Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD) sowie des Netzwerks Datenschutzexpertise zum

Referentenentwurf des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) – Stand 23.11.2016

Bezug: Ihre Mail vom 23.11.2016 – Verbändebeteiligung zum Datenschutz-Anpassungs- und Umsetzungsgesetz

Sehr geehrte Frau Dr. Wichmann,

sehr geehrte Damen und Herren,

für Ihre Einladung zur Stellungnahme zum o. g. Gesetzentwurf bedanken wir uns. Der Aufforderung kommen wir hiermit gerne nach. Die Stellungnahme ergeht im Namen der DVD wie auch des Netzwerks Datenschutzexpertise und bezieht sich insbesondere auf ein neues Bundesdatenschutzgesetz (BDSG-neu).

A Allgemeine Erwägungen

Es wird begrüßt, dass der Bundesgesetzgeber ein Gesetz zur Umsetzung der Europäischen Datenschutzgrundverordnung (EU 2016/679, künftig DSGVO) sowie der der Europäischen Datenschutzrichtlinie für Justiz und Inneres (EU 2016/680, künftig JI-Richtlinie) anstrebt. Nur so kann erreicht werden, dass die Anwender der Regelungen einen rechtssicheren Überblick haben, welche europäischen und nationalen Regelungen Gültigkeit haben, wenn die DSGVO und die JI-Richtlinie im Mai 2018 direkte Wirksamkeit entfalten.

Es sollte darauf geachtet werden, dass nationale Regelungen, denen kein eigenständiger Regelungsgehalt zukommt, europäische Vorgaben **nicht einfach wiederholen**. Vielmehr sollte im Interesse der Klarheit und Rechtssicherheit jeweils auf die direkt anwendbaren Normen verwiesen werden, wenn dadurch nicht die Gesamtverständlichkeit des Normtextes leidet. Bei der Konkretisierung europäischer Normen durch nationale Regelungen auf der

Grundlage von sog. Öffnungsklauseln, also der europarechtlichen Zulassung nationaler Rechtsetzung, sollte grundsätzlich ein **Verweis auf die zulassende europäische Norm** erfolgen.

B Ausstattung der Aufsichtsbehörden

In Ihrem Anschreiben wurde darum gebeten, eine Einschätzung abzugeben, welche ggfs. Einsparungen und welcher **Aufwand** sich **für die Länder** aus dem Vollzug des geänderten Datenschutzrechts ergeben. Die neuen Regelungen der DSGVO begründen insbesondere für die Datenschutzaufsicht, also zumeist die Dienststellen der Landesbeauftragten für Datenschutz, Aufgaben insbesondere in folgenden Bereichen:

- Zusammenarbeit mit Verantwortlichen, Auftragsverarbeitern und deren Vertretern (Art. 31 DSGVO),
- Entgegennahme und Bearbeitung der Meldungen von Datenschutzverletzungen (Breach Notification, Art. 33 DSGVO),
- Definition der Kriterien, Entgegennahme, Kommunikation, Prüfung und Bewertung von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 4 – 6 DSGVO) sowie Konsultation bei hohem Risiko (Art. 36 DSGVO),
- Entgegennahme der Meldungen von Datenschutzbeauftragten (Art. 37 Abs. 7 DSGVO) sowie Zusammenarbeit mit diesen (Art. 38 Abs. 1 lit. d, e DSGVO),
- Förderung der Ausarbeitung, Bewertung und Genehmigung von Verhaltensregeln (Art. 40 Abs. 1, 5 DSGVO) sowie die Überwachung und Kommunikation hierzu (Art. 41),
- Förderung und Überprüfung von Zertifizierungen (Art. 42, 43 DSGVO),
- Bewertung des internationalen Datentransfers durch Prüfung und Genehmigung von Vertragsklauseln und anderen Bestimmungen und gegebenenfalls Durchführung von Kohärenzverfahren hierzu sowie internationale Zusammenarbeit (Art. 46 Abs. 3, 4, 47 Abs. 1, 50 DSGVO),
- Wahrnehmung der Aufgaben nach Art. 57 DSGVO (s. o. sowie u. a. Überwachung, Durchsetzung, Information und Beratung für Öffentlichkeit, Verantwortliche u. Auftragsverarbeiter, Bearbeitung von Beschwerden, Zusammenarbeit mit anderen Aufsichtsbehörden, Festlegung von Standardvertragsklauseln und verbindlichen internen Vorschriften),
- Aufbau und Pflege von elektronischen Kommunikationsmitteln (Art. 57 Abs. 2 DSGVO),
- Wahrnehmung der Befugnisse zur Untersuchung, Abhilfe, Genehmigung und Sanktion (Art. 58 Abs. 1-3, 5 DSGVO)

- Wahrnehmung weiterer Befugnisse, z. B. im Bereich der Informationsfreiheit (Art. 58 Abs. 6 DSGVO),
- Erstellen von Jahresberichten (Art. 59 DSGVO),
- Zusammenarbeit mit den Aufsichtsbehörden des Bundes und der Länder (§ 18 BDSG-neu)
- Zusammenarbeit und Durchführung von Kohärenzverfahren (Art. 60-67 DSGVO),
- Zusammenarbeit und Beteiligung (als betroffene Aufsichtsbehörde) im Rahmen der Tätigkeit des Europäischen Datenschutzausschusses (Art. 68 Abs. 4, 70 DSGVO, § 17 BDSG-neu),
- Durchführung von Gerichtsverfahren (Art. 78 DSGVO), Anfechtung von Kommissionsentscheidungen (§ 21 BDSG-neu).

Entsprechende Aufgaben haben die Datenschutzaufsichtsbehörden auch gemäß der **JI-Richtlinie**.

Viele der o. g. Aufgaben gehen **über die bisher bestehenden Aufgaben weit hinaus**, insbesondere was neue Instrumente, die (internationale) Zusammenarbeit, Genehmigungen und die Durchführung von gerichtlichen Verfahren betrifft.

Das Bundesverfassungsgericht (BVerfG) hat festgestellt, dass insbesondere im für die Betroffenen intransparenten öffentlichen **Sicherheitsbereich** bei den Aufsichtsbehörden regelmäßige Prüfpflichten bestehen, denen viele Aufsichtsbehörden wegen der unzureichenden Ausstattung nicht oder nur unvollständig nachkommen können (BVerfG U. v. 24.04.2013, 1 BvR 1215/07, Rn. 204 ff., 217 – ATDG = NJW 2013, 1517). Es ist unbestritten, dass die Aufsichtsbehörden schon mit ihrer bisherigen Ausstattung den ihnen obliegenden Aufgaben nicht angemessen nachkommen können (Schulzki-Haddouti in Stiftung Datenschutz, Zukunft der informationellen Selbstbestimmung, 2016, S. 111 ff.; diess, Zu kurz gekommen, c´t 17/2015, 76 ff.).

