Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
www.datenschutzverein.de

Bonn, 01.02.2017

Stellungnahme zum

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) – Kabinettsvorlage für den 01.02.2017

A Allgemeine Erwägung

Es wird begrüßt, dass die Bundesregierung ein Gesetz zur Umsetzung der Europäischen Datenschutzgrundverordnung (EU 2016/679, im Folgenden DSGVO) sowie der der Europäischen Datenschutzrichtlinie für Justiz und Inneres (EU 2016/680, im Folgenden JI-Richtlinie) anstrebt. Die Anwendenden der Regelungen benötigen einen rechtssicheren Überblick darüber, welche europäischen und nationalen Regelungen Gültigkeit haben, wenn die DSGVO und die JI-Richtlinie im Mai 2018 direkte Wirksamkeit entfalten.

B Einzelstellungnahme zum Entwurf eines neuen BDSG

Zu § 1 Anwendungsbereich des Gesetzes

Die Regelung in Abs. 2 S. 3, wonach „die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen“, unberührt bleibt, ist unklar. Es trifft zwar zu, wie in der Begründung ausgeführt, dass die Regelung dem bisherigen § 1 Abs. 3 S. 2 BDSG entspricht. Die bisherige Regelung war aber auch schon bisher nicht in der Lage, das komplizierte Verhältnis zwischen besonderen Geheimnissen und Datenschutzrecht zu klären. Durch die Formulierung „die nicht auf gesetzlichen Vorschriften beruhen“ wird der falsche Eindruck vermittelt, dass untergesetzlich Berufsgeheimnisse normiert werden könnten, was unter dem Regime der DSGVO nicht zutreffen kann. Ob implizit ein Verweis auf Berufsordnungen von Heilberufskammern gemeint ist, bleibt unklar. Auf den Halbsatz kann und sollte deshalb verzichtet werden.

Zu § 2 Begriffsbestimmungen

Es wird darauf hingewiesen, dass durch das Außerkrafttreten des **bisherigen Bundesdatenschutzgesetzes** (BDSG-alt) gemäß Art. 8 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 und außerhalb des Anwendungsbereichs der Verordnung 2016/679 wegen bereichsspezifischen Regelungen 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 S. 2, wonach bei Videoüberwachung in „**öffentlich zugänglichen öffentlichen Anlagen** … oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des Schienen-, Schiffs- und Bahnverkehrs … der Schutz von Leben, Gesundheit oder Freiheit der dort aufhältigen Personen als besonders wichtiges Interesse“ gilt. Diese Regelung gibt zwar inhaltlich eine Selbstverständlichkeit wider. Zweck und voraussichtliche Wirkung dieser Regelung ist aber, dass im Rahmen der Interessenabwägung bei öffentlicher Videoüberwachung den Sicherheitsinteressen der Vorrang eingeräumt wird.

Zudem nimmt die auch für private Stellen geltende Regelung diese 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. Viele Länder haben von ihrer Befugnis Gebrauch gemacht, Videoüberwachung in ihrem Versammlungsrecht zu regulieren. Der vorliegende Entwurf steht hierzu sowohl formal wie auch inhaltlich im Widerspruch.

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).

Gemäß Abs. 2 ist der Umstand und der Verantwortliche der Videoüberwachung „**zum frühestmöglichen Zeitpunkt erkennbar** zu machen“. Die zeitliche Bezugnahme macht keinen Sinn und verursacht in der praktischen Umsetzung Probleme: Findet im öffentlichen Raum eine Videoüberwachung statt, so kann und muss diese sofort kenntlich gemacht werden.

Die Erkennbarkeit von Videoüberwachung ist wegen der teilweise bestehenden räumlichen Verhältnisse oft schwer zu realisieren. Als zusätzliche Gewährleistungsmaßnahme für Transparenz sollte daher eine **Meldepflicht** sämtlicher öffentlicher Videokameras vorgesehen werden, kombiniert mit einer Veröffentlichung im Internet. Dies hätte nicht nur einen Transparenzgewinn für die Betroffenen, sondern auch für Sicherheitsbehörden zur Folge, die so im Bedarfsfall sofort feststellen können, wo im Fall einer Ermittlungsnotwendigkeit evtl. Bildmaterial erstellt worden ist.

