02.03.2021

Stellungnahme der DSK zur Evaluierung des BDSG

Vorbemerkung:

Eine Gesetzesevaluierung dient der systematischen Überprüfung getroffener gesetzgeberischer Entscheidungen sowie als Grundlage für weitere politische Entscheidungen und Vorhaben. Grundsätzlich ist die Durchführung einer Evaluierung von gesetzlichen Regelwerken daher zu begrüßen.

Im vorliegenden Fall bleibt jedoch unklar, welcher Systematik die Evaluierung des BDSG durch das BMI folgt. Das bislang erkennbare Vorgehen beschränkt sich im Wesentlichen auf die Benennung einzelner Normen und Normgruppen sowie auf die pauschale Frage, ob diese „sachgerecht, praktikabel und normenklar" geregelt seien.

Eine Evaluierung sollte Klarheit über die Tatsachen schaffen, auf deren Grundlage dann eine politische und ggf. gesetzgeberische Entscheidung getroffen werden kann. Als Teil der Evaluierung wären zunächst präzisere Fragestellungen zu entwickeln. Wichtige Erkenntnisse wären hier – neben weiteren – die vom Gesetzgeber verfolgten Ziele, Bedingungen der Zielerreichung, Art und Maß der Erfüllung dieser Bedingungen, für die Erfüllung erforderlicher Aufwand und Verhältnis dessen zur ursprünglichen Kalkulation, unbeabsichtigte Nebenwirkungen sowie rechtliche und tatsächliche Grundrechtseinschränkungen und Verhältnis derer zur ursprünglichen Annahme. Unter Berücksichtigung dieser Aspekte erscheint es fraglich, ob die vorliegende Fragestellung ausreichend genau und zielführend ist.

Es wird darauf hingewiesen, dass das gesamte Regelungsvorhaben des DSAnpUG-EU und damit auch etwa die entsprechenden Änderungen im BVerfSchG, MADG, BNDG, SÜG und Artikel-10-Gesetz laut Begründung des DSAnpUG-EU der Evaluierungspflicht unterliegt.

I. Anwendungsbereich und Begriffsbestimmungen

Zusammenfassung:
Die DSK sieht die §§ 1 und 2 des BDSG nach den bisher gesammelten Praxiserfahrungen weitgehend als gelungen an. Zu § 1 BDSG wird lediglich eine kleinere klarstellende Gesetzesänderung im Hinblick auf § 1 Absatz 4 Satz 3 BDSG angeregt. Bei den Begriffsbestimmungen in § 2 Absatz 3 BDSG wäre eine Konkretisierung der Tatbestandsmerkmale „Aufgaben der öffentlichen Verwaltung“ und „über den Bereich eines Landes hinaus tätig werden“ wünschenswert, da die Auslegung dieser Norm, die weitreichende Konsequenzen für die Abgrenzung der Zuständigkeiten zwischen BfDI und den Aufsichtsbehörden der Länder hat, einige Schwierigkeiten bereitet.

Bei § 45 BDSG besteht aus Sicht der DSK hingegen umfassenderer Anpassungsbedarf. Hier sollte wie in der Richtlinie (EU) 2016/680 (JI-RL) in erster Linie auf den konkreten Zweck der Verarbeitungstätigkeit abgestellt, und nicht – wie es § 45 BDSG vorsieht – auch auf die allgemeine Zuständigkeit der Behörde abgestellt werden. Daneben sollte die Vorschrift die gesetzgeberischen Ziele eines einheitlichen Datenschutzregimes für polizeiliches Handeln sowie die Verfolgung von Ordnungswidrigkeiten klar zum Ausdruck bringen und zudem klarstellen, dass die Dokumentation des betreffenden polizeilichen/ordnungsbehördlichen Handelns mit vom Anwendungsbereich erfasst ist.

1. Ist der Anwendungsbereich in § 1 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

§ 1 Absatz 4 Satz 3 BDSG ist unklar formuliert: „Sofern dieses Gesetz nicht gemäß Satz 2 Anwendung findet“ kann so gelesen werden, dass die Fälle gemeint sind, in denen das Gesetz nach Satz 1 Anwendung findet, also die Anwendung auf öffentliche Stellen. Dies führt zu Verwirrung, denn dass dies nicht gemeint sein kann, erschließt sich erst nach Analyse der Vorschriften §§ 8 bis 21, 39 bis 44 BDSG im systematischen Zusammenhang. Es würde die Verständlichkeit des Textes deutlich erhöhen, wenn § 1 Absatz 4 Satz 3 BDSG wie folgt umformuliert würde: „Sofern dieses Gesetz auf nichtöffentliche Stellen gemäß Satz 2 keine Anwendung findet, …“.

Im Übrigen haben sich in der Praxis der deutschen Aufsichtsbehörden keine Probleme bei der Anwendung des § 1 BDSG gezeigt.

2. Ist der Anwendungsbereich in § 45 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Nein.

Es wird im BDSG nicht wie in der JI-RL in erster Linie auf den konkreten Zweck der Verarbeitungstätigkeit abgestellt, sondern auch auf die allgemeine Zuständigkeit der Behörde. Zu unterschiedlichen Ergebnissen führt dies bei Behörden, welche selbst keine polizeilichen Aufgaben oder Strafverfolgungsaufgaben wahrnehmen, aber einzelne Verarbeitungstätigkeiten durchführen, welche der Strafverfolgung dienen. Als Beispiel kann hier das Bundesamt für Justiz (BfJ) und der Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) genannt werden. Das BfJ ist in vielen verschiedenen Rechtsgebieten tätig und hat keine eigenen polizeilichen Aufgaben oder Strafverfolgungsaufgaben, sondern ist bezüglich des ZStV reine Registerbehörde. Das ZStV hingegen dient der Strafverfolgung und die Anwendung von Teil 3

BDSG ist sachgerecht. Nach dem Wortlaut des § 45 Satz 1 wäre dieser jedoch nicht einschlägig und das ZStV würde unter die DSGVO fallen.

Auch kommen die gesetzgeberischen Ziele eines einheitlichen Datenschutzregimes für polizeiliches Handeln sowie die Verfolgung von Ordnungswidrigkeiten im Wortlaut nicht klar zum Ausdruck. Insbesondere in Bezug auf die Einbeziehung von Ordnungswidrigkeiten kommt aus dem Wortlaut nicht klar und eindeutig zum Ausdruck, dass der Bundesgesetzgeber hier ausschließlich die Verfolgung und Ahndung von Ordnungswidrigkeiten erfasst sehen wollte und nicht bereits deren Verhütung durch nicht-polizeiliche Gefahrenabwehr.

In der Praxis führt der Wortlaut zu weiteren Problemen, die eine Klarstellung erforderlich machen. Aus dem Wortlaut geht nicht hervor, ob die Dokumentation des betreffenden polizeilichen/ordnungsbehördlichen Handelns mit vom Anwendungsbereich erfasst sein soll. Dies ist jedoch erforderlich, da es sich hierbei um Daten aus der Aufgabenerfüllung, die lediglich einer engeren Zweckbindung unterworfen werden, handelt. Solange sie zur Aufgabenerfüllung erforderlich sind, dürfen sie verarbeitet werden. Ist die Aufgabe erfüllt, entfällt diese Legitimation und die Daten müssten eigentlich gelöscht werden. Die weitere Verarbeitung ist nur noch zum Zweck der Vorsorge unter besonderen Voraussetzungen (Negativprognose, Verhältnismäßigkeit) und zum Zweck der Dokumentation der Rechtmäßigkeit polizeilichen Handelns zulässig. Die Dokumentation ist folglich eine Ausnahme vom grundsätzlichen Löscherfordernis, die zu einer engeren Zweckbindung der weiteren Verarbeitung führt. Wegen des engen Sachzusammenhanges der Dokumentation mit der zugrunde liegenden Aufgabenerfüllung führt die engere Zweckbindung jedoch nicht zu einem Wechsel des Datenschutzregimes. Auch für elektronische Akten der Polizeibehörden, soweit diese der Dokumentation der polizeilichen Aufgabenerfüllung dienen (nicht z.B. allgemeine Verwaltungs- oder Personalangelegenheiten), müssen die Vorgaben des dritten Teils BDSG gelten.

3. Sind die Begriffsbestimmungen in § 2 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Insgesamt erscheint die Norm sachgerecht, praktikabel und normenklar.

In der Prüfpraxis der deutschen Aufsichtsbehörden kommt es jedoch immer wieder zu Unsicherheiten bei der Auslegung des § 2 Absatz 3 BDSG. Für die Anwendung des BDSG und die Zuständigkeitsabgrenzung zwischen BfDI und den Aufsichtsbehörden der Länder ist entscheidend, ob es sich bei einem Verantwortlichen um eine öffentliche Stelle des Bundes handelt, oder nicht.

Nach § 2 Absatz 3 BDSG gelten Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, als öffentliche Stellen des Bundes wenn sie:

- über den Bereich eines Landes hinaus tätig werden oder
- dem Bund die absolute Mehrheit der Anteile oder die absolute Mehrheit der Stimmen zusteht.

Auf eine zusätzliche Beteiligung nicht-öffentlicher Stellen kommt es nicht an. Ist keine der beiden Voraussetzungen gegeben, handelt es sich um öffentliche Stellen der Länder.

Zunächst ist in der Praxis zu prüfen, ob es sich überhaupt um eine privatrechtliche Vereinigung öffentlicher Stellen handelt. Hierfür kommen folgende Kriterien in Betracht:

- Gesellschaftsrechtliche Beteiligung von Bund und (mindestens einem) Land,
- Mitbestimmung in Organen der Vereinigung,

- gemeinschaftliche Finanzierung im Sinne einer reinen Bezuschussung ohne jede Mitwirkungsmöglichkeit allein dürfte nicht ausreichend sein.
- Stellen in öffentlich-rechtlicher Organisationsform fallen von vornherein nicht darunter, da hier eine eindeutige Zuordnung zum jeweiligen Verband (Bund oder Land) gegeben ist; eine gemeinschaftliche Finanzierung spielt dann keine Rolle.
  Bsp.: eine öffentlich-rechtliche Stiftung nach Landesrecht bleibt auch dann öffentliche Stelle des Landes, wenn sie vom Bund mitfinanziert wird oder dieser sogar in Aufsichtsgremien mitbestimmt, z. B. Stiftung Preußische Schlösser und Gärten Berlin-Brandenburg, eine öffentlich-rechtliche Stiftung des Landes Brandenburg.

Weiteres Tatbestandsmerkmal ist, dass Aufgaben der öffentlichen Verwaltung wahrgenommen werden. Dieser Begriff wird grundsätzlich eher weit ausgelegt:

- Mitwirkung an der Aufgabenerfüllung der beteiligten öffentlichen Stellen,
- Zusammenhang zwischen öffentlicher Aufgabe und Zweck/Ziel der Vereinigung,
- Spielt es für die Ziele der Vereinigung eine Rolle, dass gerade die öffentliche Hand beteiligt ist?

Bei Einrichtungen der Wissenschaft oder der Kulturpflege, an denen Bund und Länder beteiligt sind, werden i. d. R. Aufgaben der öffentlichen Verwaltung bejaht (Goethe-Institut, Max-Planck-Gesellschaft, Deutsche Forschungsgemeinschaft, Deutsches Zentrum für Luft- und Raumfahrt).