Gemäß Art. 52 Abs. 2 DSGVO stellt jeder Mitgliedstaat sicher, „dass jede Aufsichtsbehörde mit den **personellen, technischen und finanziellen Ressourcen**, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können“.

Die **Mehrausgaben der Länder** beschränken sich nicht auf die Wahl und Bestellung des Stellvertreters des gemeinsamen Vertreters im Europäischen Datenschutzausschuss gem. § 17 BDSG-neu. Insofern ist die Aussage der Gesetzesbegründung „Weiterer neuer

Erfüllungsaufwand entsteht für die Verwaltung nicht“ (S. 4) nicht zutreffend, wenn der Gesetzentwurf und die Umsetzung der DSGVO gemeinsam betrachtet werden.

Eine nähere **Bezifferung des Ressourcenbedarfs** bei den Ländern ist im Rahmen der vorliegenden Stellungnahme nicht möglich. Hierfür bedarf es eigenständiger Untersuchungen. Unabhängig hiervon und ungeachtet der teilweise sehr unterschiedlichen Ausstattung der Aufsichtsbehörden in den Ländern ist im Rahmen einer überschlägigen Schätzung zumindest eine Verdreifachung des bisherigen Personals und eine entsprechende Erweiterung der Ressourcen nötig, um die bestehenden und künftigen Aufgaben adäquat erfüllen zu können. Mit der Aufstockung des Personals sollte umgehend begonnen werden um zu verhindern, dass bei kurzfristig nötigen Einstellungen nicht ausreichend qualifiziertes Personal eingestellt wird. Spätestens im Jahr 2020 sollte eine umfassende Erhebung durchgeführt werden, ob und inwieweit die Ausstattung der Aufsichtsbehörden den neuen Anforderungen entspricht.

C Einzelstellungnahme zum Entwurf eines neuen BDSG

Zu § 2 Begriffsbestimmungen

Eine **Wiederholung der Begriffsbestimmungen** aus Art. 4 DSGVO, wie sie in Abs. 2 geplant ist, ist nicht zu empfehlen. Vielmehr sollte auf die DSGVO verwiesen werden. Im Interesse der Rechtsklarheit besteht für den nationalen Gesetzgeber ein sehr weit gehendes Verbot, europäische Regelungen zu wiederholen (Kühling, Martini u. a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 6 ff.; vgl. auch die Gesetzesbegründung S. 68). Für Begriffsbestimmungen im Hinblick auf die JI-Richtlinie (Gesetzesbegründung S. 72) genügt ein Verweis auf die Geltung der Begriffsbestimmungen der DSGVO.

In den in § 2 BDSG-neu enthaltenen Begriffsbestimmungen fehlt eine Zuordnung der in der DSGVO verwendeten Begriffe „Behörde“, „**öffentliche Stelle**“ und „Unternehmen“ zu den auch im BDSG-neu verwendeten Begriffen „öffentliche Stelle“ und „nicht-öffentliche Stellen“. So sind gemäß Art. 4 Ziffer 18 DSGVO auch öffentliche Stellen in öffentlich-rechtlicher Trägerschaft, die am Wettbewerb teilnehmen, als Unternehmen zu betrachten, während nach dem § 2 Abs. 2 Ziff. 3 BDSG-neu nur privatrechtlich organisierte öffentliche Stellen (des Bundes) als nicht-öffentliche Stellen angesehen werden.

Es wird darauf hingewiesen, dass durch das Außerkrafttreten des **bisherigen Bundesdatenschutzgesetzes** (BDSG-alt) gemäß Art. 10 am 25.05.2018 auch die darin enthaltenen Begriffsbestimmungen aufgehoben werden, auf die weiterhin in Kraft befindliche spezifische Regelungen im deutschen Recht Bezug nehmen. Es wird deshalb angeregt, insofern eine Übergangsregelung vorzusehen.

Zu § 3 Verarbeitung durch öffentliche Stellen

Die Regelung ist wegen Art. 6 Abs. 1 lit. e überflüssig, aber auch unschädlich. Es wird empfohlen, eine explizite Bezugnahme zu Art. 6 Abs. 1 lit e DSGVO aufzunehmen.

Zu § 4 Videoüberwachung

Eine materielle Sonderregelung zur Videoüberwachung ist unzulässig, da insofern Art. 6 DSGVO weitgehend abschließend ist (Kühling/Martini u. a. S. 343 ff.; Roßnagel, Europäische Datenschutz-Grundverordnung, 2016, S. 52 f.). Dies gilt auch für den geplanten Abs. 1 Nr. 2, wonach bei Videoüberwachung durch nicht-öffentliche Stellen **Sicherheitsbelange** „in besonderem Maße zu berücksichtigen“ sind. Diese Vorrangregelung bewirkt bei der Interessenabwägung einen Vorrang von Sicherheitsinteressen bei öffentlicher Videoüberwachung, nimmt private Stellen für öffentliche polizeiliche Sicherheitsbelange in Anspruch und verletzt dadurch die Gesetzgebungsbefugnis der Länder, den Verhältnismäßigkeitsgrundsatz sowie spezifische Grundrechte wie z. B. das Versammlungsrecht gemäß Art. 8 GG. Dieses Ergebnis wird verstärkt durch die Regelung in Abs. 3, die bei Erforderlichkeit „zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten“ ohne eine Angemessenheitsprüfung eine Zweckänderung erlaubt. Auf die gesonderte Stellungnahme der DVD und des Netzwerks Datenschutzexpertise vom 06.11.2016 wird verwiesen (https://www.datenschutzverein.de/wp-content/uploads/2016/11/Stellungnahme_Videoueberwachung_06112016.pdf).

Zu § 11 Ernennung und Amtszeit der BfDI

Die § 22 Abs. 1 BDSG-alt übernehmende Regelung des Abs. 1 sieht vor, dass der deutsche Bundestag die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) „ohne Aussprache auf Vorschlag der Bundesregierung (…) mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder“ wählt. Die Wahl setzt voraus, dass die BfDI „das 35. Lebensjahr vollendet“ hat. In Abs. 1 S. 4 wird geregelt: „Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung nachgewiesene Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Dienst haben.“ Gemäß Abs. 3 ist bei einer Amtszeit von 5 Jahren eine einmalige Wiederwahl zulässig.

Die Beachtung rechtlicher Anforderungen an das Verfahren der Bestellung und die Qualifikation der Datenschutzbeauftragten stand lange Zeit nicht im Fokus öffentlicher Diskussion. Dies hat sich mit dem **Gutachten des Netzwerks Datenschutzexpertise** vom 17.11.2016 geändert, in dem sowohl die rechtlichen Anforderungen wie auch die Praxis

kritisch hinterfragt werden. Dabei erweist sich, dass die bisherige Praxis, die mit dem vorliegenden Regelungsvorschlag fortgeschrieben werden soll, gegen Vorgaben des Europarechts und des Verfassungsrechts verstößt (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi5.pdf).

