Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

AKTENZEICHEN
0.6.9.000/053/2017-00965

DATUM
27. Januar 2017

VERMERK

Stellungnahme des LfDI M-V zum DSAnpUG-EU

Der nunmehr 4. Gesetzentwurf enthält lediglich oberflächliche Schönheitsreparaturen gegenüber den vorangegangenen Entwürfen. Er verkennt nach wie vor die Voraussetzungen und Anforderungen der Öffnungsklauseln. Dies führt insbesondere zu einer exzessiven und unzulässigen Einschränkung der Betroffenenrechte. Problematisch ist zudem, dass öffentliche Stellen hinsichtlich der Durchsetzung (Vollstreckung) nach wie vor gegenüber Unternehmen privilegiert werden und die Befugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern drastisch beschnitten werden. Die Umsetzung der JI-Richtlinie in innerstaatliches Recht ist in weiten Teilen missglückt. Die Befugnisse der Aufsichtsbehörden und die Betroffenenrechte werden in einem Ausmaß eingeschränkt, das nicht mit der JI-Richtlinie vereinbar ist. Zudem wird die Rechtsprechung des Bundesverfassungsgerichts zur Übermittlung personenbezogener Daten in Drittstaaten nur unzureichend berücksichtigt.

Zu § 1 BDSG-E Anwendungsbereich

Absatz 4

Nach der Formulierung in Nr. 2 ist unklar, welches Verfahrensrecht in den Fällen des Art. 56 Abs. 2 DS-GVO anwendbar ist, wenn der Verantwortliche seinen Sitz innerhalb der Europäischen Union hat.

Zu § 3 BDSG-E Verarbeitung personenbezogener Daten durch öffentliche Stelle

§ 3 ist zu streichen. Die Vorschrift hebt den datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt auf und schafft eine Generalklausel für die Datenverarbeitung durch öffentliche Stellen. Gegenüber Art. 6 Abs. 1 lit. e DS-GVO enthält § 3 keine spezifischeren Anforderungen oder präzisere Maßnahmen und verstößt so gegen das Wiederholungsverbot. Mangels notwendiger Bestimmtheit und Abwägung mit den Interessen der betroffenen Person ist § 3 verfassungswidrig und kann den mit der Datenverarbeitung verbundenen Grundrechtseingriff nicht legitimieren.

Zu § 4 BDSG-E Videoüberwachung

Absatz 1

Zur Regelung der Videoüberwachung durch Unternehmen zur Wahrnehmung des Hausrechts fehlt es bereits an einer Öffnungsklausel.

Die Integration des Entwurfs eines „Videoüberwachungsverbesserungsgesetzes“ suggeriert, dass Videoüberwachung durch private Betreiber besonders wichtige Interessen von Dritten, wie Leben, Gesundheit oder Freiheit schützen könnte. Gefahrenabwehr in diesem Sinne ist aber Aufgabe des Staates, die er nicht an Private delegieren kann. Zudem kollidiert die Regelung mit den Versammlungsgesetzen der Länder, die eigene Vorschriften über die Zulässigkeit von Videokameras enthalten.

Absatz 2

Die Wörter *„zum frühestmöglichen Zeitpunkt“* sind zu streichen. Die Formulierung schränkt Art. 13 DS-GVO unzulässiger Weise ein, weil die Voraussetzungen des Art. 23 DS-GVO nicht vorliegen.

Zu § 16 BDSG-E Befugnisse

Absatz 2

Absatz 2 setzt die in Art. 47 der JI-Richtlinie vorgesehenen Abhilfe- und Beratungsbefugnisse der Aufsichtsbehörde nur unzureichend um. Nach Abs 2. hat die/der BfDI im Anwendungsbereich der Richtlinie weder die Befugnis, den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge mit den nach der Richtlinie erlassenen Vorschriften in Einklang zu bringen, noch die Befugnis, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Auch im Anwendungsbereich der JI-Richtlinie muss ein mit der DS-GVO vergleichbares Schutzniveau durch gleichlautende Regelungen sichergestellt werden.

Zu §§ 17, 18 BDSG-E Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

Die in § 17 getroffene Regelung über die Vertretung im Europäischen Datenschutzausschuss (EDSA) verkennt, dass sich der EDSA schwerpunktmäßig mit Themen aus dem nicht-öffentlichen Bereich beschäftigen wird, welche größtenteils in der Zuständigkeit der Länder liegen. Diese Kompetenzverteilung muss bei der Vertretung im EDSA berücksichtigt werden.

Zu § 20 BDSG-E Gerichtlicher Rechtsschutz

Absatz 1

Die Einschränkung auf Art. 78 Abs. 1, 2 DS-GVO und § 56 BDSG-E verwirrt und ist zu eng. Die Vorschrift ist zudem überflüssig. Die Eröffnung des Verwaltungsrechtsweges ergibt sich aus § 40 VwGO.

Absatz 7

Die Regelung ist reine Makulatur und verschleiert, dass gegen öffentliche Stellen nach dem Gesetzentwurf bisher unter Missachtung von Art. 58 Abs. 5 DS-GVO überhaupt keine Vollziehung möglich ist: Nach der gewählten Konstellation, dass die Datenschutzaufsichtsbehörden nur als Beklagte oder Antragsgegner im verwaltungsgerichtlichen Verfahren auftreten können (§ 20 Abs. 5 Nr. 2), richtet sich eine mögliche Vollstreckung auch eines vom Verwaltungsgericht bestätigten Verwaltungsaktes allein nach dem Verwaltungsvollstreckungsgesetz (VwVG) bzw. entsprechenden landesrechtlichen Regelungen. Diese schließen den Vollzug gegen Behörden grundsätzlich aus (vgl. § 17 VwVG), soweit ein Spezialgesetz nichts anderes bestimmt, vorliegend also das BDSG-E eine Vollstreckung gegen öffentliche Stellen zulässt. Fehlt diese Regelung, bleibt es trotz theoretischer Anordnungsbefugnis der Datenschutzaufsichtsbehörden faktisch bei der bisherigen, nicht immer wirksamen, Beanstandung gegenüber öffentlichen Stellen. Diese Ungleichbehandlung zwischen Unternehmen und öffentlichen Stellen, ist, jedenfalls soweit es die Durchsetzbarkeit der DS-GVO betrifft, mit dieser nicht vereinbar. Absatz 7 muss daher zunächst grundsätzlich die Vollstreckung gegenüber öffentlichen Stellen regeln, bevor die Anordnung der sofortigen Vollziehung (die nur die Voraussetzung für die Vollstreckung eines Grundverwaltungsaktes im Wege eines mehraktigen Vollstreckungsverfahrens schafft) thematisiert werden kann. Zudem sind auch im öffentlichen Bereich Fälle wahrscheinlich, in denen die Anordnung der sofortigen Vollziehung notwendig ist, um die Rechte

