Datenschutzrechtliche Eckpunkte zu den in die Öffentlichkeit gelangten Überlegungen des Bundesministeriums des Innern (BMI) für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)

Inhaltsverzeichnis

1. Vorbemerkung

In die Öffentlichkeit sind Überlegungen des Bundesministeriums des Innern (BMI) für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU – Stand: 5. August 2016) gelangt. In der Erwartung, dass diese nochmals eingehend überarbeitet werden, ist eine detaillierte Stellungnahme, insbesondere in Hinblick auf die Vereinbarkeit des DSAnpUG-EU mit der Datenschutzgrundverordnung (DSGVO), erst dann beabsichtigt, wenn ein belastbarer Entwurf vorliegt.

Die nachfolgenden generellen Erwägungen beschränken sich auf Artikel 1 des DSAnpUG-EU im Zusammenhang mit der Umsetzung der DSGVO. Sie sollen frühzeitig kommuniziert werden, um in die weitere Arbeit am Gesetzentwurf einfließen zu können. Materiell-rechtliche Anmerkungen zu der Umsetzung der JI-Richtlinie enthält die Stellungnahme nicht.

2. Die Anmerkungen im Einzelnen

2.1 Allgemeine Hinweise

Eine klare Trennung zwischen der Umsetzung der Regelungsaufträge und Regelungsoptionen nach der DSGVO, der Umsetzung der JI-Richtlinie und der Regelung für die nicht unionsrechtlich erfassten Bereiche ist dringend erforderlich. Die Bezeichnung "Allgemeines Bundesdatenschutzgesetz" (im Folgenden ABDSG-E) kann nicht überzeugen. Zudem sollte bei den einzelnen Paragraphen des ABDSG-E zwischen Regelungen für den öffentlichen und nicht öffentlichen Bereich differenziert werden.

2.1.1 Klare Trennung zwischen der Umsetzung der Regelungsaufträge und Regelungsoptionen nach der DSGVO, der Umsetzung der JI-Richtlinie und der Regelung für die nicht unionsrechtlich erfassten Bereiche

Es ist schwierig, die Umsetzung der Richtlinie (EU) 2016/680 (JI-Richtlinie) gemeinsam mit der Anpassung des deutschen Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) vorzunehmen. Die Umsetzung dieses Regelungsansatzes führt in der Gesamtschau dazu, dass für den Rechtsanwender bei vielen Vorschriften deren Anwendungsbereich unklar bleibt. Einzelne Regelungen gelten nur im Anwendungsbereich der DSGVO, andere nur im Zusammenhang mit der JI-Richtlinie und weitere nur für die nicht unionsrechtlich geregelten Bereiche. Daneben gibt es aber auch Bestimmungen, die für die vorgenannten Bereiche gemeinsam gelten sollen. Dies macht den Gesetzentwurf unübersichtlich und kaum handhabbar. Zur Gewährleistung des verfassungsrechtlichen Gebots der Normenklarheit sollten die unterschiedlichen Bereiche voneinander getrennt werden.

Rein vorsorglich wird darauf hingewiesen, dass die Umsetzung der JI-Richtlinie, insbesondere auch unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts, in dem bisherigen Entwurf der Vervollständigung beziehungsweise Anpassung bedarf. Zudem muss die Regelung zum Inkrafttreten korrigiert werden. Das bisher vorgesehene Datum "25. Mai 2018" entspricht den Vorgaben der DSGVO, nicht aber den Vorgaben der JI-Richtlinie, die bestimmt, dass Umsetzungsvorschriften grundsätzlich bereits ab dem 6. Mai 2018 anzuwenden sind (vergleiche Artikel 63 Absatz 1 Satz 1 und 3 JI-Richtlinie). Eine detaillierte Stellungnahme für den Bereich der JI-Richtlinie ist vorgesehen.

2.1.2 Bezeichnung des Gesetzes in Artikel 1 DSAnpUG-EU

Die Bezeichnung der Nachfolgeregelung des Bundesdatenschutzgesetzes als "allgemeines BDSG" (ABDSG-E) ist nicht verständlich. In Abgrenzung zum allgemeinen Bundesdatenschutzgesetz gibt es kein besonderes Bundesdatenschutzgesetz, nur, wie bisher auch, bereichsspezifische Regelungen.

Die Bezeichnung Bundesdatenschutzgesetz (BDSG) sollte beibehalten und Artikel 1 als Änderungsgesetz zum BDSG ausgestaltet werden.

2.1.3 Einheitliche Verwendung der Begriffe der DSGVO

Um eine einfache Anwendung und Auslegung des Gesetzes in Artikel 1 DSAnpUG-EU (ABDSG-E) zu gewährleisten, sollte das Gesetz einheitlich die Begriffe der DSGVO verwenden. Beispielsweise sollte statt der "Benennung einer oder eines Beauftragten für den Datenschutz" in § 14 ABDSG-E entsprechend dem Wortlaut in Artikel 37 DSGVO die Formulierung "Benennung eines Datenschutzbeauftragten" gewählt werden.

2.1.4 Deutliche Differenzierung zwischen den Regelungen für den öffentlichen und nicht öffentlichen Bereich

Erhebliche Schwierigkeiten bereitet es, den Adressatenkreis der einzelnen Vorschriften des ABDSG-E aus sich heraus zu überblicken. Die Frage, ob die jeweilige Vorschrift für nicht öffentliche Stellen, für öffentliche Stellen oder für beide gilt, kann vielfach erst durch Heranziehung der Gesetzesbegründung beantwortet werden.

Die fehlende Differenzierung zwischen dem öffentlichen und dem nicht öffentlichen Bereich sollte insbesondere zur Zweckänderung und im Bereich der Einschränkung von Betroffenenrechten (Kapitel 3) überprüft werden. Der Umfang der Betroffenenrechte, wie er bislang im Bundesdatenschutzgesetz (BDSG) geregelt ist, soll nach dem Gesetzentwurf im Rahmen des europarechtlich Zulässigen weitestgehend in die §§ 7 und folgende ABDSG-E überführt werden. Hierbei finden durch die gewählte "Vereinheitlichung" Einschränkungen von Betroffenenrechten, die bislang nur für den nicht öffentlichen Bereich konzipiert waren, nunmehr auch für den öffentlichen Bereich Anwendung. Im Hinblick auf die Grundsätze der Bestimmtheit, Lesbarkeit und Klarheit von Gesetzen sollte bezüglich jeder einzelnen Regelung des ABDSG-E deutlich gekennzeichnet werden, ob diese für öffentliche und beziehungsweise oder nicht öffentliche Stellen gilt. Dies darf sich nicht lediglich aus der Gesetzesbegründung, sondern muss sich bereits eindeutig aus dem jeweiligen Gesetzeswortlaut ergeben.

2.2 Bedenken hinsichtlich der Vereinbarkeit mit dem Grundgesetz und der DSGVO

Zudem bestehen Bedenken hinsichtlich der Vereinbarkeit des ABDSG-E mit dem Grundgesetz und der DSGVO. Die Regelungen sind oftmals zu unbestimmt und könnten Länderkompetenzen tangieren. Durch bloße Wiederholungen des Wortlautes der DSGVO werden Öffnungsklauseln der DSGVO, sofern diese überhaupt hinsichtlich einzelner Regelungen des ABDSG-E bestehen sollten, jedenfalls nicht ordnungsgemäß ausgefüllt.

2.2.1 Eingriff in die Gesetzgebungskompetenz der Länder

Trifft der Bundesgesetzgeber Regelungen zu den Aufsichtsbehörden der Länder wie unter anderem in §§ 16, 27, 29 und folgende ABDSG-E geschehen, ist zwischen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Ländern umstritten, ob die Gesetzgebungskompetenz des Bundes gegeben ist. Während die Aufsichtsbehörden der Länder eine Zuweisung der primären Gesetzgebungskompetenz an die Länder sehen, hält die BfDI die sich aus der Begründung des Gesetzentwurfs ergebenden Erläuterungen zur Gesetzgebungskompetenz des Bundes für zutreffend.

2.2.2 Fehlerhafte Anwendung und Ausfüllung von Öffnungsklauseln der DSGVO

Mit den Regelungen des ABDSG-E werden Regelungen getroffen, hinsichtlich derer teilweise keine Öffnungsklauseln in der DSGVO zu Gunsten des nationalen Gesetzgebers bestehen.