Der Regelungsvorschlag sieht keine öffentliche Ausschreibung der Stelle der BfDI vor und schließt ausdrücklich eine Aussprache über die Wahl aus. Dies steht in Widerspruch zu Art. 53 Abs. 1 DSGVO, wonach das Mitglied der Aufsichtsbehörde „im Wege eines **transparenten Verfahrens** ernannt wird“. Die Transparenzanforderung zielt auf eine öffentliche demokratische Debatte zur Bestellung und die Gewährleistung einer hohen Legitimation und gleicher Chancen der qualifizierten Kandidaten ab. Dies war bisher und würde auch künftig nicht gewährleistet. Die geplante Regelung ist insofern europarechtswidrig.

Art. 33 Abs. 2 Grundgesetz (GG) ist zu beachten, wonach jeder Deutsche „nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt“ hat.

Das Erfordernis eines **Mindestalters** von 35 Jahren stellt eine nicht gerechtfertigte Altersdiskriminierung dar (Art. 3 Abs. 1 GG, Art. 21 Abs. 1 Europäische Grundrechte-Charta – GRCh). Die abschließenden persönlichen Anforderungen des Art. 53 Abs. 2 DSGVO stellen nicht auf das Alter ab. Der Verweis der Gesetzesbegründung (S. 77) auf Art. 54 Abs. 1 lit. b DSGVO („sonstige Voraussetzungen“) legitimiert keine unsachlichen Anforderungen. Personen unter 35 Jahren können die geforderte Erfahrung und Sachkunde vorweisen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Das Erfordernis der Befähigung zum **Richteramt oder höheren Dienst** war historisch begründet, als die Datenschutzbeauftragten weitgehend nur für die Kontrolle des öffentlichen Bereichs zuständig waren. Das Erfordernis findet sich nicht in Art. 53 Abs. 2 DSGVO und ist auch keine adäquate Beschreibung der Qualifikation und Sachkunde. Daher sollte auf diese Einschränkung verzichtet werden.

Die Beschränkung auf eine **einmalige Wiederwahl** findet sich nicht in der abschließenden Aufzählung der personellen Anforderungen an das Mitglied der Aufsichtsbehörde in Art. 53 Abs. 2 DSGVO. Amtsinhaber, die zwei Amtsperioden absolviert haben, können regelmäßig die dort geforderte Erfahrung, Qualifikation und Sachkunde vorweisen. In der Praxis hat sich gezeigt, dass durch mehrfach wiedergewählte Datenschutzbeauftragte eine qualifizierte Amtsausübung gewährleistet wird. Angebliche Gründe für eine Beschränkung, etwa Erlahmen der Innovationsbereitschaft, treffen nicht zu. Es gibt keine Widerwahlverbote in vergleichbaren Positionen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Zu § 13 Rechte und Pflichten der BfDI

In Abs. 5 S. 2 ist vorgesehen, dass die BfDI keine **Aussagebefugnis als Zeugin** hat, soweit

die Aussage laufende oder abgeschlossene Vorgänge betrifft, „die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten“. In diesen Fällen muss das „Benehmen mit der Bundesregierung“ hergestellt werden. Was zum Kernbereich exekutiver Eigenverantwortung der Bundesregierung zu zählen ist, ist völlig unklar. Dadurch, dass schon die Möglichkeit eines solchen Betroffenseins dazu führt, dass die Aussagebefugnis von einem Benehmen mit der Bundesregierung abhängig gemacht wird, wird die Unabhängigkeit der BfDI unangemessen beeinträchtigt. Es wird vorgeschlagen, insofern eine Kann-Regelung bzgl. der Aussageverweigerung vorzusehen sowie eine Sollregelung in Bezug auf das Benehmen mit der Bundesregierung.

Zu § 14 Aufgaben der BfDI

Die DSGVO sieht als Aufgabe von Aufsichtsbehörden auch „Datenschutzzertifizierungsmechanismen und von **Datenschutzsiegeln und -prüfzeichen** nach Artikel 42 Absatz 1“ vor. (Art. 57 Abs. 1 lit. n DSGVO). Datenschutz-Zertifizierung gibt es bisher in Deutschland zwar nur auf Länderseite und ist auch künftig als Aufgabe für die BfDI nicht vorgesehen. Dies entspricht nicht den aktuellen technischen und rechtlichen Erfordernissen, die in der DSGVO erkannt und festgelegt werden.

Zu § 16 Befugnisse der BfDI

In Abs. 2 ist vorgesehen, dass außerhalb des Anwendungsbereichs der DSGVO bei der Feststellung von Datenschutzverstößen durch öffentliche Stellen – wie bisher – lediglich als „Sanktion“ eine Beanstandung zulässig ist. Diese Regelung ignoriert die Regelungsintention des neuen europäischen Datenschutzrechts, angesichts der großen Umsetzungsdefizite beim Datenschutz – auch im öffentlichen Bereich – wirksame Sanktionen zu ermöglichen. **Beanstandungen** haben sich insbesondere im Sicherheitsbereich oft als wirkungslos erwiesen, da sie kein rechtliches Instrument sind, mit dem Verantwortliche zu rechtskonformem Vorgehen gebracht werden können. Dies haben zuletzt die Datenschutzverstöße durch den Bundesnachrichtendienst (BND) gezeigt. Mit der Regelung wird gerade im Bereich der JI-Richtlinie sowie der Geheimdienste auf eine effektive Sanktionsform verzichtet. Sollen finanzielle Sanktionen sowie Unterlassungs- und Beseitigungsverfügungen nicht möglich sein, so muss der BfDI zumindest ein Klagerecht vor Gericht gegen rechtswidrige Datenverarbeitung eröffnet werden.

Die Regelung des Abs. 3 S. 1, wonach sich die Befugnisse der BfDI auch auf **Post- und Telekommunikationsgeheimnisse sowie auf Steuergeheimnisse** erstrecken, ist historisch begründet und inzwischen eine Selbstverständlichkeit, welcher es nicht bedarf. Auf sie sollte deshalb verzichtet werden.

Zu § 17 Vertretung im Europäischen Datenschutzausschuss (EDSA)

In Abs. 1 ist vorgesehen, dass die BfDI die gemeinsame Vertretung Deutschlands im Datenschutzausschuss (EDSA) wahrnimmt. Die Stellvertretung soll aus den Leitungen der Landes-Aufsichtsbehörden vom Bundesrat ausgewählt werden. Bei Angelegenheiten, die insbesondere die Länderaufsicht betreffen, soll nach Abs. 2 im EDSA vorrangig die Stellvertretung tätig werden. Diese Regelung ist nicht sachgerecht und beeinträchtigt die Unabhängigkeit der Landesaufsichtsbehörden.