Bei Videoüberwachung im öffentlichen Raum sollte zudem eine Pflicht zur **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO normiert werden, die dazu führt, dass durch Marktnachfrage Hersteller datenschutzfreundlich gestaltete, dokumentierte oder gar zertifizierte Produkte anbieten (s. u. D Weiterer dringender Änderungsbedarf beim Datenschutzrecht).

Zu § 8 Errichtung Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

In Abs. 1 S. 2 ist vorgesehen, dass der Sitz der BfDI **Bonn** sein soll. Angesichts der hohen grundrechtspolitischen Bedeutung der Stelle der BfDI ist es nicht sinnvoll, diese weiterhin derart weit von den politisch relevanten Gremien in Berlin zu lokalisieren. Daher sollte als Sitz Berlin festgelegt werden oder zumindest auf eine gesetzliche Festlegung vollständig verzichtet werden.

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 Bestellungsverfahren und an 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 theoretische 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 nur auf Länderebene 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.

Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
www.datenschutzverein.de

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 u. a. die Datenschutzverstöße durch den Bundesnachrichtendienst (BND) gezeigt, die nach den Offenlegungen von Edward Snowden bekannt geworden sind. 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.

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 kann auf den Verweis auf die Gesetzgebungskompetenz verzichtet werden.

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 gemäß Satz 3 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 öffentlicher Stellen

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. 1 wurde gegenüber den Vorentwürfen die Sicherung des Steuer- und Zollaufkommens als Rechtfertigung für eine Zweckänderung neu aufgenommen.

Diese Regelungen beziehen sich auf die in Art. 6 Abs. 1 lit. e DSGVO vorgegebenen Verarbeitungsbefugnissen, ohne jedoch bei sämtlichen Alternativen eine **Abwägung mit dem Betroffeneninteressen** vorzusehen. Damit laden diese Regelungen zu einer pauschalen Missachtung dieser Interessen ein und begründen unverhältnismäßige Informationseingriffe durch Zweckänderungen.

Zu § 26 Verarbeitung von Beschäftigtendaten

Die Wiederauflage des **missglückten § 32 BDSG**-alt (obwohl in dem vorliegenden Entwurf angereichert um wünschenswerte Ergänzungen) ist abzulehnen. Diese Norm führte zu Rechtsunsicherheit, nicht zur Präzisierung von Verarbeitungsbefugnissen und Betroffenenrechten. Zudem darf bezweifelt werden, dass die nun 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 § 27 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.

Der **Ausschluss des Auskunftsanspruchs** bei Erforderlichkeit für die wissenschaftliche Forschung und einem „unverhältnismäßigen Aufwand“ nach Abs. 2 ist zu unbestimmt und ermöglicht Forschenden mit Pauschalbegründungen die Verweigerung von Transparenz gegenüber den Betroffenen.

Zu § 29 Geheimnisschutz

Die Regelung beschreibt nur völlig unzureichend, welche Daten mit ihr erfasst werden sollen: Die Kennzeichnung von Daten danach, dass diese „nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen“, ist **zu unbestimmt** und kann 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 dem Absatz 1 werden das Informationsrecht nach Art. 14 DSGVO und das **Auskunftsrecht** nach Art. 15 DSGVO eingeschränkt, wenn die Daten „ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen“. Diese Formulierung ist für alle Beteiligten nicht kalkulierbar und zu unbestimmt. Die Unbestimmtheit der erfassten Daten erstreckt sich auf diese Beschränkung informationeller Selbstbestimmung generell und des Auskunftsanspruchs als „Magna Charta des Datenschutzes“ (s. u. zu § 34). Damit wird die grundlegende Garantie des Auskunftsanspruchs in Art. 8 Abs. 2 S. 2 GRCh verletzt, der Folgendes vorsieht: „Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten“. Diese Unbestimmtheit beruht auch auf der völlig offenen 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.

Auch die Ausnahme von der Informationspflicht in Abs. 2 ist sowohl hinsichtlich des Anwendungsbereichs wie auch des Inhaltes unbestimmt. In der Begründung (S. 104) wird auf die **Kommunikation zwischen Mandanten** von Wirtschaftsprüfern und Rechtsanwälten Bezug genommen, während in der Regelung generell der erheblich weitere Begriff der Berufsgeheimnisträger verwendet wird. Das Kundenverhältnis anderer Berufsgeheimnisträger kann auch als Mandat gekennzeichnet werden. Zudem verwendet die Ausnahmeregelung wieder eine offene, beliebig verwendbare Abwägungsformel.