der betroffenen Person zu wahren. Angesichts der Dauer verwaltungsgerichtlicher Streitigkeiten ist diese Möglichkeit in dringenden Eilfällen unverzichtbar. Ordnet die/der BfDI beispielsweise die Beseitigung einer Sicherheitslücke im 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 seitens der öffentlichen Stellen ist nicht ersichtlich. Wie jeder andere Adressat aufsichtsbehördlicher Maßnahmen hätten sie die Möglichkeit, gemäß § 80 Abs. 5 VwGO die Wiederherstellung der aufschiebenden Wirkung zu beantragen. Eine andere Möglichkeit, als durch die Anordnung der sofortigen Vollziehung der Datenschutzaufsichtsbehörden im Eilrechtsschutz die Rechte der betroffenen Person zu wahren, besteht wegen § 123 Abs. 5 VwGO nicht.

Im Übrigen fehlt eine Vorschrift zur Vollstreckung auch gegenüber Unternehmen. Die sonst anzuwendenden vollstreckungsrechtlichen Regelungen enthalten Beschränkungen hinsichtlich der Zwangsgeldhöhe (nach § 11 VwVG 25.000 €), die in Relation mit den Bußgeldtatbeständen der DS-GVO einer effektiven Durchsetzung der DS-GVO entgegenstehen.

Zu § 22 BDSG-E Verarbeitung besonderer Kategorien personenbezogener Daten

Die Regelung verstößt gegen das Wiederholungsverbot. Von bestehenden Öffnungsklauseln wird über deren Reichweite hinaus und unter Missachtung deren Anforderungen Gebrauch gemacht. Die Öffnungsklauseln in Art. 9 Abs. 2 lit. b, g, h, i, j DS-GVO ermöglichen den Mitgliedstaaten in ihren Spezialgesetzen (z. Bsp.: SGB, AMG), die in Art. 9 Abs. 2 DS-GVO abstrakt gehaltenen Verarbeitungen zu konkretisieren und die rechtliche Grundlage für die Verarbeitung in den Spezialgesetzen zu schaffen oder beizubehalten - jeweils unter der Voraussetzung, dass diese spezialgesetzlichen Regelungen ***konkret*** geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen. Die Öffnungsklauseln ermöglichen indes nicht, ein Auffanggesetz mit abstrakten Verarbeitungstatbeständen und entsprechend unspezifischen Garantien für die Grundrechte und Interessen der betroffenen Person zu schaffen. Eine untragbare, verfassungs- und europarechtswidrige Regelung enthält § 22 Abs. 2 S. 3, der im weit gefassten Bereich der Gefahrenabwehr durch öffentliche Stellen jegliche Standards der DS-GVO zur Wahrung der Rechte und Freiheiten der betroffenen Person aushebelt.

Zu §§ 23, 24 BDSG-E Verarbeitung zu anderen Zwecken

Die §§ 23, 24 BDSG-E genügen nicht den Anforderungen des Art. 6 Abs. 4 i.V.m. 23 Abs. 1 DS-GVO. Artikel 6 Abs. 4 räumt den Mitgliedstaaten ein, Rechtsvorschriften zur Zweckänderung ungeachtet der Vereinbarkeit der Zwecke zu erlassen, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DS-GVO genannten Ziele darstellen. Diesem Maßstab genügen die Regelungen nicht im Ansatz, da es an notwendigen Konkretisierungen fehlt und lediglich Regelungen der DS-GVO unter Verstoß gegen das Wiederholungsverbot wiedergegeben werden. Ebenso fehlt es an Geeigneten Garantien zur Wahrung der Rechte der Betroffenen. Nach EG 50 sollten die Vorschriften in jedem Fall gewährleisten, dass die in der DS-GVO niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über die anderen Zwecke und ihre Rechte, einschließlich des Widerspruchsrechts, unterrichtet wird. Auch diese Gewährleistung fehlt in den §§ 23, 24 BDSG-E.

Zu § 25 Datenübermittlungen durch öffentliche Stellen

Absatz 1

Die Regelung geht über Art. 6 Abs. 1 DS-GVO hinaus. Demnach ist die Übermittlung nur zulässig, wenn es zur Aufgabenerfüllung des Verantwortlichen, also der übermittelnden Stelle selbst,

erforderlich ist. Die Notwendigkeit zur Aufgabenerfüllung beim Empfänger genügt nach Art. 6 Abs. 1 DS-GVO nicht mehr. Die Öffnungsklausel in Art. 6 Abs. 2 DS-GVO ermächtigt nur zu spezifischeren Bestimmungen der Erlaubnistatbestände aus Art. 6 Abs. 1 lit. c und e DS-GVO, nicht aber zu einer Erweiterung derselben. Die Übermittlung könnte u.U. zwar unmittelbar auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden. Dieser erfordert aber eine Interessenabwägung und gilt mangels Öffnungsklausel unmittelbar.

Absatz 2

Die Regelung in Nr. 3 geht über Art. 6 Abs. 1 DS-GVO hinaus. Die Übermittlung zu diesen Zwecken könnte nach Art. 6 Abs. 1 lit f DS-GVO zulässig sein. Dieser gilt aber mit der dort vorgesehenen Interessenabwägung unmittelbar. Eine Abweichung ist mangels Öffnungsklausel unzulässig.

Zu § 26 Datenverarbeitung im Beschäftigungskontext

Die Regelungen zum Beschäftigtendatenschutz können kein Beschäftigtendatenschutzgesetz ersetzen, dass mit Blick auf Art. 88 Abs. 3 DS-GVO dringend auf den Weg gebracht werden sollte.

Absatz 2

Die Vorschrift missachtet Art. 7 Abs. 4 DS-GVO, erfüllt nicht die Anforderungen der Öffnungsklausel in Art. 88 DS-GVO und ist auch materiell-rechtlich unzutreffend. Es liegt gerade keine freiwillige Einwilligung vor, wenn für den Beschäftigten ein wirtschaftlicher Vorteil auf dem Spiel steht. Ist dieser an die Einwilligung gebunden, liegt vielmehr ein Verstoß gegen das Koppelungsverbot vor.