Hauptaufgabe des EDSA wird die Festlegung von Positionen im Bereich des **Datenschutzes im nicht-öffentlichen Bereich** (oder in der Begrifflichkeit der DSGVO: **für Unternehmen**) sein. Insofern hat die BfDI – abgesehen von Post- und Telekommunikationsunternehmen – weder Kompetenzen noch Erfahrungen. Diese liegen vielmehr bei den Landesaufsichtsbehörden.

Durch die **Bestimmung der Stellvertretung** durch den Bundesrat wird dem Bundesrat die Möglichkeit eröffnet, am Willen der Aufsichtsbehörden vorbei unter Anlegung sachfremder Erwägungen für diese deren Vertretung zu benennen. Dies kann zur Folge haben, dass die dadurch in den EDSA eingebrachten Positionen nicht die der unabhängigen Aufsichtsbehörden repräsentieren. Die Regelung ist völlig unangemessen.

Es wird vorgeschlagen, die Bestimmung der Vertretung und der Stellvertretung der deutschen Aufsichtsbehörden diesen selbst zu überlassen. Diese sollten mit qualifizierter Mehrheit ihre **Vertretung im EDSA selbst wählen**. Dieser Vorschlag entspricht der „Kühlungsborner Erklärung“ der unabhängigen Datenschutzbehörden der Länder vom 10.11.2016 (https://www.datenschutz.de/kuehlungsborner-erklaerung-der-unabhaengigen-datenschutzbehoerden-der-laender-vom-10-november-2016/).

Zu § 18 Verfahren der Zusammenarbeit der Aufsichtsbehörden

Zur Bestimmung von gemeinsamen Positionen der deutschen Aufsichtsbehörden soll gemäß Abs. 2 zunächst ein **Einigungsverfahren** angestrebt werden. Gelingt eine Einigung nicht, so soll der Vertreter bzw. in Länderangelegenheiten der Stellvertreter ein Bestimmungsrecht haben, „wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen“. Wegen der nicht repräsentativen Festlegung der Vertretung (s. o. zu § 17) wird damit in die Unabhängigkeit der Aufsichtsbehörden unangemessen eingegriffen.

Nach Abs. 3 S. 2 soll im Falle, dass eine Einigung unter den deutschen Aufsichtsbehörden nicht möglich ist, der Stellvertreter ein Bestimmungsrecht haben, wenn „die Angelegenheit die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das **Recht zur Gesetzgebung** haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betrifft“. Die Regelung ist unklar: Das Recht der Gesetzgebung liegt in vielen Fällen des

Datenschutzrechtes, insbesondere auch im nicht-öffentlichen Bereich, beim Bund, während die hier in Frage stehende Verwaltungskompetenz bei den Ländern liegt. In der Regelung ist daher der Verweis auf die Gesetzgebungskompetenz zu streichen.

Zu § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

In der Regelung werden wesentliche Inhalte des Art. 9 DSGVO wiederholt, ohne weitere Präzisierungen vorzunehmen. Diese Regelung ist wegen der reinen **Paraphrasierung** ohne eine zusätzliche Regelungsabsicht rechtswidrig (Kühling/Martini u. a., S. 6 ff. m. w. N.). Auf sie sollte verzichtet werden.

In Abs. 2 werden Aussagen gemacht, was „**angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Personen“ gemäß Art. 9 Abs. 1 DSGVO sind. Problematisch ist hierbei, dass auf die „Implementierungskosten“ Bezug genommen wird, die in Art. 32 DSGVO bzgl. der informationstechnischen Sicherheit, nicht aber bzgl. der Gestaltung von Verfahren nach Art. 25 DSGVO oder materiell-prozessualen Vorkehrungen relevant sein sollen. Selbstverständlich können solche Kosten bei Angemessenheitsentscheidungen eine Rolle spielen. Deren explizite Erwähnung eröffnet aber die Möglichkeit, spezifische Maßnahmen allein aus Kostengründen zurückzuweisen. Wenig förderlich ist auch der Verweis auf Sensibilisierungs- und Schulungsmaßnahmen (Abs. 2 Satz 2 Nr. 2). Die in Abs. 2 enthaltenen Erwähnungen sind nicht vollständig und weisen erst recht nicht auf eine Priorisierung hin. Die Regelung ist daher nicht geeignet, eine Konkretisierung der europäischen Vorgaben zu bewirken. Daher sollte auf sie verzichtet werden.

Es ist nicht erkennbar, weshalb die Anwendung von Abs. 2 im Fall des Abs. 1 lit. b (**Datenverarbeitung im Gesundheits- und Sozialbereich durch Berufsgeheimnisträger**) ausgeschlossen wird. Zwar werden auch in Art. 9 Abs. 3 DSGVO mit der Regelung zu Berufsgeheimnisträgern die angemessenen spezifischen Sicherungsmaßnahmen erwähnt, doch erfolgt dies systematisch an einem anderen Ort. Es dürfte nicht bestritten werden können, dass solche Maßnahmen auch und gerade erforderlich sind, wenn hochsensible Daten, die Berufsgeheimnissen unterliegen, verarbeitet werden.

Zu § 23 Zweckänderungen

In der Norm werden eine Vielzahl von Zweckänderungen erlaubt, die schon derzeit ihre Erlaubnisgrundlage in der DSGVO finden. Insofern sind sie überflüssig und wegen der **reinen Wiederholung** europäischer Normvorgaben unzulässig.

In Abs. 2 Nr. 1-3 werden Zweckänderungen für **nicht-öffentliche Stellen** erlaubt, für Sicherheitszwecke, zur Geltendmachung rechtlicher Ansprüche und zur Wahrung berechtigter Interessen. Dies entspricht den in Art. 6 Abs. 1 DSGVO vorgegebenen Verarbeitungsbefugnissen, ohne jedoch eine Abwägungsklausel zu enthalten, über welche die schutzwürdigen Betroffeneninteressen zu berücksichtigen sind, so wie dies Art. 6 Abs. 1 lit. f

DSGVO explizit fordert. Damit unterschreiten diese Normen in unzulässiger Weise das europäische Schutzniveau. Auf sie kann wegen der bestehenden europäischen rechtlichen Rahmenbedingungen vollständig verzichtet werden.

Die in Abs. 3 enthaltenen Zweckänderungsregelungen für **sensitive Daten** nach Art. 9 DSGVO enthalten auch keine expliziten Abwägungspflichten und paraphrasieren Art. 9 Abs. 2 DSGVO. Auch auf diese allgemeinen Regelungen sollte vollständig verzichtet werden. Bisher besteht im nationalen Recht eine Vielzahl konkretisierender bereichsspezifischer Regelungen, z. B. in den Sozialgesetzbüchern, die ihre Gültigkeit behalten. Diese genügen zur Wahrung der bisherigen – legitimen – Verarbeitungsbefugnisse.