Schwierigkeiten bereiten Unternehmen der Daseinsvorsorge, die ebenso gut ohne Beteiligung der öffentlichen Hand betrieben werden könnten:

- Z.B. Flughafen Berlin-Brandenburg GmbH,
- Ausgeschlossen sind jedenfalls reine Finanzbeteiligungen.

In der Praxis problematisch ist § 2 Absatz 3 Satz 1 Nr. 1 BDSG. Es stellt sich die Frage, wann eine Vereinigung über den Bereich eines Landes hinaus tätig wird. Nach Sinn und Zweck der Norm liegt eine Unterscheidung danach nahe, ob die Verarbeitung personenbezogener Daten über den Bereich eines Landes hinaus wirkt. Hinzukommt, dass das alleinige Anknüpfen an räumliche Gesichtspunkte vor dem Hintergrund der Kompetenzordnung des Grundgesetzes nicht ganz unproblematisch ist. In der Kommentarliteratur wird daher als zusätzliches Merkmal verlangt, dass es sich um eine Tätigkeit handeln muss, die normalerweise in bundeseigener Verwaltung ausgeübt würde (Dammann, in: Simitis, 8. Aufl., § 2 BDSG, Rn. 73). Dies lässt sich allerdings dem Wortlaut nicht entnehmen.

In der Praxis wurden vielfach in Zweifelsfällen durch Abstimmung zwischen den beteiligten Aufsichtsbehörden sachgerechte Lösungen gefunden. Da -wie dargelegt- vor allem die Tatbestandsmerkmale „Aufgaben der öffentlichen Verwaltung“ und „über den Bereich eines Landes hinaus tätig werden“ jedoch einen nicht unerheblichen Auslegungsspielraum bieten, wäre eine diesbezügliche Konkretisierung des § 2 Absatz 3 BDSG durch den Gesetzgeber hilfreich.

II. Rechtsgrundlagen für die Datenverarbeitung

Zusammenfassung:
Das BDSG zeigt sich hinsichtlich der Rechtsgrundlagen für die Verarbeitung sowie die Weiterverarbeitung personenbezogener Daten in § 4 sowie in den §§ 22-23, 25, 26 und der Vorschrift des § 29 über die Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten als teilweise unionsrechtswidrig (§ 4 Absatz 1 Satz 1 Nr. 3, § 23 Absatz 1 Nr. 2 und § 29 Absatz 3 Satz 1 BDSG) und in weiten Teilen als wenig normenklar und zu unbestimmt. Als problematisch erweist sich dabei insbesondere der Umstand, dass die unter Verwendung unbestimmter Rechtsbegriffe teilweise sehr abstrakt und allgemein gehaltenen Verarbeitungsgrundlagen auch auf Datenverarbeitungen zugeschnitten sind, welche aufgrund ihrer Eingriffstiefe in datenschutzrechtliche Grundrechtspositionen detaillierte bereichsspezifische Verarbeitungsgrundlagen erfordern, welche Art, Zweck und Umfang der Datenverarbeitung normenklar regeln. § 26 BDSG wird in seiner aktuellen Fassung seiner Aufgabe im Beschäftigtendatenschutz nicht gerecht. In der Praxis resultieren aus dem weiten Interpretationsspielraum für alle Beteiligten Unklarheiten. Um den besonderen Herausforderungen des Schutzes der datenschutzrechtlichen Grundrechtsposition im Beschäftigtendatenschutz gerecht zu werden, müssten diese normenklarer geregelt werden. Die Einschränkung der Aufsichtsbefugnisse aus Artikel 58 Absatz 1 lit. e und lit. f DSGVO durch § 29 Absatz 3 S. 1 BDSG ist nach Auffassung der DSK europarechtswidrig. § 29 Absatz 3 S. 1 BDSG schränkt die Aufsichtsbefugnisse deutlich stärker ein, als es die Öffnungsklausel in Artikel 90 Absatz 1 DSGVO vorsieht. Die Folge davon ist, dass ein prüfungsfreies Delta entsteht und eine effektive Datenschutzkontrolle zu Lasten des Schutzes personenbezogener Daten weitestgehend ausfällt.

Bei den unter Kapitel 2 BDSG gefassten §§ 48-51 BDSG handelt es sich nach Auffassung der DSK entgegen der Überschrift von Kapitel 2 nicht um eigenständige Rechtsgrundlagen. Die Überschrift ist insbesondere im Hinblick auf § 51 BDSG irreführend, da die Einwilligung nach § 51 BDSG schon dem Wortlaut nach keine Befugnis zur Datenverarbeitung darstellt. Zudem gehen die Inhalte der § 48 und § 50 BDSG nicht über die Vorgaben der JI-RL hinaus und stellen keine Konkretisierung dar. Ferner betrifft die Vorschrift des § 49 BDSG zwar die zentralen Aussagen zur Zweckbindung im Urteil des Bundesverfassungsgerichts zum BKAG (BVerfG NJW 2016, 1781), sie ist jedoch mit den in diesem Urteil getroffenen Aussagen nicht vereinbar.

1. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 3, 4, 22, 23 und 24 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

a) Zu § 4 BDSG

Die Vorschrift des § 4 BDSG wird in Bezug auf eine Datenverarbeitung nichtöffentlicher Stellen als europarechtwidrig angesehen und findet in der aufsichtsbehördlichen Praxis in diesem Bereich keine Anwendung. Auch die neuere Rechtsprechung des Bundesverwaltungsgerichts lässt keinen gegenteiligen Schluss mehr zu (Urteil vom 27.3.2019 – 6 C 2.18). Die Zulässigkeit von Videoüberwachungen zu privaten Zwecken bemisst sich demnach ausschließlich nach Artikel 6 Absatz 1 lit. f DSGVO.

Insbesondere für die Vorschrift des § 4 Absatz 1 Satz 1 Nr. 3 BDSG (Wahrnehmung berechtigter Interessen) bleibt neben Artikel 6 Absatz 1 lit. f DSGVO kein Raum mehr. Die Norm gestattet eine Videoüberwachung „*zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*“ und stellt damit eine Interessenabwägungsklausel dar, die auf die Videoüberwachung durch

nichtöffentliche Stellen zugeschnitten ist (*Buchner*, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. (2020), § 4 BDSG Rn. 12).

Auf öffentliche Stellen findet § 4 Absatz 1 Satz 1 Nr. 3 BDSG keine Anwendung. Dies zeigt sich bereits darin, dass sich eine Videoüberwachung öffentlicher Stellen in jedem Fall im Rahmen der *Aufgabenerfüllung* nach § 4 Absatz 1 Nr. 1 BDSG oder – als klarstellender Unterfall hiervon – *zur Wahrnehmung des Hausrechts* nach § 4 Absatz 1 Nr. 2 BDSG vollzieht.

Es wird daher vorgeschlagen, § 4 Absatz 1 Satz 1 BDSG wie folgt zu ändern:

"*Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch öffentliche Stellen ist nur zulässig, soweit sie*

1. *zu deren Aufgabenerfüllung*
2. *zur Wahrnehmung des Hausrechts*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen."

§ 4 Absatz 1 Satz 2 BDSG ist nach hiesiger Auffassung ersatzlos zu streichen. Infolge dessen ist auch § 4 Absatz 3 Satz 2 BDSG zu streichen.

b) Zu § 22 BDSG

Die Anwendung der Vorschrift gestaltet sich sowohl in Bezug auf ihren Absatz 1 Nr. 1 als auch Absatz 1 Nr. 2 in der Praxis schwierig. Die hierin getroffenen Regelungen geraten insbesondere in Konflikt mit den bereichsspezifischen Regelungen des jeweiligen Fachrechts, welches in großen Teilen bereits eine Verarbeitung sensibler Datenkategorien explizit regelt und den Regelungen des § 22 Absatz 1 BDSG insoweit vorgeht.

Letzteres trifft insbesondere auf Datenverarbeitungen im Bereich der sozialen Sicherheit und des Sozialschutzes zu (§ 22 Absatz 1 Nr. 1 lit. a BDSG). Solche Datenverarbeitungen haben aufgrund ihrer Eingriffsintensität ausschließlich unter dem Rechtsregime der bereits vorhandenen bereichsspezifischen Regelungen des Sozialgesetzbuches stattzufinden (vgl. insbesondere § 35 SGB I, §§ 67 ff. SGB X).

Gleiches gilt für § 22 Absatz 1 Nr. 1 lit. b BDSG. Die Norm gestattet eine Datenverarbeitung auf den Gebieten der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrages der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs. Eine Datenverarbeitung in derart sensiblen Bereichen kann nicht durch eine zentrale Generalklausel im BDSG legitimiert werden. Auch hier ist ausschließlich das jeweilige bereichsspezifische Fachrecht heranzuziehen und ggf. zu schaffen, welches sodann Art, Zweck und Umfang der Datenverarbeitung explizit zu regeln hat.

Die ausschließlich öffentlichen Stellen zustehenden Verarbeitungsgrundlagen in § 22 Absatz 1 Nr. 2 lit. a - d BDSG weisen einen insgesamt zu unbestimmten Wortlaut auf. Durch die pauschale Verwendung unbestimmter Rechtsbegriffe (*erhebliches öffentliches Interesse, zwingende Erforderlichkeit, erhebliche Gefahr für die öffentliche Sicherheit, erhebliche Nachteile/Belange für das/des Gemeinwohl(s)*) gerät die Vorschrift zu einer reinen Abwägungsnorm. Dies entspricht nach hiesigem Rechtsverständnis nicht der Intention des europäischen Gesetzgebers. Dieser fordert in der entsprechenden Öffnungsklausel des Artikel 9 Absatz 2 lit. g DSGVO vielmehr, dass die mitgliedstaatlichen Verarbeitungsgrundlagen in "*einem angemessenen Verhältnis zu den*

verfolgten Ziel[en]" stehen, "*den Wesensgehalt des Rechs auf Datenschutz* [wahren]" und "*angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen* [vorsehen]". Erforderlich hierfür ist, dass die betreffenden Rechtsgrundlagen die Datenverarbeitung so weit wie möglich ausdrücklich, d. h. insbesondere Zweck, Art, Umfang und Grenzen der Verarbeitung, normenklar und hinreichend bestimmt regeln. § 22 Absatz 1 Nr. 2 BDSG wird diesem Anspruch nicht gerecht und lässt sich allenfalls durch eine restriktive datenschutzkonforme Auslegung mit der Öffnungsklausel des Artikel 9 Absatz 2 lit. g DSGVO in Einklang bringen.

Es wird um Überprüfung des Anwendungsbereichs und ggf. Streichung der Norm gebeten.

c) Zu § 23 BDSG

§ 23 Absatz 1 Nr. 2 BDSG ist nach hiesiger Rechtsauffassung unionsrechtswidrig und sollte ersatzlos gestrichen werden. Die Vorschrift erlaubt eine zweckändernde Weiterverarbeitung von Daten in den Fällen, in welchen die Angaben einer Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen. Die Zweckänderung betrifft dabei nicht die zu prüfenden, möglicherweise unrichtigen Daten, sondern die bereits beim Verantwortlichen vorhandenen und rechtmäßig verarbeiteten Daten der betroffenen Person, welche für einen Abgleich herangezogen werden sollen.