Insbesondere Artikel 6 Absatz 4 der DSGVO, auf den unter anderem in § 6 ABDSG-E Bezug genommen wird, stellt keine generelle Ermächtigungsgrundlage für gesetzliche Regelungen im nicht öffentlichen Bereich dar, sondern kommt nur dort zum Tragen, wo bereits Öffnungsklauseln zur Regelung der Erstverarbeitung existieren.

Öffnungsklauseln können zudem nicht dadurch ausgefüllt werden, dass die Formulierungen aus der DSGVO im Wesentlichen wiederholt werden (§ 7 Absatz 2, § 8 Absatz 2 ABDSG-E).

2.3 Materiell-rechtliche Schwerpunkte

Zahlreiche Vorschriften im ABDSG-E lassen befürchten, dass mit dem DSAnpUG-EU datenschutzrechtliche Standards sinken. Die im ABDSG-E formulierten Regelungen zu den unabhängigen Datenschutzaufsichtsbehörden bedürfen zudem eingehender Überarbeitung. Die Vorschriften zum Beschäftigtendatenschutz und zum betrieblichen Datenschutzbeauftragten werden grundsätzlich begrüßt. Ergänzungen und Korrekturen werden für das Akkreditierungsverfahren, die Videoüberwachung und beim Scoring angeregt.

2.3.1 Drohende Absenkung des Datenschutzniveaus

Das ABDSG-E bleibt hinsichtlich des datenschutzrechtlichen Standards sowohl hinter dem bisherigen BDSG als auch der DSGVO zurück. Noch in den Verhandlungen zur DSGVO war es erklärtes Ziel, das hohe Datenschutzniveau in Deutschland keinesfalls preiszugeben. Während nunmehr die DSGVO datenschutzfreundliche Innovationen bereithält, sucht der vorliegende Entwurf des DSAnpUG-EU den Datenschutzstandard in Deutschland, sowohl im Verhältnis zum status quo als auch zur DSGVO, deutlich abzusenken. Insbesondere für den nicht öffentlichen Bereich

werden Möglichkeiten geschaffen, die über das Erforderliche hinausgehen und das Recht auf informationelle Selbstbestimmung unangemessen einschränken. Die häufige Fokussierung auf die wirtschaftlichen Interessen geht zu Lasten des Persönlichkeitsschutzes und steht der Harmonisierung des Datenschutzrechts in Europa entgegen. Dies zeigt sich insbesondere darin, dass das ABDSG-E die Betroffenenrechte stärker einschränkt (vergleiche §§ 7-11 ABDSG-E), als es nach der DSGVO zulässig wäre, dass das in der DSGVO angestrebte Maß an Transparenz verfehlt und die Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten (vergleiche § 5 ABDSG-E) ausgeweitet werden. Die Ausweitung der Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten (vergleiche § 5 ABDSG-E) und der in § 2 ABDSG an der Hauptniederlassung eines Unternehmens orientierte Anwendungsbereich des Gesetzes tragen ebenfalls dazu bei, dass das ABDSG-E die Ziele der DSGVO verfehlt.

2.3.1.1 Einschränkung der Betroffenenrechte

Die Einschnitte in die Betroffenenrechte stellen lediglich eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Daten der DSGVO diametral entgegen.

Artikel 23 DSGVO erlaubt den Mitgliedstaaten, durch Rechtsvorschriften bestimmte Pflichten und Rechte der DSGVO einzuschränken. Die Einschränkung muss eine zur Aufrechterhaltung der öffentlichen Sicherheit notwendige und verhältnismäßige Maßnahme darstellen (vergleiche Erwägungsgrund 73). Die Schaffung einer Ausnahme von der Informationspflicht etwa bei "unverhältnismäßigem Aufwand" entgegen Artikel 13 DSGVO (vergleiche § 7 Absatz 2; § 8 Absatz 2 Buchstabe d; § 10 Absatz 2), wegen der fehlenden Differenzierung sowohl im öffentlichen als auch nicht öffentlichen Bereich, zeugt beispielhaft von dem unverhältnismäßigen Gebrauch der Einschränkungsmöglichkeit, der den Anforderungen von Artikel 23 DSGVO nicht genügt. Die verantwortliche Stelle vor hohem Verwaltungsaufwand zu bewahren, realisiert nicht den Schutz der Rechte und Freiheiten anderer Personen nach Artikel 23 Absatz 1 Buchstabe i DSGVO. Die Vorschrift soll Dritte schützen und nicht den Verantwortlichen. Schon im Laufe des Gesetzgebungsverfahrens der DSGVO scheiterte Deutschland mit der Forderung, einen unverhältnismäßigen Aufwand als Ausnahmetatbestand zu regeln. Entsprechend der Intention der DSGVO haben die Verantwortlichen vielmehr durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Ebenso ist nicht ersichtlich, welchen in Artikel 23 DSGVO konkret genannten Zwecken die Einschränkung der Informationspflicht bei der Videoüberwachung in öffentlich zugänglichen Räumen (§ 7 Absatz 3 ABDSG) oder bei der Datenspeicherung zu Zwecken der Datensicherung und Datenschutzkontrolle (§ 8 Absatz 2 Buchstabe d ABDSG-E) dienen sollten. Alle auf Artikel 23 DSGVO gestützten Einschränkungen bedürfen einer zwingenden Überprüfung, ob die Voraussetzungen des Artikel 23 DSGVO vorliegen, der

Verhältnismäßigkeitsgrundsatz gewahrt ist und die jeweilige Formulierung von Ausnahmen dem Bestimmtheitsgrundsatz noch genügt. Außerdem sollten konkretere Regelungen zum Schutz der Rechte der Betroffenen in die einzelnen Bestimmungen des 3. Kapitels aufgenommen werden, beispielsweise dass eine Verwendung der Daten zu anderen Zwecken durch angemessene technische Maßnahmen ausgeschlossen ist, um zumindest einen Ausgleich zu den Beschränkungen der Information des Betroffenen zu erreichen.

2.3.1.2 Ausweitung der Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten

Durch das ABDSG-E werden Befugnisse zur Datenverarbeitung gegenüber den Regelungen zur DSGVO ausgeweitet. Dies zeigt sich insbesondere an der Aufgabe des grundsätzlichen Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten in § 5 ABDSG-E, der im Gegensatz zu Artikel 9 DSGVO nicht mehr als Ausnahmetatbestand formuliert ist.

Das Problem betrifft insbesondere Gesundheitsdaten (§ 4 Absatz 2 Nummern 10, 12, 15, § 5 Nummern 5, 7 ABDSG-E), biometrische Daten (§ 5 Absatz 1 Nummer 1 ABDSG-E) und die Verwendung besonderer Kategorien personenbezogener Daten im Beschäftigungsverhältnis (§ 5 Absatz 1 Nummer 6 ABDSG-E).

Die Anwendungsbereiche und das Verhältnis der einzelnen Normen bezüglich der Gesundheitsdaten zueinander sind unklar. § 4 ABDSG-E befasst sich mit der allgemeinen Zulässigkeit der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen für die Wahrnehmung im öffentlichen Interesse liegender, nicht abschließend genannter Aufgaben, § 5 ABDSG-E mit der erforderlichen Verarbeitung besonderer personenbezogenen Daten im abschließend genannten öffentlichen Interesse. In allen genannten Vorschriften sind Gesundheitsdaten betroffen. Eine Einschränkung der Person des Verarbeitenden erfolgt jedoch nur in § 4 Absatz 2 Nummer 10 und § 5 Nummer 4 ABDSG-E. In den anderen Fällen ist die Verarbeitung "ungeschützt" zugelassen, im Falle von § 5 Nummer 7 ABDSG-E zumindest mit der Möglichkeit der Pseudonymisierung (§ 5 Absatz 1 Seite 2 ABDSG-E).