Absatz 3

Die Anforderungen der Öffnungsklausel in Art. 9 Abs. 2 lit. b DS-GVO werden nicht erfüllt. Schon die Formulierung „abweichend“ lässt erkennen, dass der Entwurf missversteht, dass Art. 88 DS-GVO nur zum Erlass spezifischerer Vorschriften ermächtigt. Die Regelung erschöpft sich jedoch nahezu in der Wiederholung von Art. 9 Abs. 2 lit. b DS-GVO, ohne die erforderlichen geeigneten Garantien für die Grundrechte und die Interessen der betroffenen Person vorzusehen.

Zu §§ 27, 28 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken zu im öffentlichen Interesse liegenden Archivzwecken

Die DS-GVO stellt unterschiedliche Anforderungen an die Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Zwecken. Schon aus diesem Grund sollte davon Abstand genommen werden, einen Auffangtatbestand im BDSG-E zu schaffen und bestehende Öffnungsklauseln besser in Spezialgesetzen ausgefüllt werden. Die nach Art. 9 Abs. 2 lit. j DS-GVO erforderlichen angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person lassen sich nur angesichts konkreter Verarbeitungssituationen in den Spezialgesetzen formulieren.
Darüber hinaus müssen Maßnahmen nach Art. 89 Abs. 1 DS-GVO auch für die Bearbeitung allgemeiner personenbezogener Daten formuliert werden, nicht nur, wie bisher im Gesetzentwurf, für die Verarbeitung besonderer Kategorien personenbezogener Daten. Nach EG 162 müssen beispielsweise für die Verarbeitung personenbezogener Daten zu statistischen Zwecken der statistische Inhalt, die Zugangskontrolle und die Spezifikation für die Verarbeitung

im nationalen Recht konkretisiert werden. Dies leisten die §§ 27, 28 BDSG-E nicht ansatzweise und sind schon aus diesem Grund zu streichen.

Darüber hinaus schränken die §§ 27, 28 die Betroffenenrechte unzulässig ein. Dies zeigt sich bereits deutlich am Wortlaut von § 27 Abs. 2 Satz 2 BDSG-E, der mit der Wendung *„darüber hinaus“* dokumentiert, dass unzulässig eine weitere, über Art. 89 Abs. 2 DS-GVO hinausgehende, Ausnahme geschaffen werden soll. Dieses Vorgehen ist europarechtswidrig. Betroffenenrechte können nach Art. 89 Abs. 2, 3 DS-GVO eingeschränkt werden, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. Ein unverhältnismäßiger Aufwand steht der Erfüllung der Zwecke aber nicht entgegen und kann die Einschränkung von Betroffenenrechten nicht rechtfertigen. Vielmehr haben Verantwortliche organisatorische und technische Maßnahmen zu ergreifen, um die Rechte der Betroffenen zu wahren und gerade auch Auskunftsansprüchen nachkommen zu können.

Zu § 29 BDSG-E Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Falle von Geheimhaltungspflichten

Absatz 1

Betroffenenrechte dürfen, wenn die Voraussetzungen des Art. 23 Abs. 1 DS-GVO vorliegen eingeschränkt werden, wenn gleichzeitig die einschränkende Norm im nationalen Recht auch die Anforderungen des Art. 23 Abs. 2 DS-GVO erfüllt.

Die Regelung stellt wegen ihrer Weite weder eine den Wesensgehalt der Grundrechte und Grundfreiheiten achtende und in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme dar (vgl. Art. 23 Abs. 1 DS-GVO), noch sind die Anforderungen aus Art. 23 Abs. 2 DS-GVO umgesetzt.

Absatz 3

In Hinblick auf Berufsgeheimnisträger ist eine Einschränkung der Befugnisse der Aufsichtsbehörde weder verhältnismäßig noch zielführend. Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie z. B. Gesundheitsdaten, verarbeitet. Die Kontrollkompetenz der Datenschutzbeauftragten darf hier nicht beschnitten werden. Vielmehr ist eine wirksame datenschutzrechtliche Kontrolle besonders von Nöten. Insbesondere muss es den Aufsichtsbehörden zwingend möglich sein, Auftragsverarbeiter von Berufsgeheimnisträgern zu kontrollieren. Beschlagnahmeverbote und Zeugnisverweigerungsrechte aus der StPO dienen dem Schutz der betroffenen Person. Ermittlungsbehörden sollen nicht über Umwege an Informationen gelangen können, die Betroffene im Rahmen eines besonderen Vertrauensverhältnisses offenbart haben. Entsprechende Regelungen dienen der Wahrung eines fairen Verfahrens. Die Rolle der Aufsichtsbehörden ist jedoch mit der der Strafverfolgungsbehörden nicht vergleichbar. Kontrollen der Aufsichtsbehörden zielen unmittelbar darauf ab, das Vertrauensverhältnis zwischen Berufsgeheimnisträger und betroffener Person zu wahren, indem die Rechtmäßigkeit der Datenverarbeitung überprüft wird.

Zu § 32 BDSG-E Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Wie auch die nachfolgenden Regelungen des 2. Kapitels ist § 32 BDSG-E europarechtswidrig. Betroffenenrechte dürfen nur eingeschränkt werden, wenn

- eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt,
- zur Erreichung der Ziele in Art. 23 Abs. 1 lit. a-j dient und
- die Gesetzgebungsmaßnahme spezifische Regelungen nach Art. 23 Abs. 2 DS-GVO enthält.

Die Voraussetzungen und die Anforderungen aus Art. 23 Abs. 2 DS-GVO müssen kumulativ vorliegen. Es genügt nicht, dass eine Regelung nur eines der in Art. 23 Abs. 1 lit a-j DS-GVO genannten Ziele verfolgt. Die Regelung muss zudem verhältnismäßig sein und Maßnahmen nach Art. 23 Abs. 2 DS-GVO normieren. Die §§ 31 ff. erfüllen diese Voraussetzungen nicht.

Absatz 1

Die Einschränkung der Informationspflicht nach Abs. 1 Nr. 1 erfüllt nicht die Voraussetzungen des Art. 23 DS-GVO und kann insbesondere nicht auf Art. 23 Abs. 1 lit. i DS-GVO gestützt werden. Die verantwortliche Stelle vor hohem Verwaltungsaufwand zu bewahren, realisiert nicht den Schutz der Rechte und Freiheiten anderer Personen nach Art. 23 Abs. 1 lit. i DS-GVO. Die Vorschrift soll Dritte schützen und nicht den Verantwortlichen. Entsprechend der Intention der DS-GVO haben die Verantwortlichen vielmehr durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, dass sie ihren Informations-, Auskunfts- und Löschpflichten genügen können.

