Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

AKTENZEICHEN
0.6.9.000/053/2017-00829

DATUM
25. Januar 2017

VERMERK

Stellungnahme des LfDI M-V zum DSAnpUG-EU

Der 3. Gesetzentwurf enthält geringfügige Verbesserungen, leider auch drastische Verschlechterungen, beispielsweise bei den Regelungen zum Beschäftigtendatenschutz. 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 § 2 BDSG-E Begriffsbestimmungen

Absatz 1

Der Begriff Wettbewerbsunternehmen ist bisher lediglich in § 2 Abs. 1 und § 41 Abs. 2 erwähnt, aber nicht definiert. In Absatz 1 wird festgelegt, dass Wettbewerbsunternehmen des Bundes keine öffentlichen Stellen sind. Eine vergleichbare Regelung für die Länder fehlt in Absatz 2 und ist zu ergänzen. Anderenfalls bliebe unklar, ob für Unternehmen, die in privatrechtlicher Organisationsform insbesondere für die Kommunen Aufgaben der öffentlichen Verwaltung im Bereich der Daseinsvorsorge wahrnehmen und mit anderen Unternehmen im Wettbewerb stehen, als öffentliche oder nicht-öffentliche Stellen gelten.

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 Satz 2

Hier wird der Entwurf eines Videoüberwachungsverbesserungsgesetzes in den BDSG-E aufgenommen. Soweit der (private) Betreiber eine Videoüberwachung einsetzen möchte und die Schutzgüter Leben, Gesundheit oder Freiheit in den dort genannten Anlagen betroffen sein können, wird durch die Formulierung „gilt als…ein besonders wichtiges Interesse“ die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme beeinflusst. Es ist aber Aufgabe des Staates, für die Sicherheit seiner Bürgerinnen und Bürger zu sorgen. Diese Aufgabe kann er nicht an Private delegieren. 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.

Auch eine Regelung zum Verbot der heimlichen Videoüberwachung fehlt.

Zu § 16 BDSG-E Befugnisse

Absatz 2

In Absatz 2 werden die in Art. 47 der JI-Richtlinie vorgesehenen Abhilfe- und Beratungsbefugnisse der Aufsichtsbehörde nur unzureichend umgesetzt. Danach 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. Bei der Umsetzung der JI-Richtlinie sollte ein mit der DS-GVO vergleichbares Schutzniveau gewährleistet werden.

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

Die in § 17 getroffene Regelung über die Vertretung im Europäischen Datenschutzausschuss (EDSA) wird der innerstaatlichen Zuständigkeitsverteilung zwischen Bund und Ländern nicht gerecht. Der Vollzug der Datenschutzregelungen obliegt im föderativen System der Bundesrepublik Deutschland den Datenschutzbehörden der Länder. Die Zuständigkeit des/der BfDI beschränkt sich auf wenige spezifische Bereiche. Diesem Umstand muss bei der Vertretung der deutschen Aufsichtsbehörden im EDSA nach Art. 68 DS-GVO Rechnung getragen werden. Der LfDI M-V setzt sich daher dafür ein, dass die Vertretung der deutschen Aufsichtsbehörden im EDSA sowohl durch den/die BfDI als auch eine Landesaufsichtsbehörde erfolgen kann und die Stellvertretung dann dem jeweils anderen obliegt. Beide Vertreter sollten durch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestimmt werden.