Problematisch ist auch § 5 Absatz 1 Nummer 1 ABDSG-E, der die "Verarbeitung biometrischer Daten zu Zwecken der eindeutigen Identifikation betroffener Personen" pauschal bereits als erhebliches öffentliches Interesse genügen lässt. Es wird weder zwischen Zwecken der Wirtschaft und staatlicher Aufgabenerfüllung unterschieden, noch wird zwischen unterschiedlichen biometrischen Verfahren differenziert. Die Formulierung stellt damit einen gefährlichen Freibrief für eine uferlose Verarbeitung biometrischer Daten zu Zwecken der eindeutigen Identifikation einer Person durch die Wirtschaft und durch staatliche Stellen aus. Gleiches zeigt sich etwa bei § 5 Absatz 1 Nummer 3 ABDSG, der den Wortlaut von § 13 Absatz 2 Nummer 6 BDSG jedoch ohne die Worte "zwingend erforderlich" wiederholt. Die Ausnahmetatbestände müssen, sofern sie überhaupt Bestand haben können, als solche formuliert und gesondert für den öffentlichen und nicht öffentlichen Bereich ausgewiesen werden.

Insbesondere im Arbeitsrecht ist aufgrund § 5 Absatz 1 Nummer 6 ABDSG-E mit einer erheblichen Ausweitung der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten zu rechnen. § 5 Absatz 1 Nummer 6 ABDSG-E stellt klar, dass besondere Kategorien personenbezogener Daten zur Wahrnehmung der aus dem Arbeitsrecht erwachsende Rechte und Pflichten auch ohne Einwilligung der betroffenen Person (vergleiche Artikel 9 Absatz 2 Buchstabe b DSGVO) verarbeitet werden dürfen. Das bringt zwar zunächst eine Erleichterung für den Arbeitgeber, soweit er Daten wie die Religionszugehörigkeit, gesundheitliche Eignung et cetera für Zwecke des Arbeitsverhältnisses, etwa der Lohnabrechnung oder die Erfüllung seiner Fürsorgepflicht, verarbeitet. Allerdings besteht hier die Gefahr, dass besondere Kategorien personenbezogener Daten im Hinblick auf ihre Verarbeitung und Übermittlung, zum Beispiel beim Datentransfer im Konzern, an Schutz verlieren. Zum "Arbeitsrecht" gehören auch individualrechtliche Vereinbarungen und das kollektive Arbeitsrecht. Ob auch insoweit vereinbarte Rechte und Pflichten verhältnismäßig sind und die Interessen der Beschäftigten ausreichend berücksichtigen, ist eine Frage des Einzelfalls, kann aber nicht als Rechtsgrundlage für die Verarbeitung und Übermittlung von besonderen Kategorien personenbezogener Daten herangezogen werden.

Zu befürchten ist im Ergebnis, dass bei Beibehaltung des unspezifischen Begriffs "Arbeitsrecht" lediglich aufgrund von einzelvertraglichen Vereinbarungen besondere Kategorien personenbezogener Daten in weltweiten Konzernstrukturen übermittelt werden. Klargestellt werden sollte daher, dass dies nur aufgrund von arbeitsrechtlichen Rechtsvorschriften, vor allem gesetzlichen Regelungen beziehungsweise Betriebsvereinbarungen, möglich ist.

Im Übrigen sollte in § 5 Absatz 1 ABDSG-E zwischen öffentlichen Stellen und nicht öffentlichen Stellen differenziert und § 5 Absatz 1 Satz 1 Nummer 4 ABDSG-E durch die konkretere Regelung des § 28 Absatz 7 BDSG ersetzt werden.

2.3.1.3 Fehlende Transparenz der Datenverarbeitung

Transparenz und transparente Informationen bilden einen zentralen Bestandteil in der DSGVO. Die Einschnitte in die Betroffenenrechte durch das ABDSG-E sorgen für das Gegenteil: Eingriffe in die Datenschutzrechte der Betroffenen bleiben intransparent, sodass die Ausübung weiterer Rechte nach §§ 10 bis 13 ABDSG-E erschwert wird. Mangels nachträglicher Benachrichtigungspflichten scheitert auch eine durch den Betroffenen veranlasste ex-post-Kontrolle durch die Aufsichtsbehörden. Dies zeigt sich beispielsweise in § 9 ABDSG-E. Dieser übernimmt in § 9 Absatz 2c ABDSG-E die bisherige Regelung nach § 34 Absatz 7 in Verbindung mit § 33 Absatz 2 Seite 1 Nummer 2 BDSG, wonach eine Einschränkung des Auskunftsrechts der betroffenen Person dann besteht, wenn personenbezogene Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher beziehungsweise vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen (also gesperrt werden müssen). Diese Regelung ist mit den Zielen der DSGVO nicht mehr vereinbar. Die Erfahrung der Aufsichtsbehörden zeigt, dass Unternehmen in vielen

Fällen ihrer Pflicht zur Sperrung dieser Daten nicht nachkommen, was nicht selten zu einer (datenschutzwidrigen) zweckwidrigen Weiterverwendung führt. Diese bleibt jedoch dann unentdeckt, wenn die auskunftsersuchende betroffene Person nicht darüber informiert werden muss, dass (doch) Daten über sie gespeichert sind.

Zur besseren Transparenz sollte das ABDSG-E ferner für die zuständige Aufsichtsbehörde eine ausdrückliche Befugnis enthalten, dem Betroffenen bestimmte Mitteilungen über das wesentliche Ergebnis der datenschutzrechtlichen Kontrolle und die Feststellung von Datenschutzverstößen zu machen. Das Geheimhaltungsinteresse der verantwortlichen Stelle muss zumindest dann zurückzustehen, wenn sie rechtswidrig Daten verarbeitet.

2.3.1.4 Eingeschränkter Anwendungsbereich

Durch die Regelung zum räumlichen Anwendungsbereich des Gesetzes (§ 2 Absatz 4 ABDSG-E) wird eine Umgehung der nationalen Regelungen erleichtert.

Demnach fänden die Vorschriften nicht auf Anbieter Anwendung, die vom Ausland aus personenbezogene Daten im Inland verarbeiten.

2.3.1.5 Zweckerweiterung und Verstoß gegen Verhältnismäßigkeitsgrundsatz

Durch die teilweise unverhältnismäßigen und unbestimmten Tatbestände für die Verarbeitung personenbezogener Daten durch öffentliche Stellen im ABDSG-E (insbesondere § 4 ABDSG-E) sowie die vorgesehene Erweiterung der Möglichkeiten, Daten auch zu anderen Zwecken als jenen, zu denen sie erhoben worden sind, zu verarbeiten (vergleiche § 6 ABDSG-E), wird der bisher mit dem BDSG vorgehaltene Datenschutzstandard mit dem ABDSG-E nicht mehr erreicht. Die Vorschrift zur Verarbeitung personenbezogener Daten durch öffentliche Stellen ist zu undifferenziert und wahrt nicht das Prinzip der Verhältnismäßigkeit. Insbesondere fehlt es an der Bestimmtheit und Normenklarheit. Die verfassungsrechtlich unabdingbare Klarstellung aus § 14 Absatz 1 BDSG, dass jeder öffentlichen Stelle die Datenverarbeitung nur dann erlaubt ist, wenn sie für eine Aufgabe erforderlich ist, für die die jeweilige öffentliche Stelle sachlich, funktional und örtlich zuständig ist, wurde nicht übernommen.

Die Vorschrift unterscheidet auch nicht mehr zwischen den einzelnen Verarbeitungsformen und ihren jeweiligen Zwecken. Ebenfalls zu weit geht die von § 4 ABDSG-E eröffnete Möglichkeit, dass beispielsweise ein Gesundheitsamt, allgemein und auch präventiv ohne konkreten Anlass, Daten zur Abwehr von Gefahren für die öffentliche Sicherheit oder aber, stellvertretend, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, speichern könne.

Die Vorschriften bieten ein Einfallstor für die relativ undifferenzierte Speicherung einer Vielzahl von Daten auf Vorrat. Die Begriffe "Netz-, Daten- und Informationssicherheit" in § 4 Absatz 2 Nummer 8 ABDSG-E sind nur wenig bestimmt und eine Befristung der Speicherdauer fehlt. Die bisherige Systematik des

Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze knüpft daran an, dass es für die konkrete Datenverarbeitung zur Aufgabenerfüllung weniger darauf ankommt, ob eine Aufgabe im öffentlichen Interesse liegt, als vielmehr darauf, ob der jeweiligen öffentlichen Stelle diese Aufgabe durch Gesetz zugewiesen ist. Diese Systematik sollte beibehalten werden.

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Daher ist die Zweckbindung in Artikel 8 Absatz 2 der Europäischen Grundrechtecharta als tragendes Prinzip des Datenschutzes verankert. Die Einhaltung der Zweckbindung ist ein Kernpunkt für ein funktionierendes Datenschutzrecht (vergleiche Kernpunkte der Datenschutzkonferenz zu den Trilogverhandlungen).