Absatz 2

Absatz 2 genügt nicht den Anforderungen des Art. 23 Abs. 2 DS-GVO. Die genannten Maßnahmen bilden nur einen Bruchteil dessen ab, was nach Art. 23 Abs. 2 DS-GVO geregelt werden müsste. Absolut untragbar ist die Regelung in Satz 3, die dazu führt, dass in den genannten Fällen Art. 23 Abs. 2 DS-GVO gänzlich ignoriert wird.

Zu § 33 BDSG-E Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

Absatz 1

Die Regelung erfüllt nicht die Voraussetzungen des Art. 23 Abs. 1 DS-GVO. Allein der Umstand, dass sie die in Art. 23 Abs. 1 DS-GVO genannten Ziele verfolgt, genügt nicht. Sie muss darüber hinaus den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen, mithin verhältnismäßig sein. Insbesondere mangels Interessenabwägung fehlt es hier an der Verhältnismäßigkeit.

Zu § 34 BDSG-E Auskunftsrecht der betroffenen Person

Die Regelung zur Einschränkung des Auskunftsanspruchs in Abs. 1 Ziff. 2 ist mit den Zielen der DS-GVO unvereinbar. 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 der auskunftsersuchenden betroffenen Person nicht mitgeteilt werden muss, dass (doch) Daten über sie gespeichert sind.

Zu § 35 Recht auf Löschung

Absatz 1

Die Regelung schränkt Betroffenenrechte ein. Dies ist nur zulässig, wenn die Voraussetzungen des Art. 23 DS-GVO vorliegen. Die Voraussetzungen sind nicht gegeben. Es wurde bereits mehrfach erwähnt, dass ein unverhältnismäßiger Aufwand keine Einschränkung der Betroffenenrechte rechtfertigen kann. Vielmehr haben die Verantwortlichen technische und organisatorische Maßnahmen zu treffen, um ihre diesbezüglichen Pflichten erfüllen zu können.

Absatz 2

Für die Regelung in Satz 2 gilt das oben Gesagte.

Zu § 36 Widerspruchsrecht

Auch hier fehlen die in Art. 23 Abs. 2 DS-GVO bezeichneten Maßnahmen.

§ 39 BDSG-E Akkreditierung

Die Vorschrift verletzt die Gesetzgebungskompetenz der Länder. Zudem sollte die Akkreditierung vorzugsweise den Datenschutzaufsichtsbehörden obliegen, welche einheitliche Akkreditierungskriterienkataloge erstellen und im Rahmen eines einheitlichen Akkreditierungsverfahrens anwenden. Dies gilt insbesondere mit Blick auf die Bedeutung der Zertifizierung nach Art. 42 DS-GVO im internationalen Datenverkehr. Nach Art. 46 Abs. 2 lit. f DS-GVO sind Zertifizierungen ein Instrument für die Datenübermittlung in Drittstaaten, das keiner weiteren Genehmigung einer Aufsichtsbehörde bedarf.

§ 40 BDSG-E Aufsichtsbehörden der Länder

Nach § 39 Abs. 1 überwachen die nach Landesrecht zuständigen Behörden (Aufsichtsbehörden der Länder) im Anwendungsbereich der Verordnung bei den Unternehmen die Anwendung der Vorschriften über den Datenschutz. In den folgenden Absätzen sind zudem die Aufgaben und Befugnisse der Aufsichtsbehörden näher geregelt. Darin ist ein Eingriff in die Gesetzgebungskompetenz der Länder zu sehen.

Inhaltlich müsste die Regelung des § 40 ergänzt werden. So erstreckt § 16 Abs. 3 die Kontrollbefugnis der/des BfDI auf solche Daten, die einem besonderen Amtsgeheimnis unterliegen. Eine entsprechende Regelung für die Landesbeauftragten fehlt. Sie sollte noch hinzugefügt werden.

Zu § 43 BDSG-E Weitere Vorschriften für die Verhängung von Geldbußen

Absatz 1

In § 43 Abs. 1 sollten weitere Bußgeldtatbestände ergänzt werden, beispielsweise entsprechend des bisherigen § 43 Abs. 1 Nr. 10 BDSG wegen nicht, nicht rechtzeitig, nicht richtig oder nicht vollständig erteilter Auskunft gegenüber der Aufsichtsbehörde. Artikel 84 der DS-GVO ermächtigt den nationalen Gesetzgeber hierzu ausdrücklich, da ein Verstoß gegen Art. 58 Abs. 1 lit. a DS-GVO bisher nicht im Katalog des Art. 83 DS-GVO genannt ist. Die Bußgeldhöhe muss sich jedoch, anders als bisher im Entwurf vorgesehen, an den Bußgeldtatbeständen der DS-GVO orientieren.

Absatz 3

Die Privilegierung von öffentlichen Stellen gegenüber Unternehmen hinsichtlich der Verhängung von Bußgeldern ist vor dem Hintergrund der notwendigen Durchsetzbarkeit der DS-GVO nicht

hinnehmbar. Der auch nach § 41 Abs. 1 nunmehr anwendbare § 30 OWiG schließt Bußgelder gegen juristische Personen des öffentlichen Rechts nicht aus.

Zu § 45 BDSG-E Anwendungsbereich

Nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 gilt die JI-Richtlinie für die Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung. Indem § 45 davon ausgeht, dass davon auch Ordnungswidrigkeiten erfasst sein sollen, überdehnt er den Anwendungsbereich der Richtlinie. Eine Vielzahl von Behörden wird im Rahmen ihrer Verwaltungstätigkeit auch im Bereich der Gefahrenabwehr tätig (z. Bsp.: Gesundheitsamt, Veterinäramt) oder verfolgt Ordnungswidrigkeiten (z. Bsp.: Datenschutzaufsichtsbehörden). Es ist mit der Intention der DS-GVO nicht vereinbar, diese öffentlichen Stellen aus dem Anwendungsbereich der DS-GVO auszunehmen. Nur dann, wenn die Verwaltungsbehörden durch ausdrückliche spezialgesetzliche Regelungen Befugnisse der Staatsanwaltschaft wahrnehmen und Straftaten verfolgen (vgl. z. Bsp.: § 385 AO) ist es angebracht, diese Behörden, soweit sie in diesem engen Bereich tätig werden, der JI-Richtlinie zu unterwerfen. Grundsätzlich sollte für alle Verwaltungsbehörden, auch wenn sie Ordnungswidrigkeiten verfolgen oder im Bereich der Gefahrenabwehr tätig sind, die DS-GVO gelten.

