der Maßgabe Anwendung, dass sich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur an die Bundesregierung sowie an die für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien (Parlamentarisches Kontrollgremium, Vertrauensgremium, G 10-Kommission, Unabhängiges Gremium) wenden darf; eine Befassung der für die Kontrolle des Bundesnachrichtendienstes zuständigen Gremien setzt voraus, dass sie oder er der Bundesregierung entsprechend § 16 Absatz 2 Satz 1 Bundesdatenschutzgesetz zuvor Gelegenheit gegeben hat, innerhalb einer von ihr oder ihm gesetzten Frist Stellung zu nehmen;“

BfDI-Vorschlag:

Streichung von § 32a Abs. 1 Nr. 1 lit. b). Lit. a) wird dann unmittelbar zu Nr. 1.

Begründung:
§ 32 a Abs. 1 Nr. 1 lit. b) BNDG-E schränkt das geltende Recht (vgl. § 26 Abs. 2 Satz 3 BDSG) – das von § 14 Abs. 2 BDSG-neu fortgeschrieben wird – zu Lasten der BfDI und des Deutschen Bundestages verfassungswidrig ein**.** Nach diesem Regelungsvorschlag soll § 14 Abs. 2 BDSG-neu, wonach sich die BfDI – ebenso wie nach geltendem Recht (vgl. § 26 Abs. 2 Satz 3 BDSG) – von sich aus an den Deutschen Bundestag oder seine Ausschüsse wenden kann, in Bezug auf die den BND betreffende Sachverhalte nur mit der Maßgabe gelten, dass sich die BfDI nur an die Bundesregierung sowie an die für die Kontrolle des BND zuständigen Gremien (PKGr, G 10, Vertrauensgremium, Unabhängiges Gremium) wenden darf – und auch nur sofern der Bundesregierung entsprechend § 16 Abs. 2 Satz 1 des Gesetzentwurfs zuvor Gelegenheit zur Stellungnahme gewährt worden ist.

Dies bedeutet, dass sich die BfDI im Gegensatz zum geltenden Recht den BND betreffend nicht mehr an den Deutschen Bundestag oder seine Ausschüsse wenden dürfte – und damit insbesondere nicht an den Innenausschuss oder einen Untersuchungsausschuss des Deutschen Bundestages, der z.B. BND-relevante Sachverhalte aufklären soll.

Diese Beschränkung steht nicht nur in Widerspruch zu verfassungsgerichtlichen Vorgaben. Sie widerspricht auch der durch den Europäischen Gerichtshof geforderten Unabhängigkeit der BfDI. Zudem beschränkt diese Regelung in unzulässiger Weise das Informationsrecht des Parlaments und seiner Ausschüsse.

In Bezug auf das BfV und den MAD enthält der Gesetzentwurf keine vergleichbaren Einschränkungen für die BfDI.

Die hier vorgeschlagene Streichung würde zu einer unmittelbaren Anwendbarkeit des § 14 Abs. 2 BDSG-neu führen und damit den oben beschriebenen verfassungsrechtlichen Ansprüchen genügen.

Neben den vorgenannten grundsätzlichen Kritikpunkten sieht die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an weiteren Stellen Änderungsbedarf. Dazu gehören folgende Punkte:

- **Art. 1, § 4 BDSG-neu-E:** Die Schaffung einer nationalen Regelung zur Videoüberwachung durch nicht-öffentliche Stellen ist europarechtlich zweifelhaft. Die wortgleich aus dem Entwurf des Videoüberwachungsverbesserungsgesetzes übernommenen Änderungen tragen nicht zu einer Erhöhung der öffentlichen Sicherheit bei und sind daher unnötig.
- **Art. 1, § 27 Abs. 2 Satz 2 BDSG-neu-E:** Das Recht auf Auskunft bei der Verarbeitung personenbezogener Daten zu Forschungszwecken sollte nicht schon dann entfallen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand darstellt, da das Auskunftsrecht häufig die einzige Möglichkeit für den Betroffenen darstellt, Transparenz herzustellen.
- **Art. 2, § 26a Abs. 2 BVerfSchG-E:** Zur Vermeidung von Kontrolllücken sowie zur sachgerechten Abgrenzung zwischen den Kompetenzen der BfDI einerseits und der G-10-Kommission andererseits bedarf es einer Neuregelung des § 15 Abs. 5 Satz 2 G 10.

gez.

Andrea Voßhoff