In Abs. 3 wird bei den in § 203 Abs. 1, 2a und 3 StGB beschriebenen Daten die **Datenschutzkontrolle** durch die zuständige Aufsicht mit unbestimmten Formulierungen unverhältnismäßig beschnitten. Es soll keine Untersuchungsbefugnisse geben, „soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die

Geheimhaltungspflichten dieser Personen führen würde“. Bisher ist unbestritten, dass zu den in die Kontrolle einbezogenen Daten auch Berufsgeheimnisse gehören. Bisher gehört die Kontrolle der Wahrung des Patienten- und den Sozialgeheimnisses sogar zu den Schwerpunkten der aufsichtsbehördlichen Tätigkeit. Diese würde massiv behindert, da jeder Verantwortliche sich einer Kontrolle zunächst dadurch entziehen könnte, dass er geltend macht, seine Geheimhaltungspflichten würden verletzt. 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.

Der Gesetzentwurf geht von der falschen Annahme aus, dass Datenschutzkontrollen den Datenschutz verletzen könnten. Tatsächlich unterliegen die bei einer Kontrolle erlangten Daten einer strengen Zweckbindung. Es ist in der über 40-jährigen Geschichte der Datenschutzaufsicht noch kein Fall bekannt geworden, dass über Datenschutzkontrollen **Berufsgeheimnisse offenbart** worden wären. Dem kann durch die vorgesehene Regelung, auf die Datenschutzaufsicht die Geheimhaltungspflicht des Verantwortlichen auszuweiten, auch künftig vorgebeugt werden.

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. 104) verweist auf die bundesverfassungsgerichtliche Rechtsprechung, wonach das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet werden darf (BVerfG Urteil v. 12.04.2005 – 2 BvR 1027/02, zitiert in NJW 2005, S. 1917). Dies schließt 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 wurde die Kontrollbefugnis der Datenschutzaufsicht im nicht-öffentlichen Bereich bisher 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.).

Art. 90 DSGVO erlaubt nur Einschränkungen der Datenschutzkontrolle, die „**notwendig und verhältnismäßig**“ sind. Hierzu gibt es weder im Gesetzestext noch in der Begründung Ausführungen. Die geplante Einschränkung ist sachlich 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.

Der Begründung ist auf S. 104 zu entnehmen, dass S. 2 von Abs. 3 sich auf Daten bei **Auftragsverarbeitern von Berufsgeheimnisträgern** beziehen soll. Diese Zielsetzung ist der geplanten Gesetzesformulierung nicht zu entnehmen. Die Begründung verdreht die Rechtslage: Auftragsverarbeiter können im Rahmen einer Datenschutzkontrolle gegenüber ihren Auftraggebern nicht vertragsbrüchig werden. Das rechtliche Problem ist derzeit, dass das Outsourcing personenbezogener Datenverarbeitung seit Jahren einen Verstoß gegen die berufliche Geheimhaltungspflicht darstellt. Es ist zu begrüßen, dass insofern nun vonseiten des Bundesjustizministerium ein Referentenentwurf erarbeitet wurde, der diese rechtlich nicht akzeptable Situation auflöst. Dieser zu begrüßende Entwurf sollte umgehend eingebracht und spätestens zeitgleich mit den Umsetzungsregelungen zur DSGVO in Kraft gesetzt werden (s. u. D Weiterer dringender Änderungsbedarf beim Datenschutzrecht).

Zu § 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

Die Übernahme dieser Regelungen aus dem BDSG-alt (§§ 28b, 28b) ist in Bezug auf den Regelungsinhalt grundsätzlich zu begrüßen. Es ist aber in Frage zu stellen, ob „die Verwendung eines Wahrscheinlichkeitswerts“, insbesondere im Hinblick auf „die Zahlungsfähig- und Zahlungswilligkeit“ 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, so wie dies in der Begründung eines Vorentwurfs zum Kabinettsentwurf erwähnt wurde. Der aktuelle Entwurf äußert sich zur Regelungsberechtigung nicht.

Mit Abs. 1 soll der bisherige § 28b BDSG-alt zum Scoring 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 offensichtlich, dass dies nicht 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).

In Abs. 2 wird die Datenbeschaffung durch Auskunfteien in Bezug auf Bonitätsbewertungen mittels Scoring geregelt. Diese Regelung selbst beschränkt sich auf Scoringverfahren, in der Begründung ist aber generell von der Datenbeschaffung für **Kreditinformationssysteme** die Rede. Damit fallen Regelungsintention und Regelungsinhalt auseinander.