Zweifelhaft ist bereits, ob der nationale Gesetzgeber überhaupt ermächtigt ist, die Ausnahmen von der Zweckbindung in § 6 ABDSG-E auch für den nicht öffentlichen Bereich zu definieren. Jedenfalls sind Zweckänderungen bei nicht öffentlichen Stellen in deutlich weniger Fällen zulässig als bei öffentlichen Stellen. Viele der in § 6 ABDSG-E genannten Zwecke können allenfalls für öffentliche Stellen innerhalb der jeweiligen Zuständigkeit gelten. Zudem führt die Vielzahl und weite Fassung der Ausnahmen zu einer völligen Aufweichung des Regel-Ausnahme-Prinzips. Die vorgesehenen Zweckerweiterungen bedürfen einer eingehenden Kontrolle hinsichtlich ihrer Zulässigkeit. Bei erlaubten Zweckänderungen ist das Prinzip der Verhältnismäßigkeit und der Ausnahmecharakter von Artikel 6 Absatz 4 DSGVO zu wahren.

2.3.1.6 Berufsgeheimnisträger

Mit der Regelung in § 36 ABDSG-E überschreitet der nationale Gesetzgeber seine Regelungskompetenz. Schon die Voraussetzungen aus den Artikeln 23 und 90 DSGVO liegen nicht vor. Der Regelungsbereich müsste danach differenzieren, ob es um die Datenschutzrechte derjenigen Person geht, die durch die Geheimhaltungspflicht geschützt wird, oder um Auskunftsbegehren oder andere datenschutzrechtliche Begehren eines Dritten. Allenfalls im letzteren Fall wäre das Datenschutzrecht mit der Geheimhaltungspflicht abzuwägen.

Für die Beschränkung der Betroffenenrechte in § 36 Seite 1 Buchstabe a ABDSG-E besteht eine Öffnungsklausel nach Artikel 23 Absatz 1 DSGVO, die unzureichend ausgefüllt wird. Auch ist die Einhaltung der Voraussetzungen fraglich, da die Ausnahmen nach dem Wortlaut auch für die von den Geheimhaltungspflichten selbst geschützten Personen gelten.

Soweit es um die (Auskunfts-)Rechte von Dritten geht, wird nach gegenwärtigem Recht die Besonderheit der Schweigepflicht des Auskunftspflichtigen gemäß § 34 Absatz 7 in Verbindung mit § 33 Absatz 2 Satz 1 Nummer 3 BDSG berücksichtigt. Nach § 34 Absatz 7 BDSG besteht eine Pflicht zur Auskunftserteilung nicht, wenn der Betroffene nach § 33 Absatz 2 Satz 1 Nummern 2, 3 BDSG nicht zu benachrichtigen ist. Gemäß § 33 Absatz 2 Nummer 3 BDSG entfällt die Pflicht zur Benachrichtigung, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen. Das ist zum Beispiel dann der Fall, wenn die begehrte Auskunft die anwaltliche Schweigepflicht des Auskunftspflichtigen gemäß § 43a Bundesrechtsanwaltsordnung (BRAO) berührt. Hier überwiegt das Recht des Rechtsanwalts auf ungestörte Berufsausübung das Interesse des Betroffenen auf Auskunftserteilung, weil der Betroffene die von ihm begehrten Informationen grundsätzlich auf direktem Weg durch Inanspruchnahme der Mandanten des Rechtsanwalts auf Auskunftserteilung erhalten kann.

Eine zusätzliche Beschränkung der Rechte der betroffenen Person gemäß Artikel 23 Absatz 1 Seite 2 DSGVO in § 36 Seite 1 Buchstabe a ABDSG-E ist abzulehnen.

Die Regelung in § 36 Seite 1 Buchstabe b ABDSG-E ist ebenso wenig zulässig. Eine gesonderte Regelung für Beschränkungen der Aufsicht bei Berufsgeheimnisträgern ist weder notwendig noch verhältnismäßig, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.

Eine Beschneidung der Aufsichtskompetenzen in diesem Bereich ist daher nicht indiziert. Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie zum Beispiel Gesundheitsdaten, verarbeitet. Weder die Betroffenenrechte, noch die unterstützende Kontrollkompetenz der Datenschutzbeauftragten, dürfen hier beschnitten werden. Vielmehr ist eine wirksame datenschutzrechtliche Kontrolle, auch von Amts wegen, besonders von Nöten. Mit der Regelung in § 36 ABDSG-E wäre insbesondere in Fällen, in denen standesrechtliche Verstöße auf der Nichteinhaltung der Verschwiegenheitspflicht beruhen – bisher ein typischer datenschutzrechtlicher Prüffall bezogen auf Ärzte – eine aufsichtsrechtliche Tätigkeit unmöglich, wenn sich der Berufsgeheimnisträger auch gegenüber der Aufsichtsbehörde auf die Verschwiegenheit berufen könnte.

Die Grundsätze, die das Bundesverfassungsgericht (BVerfG) in seinem Urteil vom 12. April 2005 (BVerfG, Beschluss vom 12. April 2005 – 2 BvR 1027/02 – siehe Entwurfsbegründung) hervorgehoben hat und bei dem es um den Schutz der Verschwiegenheit im anwaltlichen Mandatsverhältnis gegenüber der Beschlagnahme durch staatliche Ermittlungsbehörden ging, sind nicht auf die Kontrolle durch unabhängige Aufsichtsbehörden übertragbar. Die Aufgabe der unabhängigen Aufsichtsbehörden besteht gerade in der Überprüfung der Geheimhaltung und der Einhaltung der datenschutzrechtlichen Anforderungen und nicht in der Verfolgung sonstiger Straftaten.

Wie bisher soll sich die Kontrollbefugnis der Datenschutzaufsichtsbehörden aufgrund der Regelungen in § 38 Absatz 3, 4 in Verbindung mit § 24 Absatz 6, 2 Seite 1

Nummer 2 BDSG auch auf personenbezogene Daten beziehen, die einem Berufsgeheimnis unterliegen. Danach schränkt die anwaltliche Verschwiegenheitspflicht die Informationsrechte der Aufsichtsbehörden, die für die Datenschutzkontrolle zuständig sind, nicht ein ("Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte", Beschluss des Düsseldorfer Kreises vom 8. und 9. November 2007). Dementsprechend sind Rechtsanwälte nicht anders zu behandeln, als jeder andere Berufszweig und als jede andere Gruppe von Freiberuflern (Thilo Weichert, Datenschutz auch bei Anwälten?, Neue Juristische Wochenschrift 2009, 550 [552]).

Auch die Einschränkung der Rechte Dritter (siehe oben) muss durch eine starke Kontrolle durch die Aufsichtsbehörden kompensiert werden. Auch diesem Zweck dient der gegenwärtige § 24 Absatz 2 Seite 1 Nummer 2 BDSG. Zur Vermeidung von indirekter Ausforschung über die Aufsichtsbehörde könnte eine dem § 19 Absatz 6 BDSG entsprechende Regelung getroffen werden, wonach – wie es bisher etwa im Bereich strafrechtlicher Ermittlungsverfahren bewährte Praxis ist – die Aufsichtsbehörde dem Betroffenen nur mitteilt, ob datenschutzrechtliche Verstöße festgestellt wurden, nicht aber, ob und welche Daten die verantwortliche Stelle verarbeitet.

Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern dürfen weder die Betroffenenrechte noch die unterstützende Kontrollkompetenz der Datenschutzbeauftragten beschnitten werden.

Die Regelung des § 36, Seite 2 ABDSG-E ist unbestimmt und zu weitreichend. Sie ist daher zu überarbeiten.

2.3.1.7 Datenverarbeitung zu wissenschaftlichen und statistischen Zwecken

Ein weiteres Beispiel für das sinkende Schutzniveau findet sich in § 34 Absatz 1 ABDSG-E. Dieser bleibt hinter den Anforderungen des § 14 Absatz 2, Nummer 9 und Absatz 5 Nummer 2 BDSG, insbesondere für besondere personenbezogene Daten, zurück. Bislang ist bei der Verarbeitung personenbezogener Daten zu Forschungszwecken in der Regel eine Einwilligung der betroffenen Personen erforderlich. Nur ausnahmsweise und unter engen gesetzlichen Voraussetzungen kann auf diese verzichtet werden.