Etwas anderes ergibt sich auch nicht aus EG 13 der JI-Richtlinie, wonach die Straftat ein eigenständiger Begriff des Unionsrechts ist, der der Auslegung durch den EuGH unterliegt. Dieser orientiert sich an der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zu Art. 6 der Europäischen Menschenrechtskonvention (EMRK). Der EGMR entscheidet von Fall zu Fall, je nach der Schwere des Verstoßes beziehungsweise der Sanktionsdrohung, ob eine vom nationalen Recht als Ordnungswidrigkeit eingestufte Handlung dem Begriff der Straftat im Sinne des Art. 6 EMRK unterfällt. Dem EGMR geht es vorrangig um die flexible Anwendbarkeit und Gewährleistung eines Mindestschutzniveaus der besonderen strafrechtlichen Garantien des Art. 6 EMRK im konkreten Beschwerdefall. Art. 5 – 7 EMRK haben elementare Verteidigungsrechte des Angeklagten zum Gegenstand, die ein Mindestmaß an Grundrechtssicherung gewährleisten sollen und deshalb möglichst weit ausgelegt werden. Zwar hat die JI-Richtlinie den Schutz natürlicher Personen bei der Datenverarbeitung durch öffentliche Stellen zu den Zwecken der Gefahrenabwehr sowie der Strafverfolgung zum Gegenstand, allerdings wirkt sich die Anwendung der DS-GVO für die betroffene Person günstiger sowohl hinsichtlich der Betroffenenrechte als auch der wirksamen Durchsetzung dieser Rechte aus. Die Rechtsprechung des EGMR kann somit nicht als Begründung dafür herangezogen werden, dass Ordnungswidrigkeiten dem unionsrechtlichen Begriff der Straftat unterfallen sollten.

Zu § 47 BDSG-E Verarbeitung personenbezogener Daten

Art. 4 der JI-Richtlinie regelt altbewährte Grundsätze für die Verarbeitung personenbezogener Daten. Diese werden in § 47 noch unvollständig umgesetzt. Insbesondere fehlt der Grundsatz der Verhältnismäßigkeit der Datenverarbeitung.

Zu § 51 BDSG-E Einwilligung

§ 51 geht davon aus, dass eine Datenverarbeitung im Anwendungsbereich der JI-Richtlinie auch aufgrund der Einwilligung der betroffenen Person erfolgen kann. Hierbei ist zu berücksichtigen, dass eine Einwilligung im Anwendungsbereich der JI-Richtlinie mangels Wahlfreiheit und damit mangels Freiwilligkeit nur in Ausnahmefällen als Rechtsgrundlage für eine Datenverarbeitung in Betracht kommt. Deutlich wird dies in EG 35: *„Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der*

betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann."

Zu § 54 BDSG-E Automatisierte Einzelentscheidung

Automatisierte Einzelentscheidungen, unter anderem auf der Grundlage von Profiling, die nachteilige Rechtsfolgen für die betroffene Personen haben oder sie erheblich beeinträchtigen, sind nach Art. 11 der JI-Richtlinie von den Mitgliedstaaten grundsätzlich zu verbieten. Ausnahmen können in einer Rechtsvorschrift vorgesehen werden, die geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet. § 54 setzt dies nur unzureichend um und lässt insbesondere die Notwendigkeit geeigneter Garantien entfallen.

Zu § 57 BDSG-E Auskunftsrecht

Für die in § 57 Abs. 1 vorgesehenen Auskunftsrechte der betroffenen Personen enthalten die Absätze 2 und 3 Einschränkungen, die nicht in der JI-Richtlinie vorgesehen sind. Abs. 2 schränkt das Auskunftsrecht für bestimmte personenbezogene Daten ein, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Nach Abs. 3 unterbleibt die Auskunftserteilung, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen. Diese Gründe sind nicht annähernd so schwerwiegend, wie die für die Einschränkung des Auskunftsrechts in der JI-Richtlinie genannten. Vielmehr darf nach Art. 15 der JI-Richtlinie das Auskunftsrecht nur zu den dort genannten Zwecken eingeschränkt werden, namentlich zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden, zum Schutz der öffentlichen Sicherheit und zum Schutz der Rechte und Freiheiten Dritter.

Eine Einschränkung der Auskunft gegenüber der Aufsichtsbehörde in § 57 Abs. 7 S. 3 ist in Art. 17 der JI-Richtlinie nicht vorgesehen und nicht nachvollziehbar.

Zu § 58 BDSG-E Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

Gemäß § 58 Abs. 2 hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender personenbezogener Daten zu verlangen, wenn ihre Verarbeitung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung gemäß § 58 Abs. 3 Nr. 3 einschränken, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. In der JI-Richtlinie ist diese Möglichkeit, die Löschung unzulässig verarbeiteter oder nicht mehr erforderlicher Daten zu umgehen, nicht vorgesehen.

Zu § 59 BDSG-E Verfahren für die Ausübung der Rechte der betroffenen Person

Es bleibt in Abs. 3 unklar, in welchen konkreten Anwendungsfällen Anträge der betroffenen Person als offenkundig oder exzessiv einzustufen sind.

In Abs. 4 muss der Grundsatz der Zweckbindung und Datenminimierung für die zusätzlich angeforderten Informationen ergänzt werden (EG 41 der Richtlinie).

Zu § 62 BDSG-E Auftragsverarbeitung

Die Mitgliedstaaten sehen nach Art. 22 Abs. 1 der JI-Richtlinie vor, dass in dem Fall, dass eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, dieser nur mit Auftragsverarbeitern arbeitet, die hinreichende Garantien dafür bieten, das geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Richtlinie erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. § 62 setzt diese Anforderungen nur in unzureichender Weise um. Insbesondere sollte in § 62 wie in Art. 28 Abs. 5 DS-GVO die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO durch einen Auftragsverarbeiter als Faktor für hinreichende Garantien für eine sorgfältige Auswahl des Auftragsverarbeiters herangezogen werden.

In Nr. 8 sollten Verweise auf § 67 (Datenschutzfolgenabschätzung) und § 71 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) ergänzt werden.

Zu § 63 BDSG-E Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie gemäß § 63 als gemeinsam Verantwortliche. Hierzu ist es im Hinblick auf multinationalen gemeinsamen Verfahren sinnvoll, dass Betroffene ihre Rechte gegenüber einem deutschen Verantwortlichen gelten machen können.

In Ergänzung zu den Vorgaben der Richtlinie sollten die gemeinsam Verantwortlichen in der in Rede stehenden Vereinbarung auch die zu treffenden technisch-organisatorischen Maßnahmen nach § 64 sowie die Verantwortlichkeiten für deren Umsetzung festlegen.