Zu § 24 Verarbeitung von Beschäftigtendaten

Die Wiederauflage des völlig **missglückten § 32 BDSG**-alt ist abzulehnen. Diese Norm führte zu Rechtsunsicherheit, nicht zur Präzisierung von Verarbeitungsbefugnissen und Betroffenenrechten. Zudem darf bezweifelt werden, dass die vorgesehene Regelung den Anforderungen des Art. 88 Abs. 2 DSGVO standhält. Es bedarf vielmehr eines umfassenden Beschäftigtendatenschutzgesetzes, wozu das Netzwerk Datenschutzexpertise die relevanten Rahmenbedingungen in seinem Gutachten vom 08.04.2016 benannt hat (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf).

Zu § 25 Zwecke der wissenschaftlichen Forschung

Die geplante Forschungsregelung ist unvollständig und unterschreitet das in der DSGVO vorgeschriebene Niveau. Unvollständig ist Abs. 1 im Hinblick auf sensitive Daten gemäß Art. 9 Abs. 1 DSGVO dadurch, dass eine Konkretisierung von angemessenen Schutzmaßnahmen, wie in Art. 9 Abs. 2 lit. j DSGVO gefordert, unterlassen wird. Art. 89 Abs. 1 DSGVO sieht vor, dass die Datenverarbeitung zu „Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (…) geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person“ zu unterliegen hat. Derartige Schranken enthält der vorgelegte Entwurf nicht. Unvollständig ist die Regelung auch im Hinblick auf die Verarbeitung von Berufsgeheimnissen, z. B. dem Patientengeheimnis unterliegenden Daten, da insofern weiterhin § 203 StGB als Hindernis zur Einbeziehung in Forschungsvorhaben bestehen bleibt. Tatsächlich werden keine ausreichenden und effektiven Schutzmaßnahmen geregelt, sondern lediglich ein Minimalkatalog beliebiger Vorkehrungen. So wird es z. B. unterlassen, ein explizites beschlagnahmesicheres Forschungsgeheimnis festzuschreiben. Unbefriedigend ist die Regelung insgesamt, da sie nicht das Ziel verfolgt, den Wirrwarr unterschiedlicher spezifischer Forschungsklauseln im Bundes- und im Landesrecht zu vereinheitlichen und zu modernisieren. Zur Sicherung des Datenschutzes in der Forschung und einer damit verbundenen Stärkung des Forschungsstandortes Deutschland bedarf es eines

umfassenden **Forschungsgesetzes**, das, um auch die Regelungsebene der Länder mit einzuschließen, als Bund-Länder-Staatsvertrag erlassen werden sollte.

Zu § 26 Berufsgeheimnisse

Die Regelung beschreibt nur völlig unzureichend, welche Daten mit ihr erfasst werden sollen und ist deshalb **zu unbestimmt**: Die Formulierung „Daten, die nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, einer Geheimhaltungspflicht unterliegen“ könnte auf jede Form eines spezifischen Geheimnisses angewendet werden, nicht nur auf Berufsgeheimnisse nach § 203 Abs. 1, (2a,) 3 StGB, § 53, 54 StPO, sondern auch auf das Sozialgeheimnis nach § 35 SGB I, ja sogar auf weitgehend unreguliert bleibende Betriebs- und Geschäftsgeheimnisse. In der Literatur wird diese Regelung – fälschlich – gar auf Amtsgeheimnisse wie z. B. das Statistik- oder das Meldegeheimnis erstreckt (Paal/Pauly, Datenschutz-Grundverordnung, 2016, Art. 90 Rn. 6). Es bedarf vielmehr einer rechtssicheren Verweisung auf einen engen Kranz aus besonderen Gründen gesondert zu behandelnder Daten.

Gemäß den Absätzen 1 und 2 werden das Informationsrecht nach Art. 14 DSGVO und das **Auskunftsrecht** nach Art. 15 DSGVO eingeschränkt, „wenn die Daten geheim gehalten werden müssen und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss“. Die Unbestimmtheit der erfassten Daten erstreckt sich auf diese Beschränkung informationeller Selbstbestimmung generell und des Auskunftsanspruchs als „Magna Charta des Datenschutzes“ (s. u. zu § 32). Damit wird die grundlegende Garantie des Auskunftsanspruchs in Art. 8 Abs. 2 S. 2 GRCh verletzt. Diese Unbestimmtheit wird erweitert durch eine völlig offene Abwägungsnorm, die weder für Anwender noch für Betroffene einschätz- und berechenbar ist. Die Einschränkung des Auskunftsanspruchs muss sich auf spezifische Fallgestaltungen beschränken, die notwendig und verhältnismäßig sind. Die vorliegende Regelung genügt diesen Anforderungen nicht und ist europarechts- und verfassungswidrig.

In Abs. 3 werden die in Abs. 1 beschriebenen Daten pauschal einer stark **beschnittenen Datenschutzkontrolle** durch die zuständige Aufsicht unterworfen. Kontrollbefugnisse sollen nur zwecks Überprüfung der Einhaltung des Art. 25 DSGVO bestehen. Art. 25 DSGVO bezieht sich auf die Technikgestaltung und datenschutzfreundliche Voreinstellungen, also auf technische und organisatorische Maßnahmen. Dabei bleibt der vorgesehene Kontrollumfang unklar, da er Art. 32, d. h. die technische Sicherheit der Verarbeitung, nicht umfasst. Umfasst sein sollen offensichtlich auch nicht Fragen der materiellen Zulässigkeit der Verarbeitung. Bisher ist es unbestritten, dass zu den in die Kontrolle einbezogenen Daten auch Berufsgeheimnisse gehören. Bisher gehört die Kontrolle der Wahrung des Patienten- und den Sozialgeheimnisses zu den Schwerpunkten der aufsichtsbehördlichen Tätigkeit. Diese würde vollständig ausgeschlossen, selbst dann, wenn die Kontrolle auf Beschwerde von Betroffenen

erfolgen würde. Im ärztlichen und psychologischen Bereich wurde die Datenschutzkontrolle bisher auch von den geprüften Stellen nicht in Frage gestellt. Sie ist vielmehr oft ein Instrument, um das Vertrauen in die jeweiligen Stellen zu erhöhen.

Durch die vorgesehene weitgehende Ausnahme von der Datenschutzkontrolle wird das von der DSGVO verfolgte Ziel einer weitgehenden **Harmonisierung** verfehlt. Sie hat auch zur Folge, dass vom Europäischen Datenschutzausschuss gemäß Art. 70 DSGVO erarbeitete Leitlinien, Empfehlungen und bewährte Verfahren nur begrenzt ein- und umgesetzt werden können.