§ 23 Absatz 1 Nr. 2 BDSG kann die zweckändernde Weiterverarbeitung gemäß Artikel 6 Absatz 4 DSGVO nur dann legitimieren, wenn die Rechtsvorschrift eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele darstellt. Diese Anforderungen erfüllt § 23 Absatz 1 Nr. 2 BDSG nicht. Es ist – selbst infolge einer weiten Auslegung – nicht erkennbar, welches der in Artikel 23 Absatz 1 lit. a - j DSGVO genannten Ziele die Norm in Bezug nimmt. Sie enthält darüber hinaus keine Einschränkungen, welche sicherstellen, dass der normierte Datenabgleich tatsächlich zum Schutz dieser Ziele stattfindet.

§ 23 Absatz 1 Nr. 3 BDSG erweist sich in seiner Variante 1 (*Abwehr erheblicher Nachteile für das Gemeinwohl*) sowie seiner Variante 5 (*zur Wahrung erheblicher Belange des Gemeinwohls*) als zu allgemein formuliert, um die Anforderungen der Artikel 6 Absatz 4, Artikel 23 Absatz 1 DSGVO zu erfüllen. Es ist insbesondere unklar, welche Sachverhalte unter diese beiden Varianten, insbesondere in Abgrenzung der Abwehr einer Gefahr für die öffentliche Sicherheit (Variante 2), subsumiert werden sollen. Die öffentliche Sicherheit umfasst bereits den Schutz der Unverletzlichkeit der objektiven Rechtsordnung, den Schutz subjektiver Rechte und Rechtsgüter sowie den Schutz des Bestandes des Staates und sonstiger Träger der öffentlichen Gewalt, ihrer Einrichtungen und Veranstaltungen. Inwieweit § 23 Absatz 1 Nr. 3, Var. 1 und 5 BDSG darüber hinaus ein eigenständiger Anwendungsbereich zukommt, ist unklar. Es wird daher angeregt, den Anwendungsbereich von § 23 Absatz 1 Nr. 3, Var. 1 u. 5 zu prüfen und die Vorschriften ggf. ersatzlos zu streichen.

2. Sind die Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Der Anwendungsbereich von § 25 Absatz 2 Nr. 1 BDSG ist weitgehend unklar. Die Norm lässt eine Übermittlung personenbezogener Daten von öffentlichen Stellen an nichtöffentliche Stellen in den Fällen zu, in welchen die Übermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich ist und die Voraussetzungen des § 23 BDSG vorliegen. Diese Regelung erscheint überflüssig, da in den Fällen der vorgenannten Aufgabenwahrnehmung die Übermittlung der aufgabenwahrnehmenden Stelle bereits auf § 3 BDSG bzw. einer

spezialgesetzlichen Übermittlungsnorm beruht. Die Übermittlung der Daten ist in diesen Fällen gerade Bestandteil der Aufgabenwahrnehmung der übermittelnden Stelle und muss folglich nicht mehr durch eine gesonderte Rechtsgrundlage legitimiert werden (*Marsch*, in: Sydow, Bundesdatenschutzgesetz 1. Auflage 2020, § 25, Rn. 18).

§ 25 Absatz 2 Nr. 2 BDSG überlässt die Interessenabwägung zwischen den Interessen des privaten Dritten und der betroffenen Person in Gänze der übermittelnden öffentlichen Stelle. Letzterer wird eine diesbezügliche Entscheidung abverlangt, ohne ihr hierbei jedoch abwägungslenkende Kriterien zu Hand zu geben. Dies erweist sich in der Praxis als problematisch, insbesondere, da unter einem "*berechtigten Interesse an der Kenntnis der zu übermittelnden Daten*" jegliches Interesse wirtschaftlicher, rechtlicher oder auch ideeller Art verstanden werden kann. Zu Recht wird die geringe Regelungstiefe dieser reinen Abwägungsnorm in der Kommentarliteratur kritisiert, mit dem Hinweis, dass es zusätzlicher gesetzlicher Regelungen – ggf. auch in Form von Verwaltungsvorschriften – bedürfe, um eine hinreichend datenschutzkonforme Rechtsanwendung zu ermöglichen (*Frenzel*, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, § 25 Rn. 13).

§ 25 Absatz 2 Nr. 3 BDSG ist als spezieller Fall des § 25 Absatz 2 Nr. 2 BDSG zu verstehen, erlaubt der öffentlichen Stelle jedoch eine zielgenauere Prüfung der jeweiligen Abwägungskriterien, da als berechtigtes Interesse an der Übermittlung nur die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche anerkannt wird. Diese rechtlichen Ansprüche sind der öffentlichen Stelle darzulegen und können von ihr entsprechend überprüft werden.

Aufgrund des Umstands, dass eine auf § 25 Absatz 2 Nr. 3 BDSG gestützte Datenübermittlung zwangsläufig mit einer zweckändernden Weiterverarbeitung auf Seiten des Dritten einhergeht, sollte die Norm indes nur die Übermittlung zur Geltendmachung zivilrechtlicher Ansprüche erlauben, da nur für diese Form der zweckändernden Weiterverarbeitung auch eine entsprechende Öffnungsklausel in Artikel 6 Absatz 4, Artikel 23 Absatz 1 lit. j DSGVO existiert (*Marsch*, in: Sydow, Bundesdatenschutzgesetz, 1. Aufl. 2020, § 25 Rn. 20).

3. Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 26 bis 31 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

a) Zu § 26 BDSG

Nein. § 26 Absatz 1 BDSG erfüllt nicht die Voraussetzungen praktikabel, normenklar und sachgerecht zu sein.

Mit § 26 BDSG macht der deutsche Gesetzgeber von der Öffnungsklausel aus Artikel 88 DSGVO Gebrauch. Die sehr offene Formulierung dieser Vorschrift führt in der Praxis zu Interpretationsspielräumen und damit zu Unklarheiten für alle Beteiligten, also Arbeitgeber, Arbeitnehmer, Personalvertretungen und Aufsichtsbehörden.

§ 26 BDSG in seiner aktuellen Fassung wird dem Beschäftigtendatenschutz nicht gerecht. Die Vorschrift regelt dieses sehr komplexe Rechtsgebiet. Komplex allein schon deswegen, weil im Rahmen des Beschäftigungsverhältnisses personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert werden. Die von § 26 BDSG umfassten Verarbeitungssituationen sind zwar vielfältig. Unbefriedigend ist es aber, dass die Rechtmäßigkeit der Datenverarbeitung fast ausschließlich anhand des Kriteriums der Erforderlichkeit bestimmt werden muss. Dadurch ist die Beurteilung der Zulässigkeit einzelner Verarbeitungs- und Überwachungsmaßnahmen in vielen Fällen für den Arbeitgeber mit Unklarheiten verbunden. Aufgrund der offenen Formulierung des § 26 BDSG kann insbesondere nicht immer eindeutig festgestellt werden, ob die Datenverarbeitung tatsächlich für die

Durchführung des Beschäftigtenverhältnisses erforderlich ist. Dadurch verbleiben zu viele Rechtsunsicherheiten, die eine rechtssichere Anwendung der Regelung erschweren, soweit nicht bereits eine dezidierte Rechtsprechung der Arbeitsgerichte erfolgt ist. Insbesondere da die im Rahmen des Beschäftigungsverhältnisses verarbeiteten personenbezogenen Daten des Arbeitnehmers oftmals auch den Kern seiner privaten Lebensführung betreffen, führen die bestehenden Unklarheiten zugleich auch zu einem Risiko für die Rechte der Beschäftigten. Auch die in den gesetzlich geregelten Fällen eröffnete Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie losgelöst vom Erhebungszweck für andere Verwendungen zu nutzen, birgt Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Zudem nehmen mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

In der Praxis hat sich unter anderem gezeigt, dass sich die Anwendungsbereiche des § 22 und des § 26 BDSG überschneiden, ohne dass klar ist, welcher der beiden Paragraphen den Vorrang genießt. Unklar bleibt auch das Verhältnis der beiden Paragraphen zu den Fallgestaltungen in Artikel 9 Absatz 2 DSGVO. Die Beschäftigtendaten betreffenden Erlaubnistatbestände sollten daher entweder in einem Beschäftigtendatenschutzgesetz aufgenommen, oder, sofern ein solches keine Mehrheit finden sollte, direkt in dem dann zu überarbeitenden § 26 BDSG, möglicherweise in einem eigenen Absatz, aufgenommen werden.

In der Praxis hat sich zudem gezeigt, dass das Verhältnis zwischen § 26 BDSG, Artikel 6 und Artikel 9 DSGVO problematisch ist. Für den Normanwender stellt sich die Frage, wann darf auf die Ermächtigungsgrundlagen aus der DSGVO zurückgegriffen werden, wenn die Verarbeitung gemäß § 26 BDSG ausgeschlossen ist.

Nach wie vor offen ist auch die Fragestellung und daher zu diskutieren, ob Kollektivvereinbarungen zusätzliche Rechtsgrundlagen sind. Artikel 88 Absatz 1 DSGVO lässt zu, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. § 26 Absatz 4 BDSG schafft hier keine Klarheit. In der Praxis ist die Frage nach wie vor umstritten, ob Kollektivvereinbarungen nach Artikel 88 Absatz 1 DSGVO Regelungen enthalten dürfen, die die Verarbeitung von Beschäftigtendaten erlauben, also zusätzliche Rechtsgrundlagen für eine Verarbeitung von Beschäftigtendaten schaffen. Die mit § 26 BDSG gegebenen Entscheidungsspielräume sollten deshalb durch eine klarere Gesetzgebung beantwortet werden und nicht den anwendenden Personen, zuständigen Behörden und Gerichten überlassen bleiben.

Die Frage, ob die Regelung des § 26 BDSG "sachgerecht, praktikabel und normenklar" ist, ist seit Sommer letzten Jahres Gegenstand der Beratungen des wissenschaftlichen Beirats Beschäftigtendatenschutz. Der wissenschaftliche Beirat hat den Auftrag, diese Frage zu beantworten und gegenüber dem BMAS Empfehlungen im Hinblick auf die Notwendigkeit eines eigenen Beschäftigtendatenschutzgesetzes bzw. denkbarer Alternativen auszusprechen. Aktuell dauern die Beratungen noch an. Mit der Abgabe der Empfehlungen ist nach jetzigem Stand nicht vor dem 2. Quartal 2021 zu rechnen. Der Beirat wird sich sowohl zu den Zielen eines besseren Beschäftigtendatenschutzes als auch zu den Wegen, wie diese Ziele erreicht werden können, äußern.

Begrüßt wird, dass die Frage, ob der Betriebs- und Personalrat als Teil der verantwortlichen Stelle zu sehen sind oder als eigene verantwortliche Stelle, Berücksichtigung im Referentenentwurf des Bundespersonalvertretungsgesetzes und des Betriebsrätestärkungsgesetz erfährt. Sie sollte auch in den Landespersonalvertretungsgesetzen Berücksichtigung finden.

b) Zu §§ 27 – 28 BDSG

Die Einschränkungen der Betroffenenrechte in § 27 Absatz 2 und § 28 Absatz 2 bis 4 BDSG werden den Anforderungen der Öffnungsklauseln in Artikel 89 Absatz 2 und 3 DSGVO nicht gerecht und sollten daher dringend überarbeitet werden.