Zu § 64 BDSG-E Anforderungen an die Sicherheit der Datenverarbeitung

Nach Art. 4 Abs. 4 der JI-Richtlinie ist der Verantwortliche für die Einhaltung der Absätze 1, 2 und 3 (Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten) verantwortlich und muss deren Einhaltung nachweisen können. Im Gesetzentwurf sollten detailliertere Vorgaben zur Umsetzung von Art. 4 Abs. 4 der JI-Richtlinie getroffen und konkrete Pflichten für Verantwortliche zum Nachweis der Einhaltung der Regelungen formuliert werden (welche Form der Nachweise, welche Dokumente, welcher Prüf- bzw. Aktualisierungsrhythmus usw.).

In Absatz 1 sollte die Terminologie aus Art. 29 Abs. 1 JI-Richtlinie verwendet werden („für die Rechte und Freiheiten natürlicher Personen“, „geeignete technische und organisatorische Maßnahmen“). In Bezug auf die „Technischen Richtlinien und Empfehlungen“ des BSI sind ergänzend auch dessen „Standards“ aufzunehmen. Zudem sollte erwogen werden, auch die Berücksichtigung der Entscheidungen des Europäischen Datenschutzausschusses zu Fragen der Sicherheit der Datenverarbeitung aufzunehmen. Wünschenswert wäre in diesem Kontext auch eine Verschärfung des Wortes „berücksichtigen“ durch Verwendung des Wortes „einhalten“.

Um die Eignung und Angemessenheit der geforderten technischen und organisatorischen Maßnahmen treffend beurteilen zu können, hat die Datenschutzkonferenz das Standard-Datenschutzmodell entwickelt. Dieses geht von den sieben Gewährleistungszielen Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Nichtverkettung und Transparenz aus, die mit entsprechenden technischen und organisatorischen Maßnahmen erreicht werden sollen. Sie beschreiben die Schutzrichtung des Datenschutzes und sind sowohl in Art. 4 der Richtlinie und in Art. 5 der Verordnung als auch in den Datenschutzgesetzen einiger Länder bereits vorgebildet. Diese Gewährleistungsziele sollten im Zuge der Umsetzung der Richtlinie im

deutschen Recht und hier insbesondere in den Absätzen 1 und 2 ausdrücklich festgelegt werden:

- *Datenminimierung: Es ist zu gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.*
- *Vertraulichkeit: Es ist zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können.*
- *Integrität: Es ist zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell und die zu ihrer Verarbeitung eingesetzten Systeme und Dienste integer bleiben.*
- *Verfügbarkeit: Es ist zu gewährleisten, dass personenbezogene Daten und die zu ihrer Verarbeitung vorgesehenen Systeme und Dienste zeitgerecht zur Verfügung stehen.*
- *Transparenz: Es ist zu gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten einschließlich der zur ihrer Umsetzung getroffenen technisch-administrativen Voreinstellungen vollständig, aktuell und einer Weise dokumentiert sind, dass sie in zumutbarer Zeitnachvollzogen werden können; personenbezogene Daten ihrem Ursprung zugeordnet werden können; und festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat.*
- *Intervenierbarkeit: Es ist zu gewährleisten, dass die Datenverarbeitung so organisiert und die eingesetzten technischen Systeme so gestaltet sind, dass eine Gewährung der Betroffenenrechte ungehindert erfolgen kann.*
- *Nichtverkettung: Es ist zu gewährleisten, dass jede Verarbeitung von personenbezogenen Daten ausschließlich im Rahmen im Vorhinein bestimmter Befugnisse für vorab festgelegte rechtmäßige Zwecke erfolgt und die Daten hierfür nach den jeweiligen Zwecken und nach unterschiedlichen Betroffenen getrennt werden können.*

Die Anforderungen von Art. 29 Abs. 2 der JI-Richtlinie sind von der Verpflichtung zur Sicherstellung dieser Schutzziele umfasst.

Darüber hinaus ist in Abs. 2 (oder in einem neuen Absatz) zusätzlich eine Pflicht zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Schutzmaßnahmen analog zur Festlegung in Art. 32 Abs. 1 lit. d DS-GVO aufzunehmen. Dies ist auch zur Umsetzung von Art. 19 Abs. 1 der JI-Richtlinie erforderlich.

Absatz 2 und Abs. 3 sind in der Gesamtschau als Vermischung von „neuen Gewährleistungszielen“ und „alten Kontrollmaßnahmen“ für den Anwender des Gesetzes nicht handhabbar. Darüber hinaus fällt auf, dass die neuen Ziele aus Abs. 2 für jede Form der Verarbeitung personenbezogener Daten gelten sollen, die alten Kontrollmaßnahmen aus Abs. 3 jedoch nur für deren automatisierte Verarbeitung.

Ebenso fällt auf, dass der Wortlaut der JI-Richtlinie in einzelnen Bereichen verändert und dabei bereits der Gedanke der Gewährleistungsziele umgesetzt wurde. Zum Beispiel wurde bei § 60 Abs. 3 Nr. 8 (Transportkontrolle) die Formulierung der Richtlinie „Verhinderung, dass (…) die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle)“ durch eine positive Formulierung mit Hilfe der Gewährleistungsziele ersetzt „Gewährleistung, dass die Vertraulichkeit und Integrität der Daten geschützt wird (Transportkontrolle)“. Allerdings wurde hierbei ein Aspekt der Verfügbarkeit, in der JI-Richtlinie dargestellt durch die Begrifflich-

keit „Verhinderung unbefugten Löschens“, bei der Formulierung des § 64 Abs. 3 Nr. 8 nicht übernommen.

Es wird daher vorgeschlagen, wie oben dargestellt, in Abs. 2 die sieben Gewährleistungsziele aufzunehmen und Abs. 3 gänzlich zu streichen. Der Nachweis, dass durch die Formulierung der Gewährleistungsziele die „Kontrollen“ der Anlage zu § 9 Satz 1 BDSG umgesetzt werden, wird im Standard-Datenschutzmodell erbracht.

Zu §§ 65, 66 BDSG-E Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten / Benachrichtigung der betroffenen Person bei der Verletzung des Schutzes personenbezogener Daten

Während der Gesetzentwurf hier von „Gefahr für die Rechtsgüter natürlicher Personen“ spricht, verwenden die Art. 30 und 31 der JI-Richtlinie den Begriff „Risiko für die Rechte und Freiheiten natürlicher Personen“. Dieser sollte vom Gesetzentwurf übernommen werden.