Die Begründung (S. 93) verweist auf die bundesverfassungsgerichtliche Rechtsprechung, wonach das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet werden darf (BVerfG U. v. 12.04.2005, NJW 2005, S. 1917). Dies schließt aber eine externe Kontrolle der Rechtmäßigkeit des Berufsgeheimnisträgers nicht aus. Es genügt, dass Abs. 2 S. 2 die Geheimhaltungspflicht auf die Aufsichtsbehörde verlängert und ein Beweisverwertungsverbot im Strafverfahren schafft. Politisch angegriffen wird die Kontrollbefugnis der Datenschutzaufsicht im nicht-öffentlichen Bereich ausschließlich durch Anwaltsorganisationen. Praktische Probleme sind in diesem Bereich aber in der 40-jährigen Aufsichtsgeschichte nur in wenigen Einzelfällen aufgetreten, die durch eine Berücksichtigung des **Mandantengeheimnisses** bei der Datenschutzkontrolle aufgelöst werden konnten. Der Anwaltschaft geht es darum, sich der unabhängigen Datenschutzkontrolle nicht zum Schutz der Mandanten und des Mandantengeheimnisses zu entziehen, sondern zur Freistellung von Kontrolle generell. Es ist unbestreitbar, dass auch Anwälte dem Datenschutzrecht unterliegen und unterliegen müssen (ausführlich dazu Weichert NJW 2009, 550 ff.; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 38 Rn. 11 m. w. N.).

Es ist nicht erkennbar, wie eine Datenschutzkontrolle durchgeführt werden soll, die sich auf Art. 25 DSGVO beschränkt, da mit einer Kontrolle von Art. 25 DSGVO oft zwangsläufig die Kenntnisnahme von Berufsgeheimnissen verbunden ist. Eine **Trennung auf Kontrollebene** zwischen technischem und materiellem Datenschutz ist zumeist nicht möglich.

Art. 90 DSGVO erlaubt nur Einschränkungen der Datenschutzkontrolle, die „**notwendig und verhältnismäßig**“ sind. Hierzu gibt es weder im Gesetzestext noch in der Begründung Ausführungen. Vielmehr ist die geplante Einschränkung in ihrem Umfang sachlich nicht begründet und nicht zu begründen. Datenschutzverstöße durch Berufsgeheimnisträger werden dadurch vollständig kontroll- und damit auch sanktionsfrei gestellt, so dass die Schutzfunktion unabhängiger Datenschutzkontrolle, die in Art. 8 Abs. 3 GRCh ausdrücklich festgeschrieben ist, verloren geht. Die Regelung ist daher verfassungs- und europarechtswidrig. Auf sie kann und sollte ersatzlos verzichtet werden.

Zu § 27 Datenübermittlung an Auskunfteien

Die Übernahme dieser Regelung aus dem BDSG-alt ist in Bezug auf den Regelungsinhalt grundsätzlich zu begrüßen. Es ist aber in Frage zu stellen, ob „die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften“ ein „wichtiges Ziel des allgemeinen öffentlichen Interesses“ der Bundesrepublik Deutschland darstellt und damit, ob die Öffnungsklausel aus Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 DSGVO greift.

Zu § 28 Scoring

Mit der Regelung soll der bisherige § 28b BDSG-alt fortgelten. Es ist fraglich, inwieweit dies durch die abschließenden Regelungen des Art. 6 Abs. 1 DSGVO ausgeschlossen ist. Wenn dies verneint wird, sind gemäß Art. 22 Abs. 2 lit. b DSGVO in jedem Fall angemessene **Maßnahmen zur Wahrung der Rechte und Freiheiten** und berechtigten Interessen der Betroffenen zu gewährleisten (Roßnagel, S. 141; Kühling/Martini u. a., S. 440 ff.). Angesichts der in Deutschland gesammelten Erkenntnisse zum Scoring ist fraglich, ob dies der Fall ist. So zeigt sich, dass bei der Eingrenzung der zulässigen Datenarten und Quellen, hinsichtlich der Einbeziehung von Sekundärdaten, der Kontrolle der Verfahren und der geforderten Relevanz und Prognosegüte große Regelungsdefizite bestehen und neue Formen des Scoring, die über die klassische Bonitätsbewertung hinausgehen, nicht hinreichend abgedeckt sind (ausführlich Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3).

Zu § 30 Informationspflichten bei der Erhebung bei Betroffenen

Nach Abs. 1 Nr. 2 rechtfertigt schon ein „**unverhältnismäßiger Aufwand**“ den Verzicht auf Informationen nach Art. 13 DSGVO zur Verarbeitung bei einer Betroffenenerhebung. Diese äußerst unbestimmte Norm ermöglicht es Verantwortlichen, ohne weiteren Rechtfertigungsbedarf keine Betroffeneninformationen bereitzustellen. Die Schwelle zur Rechtfertigung fehlender Transparenz ist zu erhöhen.

Entgegen der Regelung in Abs. 3 Satz 2 ist sofort mit der Aktivierung von Kameras über eine **Videoüberwachung** zu informieren und nicht erst zum frühestmöglichen Zeitpunkt. Die Regelung bietet Verantwortlichen Schlupflöcher, den Zeitpunkt nach hinten zu verlagern. Hier muss ein Verringern des bisherigen Niveaus (§ 6a Abs. 2 BDSG-alt) vermieden werden.

Zu § 31 Informationspflichten bei Dritterhebung

Gemäß Abs. 1 Nr. 1 lit. a genügt schon eine **Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben** einer öffentlichen Stelle, um auf eine Information der Betroffenen nach Art. 14

DSGVO zu verzichten. Angemessen ist nur eine höhere Schwelle, etwa die Beeinträchtigung einer zulässigen Aufgabenerfüllung.

Abs. 1 Nr. 2 lit. a legitimiert die Nichtinformation der Betroffenen, wenn eine erhebliche **Gefährdung der Geschäftszwecke** des Verantwortlichen angenommen wird. Dies eröffnet ein hohes Missbrauchspotenzial, da die Geschäftszwecke einseitig durch den Verantwortlichen definiert werden. Es bedarf insofern ergänzender Schutzmaßnahmen. Die in Abs. 2 genannten Vorkehrungen, die zu „geeigneten Maßnahmen zur Information für die Öffentlichkeit“ verpflichten, genügen zur Verhinderung von Missbrauch der Transparenzausnahme nicht.

Zu § 32 Einschränkung des Auskunftsanspruchs

Abs. 1 Nr. 1 rechtfertigt die Auskunftsverweigerung bei Vorliegen eines Grundes zum Verzicht auf Informationen nach den §§ 30, 31. Dies hat zur Folge, dass schon mit der **Gefährdung der Aufgabenerfüllung** oder der erheblichen Gefährdung der Geschäftszwecke die Auskunftsverweigerung begründet werden kann. Angesichts des hohen Rangs des grundrechtlich in Art. 8 Abs. 2 S. 2 GRCh garantierten Anspruchs auf Auskunft – der Magna Charta des Datenschutzes (z. B. Mallmann in Simitis, BDSG, 8. Aufl. 2014, § 19 Rn. 1) – ist dies unverhältnismäßig.