Auch bei der Bestimmung des Stimmrechts im EDSA nach Abs. 2 ist der innerstaatlichen Zuständigkeitsverteilung für den Vollzug datenschutzrechtlicher Regelungen Rechnung zu tragen. Die für den Vollzug zuständigen Aufsichtsbehörden müssen die Möglichkeit erhalten, über den Vertreter im EDSA Angelegenheiten einzubringen und ihre jeweiligen Positionen im Verfahren autonom zu bestimmen. Wir empfehlen für Abs. 2 folgende Formulierung:

„In Angelegenheiten, die die Zuständigkeit der oder des Bundesbeauftragten nach § 9 dieses Gesetzes oder die alleinige Gesetzgebungskompetenz des Bundes betreffen, ist die oder der Bundesbeauftragte stimmberechtigt. Berührt die Angelegenheit die Zuständigkeit der Aufsichtsbehörden der Länder oder die Gesetzgebungskompetenz der Länder, ist der Leiter der Aufsichtsbehörde eines Landes stimmberechtigt. Lässt sich die Zuständigkeit nicht ermitteln, ist der gemeinsame Vertreter stimmberechtigt."

Zu § 18 BDSG-E Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

Hinsichtlich der in § 18 getroffenen Regelungen über die Zusammenarbeit wird auf den Beschluss „Vorschläge zu ersten Strukturfolgerungen aus der DS-GVO" nebst Ablage der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./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.

Absatz 2

Soll dennoch an dezidierten Regelungen festgehalten werden, empfehlen wir, Abs. 2, entsprechend unseren Ausführungen zu § 17 und unter dem Vorbehalt der Annahme unseres dortigen Formulierungsvorschlags, wie folgt zu fassen:

„Soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, legen die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vor. Einigen sich der gemeinsame Vertreter und sein Stellvertreter nicht auf einen Vorschlag für einen gemeinsamen Standpunkt, entscheidet der nach § 17 Abs. 2 Stimmberechtigte. Der nach den Sätzen 1 bis 3 vorgeschlagene Standpunkt ist den Verhandlungen zu Grunde zu legen, wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen. Der Bund und jedes Land haben jeweils eine Stimme. Enthaltungen werden nicht gezählt."

Absatz 3

Für Abs. 3 empfehlen wir dementsprechend die folgende Formulierung:

„Der gemeinsame Vertreter und dessen Stellvertreter sind an den gemeinsamen Standpunkt nach den Absätzen 1 und 2 gebunden und legen unter Beachtung dieses Standpunktes einvernehmlich die jeweilige Verhandlungsführung fest. Sollte ein Einvernehmen nicht erreicht werden, entscheidet der nach § 17 Abs. 2 Stimmberechtigte über die weitere Verhandlungsführung."

Zu § 20 BDSG-E Gerichtlicher Rechtsschutz

Nach Art. 58 Abs. 5 DS-GVO ist jeder Mitgliedstaat verpflichtet, Regelungen zu schaffen, die die Aufsichtsbehörden in die Lage versetzen, sich bei Verstößen gegen die DS-GVO an gerichtlichen Verfahren zu beteiligen, um die Bestimmungen der DS-GVO durchzusetzen. Im nationalen Recht darf hier kein Unterschied zwischen Unternehmen und öffentlichen Stellen