Die Entscheidung gegen eine Meldung von Verletzungen des Schutzes personenbezogener Daten muss durch die Aufsichtsbehörde kontrollierbar und nachvollziehbar sein. Dies erfordert eine entsprechende Dokumentationspflicht, die ergänzt werden sollte.

Zu § 67 BDSG-E Durchführung einer Datenschutzfolgeabschätzung

Die Terminologie in Abs. 1 sollte der Richtlinie folgen („hohes Risiko für die Rechte und Freiheiten natürlicher Personen“). Absatz 1 sollte ergänzt werden um eine Aufzählung der Fälle, in denen eine Datenschutzfolgenabschätzung zwingend erforderlich ist (in vergleichbarer Weise wie in Art. 35 Abs. 3 DS-GVO).

Obwohl die Regelung in Abs. 2 der DS-GVO entnommen ist, lässt die Unbestimmtheit („ähnliche Verarbeitungsvorgänge mit ähnlich hohem Gefährdungspotential“) erheblichen Interpretationsspielraum. Dies wird bei Verantwortlichen eher dazu führen, auf Folgenabschätzungen zu verzichten.

In Absatz 4 S. 1 ist zu ergänzen, dass die Folgenabschätzung nicht nur den Rechten, sondern auch den berechtigten Interessen der Betroffenen Rechnung tragen muss (vgl. Art. 27 Abs. 2 Satz 1 JI-Richtlinie).

In Absatz 4 Nr. 4 ist zu ergänzen, dass die Folgenabschätzung auch eine Bewertung der geplanten Abhilfemaßnahmen enthalten muss (gem. Art. 27 Abs. 2 JI-Richtlinie), um überprüfen zu können, dass die geplanten Maßnahmen auch ausreichend sind.

Absatz 5 sollte dahingehend ergänzt werden, dass eine Überprüfung und ggf. Wiederholung der Folgenabschätzung einschließlich Neufestlegung von zu treffenden Maßnahmen jedenfalls dann erforderlich ist, wenn sich z. B. die Gefährdungslage ändert. Ergänzend sollten weitere Kriterien aufgenommen werden, wie etwa Änderungen der Rechtslage oder der verwendeten Technologien, Datenschutzvorfälle, regelmäßige Prüffristen.

Zu § 69 BDSG-E Anhörung der oder des Bundesbeauftragten

Nach Art. 28 Abs. 1 sehen die Mitgliedstaaten vor, dass der Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung personenbezogener Daten „in neu anzulegenden Dateisystemen“ in den in lit. a und b näher bezeichneten Fällen die Aufsichtsbehörde konsultiert. Demgegenüber ordnet der Gesetzentwurf dies lediglich „vor der Inbetriebnahme neuartiger wesentlicher Dateisysteme und Verfahren zur Verarbeitung personenbezogener Daten“ an. Diese Beschränkung der Anhörung auf „neuartige wesentliche Dateisysteme und Verfahren“ ist zu unbestimmt und entspricht nicht den Festlegungen der Richtlinie.

Art. 28 Abs. 3 der JI-Richtlinie, nach dem die Mitgliedstaaten vorsehen, das die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellen kann, die der Pflicht zur vorherigen Konsultation nach Art. 28 Abs. 1 unterliegen, wurde offensichtlich nicht umgesetzt.

In Absatz 4 sollten die Ausnahmefälle weiter eingeschränkt werden (z.B. „Behinderung der Aufgabenerfüllung“ oder „Unmöglichkeit der Aufgabenerfüllung“), da die gegenwärtige Formulierung zu große Spielräume lässt: Es ist zu erwarten, das Verarbeitungen durch Verantwortliche in der Regel so eingestuft werden, dass sie erhebliche Bedeutung haben und dringlich zu beginnen sind, obwohl die Anhörung der/des BfDI zur Folgenabschätzung noch nicht abgeschlossen ist. Was in diesem Fall eine anschließende „gebührende Berücksichtigung der Empfehlungen der/des BfDI“ bedeutet, ist unklar und verschärft das Problem.

Zu § 70 BDSG-E Verzeichnis

Das Verhältnis zwischen dem Verzeichnis der Verarbeitungstätigkeiten und der Beschreibung der einzelnen Verfahren ist unklar. Gemeint kann nur sein, dass für jedes Verfahren zur Verarbeitung personenbezogener Daten (jede Verarbeitungstätigkeit) eine gesonderte Beschreibung zu erstellen ist. Die einzelnen Beschreibungen sind im Verzeichnis der Verarbeitungstätigkeiten aufzulisten. Artikel 24 der JI-Richtlinie verfolgt das Ziel, bei dem Verantwortlichen und beim Auftragsverarbeiter eine Gesamtübersicht über alle eingesetzten Verarbeitungstätigkeiten zu erstellen. Zu diesem Zweck sollten entsprechende Verzeichnisse ausnahmslos zentral beim behördlichen Datenschutzbeauftragten geführt werden.

In Absatz 1 Nr. 8 wird vorgeschlagen, auch Fristen für die Überprüfung der Einschränkung der Verarbeitung (ehemals Sperrung) aufzunehmen.

Aufgrund positiver Praxiserfahrungen sollte ergänzend zu den Vorgaben der Richtlinie erwogen werden, das Verzeichnis der Verarbeitungstätigkeiten um die Bezeichnung des Verfahrens, um eine allgemeine Beschreibung der verwendeten Datenverarbeitungsanlagen und der Software(versionen), ggf. um das Ergebnis der Datenschutzfolgenabschätzung sowie um eine (schriftliche oder elektronische) Bestätigung des Verantwortlichen zur formalen Freigabe des Verfahrens zu ergänzen.

Weiterhin sollte festgelegt werden, dass das Verzeichnis regelmäßig überprüft und insbesondere bei Änderungen fortzuschreiben ist.

Zu § 71 BDSG-E Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Regelungen zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sollten auch Auftragsverarbeiter in die Pflicht nehmen. In Abs. 1 führt die Aufnahme der Anforderungen aus Art. 20 JI-Richtlinie und aus dem bisherigen § 3a BDSG zu Dopplungen. Weiterhin sollte an Stelle des Begriffs „Datensparsamkeit“ der Begriff „Datenminimierung“ genutzt werden. Darüber hinaus ist der Begriff „Anonymisierung“ (wegen der Übernahme von § 3a BDSG) in den bisher in § 2 Abs. 2 BDSG-E enthaltenen Begriffsbestimmungen aufzunehmen.

Nach Art. 25 Abs. 3 DS-GVO kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Dieser Aspekt sollte auch in § 71 BDSG-E erwähnt werden.