Dies gilt erst recht für die Möglichkeit für nicht-öffentliche Stellen nach Abs. 2, die Auskunft unter Verweis auf die Wahrung von **Geschäftsgeheimnissen** zu verweigern. Individuelle Daten eines Betroffenen können nicht als Geheimnisse diesem gegenüber anerkannt werden (ULD/GP Forschungsgruppe, Scoring-Gutachten, S. 44 ff. gegen BGH NJW 2014, 341). Die Ausnahme von der Auskunft ist ersatzlos zu streichen.

Zu § 33 Einschränkung der Löschungsverpflichtung

Abs. 1 sieht vor, dass keine Löschpflicht besteht, „wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit **unverhältnismäßigem Aufwand** möglich ist“. Diese Regelung steht im Widerspruch zu Art. 25, 32 DSGVO zu den technisch-organisatorischen Maßnahmen, wozu auch die Intervenierbarkeit von Daten gehört, die bei der Gestaltung der Systeme beachtet werden muss. Automatisierte Verfahren, die in der Vergangenheit nicht in der Lage waren, spezifische Löschungen vorzunehmen, wurden inzwischen überarbeitet. Die Norm würde dazu einladen, Verfahren zu etablieren, mit denen mangels Löschbarkeit der Daten auf obligatorische Datenlöschungen verzichtet werden könnte.

Zu § 34 Einschränkung des Widerspruchsrechts

Nach der Regelung besteht kein Recht auf Widerspruch nach Art. 21 Abs. 1 DSGVO, wenn die Verarbeitung erforderlich und der Widerspruch „die Verwirklichung des Zwecks der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde“. Die Verarbeitung der

Daten soll nur für Zwecke des § 22 Abs. 1 (Erlaubnisnorm für sensitive Daten) zulässig sein. Eine Zweckänderung soll nur entsprechend Art. 21 Abs. 1 S. 2 DSGVO zulässig sein. Dieser Vorschlag bringt das Recht, Widerspruch einzulegen und das Recht, auf der Grundlage eines Widerspruchs eine Veränderung bei der Datenverarbeitung zu bewirken, durcheinander. Ein Widerspruch ist für sich nicht in der Lage, einen Verarbeitungszweck ernsthaft zu beeinträchtigen, sondern lediglich die sich evtl. daraus ergebende Einschränkung der Verarbeitung. Die Bezugnahme auf sensitive Daten erschließt sich nicht. Ebenso wenig erschließt sich der Verweis auf Art. 21 Abs. 1 S. 2 DSGVO. Die Regelung ist überflüssig und sollte gestrichen werden.

Zu § 36 Datenschutzbeauftragte nicht-öffentlicher Stellen

Es ist zu begrüßen, dass die **bewährten Regelungen aus dem BDSG-alt** in das BDSG-neu übernommen werden. Immer noch sehr viele Unternehmensleitungen sind der Ansicht, dass sie sich nicht um die Umsetzung des Datenschutzes kümmern müssten, solange sie keinen Datenschutzbeauftragten zu bestellen haben. Diese Einstellung kann sich durch die deutlich gestiegenen Höchstgrenzen für Bußgelder im Lauf der Zeit wandeln. Aber durch die Beibehaltung der bisherigen Regelungen zur Bestellpflicht von Datenschutzbeauftragten wird eine präventive Umsetzung des Datenschutzes – die aus Betroffenensicht unbedingt erforderlich ist – gefördert.

Zu § 37 Akkreditierung von Zertifizierungsstellen

Die nationale Umsetzungsnorm zu den Art. 42, 43 DSGVO zur datenschutzrechtlichen Zertifizierung und zur Erteilung von Datenschutzgütesiegeln und -prüfzeichen beschränkt sich darauf, die zuständigen Aufsichtsbehörden in Bund und Ländern zu verpflichten, sich gegenseitig und die Deutsche Akkreditierungsstelle über die Erteilung, Versagung und den „Widerruf einer Akkreditierung“ zu unterrichten. Diese äußerst schlanke Regelung lässt praktisch alles hinsichtlich der Akkreditierung von Prüfstellen und der von diesen vorzunehmenden Zertifizierungen im **Unklaren**. Dies veranlasst die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle, alles Wesentliche in eigener Verantwortung zu regeln. Dies ist äußerst unbefriedigend.

Zu § 38 Aufsichtsbehörden im nicht-öffentlichen Bereich

Der Entwurf lässt offen, ob **Post- und Telekommunikationsunternehmen** – wie bisher (§ 115 Abs. 4 TKG, § 42 Abs. 3 PostG) – von der BfDI oder von den Aufsichtsbehörden der Länder kontrolliert werden sollen.

Zu § 40 Verhängung von Geldbußen

Abs. 3 sieht vor, dass gegen Behörden und **öffentliche Stellen des Bundes** keine Geldbußen verhängt werden, soweit diese nicht wettbewerblich tätig sind. Mit der Regelung, die sich auf

die Öffnungsklausel des Art. 83 Abs. 7 DSGVO beruft, werden öffentliche Stellen von Bußgeldverfahren vollständig freigestellt. Dies entspricht nicht den Intention der DSGVO und dem Ziel, die bestehenden Vollzugsdefizite durch verbesserte Sanktionen – im öffentlichen wie im nicht-öffentlichen Bereich – abzubauen.

Zu § 42 Strafantragserfordernis

Zur Strafverfolgung von Verstößen nach § 41 bedarf es eines Antrags. Antragsberechtigt sollen sein „die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde“. Damit sollen strafbare Datenschutzverstöße weiterhin kein Offizial-, sondern ein **Antragsdelikt** sein, was der gesellschaftlichen Bedeutung vieler Datenschutzdelikte nicht gerecht wird (Schulzki-Haddouti, Papiertiger, c´t 10/2016, 162 ff.).

Zu Teil 3 (§§ 43-79) Verarbeitung nach der JI-Richtlinie

Zu den Regelungsvorschläge der §§ 43 bis 79 wird aktuell keine Stellung genommen. Eine spätere Bewertung bleibt vorbehalten.