gemacht werden. Auch gegenüber öffentlichen Stellen muss die DS-GVO grundsätzlich durchgesetzt werden können. Es darf nicht dabei bleiben, dass Verstöße lediglich festgestellt werden können. Nach dem derzeitigen Gesetzentwurf ist eine Durchsetzung der DS-GVO gegenüber öffentlichen Stellen jedoch nicht realisierbar. Der vorliegende Gesetzentwurf regelt zwar die Beteiligung der Aufsichtsbehörden an verwaltungsgerichtlichen Verfahren und geht, wie § 20 Abs. 7 BDSG-E verdeutlicht, auch davon aus, dass der Erlass von Verwaltungsakten und deren Vollstreckung durch die Datenschutzaufsichtsbehörden auch gegenüber anderen Behörden zulässig sein sollen. Es fehlt aber an einer gesetzlichen Regelung, diese Theorie in die Praxis umzusetzen. Im Verwaltungsverfahren richtet sich die Vollstreckung entweder nach der Verwaltungsgerichtsordnung (VwGO) oder dem Verwaltungsvollstreckungsgesetz (VwVG) bzw. den entsprechenden landesrechtlichen Vorschriften. Eine Vollstreckung nach der VwGO kommt jedoch vorliegend nicht in Betracht. Diese setzt grundsätzlich einen vollstreckbaren Tenor voraus. Nach § 20 Abs. 5 Nr. 2 sind die Datenschutzaufsichtsbehörden jedoch nur als Beklagte (einer Anfechtungsklage) oder Antragsgegner (im vorläufigen Rechtsschutz) beteiligungsfähig. Der Gesetzentwurf sieht damit keine Beteiligung der Datenschutzaufsichtsbehörden in diesen Verfahren vor, die diese in die Lage versetzen würden, nach den Vorschriften der VwGO zu vollstrecken. Obsiegt die Datenschutzaufsichtsbehörde, wird die Anfechtungsklage abgewiesen, es gibt keinen vollstreckbaren Tenor und der angefochtene Verwaltungsakt der Datenschutzaufsichtsbehörde wird rechtskräftig. Gegenüber Unternehmen kann nun nach den Regelungen der Verwaltungsvollstreckung die DS-GVO durchgesetzt werden. Gegenüber öffentlichen Stellen hindern § 17 VwVG und die entsprechenden landesrechtlichen Regelungen jedoch die Durchsetzung, da die Vollstreckung hier nur zulässig ist, wenn eine spezialgesetzliche Regelung dies vorsieht. Eine entsprechende spezialgesetzliche Regelung muss daher zwingend im BDSG-E aufgenommen werden. Dies gilt insbesondere mit Blick auf die öffentlich-rechtlichen Wettbewerbsunternehmen, gegen welche nach § 41 Abs. 2 BDSG-E auch Bußgelder verhängt werden können.

Für Unternehmen sollte im Gesetz zudem eine klarstellende Regelung zur Vollstreckung getroffen und insbesondere Zwangsgelder beziffert werden. Wir empfehlen daher, folgenden Abs. 8 zu ergänzen:

> *„Die Bundesbeauftragte oder der Bundesbeauftragte kann ihre oder seine Maßnahmen zur Untersuchung nach Art. 58 Abs. 1 a-c, e und f DS-GVO und zur Abhilfe nach Art. 58 Abs. 2 b-h und j anstelle oder neben der Verhängung von Bußgeldern mit Zwangsmitteln nach den Bestimmungen des Verwaltungs-Vollstreckungsgesetzes durchsetzen. Dabei kann er oder sie die Zwangsmittel für jeden Fall der Nichtbefolgung oder Behinderung androhen. Die Höhe des Zwangsgelds beträgt bis zu 500.000,- Euro. Die Sätze 1-3 gelten auch für öffentliche Stellen.“*

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

In § 20 Abs. 7 zeigt sich, dass auch nach dem Grundverständnis des Gesetzentwurfes Datenschutzaufsichtsbehörden auch gegenüber öffentlichen Stellen Verwaltungsakte erlassen und diese notfalls auch vollstrecken können. Der Ausschluss der Anordnung der sofortigen Vollziehung ist jedoch problematisch. Auch im öffentlichen Bereich sind 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.

Zu § 21 BDSG-E Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission

Absatz 1

Der Anwendungsbereich des vorgesehenen Klagerechts der Aufsichtsbehörden wurde zwar gegenüber den bisherigen Entwürfen erweitert, ist aber nach wie vor zu eng. Durch die Verwendung des allgemeinen Begriffs „Verstöße“ in Art. 58 Abs. 5 DS-GVO kommt der Wunsch des europäischen Verordnungsgebers zum Ausdruck, für möglichst viele Maßnahmen den Rechtsweg zu eröffnen. Dies betrifft grundsätzlich alle abstrakt-generellen 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 EuGH ermöglichen, die unionsweit einheitliche Rechtsanwendung zu kontrollieren und somit zur Harmonisierung des Datenschutzrechts beizutragen.