Gemessen etwa an den differenzierten Regelungen des § 40 BDSG und in Artikel 89 Absatz 1 Seite 4 DSGVO wird hier beispielsweise auf die gesetzliche Normierung eines "Stufenverhältnisses" (in der Regel Verarbeitung anonymisierter Daten; nur wenn dies nicht geht: Verarbeitung pseudonymisierter Daten; nur wenn das nicht geht: Verarbeitung personenbezogener Daten; die beiden letzten Stufen allerdings nur unter der Voraussetzung weiterer konkret normierter Anforderungen) verzichtet. Wie die langjährige Erfahrung im Forschungsbereich zeigt, ist eine solche gesetzlich verankerte Differenzierung als Ausformung des Erforderlichkeitsgrundsatzes jedoch unverzichtbar.

Der § 34 ABDSG-E unterscheidet nicht mehr zwischen sonstigen und besonderen personenbezogenen Daten und lässt bereits ein überwiegendes wissenschaftliches Interesse für die Verarbeitung auch sensibler Daten, wie genetischer, biometrischer und Gesundheitsdaten, ohne Einwilligung des Betroffenen, genügen. Zudem fehlen Vorgaben zu Sicherungsmaßnahmen und technisch-organisatorischen Maßnahmen.

Das Verhältnis der Regelungen zur Datenverarbeitung zu statistischen Zwecken zu den spezialgesetzlichen Statistikgesetzen ist unklar und enthält in der vorliegenden Form inkonsistente Doppelregelungen.

2.3.2 Stellung der unabhängigen Datenschutzaufsichtsbehörden der Länder

Die Einführung eines Klagerechts für die unabhängigen Datenschutzaufsichtsbehörden wird begrüßt, bedarf aber einer Erweiterung. Die Ausgestaltung der Regelungen zur Vertretung der Aufsichtsbehörden im Europäischen Datenschutzausschuss und zur Zusammenarbeit ist zwischen der BfDI und den unabhängigen Aufsichtsbehörden der Länder umstritten, bedarf aber in jedem Fall der Überarbeitung.

2.3.2.1 Klagerecht

Die Schaffung eines Klagerechts, wie in § 28 ABDSG vorgesehen, wird begrüßt. Vor dem Hintergrund der Möglichkeiten in Artikel 58 Absatz 5 DSGVO und Artikel 47 Absatz 5 JI-Richtlinie ist der Anwendungsbereich jedoch zu eng. Durch die Verwendung des allgemeinen Begriffes "Verstöße" in den Artikel 58 Absatz 5 DSGVO und Artikel 47 Absatz 5 JI-Richtlinie kommt der Wunsch des europäischen Verordnungsgebers beziehungsweise Richtliniengebers zum Ausdruck, für möglichst viele Maßnahmen den Rechtsweg zu eröffnen. Dies betrifft nicht nur Angemessenheitsentscheidungen nach Artikel 45 DSGVO, sondern auch andere Rechtsakte der Kommission, wie beispielsweise Standardvertragsklauseln und andere abstrakt-generelle Regelungen, unabhängig davon, ob diese von der Europäischen Kommission oder vom nationalen Gesetzgeber erlassen werden. Insbesondere muss eine abstrakte Klärung unabhängig vom Vorliegen einer Beschwerde von Betroffenen möglich sein. Eine Erweiterung des Klagerechts in diesem Sinne würde es dem Europäischen Gerichtshof (EuGH) ermöglichen, die unionsweit einheitliche Rechtsanwendung zu kontrollieren und somit zur Harmonisierung des Datenschutzrechts beizutragen.

2.3.2.2 Vertretung im Europäischen Datenschutzausschuss

Wie die Vertretung im Europäischen Datenschutzausschuss zu erfolgen hat, ist zwischen der BfDI und den unabhängigen Datenschutzaufsichtsbehörden der Länder umstritten.

Die Formulierung in § 29 ABDSG-E entspreche aus Sicht der Aufsichtsbehörden der Länder nicht der föderalen Kompetenzordnung des Grundgesetzes. § 29 Absatz 2 ABDSG-E sei bereits missverständlich formuliert. Nach der Gesetzesbegründung könne der Stellvertreter "gemäß Absatz 2 von dem gemeinsamen Vertreter verlangen, die Verhandlungsführung und das Stimmrecht übertragen zu erhalten, soweit die Angelegenheit in die sachliche Alleinzuständigkeit der Länderaufsichtsbehörden fällt". Die Gesetzesbegründung knüpfe demnach an die Vollzugstätigkeit an. Der Gesetzesvollzug ist im Datenschutz überwiegend den Ländern übertragen. Der Gesetzeswortlaut beziehe sich hingegen eher auf die ausschließliche Gesetzgebungskompetenz der Länder. Wegen der vielfach konkurrierenden Gesetzgebungskompetenz könne damit das Stimmrecht bei der BfDI verbleiben, obgleich die Vollzugszuständigkeit bei den Ländern liege.

Für die Anknüpfung an die Vollzugskompetenz spreche zunächst, dass die Vertretung im Ausschuss Verwaltungshandeln betreffe und die Verwaltung nach den Vorgaben des Grundgesetzes grundsätzlich Angelegenheit der Länder sei. Die überwiegende Mehrheit der im Ausschuss zu behandelnden Angelegenheiten dürfte die Datenschutzaufsicht gegenüber nicht öffentlichen Stellen betreffen. Diese sei und bleibe im Wesentlichen den Aufsichtsbehörden der Länder vorbehalten. Diese seien die für die nicht öffentlichen Stellen in Artikel 51 Absatz 1 DSGVO genannten unabhängigen Aufsichtsbehörden und unterlägen selbst der Verpflichtung nach Artikel 51 Absatz 2 DSGVO, einen Beitrag zur einheitlichen Anwendung der DSGVO zu leisten ("Jede Aufsichtsbehörde"). Damit liege es nach der bundesstaatlichen Aufgabenverteilung mehr als nahe, in allen Angelegenheiten, die diese Zuständigkeit der Länder betreffen, entsprechend der Gesetzesbegründung dem Vertreter der Länder auf dessen Verlangen die Verhandlungsführung und das Stimmrecht zu übertragen. Nur so könnten ein Leerlaufen des Länderstimmrechts und ein Widerspruch mit der Vollzugspraxis der Länder verhindert werden.

Auch das Konzept, wonach die beziehungsweise der Bundesdatenschutzbeauftragte (BfDI) dauerhaft als Vertreterin beziehungsweise Vertreter gesetzt ist, während die Stellvertretung stets der Ländervertretung zufällt, erscheine vor dem Hintergrund der aufsichtsbehördlichen Landeskompetenzen nicht plausibel.

Die Unabhängigkeit der Datenschutzbeauftragten lege zudem eine Wahl des Ländervertreters durch die Aufsichtsbehörden der Länder selbst nahe.

Demgegenüber begrüßt die BfDI die in § 29 Absatz 1 ABDSG-E festgelegte Zuweisung der Aufgabe des gemeinsamen Vertreters nach Artikel 68 Absatz 4 DSGVO an die BfDI und unterstützt die in der Begründung dafür genannten Gründe. Die Stellung des Landesvertreters als Stellvertreter im Sinne von Artikel 68 Absatz 3 DSGVO begegne aus ihrer Sicht ebenfalls keinen Einwänden.

Die Zuständigkeitsübertragung auf den Landesvertreter (§ 29 Absatz 2 ABDSG-E) regele nach ihrer Auffassung drei Fallvarianten, in denen die BfDI dem Landesvertreter die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss (EDSA) übertragen müsse. Dies sei neben der ausschließlichen Gesetzgebungszuständigkeit der Länder und der Einrichtung von

Landesbehörden auch "das Verfahren von Landesbehörden". Die BfDI legt der Formulierung des Gesetzestextes das Verständnis zugrunde, dass mit "Verfahren von Landesbehörden" nicht dasjenige vor den Aufsichtsbehörden im Sinne von § 27 ABDSG-E gemeint sei, sondern allgemein das Verfahren von (anderen) Landesbehörden, das heißt der öffentliche Bereich der Länder. Um dies deutlich zu machen und jeden Zweifel auszuschließen, solle die Begründung eindeutig und präzise klarstellen, dass sich "Verfahren von Landesbehörden" ausschließlich auf solche außerhalb der Datenschutzaufsichtsbehörden beziehe und deren Verfahren (das heißt der nicht öffentliche Bereich) hier nicht gemeint seien. Die BfDI hält die Übertragung der Aufgabe des gemeinsamen Vertreters auf an ihre Behörde auch für sachgerecht, da sie die notwendige Kontinuität sichern könne, eine langjährige Erfahrung im Bereich des europäischen Datenschutzes habe und am ehesten über die erforderlichen Ressourcen verfüge.