D Weitere gesetzliche Änderungen

Zu Artikel 2 Änderung des Bundesverfassungsschutzgesetzes

In § 26a Abs. 2 ist vorgesehen, die Datenschutzkontrolle der BfDI auszuschließen, „soweit die Einhaltung von Vorschriften der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegt“. In der Vergangenheit hat sich gezeigt, dass die Datenschutzkontrolle der bundesdeutschen Geheimdienste unzureichend ist. Ein Grund hierfür liegt darin, dass die G-10-Kommission und die Kontrolle durch die BfDI sich gegenseitig ausschließen, obwohl in tatsächlicher wie auch in rechtlicher Hinsicht Überschneidungen bestehen. Die **Kontrolle durch die G-10-Kommission** und die BfDI unterscheiden sich sowohl hinsichtlich der Methode wie auch der Fragestellung. Es ist daher gerechtfertigt, sich überschneidende Kontrollen zuzulassen. Hierdurch wird auch vermieden, dass z. B. durch Zuordnungsprobleme kontrollfreie Räume entstehen. Entgegen der Gesetzesbegründung (S. 120) ist die Regelung nicht geeignet, die bisher aufgetretenen Kontrolllücken zu beseitigen. Es ist nicht erkennbar, weshalb, wie in der Begründung aufgeführt, zwischen der G-10-Kommission und der BfDI konträre Ergebnisse entstehen können sollen. Selbst wenn dies der Fall wäre, bestünde insofern kein „Risiko“, sondern allenfalls die Chance einer zweiten Meinung, zumal weder der BfDI noch der G-10-Kommission exekutive Durchgriffsrechte zugestanden werden.

In § 27 Abs. 1 ist vorgesehen, dass § 16 Abs. 1 des neuen BDSG nicht gelten soll, welcher der BfDI bei Feststellung von Datenschutzverstößen Untersuchungs- und Abhilfebefugnisse gemäß der DSGVO zugesteht, nachdem eine umfassende Anhörung stattgefunden hat. Es ist

nicht erkennbar, weshalb diese Regelung, die die **Abstellung von Datenschutzverstößen** sicherstellen soll, für nicht anwendbar erklärt wird.

Zu Artikel 7 - Änderung des aktuellen Bundesdatenschutzgesetzes

§ 42b - Antrag der Aufsichtsbehörde auf gerichtliche Überprüfung von Angemessenheitsbeschlüssen der EU-Kommission

Es ist zu begrüßen, dass diese Regelung als eigenständige Änderung in das BDSG-alt eingefügt werden soll (siehe Art. 10 - Inkrafttreten/Außerkrafttreten) und am Tag nach der Verkündung dieses Gesetzes – und nicht erst am 25.05.2018 – in Kraft treten soll.

E Weiterer dringender Änderungsbedarf beim Datenschutzrecht

Der Entwurf behandelt einige Bereiche des Datenschutzes nicht, die dringend einer Regelung bedürfen.

Abgesehen von den schon genannten Themen des Beschäftigtendatenschutzes sowie des Datenschutzes im Bereich der Forschung gilt dies insbesondere für eine Regulierung der Auftragsdatenverarbeitung von Berufsgeheimnissen unterliegenden Verantwortlichen. In seiner Stellungnahme „Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO“ vom 09.05.2016 hat das Netzwerk Datenschutzexpertise darauf hingewiesen, dass **IT-Dienstleister**, die z. B. Anwalts- oder Arztpraxissysteme administrieren oder hochkomplexe IT-Systeme in Krankenhäusern oder medizinischen Laboren verwalten, nicht den in der StPO gesicherten Vertraulichkeitsschutz genießen und nicht der straf- und standesrechtlichen Schweigepflicht unterliegen, weshalb Berufsgeheimnisträger diesem Personenkreis nach dem derzeit geltenden Recht keinen Zugang zu Patienten- oder Klientendaten gewähren dürfen (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/empf_2016_nat_regelungsbedarf.pdf). Dies beeinträchtigt die Aufgabenwahrnehmung der besonders geschützten Berufsgruppen und letztlich die Rechtssicherheit aller Beteiligten. Dem kann durch eine Erweiterung der Geheimhaltungspflicht und durch eine Offenbarungsbefugnis abgeholfen werden.

In der DSGVO und in der Folge auch im nationalen Umsetzungsgesetz besteht zudem ein großes datenschutzrechtliches Defizit darin, dass als Adressaten der Normen lediglich Verantwortliche und Auftragsverarbeiter benannt werden, nicht aber **Hersteller bzw. Anbieter von IT-Produkten** (Hard- und Software), mit denen personenbezogene Daten verarbeitet werden. Tatsächlich beruhen viele Gefährdungen und Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung darauf, dass Verantwortliche oder Auftragsverarbeiter IT-Produkte einsetzen, die nicht den Anforderungen der DSGVO (z. B. der Art. 25, 32) genügen bzw. genügen können. In Ermangelung einer hinreichenden Kontrolle oder von technischen Einflussmöglichkeiten ist dies Verantwortlichen bzw. Auftragsverarbeitern oft nicht bewusst oder für diese nicht korrigierbar. Vorgegebene Verarbeitungsvorgänge, etwa in Form von Online-Formularen oder voreingestellten

Datenweiterleitungen, sind oft weder hinreichend dokumentiert noch durch die (formalrechtlich verantwortlichen) Nutzenden beeinflussbar. Die ungenügende Umsetzung von Privacy by Default und Privacy by Design (vgl. auch Art. 25 DSGVO) oder generell unterlassene Maßnahmen zur Erhöhung der IT-Sicherheit durch die Hersteller führen oft dazu, dass nötige technisch-organisatorische Maßnahmen unterbleiben oder materiell-rechtliche Verstöße vorgegeben werden.

Ein modernes Datenschutzgesetz muss daher – ähnlich wie eine Adressierung von Straßenverkehrsvorschriften an die Kfz-Hersteller – auch die Hersteller und Anbieter von IT-Produkten, die der personenbezogenen Datenverarbeitung dienen, einbeziehen. Dies kann in der Form erfolgen, dass diesen z. B. bestimmte **verpflichtende Datenschutzstandards** präventiv wirkend vorgegeben werden oder dadurch, dass diesen im Fall datenschutzwidriger Produkte Haftungsrisiken auferlegt werden. Die bisher vorgesehenen freiwilligen Zertifizierungen, die auf eine Selbstregulierung des Marktes setzen, genügen nicht, um die systematische Verbreitung von Datenschutzverstößen einzudämmen.

Für Rückfragen stehen wir gerne zur Verfügung

mit freundlichen Grüßen

Dr. Thilo Weichert (für das Netzwerk Datenschutzexpertise und die Deutsche Vereinigung für Datenschutz e.V.)

Frank Spaeing (Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.)

Werner Hülsmann (stellv. Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.)

Kontakt:

- Dr. Thilo Weichert, Waisenhofstr. 41, 24103 Kiel,
  Tel.: 0431 9719742,
  E-Mail: weichert@datenschutzverein.de od. weichert@netzwerk-datenschutzexpertise.de
- Frank Spaeing, Vorsitzender der DVD
  Maiglöckchenweg 11, 06122 Halle (Saale)
  Tel.: 0172 6043135
  E-Mail: spaeing@datenschutzverein.de
- Werner Hülsmann, stellv. Vorsitzender der DVD
  Kurfürstenstr. 6, 12105 Berlin Mariendorf
  und Münchener Str. 101 / Geb. 01, 85737 Ismaning
  Tel.: 030 / 22 43 84 36 – mobil: 0177 /28 28 681
  E-Mail: huelsmann@datenschutzverein.de