Zu § 22 BDSG-E Verarbeitung besonderer Kategorien personenbezogener Daten

Die Regelungen wurden gegenüber den vorangegangenen Entwürfen teilweise verbessert. Deutlich wird dies u.a. in Abs. 1 Nr. 1 lit. b des Gesetzes, der nunmehr Art. 9 Abs. 3 DS-GVO berücksichtigt.

Dennoch bleibt es dabei, dass insbesondere Satz 2 das in Art. 9 Abs. 1 DS-GVO normierte Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aufhebt. Bestehende Öffnungsklauseln werden über deren Reichweite hinaus und unter Missachtung ihrer Anforderungen ausgefüllt. Die Erlaubnistatbestände 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. Gleichzeitig aber müssen 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. Die nunmehr ergänzte Interessenabwägung und die Maßnahmen nach Absatz 2 sind zwar zu begrüßen, es fehlt aber an angemessenen und vor allem ***spezifischen*** Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person.

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

In den §§ 23 und 24 BDSG-E wurde nunmehr der Regelungsgehalt aufgeteilt, der in den vorangegangen Entwürfen noch in einem § 23 zusammengefasst war. Die Vorschriften sind

nunmehr leichter verständlich und dem restriktiven Charakter von Art. 23 DS-GVO wurde, jedenfalls deutlicher als in den vorangegangenen Entwürfen, Rechnung getragen. Dennoch genügen die §§ 23, 24 BDSG-E nicht den Anforderungen des Art. 6 Abs. 4 i.V.m. 23 Abs. 1 DS-GVO. Artikel 6 Abs. 4 DS-GVO 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. 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. 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 allein 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.

Untragbar ist nunmehr die Regelung zur Zweckänderung in Satz 2. Die bisherige Regelung aus dem BDSG darf nicht übernommen werden, da sie mit Art. 6 Abs. 4 i.V.m. 23 Abs. 1 DS-GVO unvereinbar ist.

Zu § 26 Datenverarbeitung im Beschäftigungskontext

Die Regelungen zum Beschäftigtendatenschutz wurden gegenüber den vorangegangenen Entwürfen deutlich intensiviert. Dennoch können sie 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. Art. 88 DS-GVO verlangt spezifischere Regelungen. Die Regelung in Abs. 3 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, im BDSG-E einen Auffangtatbestand für alles zu schaffen. Bestehende Öffnungsklauseln sollten 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 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, 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 nur dann eingeschränkt werden, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen würden und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig wären. 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 2

In Hinblick auf Berufsgeheimnisträger ist eine Einschränkung der Befugnisse der Aufsichtsbehörden 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 unabhängigen Aufsichtsbehörden zielen unmittelbar darauf ab, das Vertrauensverhältnis zwischen Berufsgeheimnisträger und betroffener Person zu wahren, indem die Rechtmäßigkeit der Datenverarbeitung überprüft wird. Sie erfolgen im Interesse der betroffenen Personen und letztlich auch der Berufsgeheimnisträger. Mit einem neuen Gesetzentwurf der Bundesregierung zur Verhinderung von Abrechnungsbetrug, das in den nächsten Wochen in den Bundestag eingebracht werden soll,[1] sollen auch die Kompetenzen der dafür zuständigen Aufsichtsbehörden erweitert werden. Wird dies tatsächlich im Gesetz umgesetzt, ist nicht nachvollziehbar, warum Aufsichtsbehörden nach diesem Gesetz mehr Befugnisse gegenüber Berufsgeheimnisträgern haben sollten, als die Datenschutzaufsichtsbehörden.

Zu § 31 BDSG-E Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Wie auch die nachfolgenden Regelungen des 2. Kapitels ist § 31 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.

[1] http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/koalition-will-manipulation-von-arzt-diagnosen-verhindern-14704452.html.

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 § 32 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. Insbesondere mangels Interessenabwägung fehlt es hier an der Verhältnismäßigkeit.