Einigkeit besteht darüber, dass eine Klarstellung im Gesetz wünschenswert ist, wonach der Gemeinsame Vertreter und sein Stellvertreter sich bei Abwesenheit gegenseitig vertreten können, was eine Vertretung durch Mitarbeiter jedoch nicht ausschließt.

2.3.2.3 Einrichtung einer zentralen Anlaufstelle

Hinsichtlich der Einrichtung der zentralen Anlaufstelle bei der BfDI (vergleiche § 29 Absatz 1 Seite 1 ABDSG-E) ist eine Klarstellung erforderlich, dass die zentrale Anlaufstelle nicht selbst Aufgaben wahrnimmt, für die die anderen Aufsichtsbehörden (namentlich die Aufsichtsbehörden der Länder nach § 27 ABDSG-E) zuständig sind, sondern dass der zentralen Anlaufstelle allein eine unterstützende Funktion zukommt. Ausweislich des Wortlauts des Erwägungsgrunds 119 DSGVO soll die zentrale Anlaufstelle die Beteiligung der anderen in einem Mitgliedstaat existierenden Datenschutzaufsichtsbehörden sicherstellen, nicht jedoch selbst die Beteiligung wahrnehmen oder ersetzen. Aus Gründen der Rechtsklarheit ist dies im Gesetzestext selbst zu verdeutlichen. Es muss sichergestellt sein, dass auch die Aufsichtsbehörden der Länder nach § 27 ABDSG-E in gleicher Weise effektiv an der Willensbildung im Europäischen Datenschutzausschuss teilnehmen können, wie bislang im Rahmen der Artikel-29-Gruppe und deren Arbeitsgruppen. Auch wenn die zentrale Anlaufstelle von der BfDI bereitgestellt wird, ist eine eindeutige Trennung im Hinblick auf Organisation und Berichtspflichten zwischen der zentralen Anlaufstelle und dem übrigen Personal der BfDI unerlässlich. Als Modell könnte insoweit die Stellung des Sekretariats des Europäischen Datenschutzausschusses (Artikel 75 DSGVO) dienen, das vom Europäischen Datenschutzbeauftragten bereitgestellt wird. Ähnlich wie das Sekretariat nimmt auch die zentrale Anlaufstelle nur unterstützende Aufgaben wahr. Leitlinie für die zentrale Anlaufstelle muss es sein, ein Gleichgewicht in Hinblick auf die effektive Mitwirkung aller deutschen Datenschutzaufsichtsbehörden an der Willensbildung im Europäischen Datenschutzausschuss auch an dieser Stelle zu gewährleisten.

2.3.2.4 Zusammenarbeit

Hinsichtlich der in § 30 ABDSG-E getroffenen Regelungen über die Zusammenarbeit wird auf den Beschluss "Vorschläge zu ersten Strukturfolgerungen aus der DSGVO" nebst Ablage der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6. und 7. April 2016 in Schwerin verwiesen.

Danach sind Zuständigkeitsregelungen sowie die Beteiligung in den Verfahren der Zusammenarbeit und der Kohärenz, soweit sie Außenwirkung entfalten, durch Gesetz zu treffen. Dieses sollte sich darauf beschränken, die Aufsichtsbehörden zu verpflichten in den erforderlichen Fällen eine Abstimmung mit dem Ziel der einheitlichen Votierung vorzunehmen. Die Einzelheiten sollten die unabhängigen Aufsichtsbehörden autonom regeln.

Eine weitergehende Stellungnahme hierzu ist beabsichtigt.

2.3.2.5 Ergänzung zur örtlichen Zuständigkeit

Wünschenswert ist schließlich eine Klärung der örtlichen Zuständigkeit im nicht öffentlichen Bereich, soweit kein grenzüberschreitender Bezug vorliegt. Bei der örtlichen Zuständigkeit der Aufsichtsbehörden weichen derzeit Praxis und Recht gelegentlich voneinander ab. Die Verwaltungsverfahrensgesetze der Länder legen in der Regel eine Anknüpfung an die Betriebsstätte nahe, während verbreitete Praxis der Aufsichtsbehörden eine Orientierung am Sitz der verantwortlichen Stelle ist. Beides ist inkompatibel mit dem Prinzip der DSGVO, an der Hauptniederlassung anzuknüpfen.

2.3.3 Beschäftigtendatenschutz

Es wird begrüßt, dass das ABDSG-E von der Regelungsbefugnis des Artikel 88 DSGVO zumindest durch Übernahme der bisherigen Regelungen des BDSG Gebrauch macht, insbesondere vor dem Hintergrund, dass sich die Ausgestaltung der Beschäftigungsverhältnisse in Deutschland deutlich von der in anderen Mitgliedstaaten unterscheidet. Das Arbeitsrecht im weitesten Sinne ist ein stark national geprägter Rechtsbereich, weshalb bewährte Mechanismen und Grundsätze trotz europäischer Harmonisierung soweit möglich beibehalten werden sollten. Die Forderung eines bereichsspezifischen Beschäftigtendatenschutzes bleibt bestehen. Deshalb kann die Übernahme der bisherigen Regelung auch in Hinblick auf die zu beachtenden Anforderungen des Artikels 88 Absatz 2 DSGVO nur als Merkposten für die Schaffung eines überzeugenden nationalen Beschäftigtendatenschutzes gelten.

2.3.4 Betriebliche Datenschutzbeauftragte

Zuzustimmen ist auch den Regelungen in den §§ 14 folgende ABDSG-E zum betrieblichen Datenschutzbeauftragten. Jedoch sollte das Merkmal der Zuverlässigkeit (keine Interessenskollision, persönliche Integrität) ergänzt und

sichergestellt werden, dass die bisherigen flankierenden Regelungen, wie zum Beispiel zum Abberufungsschutz (vergleiche § 4f Absatz 3 Seite 4 BDSG), vollumfänglich erhalten bleiben. Die Pflicht zur Meldung der beziehungsweise des benannten Datenschutzbeauftragen sollte auch weiterhin gegenüber der zuständigen Aufsichtsbehörde bestehen (§ 14 Absatz 4 Seite 1 und Seite 2 ABDSG-E).

2.3.5 Akkreditierung

Die Doppelzuständigkeit für die Akkreditierung in § 16 ABDSG-E ist hinsichtlich einer gleichmäßigen Akkreditierung kontraproduktiv. Die Akkreditierung sollte vorzugsweise denjenigen Stellen überlassen werden, welche über große Expertise und Kenntnisse im Bereich des Datenschutzes verfügen. Dies sind die Fachaufsichtsbehörden für den Datenschutz, welche einheitliche Akkreditierungskriterienkataloge erstellen und im Rahmen eines einheitlichen Akkreditierungsverfahrens anwenden.

2.3.6 Videoüberwachung

Die Verarbeitung durch Videoüberwachung erhobener personenbezogener Daten durch öffentliche Stellen des Bundes ist nur unzureichend geregelt. Es fehlen Regelungen zur Erhebung der Daten, was insbesondere auch dann relevant wird, wenn eine Beobachtung ohne Speicherung erfolgt, sowie zur Weiterverarbeitung gespeicherter Daten zu anderen Zwecken. Die entsprechenden Regelungen aus dem BDSG werden nicht vollständig übernommen. Notwendig sind insbesondere die Normierung einer engen Zweckbestimmung sowie die ausdrückliche Verankerung des Erforderlichkeitsprinzips und Verhältnismäßigkeitsprinzips. Zudem sind die Regelungen zur Einschränkung der Informationspflichten zu weitgehend und bleiben hinter dem Datenschutzniveau der DSGVO zurück.