Zunächst fehlt in beiden Vorschriften der in Artikel 89 Absatz 2 und 3 DSGVO niedergelegte Grundsatz, dass Einschränkungen der Betroffenenrechte zu Zwecken der Forschung, der Archivierung und zu statistischen Zwecken nur unter der Voraussetzung eingeführt werden dürfen, dass bei der Verarbeitung Bedingungen und Garantien gemäß Artikel 89 Absatz 1 DSGVO zu gewährleisten sind. Es muss sich also um Verarbeitungen handeln, bei denen der Grundsatz der Datenminimierung (Artikel 5 Absatz 1 lit. c DSGVO) durch wirksame technische und organisatorische Maßnahmen (Artikel25 und 32 DSGVO) in besonderer Weise zu sichern ist, wobei die Abwägungsklauseln der Artikel 25 und 32 DSGVO, die eine Abwägung mit den wirtschaftlichen Interessen des Verantwortlichen erlauben, im Rahmen von Artikel 89 Absatz 1 DSGVO gerade nicht gelten. Verarbeitungen zu Forschungszwecken, zu Archivzwecken im öffentlichen Interesse und zu statistischen Zwecken fallen nur dann in den Anwendungsbereich der Öffnungsklauseln in Artikel 89 Absatz 2 und 3, wenn sie solche Bedingungen und Garantien erfüllen. Der Verweis auf Artikel 89 Absatz 1 DSGVO sollte dringend in § 27 Absatz 2 und § 28 Absatz 2 bis 4 BDSG eingefügt werden.

Weiterhin werden § 27 Absatz 2 und § 28 Absatz 4 BDSG der Anforderung der qualifizierten Erforderlichkeit aus Artikel 89 Absatz 2 und 3 DSGVO nicht gerecht. Einschränkungen der Betroffenenrechte nach Artikel 89 Absatz 2 und 3 kann der Gesetzgeber im Mitgliedstaat nur treffen, soweit die uneingeschränkte Geltung der genannten Betroffenenrechte voraussichtlich die Verwirklichung der „privilegierten“ Zwecke unmöglich machen oder ernsthaft beeinträchtigen würde und die Ausnahmen von diesen Rechten im Unionsrecht oder im Recht der Mitgliedstaaten notwendig sind für die Erfüllung dieser Zwecke. Angesichts der Weite der möglichen Beschränkungen ist diese Prüfung besonders sorgfältig durchzuführen. Zunächst ist auf den Maßstab der Erforderlichkeit einzugehen. Dieser darf nicht von vornherein mit einer Ressourcenfrage gleichgesetzt werden. So können Betroffenenrechte keinesfalls schon deshalb umfassend ausgesetzt werden, weil ihre Erfüllung für den Verantwortlichen einen zusätzlichen Aufwand bedeuten würde und er die nötigen Ressourcen z.B. von seinen Forschungsressourcen abziehen müsste. So ist zum Beispiel schwer vorstellbar, dass die Gewährleistung des Auskunftsrechts Forschungszwecke, statistische Zwecke oder Archivierungszwecke generell unmöglich macht oder ernsthaft beeinträchtigt. Dies mag durch ein sehr hohes Aufkommen an Auskunftsersuchen oder durch die konkrete Form der Anfrage in Einzelfällen für einen kurzen Zeitraum vorkommen, wird aber weder die Regel sein noch in den Einzelfällen immer einen Dauerzustand darstellen.

Nicht erforderlich zur Aufrechterhaltung der Zweckerreichung ist es zum Beispiel, allgemein für die Zwecke des Artikel 89 Absatz 2 und 3 DSGVO das Auskunftsrecht auszuschließen, denn ein milderes, ebenso effektives Mittel wäre es zum Beispiel, eine Vorschrift zu schaffen, die beim Vorkommen hoher Zahlen von Auskunftsersuchen einem Verantwortlichen im Einzelfall erlaubt, Auskunftsersuchen mit einer längeren Frist zu beantworten oder die bei umfassenden Auskunftsanfragen die inhaltliche Reichweite des Auskunftsanspruchs beschränkt. Insgesamt müssen Regelungen geschaffen werden, die den Grundrechtseingriff, den die Ausnahmen von den Betroffenenrechten darstellen, auf das absolut notwendige Maß herabsetzen, indem sie die Einschränkung der Betroffenenrechte an im Einzelfall zu prüfende Tatbestandsmerkmale knüpfen und differenziertere Einschränkungen vorsehen als das völlige Aussetzen der Betroffenenrechte. Eine Regelung des Einzelfalls ist hierzu keinesfalls notwendig, wohl aber eine Regelung, die klare und verhältnismäßige Kriterien für die Anwendung durch die Verantwortlichen schafft. Diesem Auftrag ist der Gesetzgeber mit § 27 Absatz 2, und § 28 Absatz

4 BDSG bisher nicht nachgekommen, sondern hat die Betroffenenrechte breit und umfassend in übermäßiger Weise eingeschränkt.

Gemäß § 27 Absatz 2 Satz 1 BDSG sind die Betroffenenrechte in Artikel 15, Artikel 16. Artikel 18 und Artikel 21 DSGVO beschränkt, soweit sie voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung zum Erreichen dieser Zwecke notwendig ist. § 27 betrifft alle Kategorien personenbezogener Daten.

Satz 1 gibt den Text des Artikel 89 Absatz 2 DSGVO wieder, ohne ihn in irgendeiner Hinsicht zu konkretisieren. Die Norm ist so nah am Wortlaut, dass fraglich erscheint, ob sie nicht gegen das Normwiederholungsverbot verstößt. Der Gesetzgeber hat hier seine Aufgabe nicht erfüllt, den Verantwortlichen klare Kriterien an die Hand zu geben, um Einschränkungen im Einzelfall grundrechtsschonend auszuführen. Stattdessen liegt die Bewertung, wann Betroffenenrechte tatsächlich Forschungs- und Statistikzwecke ernsthaft beeinträchtigen, und inwieweit daraufhin eine Einschränkung der Betroffenenrechte zulässig ist, vollständig bei den Verantwortlichen. Diese werden voraussichtlich häufig weit über das zulässige Maß der Beschränkungen hinausgehen und pauschal Betroffenenrechte im Bereich der Forschung und Statistik weitgehend aufheben. Zur Begründung für die breite und undifferenzierte Vorschrift gibt die Gesetzesbegründung an, dass etwa Ethikkommissionen ohne Einschränkung der Betroffenenrechte bestimmte Forschungsprojekte ablehnen könnten. Diese Begründung ist nicht überzeugend. Sie kann den tiefen Eingriff in die Betroffenenrechte nicht aufwiegen.

Gemäß § 27 Absatz 2 Satz 2 BDSG besteht das Recht auf Auskunft außerdem dann nicht, wenn die personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Mit § 27 Absatz 2 Satz 2 BDSG nimmt der Gesetzgeber eine Konkretisierung vor, die in vergleichbarer Form auch schon in § 33 Absatz 2 Satz 1 Nr. 5 BDSG a.F. enthalten war. Obwohl der Gesetzgeber die Regelung auf Artikel 23 Abs. 1 DSGVO stützt, ist richtigerweise Artikel 89 Absatz 2 DSGVO die einschlägige Öffnungsklausel, denn die Norm schützt nicht die Rechte Dritter, sondern den Verantwortlichen vor unverhältnismäßigem Aufwand. Den besonderen Anforderungen des Artikel 23 Absatz 1 und Abs. 2 DSGVO wird die Norm ohnehin nicht gerecht.

An das Merkmal des unverhältnismäßigen Aufwands im Sinne der Vorschrift wären hohe Anforderungen zu stellen, damit die Norm Artikel 89 Absatz 2 DSGVO gerecht würde. In die Bewertung des Aufwands müsste insbesondere mit einfließen, ob auch andere Mittel als der völlige Ausschluss des Auskunftsrechts, etwa eine Auskunft mit längerer Frist als üblich, geeignet sind, den Aufwand auf ein verhältnismäßiges Maß zu senken. Dies sollte dringend im Text der Vorschrift klargestellt werden, denn die derzeitige Formulierung der Vorschrift wird voraussichtlich nicht dazu führen, dass Verantwortliche in derart grundrechtsschonender Weise vorgehen, sondern eher dazu führen, dass schon bei vergleichsweise geringem Aufwand das Auskunftsrecht vollständig ausgeschlossen wird.

§ 28 Absatz 2 BDSG sieht vor, dass das Recht auf Auskunft der betroffenen Person gem. Artikel 15 DSGVO nicht besteht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen. Die Regelung entspricht § 14 Absatz 1 Bundesarchivgesetz (BArchG.) § 28 Absatz 2 BDSG erscheint als verhältnismäßige Einschränkung. Archive müssen aufgrund dieser Vorschrift weiterhin nach personenbezogenen Daten der betroffenen Person suchen und diese beauskunften, soweit sie verschlagwortet und daher auffindbar sind, ohne sämtliches Archivgut zu lesen. Auch die Anforderung, dass die betroffenen Personen geeignete Angaben zum Auffinden des Archivguts bereitzustellen haben, erscheint nicht unverhältnismäßig.

Das Recht auf Berichtigung (Artikel 16 DSGVO) besteht gemäß § 28 Absatz 3 DSGVO nicht zu Archivzwecken im öffentlichen Interesse. Ausgleichend hat die betroffene Person aber das Recht, den Unterlagen eine Gegendarstellung hinzuzufügen. Die Regelung entspricht § 14 Absatz 4 BArchG. Die Einschränkung erscheint notwendig, da die Berichtigung von Archivgut, den Zweck der Archivierung im öffentlichen Interesse ernsthaft beeinträchtigen würde. Durch das Recht zur Gegendarstellung werden die Rechte der Betroffenen aber in grundrechtsschonender Weise nur soweit eingeschränkt wie erforderlich.

Gemäß § 28 Absatz 4 DSGVO bestehen die Rechte auf Einschränkung der Verarbeitung (Artikel 18 Absatz 1 lit. a, b und d DSGVO), auf Datenübertragbarkeit (Artikel 20 DSGVO) und auf Widerspruch (Artikel 21 DSGVO) nicht, soweit diese voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind. Auch diese Regelung wiederholt lediglich den Wortlaut der Öffnungsklausel ohne zu konkretisieren. Die Vorschrift leidet damit an denselben Mängeln wie § 27 Absatz 2 BDSG. Als Konkretisierung wäre es hier zum Beispiel möglich gewesen, die Rechte aus Artikel 18 und 21 DSGVO unter konkreten Kriterien einzuschränken, da diese besonders häufig in Konflikt mit dem Zweck der Archivierung geraten, im Hinblick auf das Recht auf Datenübertragbarkeit jedoch eine vergleichbare Konstruktion zu wählen wie in § 28 Absatz 2 BDSG.

c) Zu § 29 BDSG

Die Norm ist nach Auffassung der DSK teilweise europarechtswidrig. Die DSK hat bereits im Gesetzgebungsverfahren und in ihren Forderungen für die jetzt laufende Legislaturperiode die Streichung wegen Europarechtswidrigkeit gefordert. An dieser Forderung wird festgehalten.

Die Praxis hat gezeigt, dass die bereits geäußerten Bedenken gegenüber § 29 Absatz 3 Satz 1 BDSG begründet sind. Der nationale Gesetzgeber sollte von dieser Einschränkung der Aufsichtsbefugnisse Abstand nehmen. Dies ist auch möglich, da Artikel 90 Absatz 1 DSGVO eine fakultative Öffnungsklausel für den nationalen Gesetzgeber ist.

Grundsätzlich können gemäß Artikel 90 Absatz 1 DSGVO die Aufsichtsbefugnisse aus Artikel 58 Absatz 1 lit. e und lit. f DSGVO eingeschränkt werden, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschrift gilt in Bezug auf personenbezogene Daten, die der Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.