Zu § 33 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 § 34 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 hier allerdings nicht gegeben. Es wurde bereits mehrfach erwähnt, dass ein unverhältnismäßiger Aufwand keine Einschränkung von Betroffenenrechten 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 § 35 Widerspruchsrecht

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

§ 38 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.

§ 39 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 § 39 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 § 41 BDSG-E Weitere Vorschriften für die Verhängung von Geldbußen

In § 41 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.

Vor dem Hintergrund der notwendigen Durchsetzbarkeit der DS-GVO ist die Vorschrift des § 41 Abs. 2, wonach gegen Behörden und sonstige öffentliche Stellen mit Ausnahme der Wettbewerbsunternehmen keine Bußgelder verhängt werden sollen, problematisch. Der im Bereich der DS-GVO nicht 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 § 44 nur unvollständig umgesetzt. Nicht übernommen werden die Grundsätze der Verhältnismäßigkeit der Datenverarbeitung und der sachlichen Richtigkeit der verarbeiteten Daten.

Zu § 50 BDSG-E Einwilligung

§ 50 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 § 53 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, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen erlaubt. In § 53 Abs. 1 S. 2 heißt es demgegenüber: *„Die Vorschrift muss sicherstellen, dass die berechtigten Interessen und Rechtsgüter in der betroffenen Person gewahrt werden. Dies ist insbesondere der Fall, wenn eine inhaltliche Bewertung und darauf gestützte Entscheidung durch den Verantwortlichen herbeigeführt und verlangt werden kann.“* Damit wird die in der JI-Richtlinie formulierte Mindestanforderung zur Regelanforderung.

Ausnahmen vom Verbot der automatisierten Einzelentscheidung sollten nur unter den bislang in § 6a Abs. 1 BDSG und den Landesdatenschutzgesetzen, insbesondere in § 9 DSG NRW geregelten Voraussetzungen zugelassen werden. Außerdem sollte sichergestellt werden, dass auf Profiling beruhende Entscheidungen, die für die betroffene Person eine nachteilige Rechtsfolge haben oder sie erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten zum Zweck der Bewertung einzelner Persönlichkeitsmerkmale gestützt werden dürfen, ohne dass der betroffenen Person die

Geltendmachung der eigenen Interessen möglich gemacht worden ist (vgl. hierzu § 4 Abs. 4 DSG NRW).

Zu § 54 BDSG-E Auskunftsrecht

Für die in § 54 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 Auskunfterteilung, 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.

Die in § 54 Abs. 6 S. 3 vorgesehene Einschränkung der Auskunft gegenüber der Aufsichtsbehörde ist in Art. 17 der JI-Richtlinie nicht vorgesehen. Wird die betroffene Person nach § 54 Abs. 5 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie gemäß § 54 Abs. 6 S. 1 ihr Auskunftsrecht auch über die/den BfDI ausüben. Macht die betroffene Person von diesem Recht Gebrauch, ist die Auskunft gemäß § 54 Abs. 6 S. 3 auf ihr Verlangen der/dem BfDI zu erteilen, soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

Zu § 52 BDSG-E Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

Gemäß § 52 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 § 52 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 § 56 BDSG-E Verfahren für die Ausübung der Rechte der betroffenen Person

Benachrichtigungen nach den §§ 62, 68 und 69 und die Bearbeitung von Anträgen nach den §§ 51 und 52 erfolgen nach § 56 Abs. 2 unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen der betroffenen Person kann der Verantwortliche allerdings entweder eine angemessene Gebühr verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. Unklar bleibt jedoch, in welchen konkreten Anwendungsfällen Anträge der betroffenen Person als offenkundig oder exzessiv einzustufen sind.