So regelt § 7 Absatz 3 Seite1 ABDSG-E, dass die Informationspflicht bei öffentlicher und nicht öffentlicher Videoüberwachung entfällt. Der § 7 Absatz 3 Seite 2 ABDSG-E bestimmt, dass in diesem Fall der Umstand der Beobachtung und der Verantwortliche durch geeignete Maßnahmen erkennbar gemacht werden soll. Insoweit ist § 7 Absatz 3 Seite 2 ABDSG-E fast wortgleich mit § 6 b Absatz 2 BDSG. Die Erkennbarmachung der Videoüberwachung erfolgt in der Praxis zum Beispiel durch Anbringen eines Piktogramms gemäß Deutscher Industrienorm (DIN) 33450 in Verbindung mit der Anschrift der verantwortlichen Stelle.

Die (umfassendere) Informationspflicht gemäß Artikel 13 DSGVO wird nunmehr bezüglich der Videoüberwachung durch öffentliche wie auch durch nicht öffentliche Stellen eingeschränkt. Das Recht auf Information aus Artikel 13 Absatz 3 und 4 DSGVO soll gemäß § 7 Absatz 2 ABDSG-E entfallen, soweit die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde. Diese Beschränkung der Informationspflicht diene – so der Entwurf – dem Schutz der Rechte und Freiheiten anderer Personen (Artikel 23 Absatz 2 Buchstabe c und Absatz 1 Buchstabe i DSGVO).

Damit verkennt der Gesetzentwurf die Intention des Artikels 23 DSGVO.

Nach der Gesetzessystematik der DSGVO können Pflichten und Rechte der DSGVO gemäß Artikel 23 beschränkt werden. Dazu gehören auch die Informationspflichten gemäß Artikel 13 DSGVO. Diese Beschränkungen dürfen jedoch nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren und müssen eine in der demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen. Diese Maßnahmen sollen nach Artikel 23 Absatz 1 Buchstaben a-h DSGVO öffentliche Belange der Sicherheit, Justiz und des Ordnungsrechts sicherstellen. Artikel 23 Absatz 1 Buchstaben i und j DSGVO betreffen den privaten Bereich. Artikel 23 Absatz 1 Buchstabe I DSGVO soll den Schutz der betroffenen Personen oder der Rechte und Freiheiten anderer Personen sicherstellen.

Die Beschränkung der Informationspflichten durch § 7 Absatz 2 ABDSG-E wegen unverhältnismäßigen Aufwandes der Informationserteilung schafft hingegen nur Erleichterungen für den Verantwortlichen der Videoüberwachung. Dies widerspricht aber gerade Sinn und Zweck des Artikels 23 DSGVO. Hiernach soll der Schutz der betroffenen Personen und der Rechte und Freiheiten anderer Personen durch die Beschränkung sichergestellt werden.

Im Entwurf wird zudem nur geregelt, dass der Verantwortliche Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person zu ergreifen hat. Gemäß Artikel 23 Absatz 2 DSGVO müssen dafür aber gegebenenfalls spezifische Vorschriften in Bezug auf den Umfang der vorgenommenen Beschränkung geschaffen werden. Die Überleitung des Schutzzwecks der Maßnahme auf die verantwortliche Person ist vor dem Hintergrund des Artikels 23 DSGVO nicht ausreichend, weil eine konkretisierende Regelung wie in Artikel 14 Absatz 5 Buchstabe b DSGVO fehlt.

Nicht mehr vorgesehen ist eine Regelung wie in § 6b Absatz 4 BDSG über die Informationspflicht für den Fall, dass die Daten aus einer Videoüberwachung einer bestimmten Person zugeordnet werden. Hierbei handelt es sich um eine Identitätsverknüpfung, von der die betroffene Person nicht mit einem bloßen Hinweis auf die Videoüberwachung Kenntnis erlangen kann. Der Schutz der Rechte der betroffenen Personen wird mit dieser Regelung keinesfalls sichergestellt.

Schließlich sollte, soweit dies nach den Öffnungsklauseln möglich ist, eine Regelung beziehungsweise Klarstellung in Bezug auf ein Verbot der heimlichen Videoüberwachung erfolgen.

2.3.7 Auskunfteien

Die Übernahme der Vorschrift des § 28a BDSG entspricht dem ganz überwiegenden Wunsch der Aufsichtsbehörden, auch wenn die europarechtliche Anknüpfung diskutiert wird. Sie wird daher grundsätzlich begrüßt.

Die Löschfristen für Auskunfteien in § 35 Absatz 2 Seite 2 Nummer 4 BDSG sowie die Regelung zur Auskunftserteilung nach § 34 Absatz 8 BDSG sollten ebenfalls übernommen werden.

2.3.8 Scoring

Zuzustimmen ist auch der Übernahme von § 28b BDSG. Die entsprechende Regelung bedarf aber einer deutlichen Verbesserung.

2.4 Regelungen zur Durchsetzbarkeit der DSGVO

Nach Artikel 58 Absatz 5 DSGVO muss jeder Mitgliedstaat durch Rechtsvorschriften dafür sorgen, dass die jeweiligen unabhängigen Aufsichtsbehörden die DSGVO in den Mitgliedstaaten auch durchsetzen können. Dieser Aufforderung sollte insbesondere im Bereich der Verwaltungsvorschriften und Bußgeldvorschriften Rechnung getragen werden.

2.4.1 Verwaltungsverfahren

Die DSGVO muss gegenüber öffentlichen und nicht öffentlichen Stellen gleichermaßen durchsetzbar sein. Insoweit unterscheidet die DSGVO nicht. Es fehlt daher zunächst eine Regelung zur Vollstreckung von Verwaltungsakten gegenüber Behörden und sonstigen öffentlichen Stellen. § 17 Verwaltungs- und Verfassungsgesetz (VwVG) schließt, ebenso wie die meisten Verwaltungsvollstreckungsregelungen der Landesgesetze, unter Berücksichtigung des koordinationsrechtlich geprägten Verhältnisses zwischen Hoheitsträgern den Vollzug gegen Behörden und juristische Personen des öffentlichen Rechts aus, soweit nicht etwas anderes bestimmt ist. Hier besteht Handlungsbedarf. Einerseits bedarf es zumindest einer Klarstellung, ob entsprechend der Regelung in § 42 Absatz 3 Seite 2 ABDSG-E die Vollstreckung gegen öffentliche Stellen, die mit anderen Verarbeitern im Wettbewerb stehen, möglich ist. Darüber hinaus ist es mit den Grundsätzen der DSGVO kaum vereinbar, wenn den Aufsichtsbehörden gegenüber Behörden und sonstigen öffentlichen Stellen im Sinne des § 2 Absatz 1 ABDSG-E kein Mittel zur Seite gestellt wird, datenschutzrechtliche Verstöße auch tatsächlich abzustellen. Jedenfalls für gerichtlich festgestellte Verstöße verlangt Artikel 58 Absatz 5 DSGVO, dass der nationale Gesetzgeber die Aufsichtsbehörde in die Lage versetzt, die Bestimmungen dieser Verordnung durchzusetzen und nicht lediglich mögliche Verstöße feststellen zu lassen. Bei dieser bloßen Beanstandung durch die Aufsichtsbehörden verbliebe es aber faktisch, wenn im ABDSG-E keine Regelung aufgenommen wird, die die Vollstreckung gegen Behörden und sonstige öffentliche Stellen zulässt.

Fragwürdig erscheint auch der Ausschluss der Anordnung der sofortigen Vollziehung gegenüber öffentlichen Stellen mit Ausnahme der Wettbewerbsunternehmen. 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 nicht dazu führen, dass wegen der aufschiebenden Wirkung dieser Zustand auf unbestimmte Dauer anhält. Ein Rechtsschutzdefizit der öffentlichen Stellen ist ebenfalls nicht ersichtlich. Wie jeder andere Adressat der aufsichtsbehördlichen Maßnahmen hätten sie die Möglichkeit, gemäß § 80 Absatz 5 Verwaltungsgerichtsordnung (VwGO) die Wiederherstellung der aufschiebenden Wirkung zu beantragen. Ob der in der Begründung als Alternative angesprochene Antrag auf einstweilige Anordnung statthaft wäre, ist zu bezweifeln. Dieser ist ein Rechtsschutzinstrument gegen (drohende) Maßnahmen von Behörden, ermöglicht es aber den Behörden nicht, ihrerseits Aufsichtsbefugnisse im Eilfall mit Hilfe des Gerichts durchzusetzen.