Die in Artikel 29 Absatz 3 S. 1 BDSG gewählte Formulierung geht hierüber hinaus und überdehnt den in Artikel 90 Absatz 1 DSGVO eröffneten Spielraum.

Die Formulierung in § 29 Absatz 3 Satz 1 BDSG schließt die Befugnisse der Aufsicht aus Artikel 58 Absatz 1 lit. e und lit. f DSGVO für alle Personen aus, die in § 203 Absatz 1, 2 a und 3 des StGB genannt sind oder deren Auftragsverarbeiter. Eine Abwägung im Hinblick auf die Frage der Notwendig- und Verhältnismäßigkeit findet nicht statt. Die Gesetzesbegründung zu § 29 BDSG fängt dies nicht auf.

Die Folge ist, dass eine effektive Datenschutzkontrolle bei den in § 203 Absatz 1, 2a und 3 StGB genannten Personen nahezu unmöglich wird.

Mit Artikel 58 Absatz 1 lit. e und f DSGVO sind die Kernbefugnisse der Kontrolle durch die Aufsichtsbehörde ausgeschlossen. Eine Prüfung der Aufsicht vor Ort, beispielsweise wegen der Kontrolle der getroffenen technisch-organisatorischen Maßnahmen oder Fragen des Beschäftigtendatenschutzes ist so ebenfalls ausgeschlossen. Die Aufsichtspraxis hat dies bestätig.

Die Aufsichtsbehörden können teilweise keine Prüfungen mehr in der Arztpraxis oder Anwaltskanzlei vornehmen, weil sich der Inhaber der Arztpraxis oder der Anwalt auf § 29 Absatz 3 Satz 1 BDSG berufen. Dabei müsste dies, bei richtiger Umsetzung des Artikel 90 Absatz 1 DSGVO möglich sein. Unabhängig davon ist grundsätzlich nur die Einschränkung der Prüfung zulässig, die sich auf den einen Teilbereich bezieht und nach Artikel 90 Absatz 1 DSGVO auch nur dann, wenn dies notwendig und verhältnismäßig ist.

Das so entstandene prüfungsfreie Delta bedeutet, dass personenbezogene Daten komplett ohne Kontrolle durch Aufsicht sind und in der Zukunft auch wären. Dies kann auch nicht durch eine Aufsicht durch die berufsständischen Organisationen, beispielsweise die Rechtsanwaltskammern, aufgefangen werden. Allein schon die Anforderungen der DSGVO an eine unabhängige Datenschutzaufsicht stünden dem entgegen.

§ 29 Absatz 3 BDSG führt außerdem dazu, dass die Aufsichtsbehörde nicht in jedem Fall den Betroffenen bei der Durchsetzung ihrer durch die DSGVO gesicherten Betroffenenrechte, beispielsweise Patient gegenüber Arzt oder Mandant gegenüber Anwalt, unterstützen und die Durchsetzung kontrollieren kann.

Zusammenfassend sollte § 29 Absatz 3 Satz 1 BDSG dringend auf seine Europarechtskonformität geprüft werden. Sofern Artikel 29 Absatz 3 Satz 1BDSG nicht gestrichen wird, muss die in Artikel 90 Absatz 1 DSGVO geforderte Abwägung von Notwendigkeit und Verhältnismäßigkeit der Einschränkung vorgenommen werden und im Wortlaut der Norm Berücksichtigung finden. Wenn die Norm geändert wird, sollte auch die Verweisung in § 29 Absatz 3 Satz 1 BDSG auf § 203 Absatz 2a StGB aktualisiert werden. § 203 Absatz 2a StGB wurde mittlerweile aufgehoben. Es würde der Normenklarheit dienen, den Verweis zu streichen.

d) Zu §§ 30 – 31 BDSG

Keine Anmerkungen.

4. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 48 bis 51 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Nein.

Bei den Vorschriften der §§ 48-51 BDSG handelt es sich nach Auffassung der DSK nicht um eigenständige Rechtsgrundlagen. Dies sollte schon in der Kapitelüberschrift klargestellt werden. Diese könnte etwa lauten:

„Allgemeine Anforderungen an die Verarbeitung personenbezogener Daten“.

a) Zu § 48 BDSG

§ 48 BDSG ist eine verunglückte Vorschrift. Der Inhalt der Vorschrift geht nicht über die Vorgaben der JI-RL hinaus und stellt keine Konkretisierung dar. Absatz 1 ist als Rechtsgrundlage formuliert. Das ist aber nicht sinnvoll und auch verfassungsrechtlich bedenklich, weil die Vorschrift außer der vagen Formulierung „unbedingt erforderlich“ keine besonderen tatbestandlichen Vorgaben enthält. Diese Formulierung ist im Lichte der aktuellen verfassungsgerichtlichen Rechtsprechung zu sehen, die derartigen Formulierungen keine hohe Eingriffsschwelle zumisst (vgl. zuletzt BVerfG NJW 2020, 2235 und NJW 2020, 2699). Deshalb ist auch der in der Kommentarliteratur geäußerten Kritik zuzustimmen, nach der § 48 BDSG eine Art unspezifische Generalklausel ist, die unter dem Gesichtspunkt der Bestimmtheit einer verfassungskonformen Reduktion dahingehend

bedarf, dass intensive Grundrechtseingriffe nicht auf § 48 BDSG gestützt werden können (so zutreffend Schwichtenberg in: Kühling/Buchner, DSGVO BDSG, 3. Auflage 2020 § 48 BDSG Rn. 7 m.w.N.). Damit schafft sie für den Bereich der besonders zu schützenden Daten gerade keinen besonderen Schutz. In welchen Fällen Polizei- und Strafverfolgungsbehörden sensitive Daten verarbeiten dürfen, sollte ausschließlich in den Fachgesetzen geregelt und entsprechend klargestellt werden. Zielführender wäre es daher, § 48 BDSG in der Weise zu fassen, dass die Vorschrift zusätzlich zur jeweils anwendbaren Rechtsgrundlage besondere Bedingungen festlegt (besondere Garantien).

Entschärft wird das praktische Problem zwar dadurch, dass § 48 BDSG sicherlich bereichsspezifische Vorschriften vorgehen (Schwichtenberg in: Kühling/Buchner, DSGVO BDSG, § 48 BDSG Rn. 7). Die Frage, welche Norm spezieller ist und der allgemeinen Norm des § 48 BDSG vorgeht, lässt sich aber nicht immer eindeutig beantworten. Dies erhöht in der Praxis das Risiko unsachgemäßer Ergebnisse. So hat beispielsweise das VG Hamburg für Datenabgleiche bei Videoaufnahmen § 48 BDSG angewandt (VG Hamburg Urteil vom 23.10.2019 – 17 K 203/19). Das ist aber schon deshalb nicht überzeugend, weil § 48 BDSG insofern nur den Umstand berücksichtigt, dass biometrische Daten verarbeitet werden. Das kann allein aber nicht maßgeblich sein. Denn die Vorschrift berücksichtigt zum Beispiel nicht die besondere Eingriffsintensität umfangreicher Datenabgleiche. Strafprozessordnung und Polizeirecht sortieren Eingriffs- bzw. Standardmaßnahmen nach Art und Zielrichtung der Maßnahme und Zweck der Datenverarbeitung. Daran knüpft § 48 BDSG jedoch nicht bzw. sehr eingeschränkt an. Im Ergebnis erweist sich § 48 BDSG rechtssystematisch deshalb als Fremdkörper ohne sinnvollen Anwendungsbereich und ohne nennenswerten zusätzlichen Schutz für besonders schützenswerte Daten.

b) Zu § 49 BDSG

§ 49 BDSG betrifft die zentralen Aussagen zur Zweckbindung im Urteil des Bundesverfassungsgerichts zum BKAG (BVerfG NJW 2016, 1781). Die Vorschrift ist nicht mit den Aussagen des Urteils vereinbar. Die Zwecke der Gefahrenabwehr und der Strafverfolgung werden nicht hinreichend differenziert. Das BVerfG hält eine Übermittlung personenbezogener Daten aus eingriffsintensiven Ermittlungsmaßnahmen zum einen nur für zulässig, wenn ein gleichgewichtiger Rechtsgüterschutz besteht. Darüber hinaus muss sich aus einem hinreichend spezifischen Anlass ein konkreter Ermittlungsansatz ergeben. Ein lediglich potentieller Ermittlungsansatz oder gar eine allgemeine Nützlichkeit ist nicht ausreichend. Vor diesem Hintergrund sollten die Anforderungen an die Zulässigkeit von Zweckänderungen konkret im Fachrecht geregelt werden.

c) Zu § 50 BDSG

§ 50 BDSG geht nicht über die Vorgaben des Artikel 4 Absatz 3 JI-RL hinaus und stellt keine Konkretisierung dar. Insofern mangelt es der Vorschrift an der erforderlichen Bestimmtheit, insbesondere mit Blick auf die Forderung nach geeigneten Garantien. Es bedarf auch hier einer Ausgestaltung im jeweiligen Fachrecht. Dies sollte klargestellt werden.

d) Zu § 51 BDSG

Die Einwilligung nach § 51 BDSG gibt schon dem Wortlaut nach keine Befugnis zur Datenverarbeitung. Sie unterscheidet sich insoweit ganz wesentlich von der Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 lit. a DSGVO, die bei Vorliegen der gesetzlichen Voraussetzungen (Informiertheit, Freiwilligkeit, Unmissverständlichkeit) die Verarbeitung von personenbezogenen Daten zulässt. Demgegenüber bedarf es im Anwendungsbereich von Teil 3 BDSG stets einer spezifischen fachgesetzlichen Rechtsgrundlage, die eine bestimmte Verarbeitung im Falle der Einwilligung zulässt (vgl. EG 35 JI-RL).

§ 51 BDSG regelt sodann den weiteren Umgang mit einer entsprechend erteilten Zustimmung. Irreführend ist hier vor allem die Platzierung der Vorschrift unter der Kapitelüberschrift „Rechtsgrundlagen der Verarbeitung personenbezogener Daten“. Diese sollte geändert werden.

III. Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen

Zusammenfassung:
Was den Abberufungs- und Kündigungsschutz für Datenschutzbeauftragte betrifft, sollte der Gesetzgeber die zu erwartende Rechtsprechung des EuGH zur Vereinbarkeit von § 6 Absatz 4 Satz 2 BDSG mit Artikel 38 Absatz 3 Satz 2 DSGVO beachten. Die Anhebung des Schwellenwerts in § 38 Absatz 1 BDSG auf 20 beschäftigte Personen hat sich nach den Erfahrungen der deutschen Aufsichtsbehörden nicht als sachgerecht und praktikabel erwiesen.

1. Sind die Regelungen zu Datenschutzbeauftragten öffentlicher Stellen in den §§ 5 bis 7 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die aufgeführten Bestimmungen sind inhaltlich nicht zu beanstanden. Nach abstrakter Betrachtung weisen diese Redundanzen zu den Artikel 37 ff. DSGVO auf. Allerdings hat der Gesetzgeber mit den §§ 5-7 BDSG zugleich die JI-RL umgesetzt und Regelungen zu den Aufgaben des Datenschutzbeauftragten für die öffentlichen Bereiche außerhalb der Anwendbarkeit des EU-Rechts (z.B. Nachrichtendienste, vgl. § 85 BDSG) geschaffen. Ausweislich der Gesetzesbegründung war damit die Sicherstellung einer „kohärenten Rechtsstellung des behördlichen Datenschutzbeauftragten in der gesamten Bundesverwaltung" beabsichtigt (BT-Dr. 18/11325, S. 82).