Zu § 76 BDSG-E Protokollierung

Die Regelung zur Protokollierung sollte weiter ergänzt werden. Die Vorgaben des Art. 25 der JI-Richtlinie dürfen trotz ihres Umfangs und Detaillierungsgrades nicht als abschließende Vollregelung verstanden werden. Weder legt Art. 25 alle revisionssicher auszugestaltenden Prozesse fest, noch trifft die Vorschrift alle für den Umfang mit Protokolldaten erforderlichen Regelungen. Vielmehr beschränkt sich die Vorschrift auf die Protokollierung der Zugriffe der Nutzerinnen und Nutzer.

In § 76 Abs. 1 sollte explizit festgelegt werden, dass auch administrative Vorgänge (z. Bsp. Löschläufe, Datenbankzugriffe, Erstellung von Backups) zu protokollieren sind, da diese unter Umständen einen weit größeren Einfluss als einzelne Verarbeitungsvorgänge haben. Darüber hinaus ist eine automatische Protokollierung der Datenübertragung an Schnittstellen von Verfahren zu anderen Verfahren erforderlich. Schließlich sollten Aufbewahrungsfristen für Protokolldaten geregelt werden. In Bezug auf die Protokolldaten für einzelne Verarbeitungsvorgänge ist es sinnvoll, Protokolldaten ebenso lange wie die gespeicherten Daten aufzubewahren. Dabei sind Teillöschungen (z. Bsp. Tilgungen im BZR) zu berücksichtigen – die jeweils relevanten Protokolldaten sind ebenfalls mit der Löschung der gespeicherten Daten zu löschen.

Die Regelung über die Zweckbindung von Protokolldaten lässt offen, zu welchen Zwecken die Daten konkret verwendet werden dürfen. Protokollierung ist eine Verfahrenssicherung, die den Grundrechtseingriff der Datenverarbeitung abmildern soll. Sie darf deshalb nicht ihrerseits zu zusätzlichen Grundrechtseingriffen führen. Insbesondere muss klargestellt werden, dass gespeicherte Protokolldaten nicht für Zwecke der Gefahrenabwehr und Strafverfolgung verwendet werden dürfen. Artikel 25 Abs. 2 JI-Richtlinie, 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.

Zu § 77 BDSG-E Vertrauliche Meldung von Verstößen

Es sollte ergänzend darauf hingewiesen werden, dass der Verantwortliche für diese Meldungen (sowohl für den Meldevorgang selbst als auch für das Ergebnis des Meldevorgangs) die erforderlichen Maßnahmen und Vorkehrungen trifft.

Zu § 79 BDSG-E Datenübermittlung bei geeigneten Garantien

§ 79 regelt die Übermittlung von personenbezogenen Daten an Drittstaaten ohne Angemessenheitsbeschluss der Kommission vorbehaltlich geeigneter Garantien. Der Begriff der geeigneten Garantien ist in Art. 37 der JI-Richtlinie nicht näher bestimmt. Offen bleibt insbesondere, inwieweit diese Garantien den Anforderungen zu entsprechen haben, die im Rahmen eines Angemessenheitsbeschlusses nach Art. 36 Abs. 2 der JI-Richtlinie von der Kommission festzustellen sind.

Der hier bestehende Umsetzungsspielraum ist nach Maßgabe der vom Bundesverfassungsgericht in seiner Entscheidung zum BKAG vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/09, Rn. 329 – 341) aufgestellten Anforderungen auszufüllen. Danach erfordert die Übermittlung von Daten an das Ausland eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen, die Vergewisserung über einen rechtsstaatlichen Um-

gang mit diesen Daten im Empfängerland und der Sicherstellung einer wirksamen inländischen Kontrolle und entsprechende normenklare Grundlagen im deutschen Recht.

Für die Übermittlung von Daten an das Ausland sind danach im Einzelnen die folgenden Voraussetzungen ausdrücklich vorzusehen:

- Die Übermittlung muss der Aufdeckung vergleichbar gewichtiger Straftaten oder dem Schutz vergleichbar gewichtiger Rechtsgüter dienen, wie sie für die ursprüngliche Datenerhebung maßgeblich waren (Rn. 330).

- Aus den übermittelten Informationen oder der Anfrage des Empfängers müssen sich konkrete Ermittlungsansätze im Einzelfall ergeben (Rn. 330).

- Die Nutzung ist auf die Aufdeckung vergleichbar gewichtiger Straftaten oder den Schutz vergleichbar gewichtiger Rechtsgüter, wie sie der Erhebung zu Grunde lagen, zu beschränken (Rn. 331).

- Erlaubt ist eine Übermittlung der Daten ins Ausland nur, wenn auch durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Das heißt, dass die bei der Übermittlung mitgeteilten Grenzen durch Zweckbindung und Löschungspflichten sowie grundlegende Anforderungen an Kontrolle und Datensicherheit bei der Verwendung der Daten wenigstens grundsätzlich Beachtung finden müssen (Rn. 335).

- Es ist sicherzustellen, dass die übermittelten Daten im Empfängerstaat weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden und der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird (Rn. 336).

- Zur Gewährleistung des geforderten Schutzniveaus im Empfängerstaat kann der Gesetzgeber eine generalisierende tatsächliche Einschätzung der Sach- und Rechtslage der Empfängerstaaten durch das Bundeskriminalamt ausreichen lassen. Wenn sich Entscheidungen mit Blick auf einen Empfängerstaat nicht auf solche Beurteilungen stützen lassen, bedarf es einer mit Tatsachen unterlegten Einzelfallprüfung, aus der sich ergibt, dass die Beachtung jedenfalls der grundlegenden Anforderungen an den Umgang mit Daten hinreichend gewährleistet ist (Rn. 337, 338).

- Die Vergewisserung über das geforderte Schutzniveau - sei es generalisiert, sei es im Einzelfall - ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können (Rn. 339).

- Die Übermittlungsvorgänge sind zum Zwecke der Überprüfung in geeigneter Form zu protokollieren (Rn. 340).

- Gesetzlich sicherzustellen sind zudem sind regelmäßige Berichte gegenüber Parlament und Öffentlichkeit (Rn. 340).

Verfassungsrechtliche Anforderungen, die für alle Fachgesetze gelten, müssen bereits im BDSG geregelt werden. Das leistet der Gesetzentwurf bislang nicht.

Zu § 80 BDSG-E Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien

Auch hier wird versäumt, den bestehenden Umsetzungsspielraum nach Maßgabe der vom Bundesverfassungsgericht in seiner Entscheidung zum BKAG vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/09, Rn. 329 – 341) aufgestellten Anforderungen auszufüllen.