Zu § 32 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.

Zu § 33 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. Dies ist eine unverhältnismäßige Beeinträchtigung des Transparenzanspruchs der Betroffenen. Angemessen wäre allenfalls 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. Für eine angemessene Regelung bedürfte es 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 § 34 Einschränkung des Auskunftsanspruchs

Abs. 1 Nr. 1 rechtfertigt die Auskunftsverweigerung bei Vorliegen eines Grundes zum Verzicht auf Informationen nach den § 33. Dies hat zur Folge, dass schon mit der **Gefährdung der Aufgabenerfüllung** oder der erheblichen Gefährdung der Geschäftszwecke die Auskunftsverweigerung begründet werden kann. Die Wahrung von angeblichen Geschäftsgeheimnissen, die in personenbezogenen Daten bestehen, können, anders als die Regelung suggeriert, eine Auskunftsverweigerung nicht rechtfertigen (ULD/GP Forschungsgruppe, Scoring-Gutachten, S. 44 ff. gegen BGH NJW 2014, 341). Diese Ausnahme von der Auskunftspflicht ist ersatzlos zu streichen. 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 die Einschränkung des Auskunftsanspruchs unverhältnismäßig und verfassungswidrig.

Zu § 35 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. Solche Maßnahmen zielen auch auf die Intervenierbarkeit von Daten ab, 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 nun dazu einladen, Verfahren zu etablieren, mit denen mangels Löschbarkeit der Daten auf obligatorische Datenlöschungen verzichtet werden könnte.

Zu § 36 Einschränkung des Widerspruchsrechts

Nach der Regelung besteht kein Recht auf Widerspruch nach Art. 21 Abs. 1 DSGVO, „soweit an der Verarbeitung ein **zwingendes öffentliches Interesse** besteht, das die

Interessen der betroffenen Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet“. Diese Norm 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; dies gilt allenfalls für die sich evtl. daraus ergebende Einschränkung der Verarbeitung. Die Regelung ist überflüssig und sollte gestrichen werden.

Zu § 37 Automatisierte Entscheidung über medizinische Entgelte

In Abs. 1 Nr. 2 und Abs. 2 ist vorgesehen, dass automatisierte Entscheidungen „auf der Anwendung verbindlicher **Entgeltregelungen für Heilbehandlungen**“ beruhen und dabei Gesundheitsdaten verarbeitet werden dürfen, wenn angemessene Sicherungsmaßnahmen vorgesehen sind. Diese insbesondere auf den Versicherungsbereich abzielende Norm ist in einem allgemeinen Datenschutzgesetz systemfremd.

Die Regelung ist insofern gefährlich, dass sie im Interesse der Kosteneffizient der Abrechnung von Heilbehandlungen den Betroffenen aufgibt, zur Wahrung ihrer Interessen aktiv zu werden, wozu viele Menschen kognitiv oder auch aus anderen Gründen nicht in der Lage sein werden. Zwar fordert die Regelung, dass bei antragsablehnenden Entscheidungen „angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person“ getroffen werden müssen, doch sind diese möglichen Maßnahmen derart unbestimmt formuliert, dass die Regelung dazu führen kann, dass Patienten bei der Abrechnung medizinischer Leistungen über den Tisch gezogen werden. Eine Regelung der Automatisierung in diesem Bereich muss in einem speziellen Gesetz unter **konkreter Benennung der Sicherungsmaßnahmen** erfolgen. Dies gilt auch vor dem Hintergrund, dass die geplante Regelung Vorbild sein könnte für eine Vielzahl weiterer automatisierter Abrechnungsverfahren.

Zu § 38 Datenschutzbeauftragte nicht-öffentlicher Stellen

Es ist zu begrüßen, dass die **bewährte Normierung aus dem BDSG** zum Datenschutzbeauftragten in der Wirtschaft inhaltlich weitgehend übernommen werden soll. 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. Durch die Beibehaltung der bisherigen Regelungen zur Bestellpflicht von Datenschutzbeauftragten

wird eine präventive Umsetzung des Datenschutzes – die aus Betroffenensicht unbedingt erforderlich ist – gefördert.