Hat der Verantwortliche begründete Zweifel an der der Identität der betroffenen Person, die Auskunfts-, Löschungs- und Berichtigungsansprüche geltend macht, kann er bei der betroffenen Person nach § 56 Abs. 3 zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind. Hier ist hervorzuheben, dass die personenbezogenen Daten, die zur Bestätigung der Identität erhoben wurden, auch nur für diese Zwecke verarbeitet und nicht länger gespeichert werden dürfen, als es für diesen Zweck notwendig ist (EG 41 der Richtlinie).

Zu § 59 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. § 59 setzt diese Anforderungen nur in unzureichender Weise um. Insbesondere sollte in § 59 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 Abs. 5 sollte die Nr. 5 auf zwei separate Punkte aufgeteilt werden, da sowohl die Informationspflicht der Auftragsverarbeiter als auch ihre Duldungs- und Mitwirkungspflicht bei Überprüfungen jeweils für sich genommen von großer Bedeutung sind. In Nr. 8 sollten Verweise auf § 63 (Datenschutzfolgenabschätzung) und § 67 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) ergänzt werden.

Systematisch sollten die Regelungen über die Auftragsverarbeitung nach den allgemeinen Anforderungen an die Sicherheit der Datenverarbeitung platziert werden, da sie darauf Bezug nehmen.

Zu § 60 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“.

Der letzte Satz von Abs. 1 kann entfallen, da der Aufwand zur Umsetzung der Maßnahmen bereits im Satz 1 als ein Kriterium enthalten ist.

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

Begrifflichkeit „Verhinderung unbefugten Löschens“, bei der Formulierung des § 60 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 §§ 61, 62 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 in § 61 noch ergänzt werden sollte. § 61 Abs. 2 gehört systematisch besser zu § 59, findet sich allerdings auch in Art. 30 Abs. 2 JI-Richtlinie.

Zu § 63 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 § 64 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, dass 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 § 65 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. 7 sollten explizit Angaben zur Rechtsgrundlage der Übermittlung aufgenommen werden (vgl. Art. 24 Abs. 1 lit. g der JI-Richtlinie). In Bezug auf 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 § 66 BDSG-E Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie gemäß § 66 als gemeinsam Verantwortliche. Hierzu ist festzulegen, dass sich Betroffene an jede der an dem Verfahren beteiligten gemeinsam Verantwortlichen wenden können. Diese Möglichkeit wird in Art. 21 Abs. 2 der JI-Richtlinie explizit vorgesehen. Dies ist auch deswegen sinnvoll, weil die Festlegungen in der angesprochenen Vereinbarung der Verantwortlichen zunächst nur Innenwirkung haben. Weiterhin 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 § 60 sowie die Verantwortlichkeiten für deren Umsetzung festlegen.

Zu § 67 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 § 67 BDSG-E erwähnt werden.

Zu § 73 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 § 73 Abs. 1 sollte ergänzend zur Richtlinie auch bei Veränderungen, Kombinationen und Löschungen von Daten die Identität des Verursachers bestimmt werden können. Weiterhin 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 § 74 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 nach §§ 60, 67 BDSG-E erforderlichen Maßnahmen und Vorkehrungen trifft.

Zu § 76 BDSG-E Datenübermittlung bei geeigneten Garantien

§ 76 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 Umgang 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 § 77 BDSG-E Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien

Ausnahmsweise können die Mitgliedstaaten nach Art. 38 Abs. 1 der JI-Richtlinie in den dort genannten Fällen auch dann Übermittlungen an ein Drittland oder an eine internationale Organisation zulassen, wenn weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete Garantien im Sinne des Art. 37 der JI-Richtlinie vorliegen. Als Schranke normiert Art. 38 Abs. 2 der JI-Richtlinie ein Abwägungserfordernis, wonach eine Übermittlung unterbleibt, wenn die übermittelnde zuständige Behörde feststellt, dass Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

Der hier ebenfalls bestehende Umsetzungsspielraum ist wiederum 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. Das unterbleibt, da § 77 Abs. 2 S. 1 die Schranke des Art. 38 Abs. 2 der JI-Richtlinie lediglich wiederholt.