Insbesondere der in § 6 Absatz 4 BDSG normierte Abberufungs- und Kündigungsschutz erweist sich in der Praxis als effizient, was auch in der arbeitsrechtlichen Rechtsprechung deutlich wird. Unabhängig davon sollte der Gesetzgeber die weiteren Entwicklungen auf europäischer Ebene im Auge behalten: Nach der Vorlage im Rahmen eines Vorabentscheidungsverfahrens nach Artikel 267 AEUV hat das BAG mit Beschluss vom 30.07.2020 (Az.: 2 AZR 225/20) dem EuGH u.a. eine Auslegungsfrage zur Vereinbarkeit von § 6 Absatz 4 Satz 2 BDSG mit Artikel 38 Absatz 3 Satz 2 DSGVO vorgelegt. Mit der erwarteten Entscheidung des EuGH könnte ein gesetzgeberischer Änderungsbedarf entstehen

2. Sind die Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die Anhebung des Schwellenwertes auf 20 beschäftigte Personen erwies sich nicht als sachgerecht und praktikabel. Hierzu wird in der Antwort zum folgenden Fragenkomplex ausgeführt.

3. Mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) wurde in § 38 Absatz 1 Satz 1 BDSG die maßgebliche Zahl der Personen, ab der ein betrieblicher Datenschutzbeauftragter zu benennen ist, von 10 auf 20 angehoben. Angestrebt wurde damit vor allem eine Entlastung kleiner und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine.

    a) Welche Wirkungen hat die Änderung des § 38 Absatz 1 Satz 1 BDSG nach Ihrer Kenntnis erzielt?

b) Hat die Änderung der Norm nach Ihrer Kenntnis zu einer Erleichterung für Unternehmen und Vereine geführt?

Die Beantwortung der Fragen unter a) und b) erfolgt im Zusammenhang.

Mit der Anhebung des Schwellenwertes auf 20 beschäftigte Personen war weder eine Entbürokratisierung, noch eine sonstige Entlastung von Unternehmen und Vereinen erreichbar. Es traten vielmehr gegenteilige Effekte ein. Keinesfalls würde von den Aufsichtsbehörden eine weitere Anhebung des Schwellenwertes befürwortet. In diesem Kontext wird auf folgende Punkte hingewiesen:

Zahlreiche Unternehmen und Vereine trennten sich nach Inkrafttreten des angehobenen Schwellenwertes von extern beauftragten Datenschutzbeauftragten bzw. Benennungen von internen Datenschutzbeauftragten wurden aufgehoben, ohne die damit verbundenen Auswirkungen zu bedenken. Die hierdurch entstandenen Lücken bei der Sicherstellung der internen Kontrolle, der ordnungsgemäßen Schulung und Sensibilisierung von Beschäftigten, der konformen Erfüllung von Rechten betroffener Personen, der Überprüfung strategischer Planungen bei der Verarbeitung personenbezogener Daten und bei der Gewährleistung einer sicheren Datenverarbeitung wurden nach den Erkenntnissen der aufsichtsbehördlichen Prüfpraxis nicht durch alternative Kontrollkonzepte beseitigt. Dabei sind die Unternehmen und Vereine allerdings auch ohne Benennung eines Datenschutzbeauftragten weiterhin verpflichtet, die datenschutzrechtlichen Vorgaben zu erfüllen. Die Abberufung der Datenschutzbeauftragten führte bei den genannten Verantwortlichen zu einem spürbaren Kompetenz- und Kontrollverlust. Unternehmen und Vereine ohne Benennungspflicht für DSB befassen sich nicht oder kaum mit der Erfüllung datenschutzrechtlicher Vorgaben. Das Schutzniveau für Kunden- bzw. Mitgliederdaten wird dabei merklich abgesenkt.

Erfolgte keine Benennung von Datenschutzbeauftragten, muss Kompetenz und Wissen teuer zugekauft werden. Kurzfristigen finanziellen Erleichterungen infolge der Beendigung von Verträgen mit externen Datenschutzbeauftragten stehen langfristige monetäre Belastungen gegenüber. Für die Unternehmen und Vereine traten mit der Anhebung des Schwellenwertes damit keine finanziellen Entlastungen ein. Deutlich wird dies etwa im Rahmen von aufsichtsbehördlichen Prüfungen, in welchen nach den getroffenen Feststellungen in technische Lösungen investiert wurde, denen keine datenschutzkonforme Konzeption zugrunde liegt. Darüber hinaus fehlt den betroffenen Stellen häufig das Problembewusstsein für die Erfüllung datenschutzrechtlicher Verpflichtungen, einschließlich der technisch-organisatorischen Anforderungen bei der Einführung und Verwendung von Informations- und Kommunikationstechnik.

Unternehmen und Vereine ohne benannte Datenschutzbeauftragte stehen in der Gefahr, häufiger Verstöße gegen Datenschutzvorschriften zu begehen, was sich teilweise auch in der Einleitung von Bußgeldverfahren zeigte.

Im Falle der Nichtbenennung von Datenschutzbeauftragten fehlen für die Aufsichtsbehörden oft kompetente Ansprechpartner (vgl. Artikel 39 Absatz 1 lit. d DSGVO). Der bestehende Kompetenzverlust erschwert für die Unternehmen und Vereine die Kommunikation mit den Aufsichtsbehörden im Rahmen von Prüfungen, mit betroffenen Personen etwa bezüglich der Geltendmachung von Rechten nach den Artikel 12 ff. DSGVO oder mit Vertragspartnern, z.B. bei der Durchführung einer Auftragsverarbeitung oder der Wahrnehmung einer gemeinsamen Verantwortung.

Von freiwilligen Benennungen (betrieblicher) Datenschutzbeauftragter haben Unternehmen und Vereine nach Kenntnis der Aufsichtsbehörden bisher nur äußerst selten Gebrauch gemacht.

IV. Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden

Zusammenfassung:
Die DSK hält es für außerordentlich wichtig, im Rahmen der Evaluierung zu prüfen, wie die Vertretung der Aufsichtsbehörden der Länder im Europäischen Datenschutzausschuss (EDSA) sichergestellt werden kann, auch wenn der Bundesrat entgegen § 17 Absatz 1 Satz 2 BDSG keinen Stellvertreter wählt. Im Übrigen haben sich die Willensbildungs- und Abstimmungsprozesse unter den deutschen Aufsichtsbehörden in Angelegenheiten der Europäischen Union und der innerdeutsche Kohärenzmechanismus nach § 18 BDSG mit seiner derzeitigen Anwendungspraxis grundsätzlich bewährt und bislang überwiegend zu sachgerechten Ergebnissen geführt, wobei jedoch in der Praxis Unklarheiten hinsichtlich des Anwendungsbereiches des § 18 BDSG bestehen. In § 19 Absatz 2 Satz 1 BDSG würde eine klarstellende Regelung begrüßt werden, welche Aufsichtsbehörde die Federführung innehat, falls es mehrere Niederlassungen, aber keine Hauptniederlassung in Deutschland gibt. Zur Auflösung von Zuständigkeitsstreitigkeiten in Fällen rein innerstaatlicher Datenverarbeitungen erscheint die Regelung in § 40 Absatz 2 Satz 2 BDSG nicht sachgerecht, weil in der Praxis das Vorschlagsrecht über die örtliche Zuständigkeit einer Landesbehörde überwiegend beim BfDI liegt.

Darüber hinaus hält es die DSK für dringend erforderlich, die aufsichtsbehördlichen Befugnisse im BDSG zu erweitern, indem gegenüber öffentlichen Stellen die Durchsetzung von Maßnahmen mit Zwangsmitteln sowie die Anordnung der sofortigen Vollziehung ermöglicht wird. Außerdem sollten Beschlagnahmerechte bereits im verwaltungsrechtlichen Kontrollverfahren vorgesehen sowie zwei gesetzliche Klarstellungen ins BDSG aufgenommen werden, dass Entscheidungen über Abhilfemaßnahmen und Sanktionen veröffentlicht werden können und dass bei rechtswidrigen Videoüberwachungsanlagen auch deren Rückbau verfügt werden darf. Zudem sind die Regelungen des § 16 Absatz 2 und 3 BDSG, mit denen der der BfDI im Bereich der JI-RL sowie außerhalb des Geltungsbereichs des EU-Rechts auf das Instrument der Warnung und der Beanstandung beschränkt bleibt, im Hinblick auf die in Artikel 47 Absatz 2 JI-RL geregelte Verpflichtung, wirksame Abhilfebefugnisse zu gewähren, unzulänglich. Des Weiteren fehlt in § 16 BDSG eine ausdrückliche Regelung der nach Artikel 47 Absatz 1 JI-RL erforderlichen Untersuchungsbefugnisse des BfDI. Ferner wäre es vor allem im Hinblick auf nationale Normen, die von der Aufsichtsbehörde aufgrund des Anwendungsvorrangs des Unionsrechts nicht angewendet werden, wünschenswert, wenn die Behörde in solchen Fällen selbst eine gerichtliche Entscheidung beantragen könnte.

Im Übrigen spricht sich die DSK dafür aus, dass der Gesetzgeber die Evaluierung zum Anlass nehmen sollte, eine Institutionalisierung der DSK voranzutreiben, Regelungen für die Zusammenarbeit der Aufsichtsbehörden einzuführen, die denen in Kapitel VII der DSGVO vergleichbar sind, sowie gesetzliche Rahmenbedingungen für die Einrichtung einer dauerhaften DSK-Geschäftsstelle zu schaffen.

1. Ist die Zusammenarbeit der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Mit Geltung der DSGVO ab dem 25.05.2018 hat der EDSA die „Artikel 29-Gruppe“ abgelöst. Der EDSA besteht aus den Leitern der Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Deutscher Vertreter im EDSA ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) als gemeinsamer Vertreter. Als Stellvertreterin oder Stellvertreter ist die Leiterin oder der Leiter der Aufsichtsbehörde eines Landes vorgesehen (Stellvertreter).

Nach § 17 Absatz 1 BDSG obliegt dem Bundesrat die Wahl der Stellvertreterin oder des Stellvertreters. Bis heute hat der Bundesrat entgegen der eindeutigen gesetzlichen Verpflichtung aus § 17 Absatz 1 Satz 2 BDSG keine Stellvertreterin bzw. keinen Stellvertreter gewählt. Der Hamburgische Datenschutzbeauftragte Prof. Dr. Johannes Caspar vertritt die Aufsichtsbehörden der Länder mehr als zweieinhalb Jahre nach Inkrafttreten der DSGVO, ohne offizieller Stellvertreter zu sein. Aus Sicht der Datenschutzaufsichtsbehörden sollte daher im Rahmen der Evaluierung geprüft werden, wie eine Vertretung der Aufsichtsbehörden der Länder im EDSA sichergestellt werden kann, wenn der Bundesrat seine gesetzliche Verpflichtung nicht erfüllt.