2.4.2 Ordnungswidrigkeitenverfahren

Die Frage, ob Bußgelder gegen Behörden und sonstige öffentliche Stellen verhängt werden können, sollte im Ermessen der Aufsichtsbehörden liegen. Des Weiteren müssen Bußgeldtatbestände und Verweise auf Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) ergänzt werden. Zuzustimmen ist den Regelungen zur Zuständigkeit der Landgerichte und der Verfahrensbeteiligung der Aufsichtsbehörden im gerichtlichen Verfahren.

2.4.2.1 Bußgelder gegen öffentliche Stellen

Vor dem Hintergrund der notwendigen Durchsetzbarkeit der DSGVO ist die Vorschrift in § 42 Absatz 3 ABDSG-E, wonach gegen Behörden und sonstige öffentliche Stellen mit Ausnahme der Wettbewerbsunternehmen keine Bußgelder verhängt werden sollen, zu hinterfragen. Der im Bereich der DSGVO nicht anwendbare § 30 OWiG schließt Bußgelder gegen juristische Personen des öffentlichen Rechts nicht aus, allerdings wird hier immer wieder kritisch angemerkt, dass Bußgelder gegen juristische Personen des öffentlichen Rechts ihre sanktionierende Wirkung verfehlen und Gelder im öffentlichen Haushalt lediglich die Titel wechseln. Für Verstöße gegen die DSGVO kommt hinzu, dass Bußgelder, anders als Zwangsmittel, die Durchsetzung der DSGVO nicht unmittelbar erzwingen können. Allerdings sollte die Entscheidung in das pflichtgemäße Ermessen der unabhängigen Datenschutzaufsichtsbehörden gestellt werden.

2.4.2.2 Weitere Bußgeldtatbestände

Soweit man für § 42 Absatz 1 ABDSG-E eine Regelungskompetenz des nationalen Gesetzgebers bejaht, sollten die auf Mitarbeiter erweiterten Bußgeldtatbestände ausformuliert und nicht lediglich auf Artikel 83 DSGVO verwiesen werden. Geht man

davon aus, dass die Tatbestände, auf die Artikel 83 DSGVO verweist, nur für Verantwortliche oder Auftragsverarbeiter gelten, besteht zwar eine Regelungskompetenz, allerdings muss dann ein neuer Tatbestand formuliert werden, der nicht auf Verantwortliche beschränkt ist. In der derzeitigen Fassung genügt die Vorschrift nicht dem Bestimmtheitsgebot. Geht man indes davon aus, dass Artikel 83 DSGVO nebst Verweisen auch für Mitarbeiter gilt, besteht keine Regelungskompetenz des nationalen Gesetzgebers.

Zudem wird die Bußgeldgrenze ohne nähere Begründung in Anlehnung an die bislang geltende Regelung im BDSG auf 300.000 Euro beschränkt. Wenn man davon ausgehen sollte, dass Mitarbeiter von verantwortlichen Stellen nicht vom Regelungsgehalt des Artikel 83 DSGVO erfasst werden und den Mitgliedstaaten insoweit ein eigenes Regelungsrecht zukommt, sollten sich entsprechende Bußgeldbestimmungen jedenfalls an den in der DSGVO genannten Bußgeldgrenzen orientieren. Da nach Artikel 83 Absatz 1 DSGVO Geldbußen verhältnismäßig sein müssen, besteht auch keine Gefahr der übermäßigen Belastung von Mitarbeitern durch die Festlegung zu hoher Geldbußen für einen von ihnen zu verantwortenden Verstoß.

Darüber hinaus sollten weitere Bußgeldtatbestände ergänzt werden.

Sofern der Gesetzgeber davon ausgeht, dass die DSGVO keinen Bußgeldtatbestand wegen nicht erteilter Auskunft gegenüber der Aufsichtsbehörde enthält, wäre ein solcher entsprechend § 43 I Nummer 10 BDSG zu schaffen. Ohne einen solchen Bußgeldtatbestand ist eine wirksame Aufsichtstätigkeit nicht denkbar. Verstöße gegen die in § 33 ABDSG-E aufgenommene Regelung für die Datenverarbeitung im Beschäftigtenkontext sind ebenfalls nicht explizit bußgeldbewährt. Darüber hinaus fehlt es in § 42 Absatz 2 ABDSG-E an einem Bußgeldrahmen.

2.4.2.3 Zuständigkeit der Landgerichte

Zu befürworten ist die Regelung zur Zuständigkeit des Landgerichts für die Prüfung von Bußgeldbescheiden über 5.000 Euro. Hierfür spricht zum einen die gravierende Erhöhung des Bußgeldrahmens von 300.000 Euro nach dem derzeit geltenden BDSG auf bis zu 20 Millionen Euro beziehungsweise bis zu 4 Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres im Falle eines Unternehmens gemäß Artikel 83 Absatz 4 bis 6 DSGVO. Zum anderen legt dies auch die Übernahme des kartellrechtlichen funktionalen Unternehmensbegriffs in der DSGVO nahe, da die Regelungen zur gerichtlichen Zuständigkeit in Kartellverfahren sogar das Oberlandesgericht als Eingangsinstanz bestimmen (vergleiche § 83 Absatz 1 Gesetz gegen Wettbewerbsbeschränkungen – GWB).

2.4.2.4 Beteiligung der Aufsichtsbehörden im gerichtlichen Verfahren

Ebenfalls zu befürworten ist, dass gemäß § 50 Absatz 1 Seiten 4-8 ABDSG-E zukünftig die Aufsichtsbehörden anstelle der Staatsanwaltschaft direkte Beteiligte in

Gerichtsverfahren über datenschutzrechtliche Bußgeldbescheide werden sollen. Zum einen wird hierbei der Expertise der Aufsichtsbehörden in Datenschutzangelegenheiten Rechnung getragen und somit die Qualität der gerichtlichen Auseinandersetzung bedeutend gestärkt. Zum anderen wird dadurch die in Artikel 52 Absatz 1 DSGVO normierte "völlige" Unabhängigkeit der Aufsichtsbehörden gewährleistet.

2.4.2.5 Anwendbarkeit des Gesetzes für Ordnungswidrigkeiten

Es wird begrüßt, dass die Regelungen des Gesetzes für Ordnungswidrigkeiten (OWiG) nicht pauschal für anwendbar erklärt werden und insbesondere § 130 OWiG keine Anwendung findet. Dem europarechtlich geltenden funktionalen Unternehmensbegriff (vergleiche Artikel 101, 102 Vertrag über die Arbeitsweise der Europäischen Union) wird so hinreichend Rechnung getragen.

Dennoch fehlen Verweise auf Bestimmungen des OWiG. So sollte § 3 OWiG (Bestimmtheitsgebot) für anwendbar erklärt werden. Ferner bestehen keine Bedenken gegen die Anwendung von § 29 OWiG. Die §§ 40-44 OWiG regeln die Zuständigkeit der Staatsanwaltschaft für Strafsachen, die Abgabe an die Staatsanwaltschaft sowie gegebenenfalls die Rückgabe an die Verwaltungsbehörde. Sollte die Staatsanwaltschaft eine Strafsache einstellen, verbliebe für die Aufsichtsbehörde weiterhin die Möglichkeit, ein Bußgeld festzusetzen (§ 41 Absatz 2, § 43 Absatz 1 OWiG). Die Anwendung von § 40 OWiG müsste daher mit der Maßgabe erfolgen, dass eine Einstellung hinsichtlich der die Straftat "begleitenden" Ordnungswidrigkeit nur im Einvernehmen mit der Aufsichtsbehörde möglich ist.

Kritisch gesehen wird auch die Regelung in § 60 ABDSG-E. Da dieser aber auf den Anwendungsbereich der JI-Richtlinie beschränkt ist, erfolgen Ausführungen hierzu wie angekündigt gesondert.

2.5 Gestaltung des Medienprivilegs

Artikel 85 Absatz 2 DSGVO enthält einen Auftrag an die Mitgliedsstaaten, Ausnahmen von bestimmten Kapiteln der DSGVO zu regeln, soweit dies erforderlich ist, um bei der Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen oder literarischen Zwecken das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang zu bringen.

Der Gesetzgeber sollte das so genannte "Medienprivileg" in klaren Regelungen gestalten, um mit praktikablen Kriterien Klarheit über die künftige Reichweite zu schaffen und um hierbei auch die bereits bestehende Rechtsunsicherheit bezüglich der Privilegierung von teilweise redaktionell bearbeiteter Meinungsverbreitung über das Internet zu beseitigen.