Zu § 39 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 und die Deutsche Akkreditierungsstelle für die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, für zuständig zu erklären. 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. Nötig sind insbesondere Regelungen, mit denen schon im Rahmen des Zertifizierungsverfahrens und nicht erst durch eine Intervention der zuständigen Aufsichtsbehörden die Qualität der Zertifizierungen gewährleistet wird. Ohne eine solche Qualitätssicherung können Zertifikate zur Umgehung des Datenschutzes und zum Vertuschen von Datenschutzverstößen missbraucht werden.

Zu § 42 Strafantragserfordernis

Zur Strafverfolgung von Datenschutzverstößen bedarf es nach Abs. 3 wie bisher 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 der Datenschutzdelikte nicht gerecht wird (Schulzki-Haddouti, Papiertiger, c´t 10/2016, 162 ff.).

Zu § 43 Verhängung von Geldbußen gegenüber öffentlichen Stellen

Abs. 2 sieht vor, dass gegen Behörden und **öffentliche Stellen des Bundes** keine Geldbußen verhängt werden. 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 Teil 3 (§§ 45-84) Verarbeitung nach der JI-Richtlinie

Zu den Regelungsvorschläge der §§ 45 bis 84 wird aktuell keine Stellung genommen. Eine spätere Bewertung bleibt vorbehalten.

Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
www.datenschutzverein.de

C Weitere gesetzliche Änderungen

Zu Artikel 2 Änderung des Bundesverfassungsschutzgesetzes

In § 13 Abs. 2 wird die Beschränkung der Verarbeitung (früher Sperrung) von Daten beim Bundesamt für Verfassungsschutz geregelt. Gemäß S. 2 genügt es für die **Verarbeitungsbeschränkung**, dass die Daten „mit einem entsprechenden Vermerk versehen“ werden. Dies gewährleistet nicht, dass keine weitere Nutzung dieser Daten erfolgt. Es muss sichergestellt werden, dass die verarbeitungsbeschränkten Daten den Nutzenden nicht mehr angezeigt werden und somit auch nicht unerkannt und evtl. gar unbewusst bei der Aufgabenwahrnehmung verwendet werden.

In § 26a Abs. 2 ist vorgesehen, die Datenschutzkontrolle der BfDI auszuschließen, „soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt“. In der Vergangenheit hat sich gezeigt, dass die Datenschutzkontrolle der bundesdeutschen Geheimdienste, anders als in der Begründung (S. 131) behauptet, unzureichend ist. Ein Grund hierfür liegt darin, dass die Tätigkeit der 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 der 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 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, mit der die **Abstellung von Datenschutzverstößen** sichergestellt werden soll, für nicht anwendbar erklärt wird.

Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
www.datenschutzverein.de

DVD Deutsche Vereinigung für Datenschutz e. V.

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 bisherige BDSG-alt eingefügt werden soll (siehe Art. 8 - Inkrafttreten/Außerkrafttreten) und am Tag nach der Verkündung dieses Gesetzes – und nicht erst am 25.05.2018 – in Kraft treten soll.

D 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. **IT-Dienstleister**, die z. B. Anwalts- oder Arztpraxissysteme administrieren oder hochkomplexe IT-Systeme in Krankenhäusern oder medizinischen Laboren verwalten, genießen bisher nicht den in der StPO gesicherten Vertraulichkeitsschutz und unterliegen nicht der straf- und standesrechtlichen Schweigepflicht. Dies hat zur Folge, dass Berufsgeheimnisträger diesem Personenkreis bisher nach dem derzeit geltenden Recht keinen Zugang zu Patienten- oder Klientendaten gewähren dürfen. Dieses Defizit wird (noch nicht bzgl. des strafprozessualen Schutzes) durch einen Referentenentwurf eines „Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“, den das Bundesministerium für Justiz und Verbraucherschutz am 15.12.2016 vorlegte (teilweise) beseitigt. Es wird dringend geraten, diesen Entwurf beschleunigt zu bearbeiten und gemeinsam mit dem Umsetzungsgesetz zur DSGVO zu behandeln und zu verabschieden (http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf;jsessionid=BB2D99E0FC070F2722D3C358448A65F6.1_cid324?__blob=publicationFile&v=1).

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 auch in der Form erfolgen, dass diesen, z. B. über Anforderungen an die Datenschutz-Folgenabschätzung, 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 die DVD:

Dr. Thilo Weichert (Vorstandsmitglied der Deutschen 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.)