§ 18 BDSG regelt das Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union. Die für die Zusammenarbeit erforderlichen Willensbildungs- und Abstimmungsprozesse werden durch die beim BfDI eingerichtete Zentrale Anlaufstelle (ZASt) koordiniert und haben aus Sicht der Aufsichtsbehörden bisher grundsätzlich zu sachgerechten Ergebnissen geführt. Allerdings besteht innerhalb der DSK ein Dissens hinsichtlich der bedeutsamen Frage, ob mit der Gesetzesbegründung (BT-Drs. 18/11325, S. 90) bereits im Kooperationsverfahren (Artikel 60-62 DSGVO) ein gemeinsamer Standpunkt nach § 18 BDSG herbeizuführen ist oder ggf. erst im Stadium des Kohärenzverfahrens (Artikel 63 ff. DSGVO)[1].

§ 18 BDSG sieht ein zweistufiges Verfahren zur Herstellung eines gemeinsamen Standpunkts vor, bestehend aus Einvernehmensphase und streitigem Verfahren. Für den Fall, dass im Beteiligungsverfahren nach § 18 Absatz 1 BDSG kein Einvernehmen zustande kommt, ist ein gemeinsamer Standpunkt nach § 18 Absatz 2 BDSG einzuholen. Für die Festlegung dieses gemeinsamen Standpunkts hat der Gesetzgeber das Mehrheitsprinzip festgelegt. Dieser innerdeutsche Kohärenzmechanismus, wie er derzeit in der Praxis angewendet wird, hat sich bislang durchaus bewährt und zu sachgerechten Ergebnissen geführt. Eine erfolgreiche Beteiligung der deutschen Aufsichtsbehörden, wie sie die DSGVO vorsieht (Artikel 51 Absatz 3 DSGVO, Erw.-Gr. 119), kann ohne die Akzeptanz von Mehrheitsentscheidungen letztlich nicht funktionieren.

2. Sind die Zuständigkeiten der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Für das Verfahren der Zusammenarbeit und Kohärenz trifft § 19 BDSG Verfahrensregelungen zur innerstaatlichen Zuständigkeit der Aufsichtsbehörden des Bundes und der Länder. Hierzu knüpft § 19 Absatz 1 BDSG die innerdeutsche Federführung an die Aufsichtsbehörde des Bundeslandes, in dem die Hauptniederlassung oder einzige Niederlassung in der EU gelegen ist.

Ungeregelt ist in § 19 Absatz 2 Satz 1 BDSG der Fall, dass es mehrere Niederlassungen in Deutschland gibt, aber keine Hauptniederlassung. Geht eine Beschwerde in einem Land ein, in dem es keine Niederlassung gibt, muss zwar abgegeben werden, es ist aber unklar, an welche Behörde. Ob für diesen Fall auf § 40 Absatz 2 BDSG zurückgegriffen werden kann, ist unklar. Die Regelung des § 19 Absatz 2 Satz 1 BDSG erscheint somit als unvollständig und insoweit nicht praktikabel. Denkbar wäre eine entsprechende Anknüpfung an die Regelung in § 19 Absatz 1 Satz 3 oder in § 40 Absatz 2 Satz 2 BDSG und die Festlegung der zuständigen Behörde im Verfahren nach § 18 Absatz 2 BDSG.

[1] BfDI und die Aufsichtsbehörden der Länder werden dazu jeweils eigene Stellungnahmen im Rahmen des Evaluierungsprozesses abgeben.

3. Hat sich aus Ihrer Sicht die Regelung in § 40 Absatz 2 BDSG bewährt, wonach sich, wenn der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen hat, die zuständige Aufsichtsbehörde entsprechend Artikel 4 Nummer 16 DSGVO nach der Hauptniederlassung bestimmt?

Für den Fall, dass ein Verantwortlicher über mehrere inländische Niederlassungen verfügt, sieht § 40 Absatz 2 Satz 1 BDSG eine Zuständigkeitskonzentration der Aufsichtsbehörde am Ort der Hauptniederlassung vor. Hierbei handelt es sich im Vergleich zur Rechtslage unter dem BDSG a. F. um eine sehr bedeutsame Vorschrift für Unternehmen, welche sich ungeachtet verschiedener Niederlassungen im eigentlichen Zuständigkeitsbereich mehrerer Aufsichtsbehörden nur mit der Aufsichtsbehörde am Ort der Hauptniederlassung auseinandersetzen müssen.

Kommt eine einvernehmliche Einigung nicht zustande, obliegt das Vorschlagsrecht über die Zuständigkeit zunächst nach § 18 Absatz 2 Satz 1 Alternative 1 BDSG der zuständigen federführenden Behörde i.S.d. § 19 Absatz 1 BDSG. Da sich diese nach Artikel 19 Absatz 1 BDSG nach der Hauptniederlassung bzw. der einzigen Niederlassung bestimmt und § 40 Absatz 2 Satz 2 BDSG voraussetzt, dass über die Hauptniederlassung Zweifel bestehen, kann diese Variante hier nicht angewendet werden. In Ermangelung einer federführenden Aufsichtsbehörde obliegt das Vorschlagsrecht über die Zuständigkeit gemäß § 18 Absatz 2 Satz 1 Alternative 2 BDSG dem gemeinsamen Vertreter im EDSA bzw. dessen Stellvertreter. Besteht zwischen dem gemeinsamen Vertreter und dem Stellvertreter Uneinigkeit, kommt dem Stellvertreter in Fällen, welche eine Angelegenheit betreffen, für welche die Länder allein das Recht der Gesetzgebung haben oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, nach § 18 Absatz 2 Satz 2 BDSG das Vorschlagsrecht zu. In allen anderen Fällen der Uneinigkeit unterbreitet gemäß § 18 Absatz 2 Satz 3 BDSG der gemeinsame Vertreter den Vorschlag. Das führt im Hinblick auf § 40 Absatz 2 BDSG in der Konsequenz zu dem fragwürdigen Ergebnis, dass das Vorschlagsrecht über die örtliche Zuständigkeit einer Landesbehörde in der Mehrzahl der Streitfälle beim BfDI liegt.

4. Sind die Befugnisse der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Jede Aufsichtsbehörde kann gemäß Artikel 58 Absatz 2 DSGVO und Artikel 47 Absatz 2 der JI-RL verbindliche Anordnungen gegenüber öffentlichen Stellen treffen. Nach Artikel 58 Absatz 4 DSGVO und Artikel 47 Absatz 4 der JI-RL bedarf es hierfür ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta der Grundrechte der EU. Das Verfahrensrecht darf unter anderem nicht dazu führen, dass die Durchsetzung der in der DSGVO und der in der JI-RL normierten Grundsätze behindert wird. Das ist allerdings derzeit der Fall.

a) Nach § 17 Verwaltungsvollstreckungsgesetz (VwVG) sind Zwangsmittel gegen Behörden und juristische Personen des öffentlichen Rechts unzulässig, soweit nicht etwas anderes bestimmt ist. Ohne eine bereichsspezifische Regelung können Anordnungen der oder des BfDI entgegen den Vorgaben der DSGVO und der JI-RL zu deren Verbindlichkeit nicht vollzogen werden. Die fehlende Vollstreckbarkeit von Anweisungen und Untersagungen durch Zwangsmittel gegenüber Behörden und juristische Personen des öffentlichen Rechts verstößt gegen das europäische Effektivitätsgebot. Daher muss im Sinne der zweiten Alternative des § 17 VwVG „etwas anderes bestimmt“ und eine Vorschrift im BDSG geschaffen werden, die der oder dem

BfDI die Anwendung von Zwangsmitteln im Fall des Nichtnachkommens von Anordnungen durch öffentliche Stellen ausdrücklich erlaubt.

Zwangsmaßnahmen sind ausweislich der in § 17 VwVG normierten besonderen Ausnahme sowie der ergangenen Rechtsprechung auch gegenüber öffentlichen Stellen verfassungsrechtlich zulässig (vgl. BGH Beschluss vom 18.03.1992 – 1 BGs 90/92; 2 BJs 186/91-5 zitiert nach NJW 1992, 1973 zur Beschlagnahme von Akten beim Amt für Verfassungsschutz). Entsprechende Regelungen für andere Aufsichtsbehörden gibt es bereits (vgl. § 17 Absatz 1 Satz 3 FinDaG, § 76 WVG, § 22 Absatz 3 Satz 4 ArbSchG). Eine Ausnahme zur Vollstreckbarkeit von behördlichen Abhilfebefugnissen gegenüber öffentlichen Stellen ist für die Datenschutzaufsichtsbehörden auch sachgerecht und notwendig, da diese aus der Verwaltungshierarchie ausgegliedert sind und die Umsetzung von Anweisungen oder Untersagungen bei einem Ignorieren der Maßnahmen oder bei gegenteiliger Meinung der Rechts- und Fachaufsicht daher nicht sichergestellt ist. Daher sollte in § 16 BDSG eine z. B. an § 17 Absatz 1 Satz 3 FinDaG orientierte Regelung vorgesehen werden, dass der BfDI seine Maßnahmen mit Zwangsmitteln durchsetzen kann und dies auch gegenüber öffentlichen Stellen gilt. Eine solche Regelung im BDSG könnte den Anlass geben, dass entsprechende Regelungen auch in den Landesdatenschutzgesetzen aufgenommen werden.

b) Ein weiteres rechtliches Defizit liegt in § 20 Absatz 7 BDSG begründet, wonach die Aufsichtsbehörde gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nr. 4 VwGO anordnen darf. Damit wird ein unmittelbar wirksamer Datenschutz durch die angeordnete Maßnahme verhindert. Eine rechtswidrige Datenverarbeitung oder ein sonstiger Verstoß gegen datenschutzrechtliche Bestimmungen könnte bis zu einer endgültigen gerichtlichen Entscheidung, die aufgrund der Belastung der Gerichte und/oder der Vielschichtigkeit der Fälle teilweise erst Jahre nach der Entscheidung der Aufsichtsbehörde erfolgt, nicht zwangsweise abgestellt werden. Gleichzeitig verstößt § 20 Absatz 7 BDSG gegen die Vorgaben der DSGVO: Die Aufsichtsbehörde muss gemäß Artikel 58 Absatz 2 DSGVO über umfassende Abhilfebefugnisse verfügen. Insoweit hat zwischen ihr und der betroffenen Behörde ein Subordinationsverhältnis zu bestehen, ohne dass nach Beginn des Vollzugs der getroffenen Verwaltungsentscheidung differenziert wird. Die derzeitige Regelung in § 20 Absatz 7 BDSG ist zudem auch zum Schutz der betroffenen Behörde nicht erforderlich, weil diese in ihrem Handeln ihrerseits durch § 80 Absatz 5 VwGO geschützt ist, wonach sie jederzeit die Möglichkeit hat, gerichtlich eine Anordnung der sofortigen Vollziehung überprüfen zu lassen. Die verbindliche Entscheidung trifft demnach auch in einem solchen Fall allein das Verwaltungsgericht.

c) In Anlehnung an das Gesetz gegen Wettbewerbsbeschränkungen (GWB) sollten die Datenschutzbehörden im BDSG auf Grundlage von Artikel 58 Absatz 6 Satz 1 DSGVO mit einem Beschlagnahmerecht bereits im verwaltungsrechtlichen Aufsichts- und Kontrollverfahren ausgestattet werden, um ebenso wie die Kartellbehörden Beweismittel bereits während der Kontrolle sicherstellen zu können (vgl. §§ 57, 58 GWB).

d) Des Weiteren wäre es wünschenswert, wenn die Aufsichtsbehörden im BDSG eine eigene Klagebefugnis erhalten würden, um Rechtsnormen gerichtlich überprüfen lassen zu können, die sie für europarechtswidrig oder – außerhalb des Anwendungsbereichs der DSGVO und der JI-Richtlinie – für verfassungswidrig erachten. Im Hinblick auf die Rechtssicherheit erscheint es problematisch, wenn Aufsichtsbehörden gesetzliche Normen für europarechtswidrig und aufgrund des Anwendungsvorrangs des europäischen Sekundärrechts für unanwendbar halten, ein Verantwortlicher diese aber anwendet. Es erscheint problematisch, wenn ein

Verantwortlicher in einem solchen Fall erst eine Untersagung oder gegebenenfalls sogar ein Bußgeld riskieren müsste, obwohl er sich am Wortlaut des nationalen Gesetzes orientiert hat. Daher wäre es unter rechtsstaatlichen Gesichtspunkten sinnvoll, zu prüfen, ob den Aufsichtsbehörden ein Verfahren zur Verfügung gestellt werden könnte, um ihrerseits eine gerichtliche Entscheidung herbeiführen zu können, bei welcher die fragliche Norm inzident überprüft werden kann. Dasselbe gilt für die Frage der Vereinbarkeit nationaler Normen außerhalb des Europarechts, z.B. im Bereich der Nachrichtendienste, da hier der Rechtsschutz des Betroffenen ohnehin sehr eingeschränkt ist und die Datenschutzaufsichtsbehörde Datenschutzverstöße aufgrund verfassungswidriger Normen nicht abstellen kann. Vergleichbar ist beispielsweise in § 19 Absatz 5 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) die Regelung enthalten, dass die oder der Hessische Datenschutzbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit einer von ihr oder ihm getroffenen verbindlichen Entscheidung beantragen kann, wenn eine Behörde oder öffentliche Stelle die verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht.

e) Ferner fehlt im BDSG eine ausdrückliche Bestimmung, wonach die Aufsichtsbehörden berechtigt sind, Entscheidungen über Abhilfemaßnahmen und Sanktionen, die wegen Datenschutzverstößen getroffen wurden, zu veröffentlichen. Auf der Grundlage der Grundsätze des BVerfG zum Informationshandeln staatlicher Stellen sowie gestützt auf Artikel 58 Absatz 3 lit. b DSGVO können zwar nach Abwägung im Einzelfall grundsätzlich bereits nach der lex lata Bußgeldentscheidungen veröffentlicht werden. Gleichwohl könnte eine gesetzliche Grundlage mehr Rechtssicherheit für die Aufsichtsbehörden bieten und dazu führen, dass von dieser Möglichkeit vermehrt Gebrauch gemacht wird. Veröffentlichungen über getroffene Bußgeldentscheidungen tragen besonders zur Sensibilisierung und Aufklärung der Öffentlichkeit sowie zur Abschreckung bei. Darüber hinaus sollten aber auch Entscheidungen über andere Abhilfemaßnahmen (z. B. Untersagung einer bestimmten Datenverarbeitung) veröffentlicht werden können. In Bezug auf Datenschutzverstöße internationaler Unternehmen, die über keine Niederlassung in der EU / im EWR verfügen, könnte die Veröffentlichung von Entscheidungen der Aufsichtsbehörden zudem eine Alternative zur fehlenden Vollstreckbarkeit im Drittland sein, um auf festgestellte Verstöße innerhalb der Union reagieren zu können. Eine gesetzliche Regelung im BDSG könnte sich beispielsweise an § 53 Absatz 5 GWB oder § 124 WpHG orientieren.

f) Zudem sollte durch den Gesetzgeber die Einführung einer Befugnis für die Aufsichtsbehörden zur Anordnung des Abbaus von Videoüberwachungsanlagen geprüft werden. Eine entsprechende Befugnis könnte eine sinnvolle Ergänzung zu Untersagungsverfügungen wegen des Betriebs unzulässiger Kameras darstellen. In der Rechtsprechung wird es nicht einheitlich beurteilt[2], ob die Anordnung zur Demontage von Verarbeitungsanlagen von der derzeitigen Kompetenz der Aufsichtsbehörden umfasst ist. Insofern kann im Bereich Videoüberwachung ein gewisses Durchsetzungsdefizit bestehen, wenn eine Kamera nur abgeschaltet wurde, aber funktionstüchtig bleibt und jederzeit wieder einsetzbar ist. Außerdem könnte möglicherweise auch eine abgeschaltete Kamera einen Überwachungsdruck bei Betroffenen auslösen, wenn nicht von außen erkennbar ist, ob die Kamera weiterhin deaktiviert ist.

[2] Bejahend VG Weimar, Urt. v. 04.11.2015 – I K 1269/14We; ablehnend VG Oldenburg, Urt. v. 12.03.2013 – 1 A 3850/12 (beides zitiert nach Nguyen, in: Gola, DSGVO, Artikel 58 Rn. 20). Aktuell ablehnend VG Mainz, Urt. v. 24.09.2020 – 1 K 584/19.MZ.

g) Auch bleibt der BfDI nach § 16 Absatz 2 und 3 BDSG im Bereich der JI-RL sowie außerhalb des Geltungsbereichs des EU-Rechts auf das Instrument der Warnung und der Beanstandung beschränkt. Dieses Problem betrifft § 16 Absatz 2 und 3 BDSG auch insoweit, als er über § 27 Nr. 1 BVerfSchG, § 13 Nr. 1 MADG und § 32a S. 1 Nr. 1 a) BNDG Anwendung auf den nachrichtendienstlichen Bereich findet. Artikel 47 Absatz 2 JI-RL enthält hingegen die Verpflichtung wirksame Abhilfebefugnisse zu gewähren und Artikel 47 Absatz 5 JI-RL die Verpflichtung, Möglichkeiten einer gerichtlichen Klärung zu regeln. Beides enthält die Regelung im BDSG nicht. Das Instrument der Beanstandung ist nicht verbindlich und letztlich nicht durchsetzbar. Vertritt der Verantwortliche bzw. dessen Aufsichtsbehörde eine andere Rechtsauffassung als die Datenschutzaufsicht, besteht keine Möglichkeit der Durchsetzung oder Einleitung einer gerichtlichen Klärung der Frage, ob die betreffende Verarbeitung rechtswidrig ist. Die Unzulänglichkeit der Regelungen des § 16 Absatz 2 und 3 BDSG zeigt sich insbesondere auch in dem Fall, in dem der Datenschutzverstoß durch eine oberste Bundesbehörde begangen wird, diese also selbst Adressat der Beanstandung mit der Bitte um Stellungnahme ist. Hier entfällt der vom Gesetz vorgesehene Devolutiveffekt, durch den die Beseitigung der datenschutzwidrigen Tätigkeit einer Verwaltungsbehörde erhofft werden kann. Fehlt die Möglichkeit, eine andere, nächsthöhere Instanz als die kontrollierte Stelle mit der Beanstandung zu adressieren, steht zu erwarten, dass dem kritisierten datenschutzwidrigem Verhalten nicht abgeholfen wird. Das Mittel der Beanstandung ist insbesondere in dieser Konstellation wirkungslos. Der BfDI kann mit diesen Mitteln keine wirksame Abhilfe herbeiführen. Um den Befugnissen Wirksamkeit zu verleihen, bedarf es – wie im Anwendungsbereich DSGVO– der Möglichkeit, verbindliche Anordnungen zu treffen. Ohne ergänzende fachgesetzliche Regelung sind die Vorgaben der JI-RL unzureichend umgesetzt. Auch im nachrichtendienstlichen Bereich führt dies zu einer nicht ausreichenden Wirksamkeit der aufsichtlichen Tätigkeit.
   Die nach wie vor nicht abgeschlossene Umsetzung im Fachrecht zeigt deutlich, dass die wirksamen Abhilfebefugnisse für den JI-Bereich einheitlich im BDSG geregelt werden sollten. Der BfDI fordert auch für den nachrichtendienstlichen Bereich aus den genannten Gründen schon seit längerer Zeit Abhilfe- und Sanktionsbefugnisse vergleichbar denen der DSGVO bzw. der JI-RL (vgl. 27.TB Nr. 1.2.1). Würde die kontrollierte Stelle dagegen gerichtlich vorgehen, könnte der Streit rechtssicher für alle Beteiligten geklärt werden.

h) Schließlich ist eine Klarstellung der nach Artikel 47 Absatz 1 JI-RL erforderlichen Untersuchungsbefugnisse des BfDI wünschenswert. Im Gegensatz zu Artikel 58 DSGVO, der Untersuchungs- und Anordnungsbefugnisse klar voneinander trennt und ausdifferenziert regelt, ist § 16 BDSG systematisch unglücklich aufgebaut. Eine ausdrückliche Regelung der Untersuchungsbefugnisse fehlt. § 16 BDSG beschränkt sich auf die Verpflichtungen der Verantwortlichen, dem BfDI und seinen Beauftragten Zugang zu Gebäuden, Anlagen und Daten zu gewähren und alle Informationen bereitzustellen. Es verwundert, dass dieser Verpflichtung keine ausdrückliche Befugnis des BfDI gegenübersteht, Zugang oder Auskünfte zu verlangen. In systematischer Hinsicht ist nicht nachvollziehbar, warum in § 16 BDSG für den Bereich der JI-RL zunächst die Abhilfebefugnisse und erst danach die Untersuchungen des BfDI geregelt werden. Zur Klarstellung sollten daher ausdrückliche Untersuchungsbefugnisse nach dem Vorbild des Artikel 58 Absatz 1 DSGVO geregelt werden und diese den Abhilfebefugnissen und den Mitwirkungspflichten der Verantwortlichen vorangestellt werden.

5. Gibt es aus Ihrer Sicht neben den in den Fragen 1 bis 3 angesprochenen Aspekten Änderungsbedarf bei der Regelung der Datenschutzaufsicht im BDSG und wenn ja, worin besteht er?

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben sich in der DSK zusammengeschlossen. Die DSK besteht aus der oder dem BfDI, den Landesbeauftragten für den Datenschutz und der Präsidentin oder dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht. Die DSK hat das Ziel, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Die DSK fördert den Datenschutz und verständigt sich auf gemeinsame Positionen der Datenschutzaufsichtsbehörden des Bundes und der Länder. Allerdings ist dieser Zusammenschluss als DSK bislang lediglich informell. Zwar sind mittlerweile in der Geschäftsordnung der DSK Mehrheitsentscheidungen vorgesehen, dennoch besteht in der DSK keine Möglichkeit, rechtlich verbindliche Beschlüsse zu fassen. Diese Situation ist angesichts der Anforderungen der DSGVO nicht mehr zeitgemäß. Der Bundesgesetzgeber sollte deshalb die Evaluierung des BDSG zum Anlass nehmen, eine Institutionalisierung der DSK voranzutreiben. Soweit dies durch den Bundesgesetzgeber nicht möglich ist, könnte darüber nachgedacht werden, auf der Grundlage eines Staatsvertrages ein entsprechendes Vorhaben umzusetzen, wofür es in anderen Rechtsbereichen bereits mögliche Vorbilder gibt (z. B. Glücksspielkollegium nach § 9a Absatz 5 bis 8 GlüStV, Kommission für Zulassung und Aufsicht sowie Kommission für Jugendmedienschutz nach § 104 Absatz 2 MStV). Zugleich müssten in diesem Zusammenhang Regelungen für die Zusammenarbeit der Aufsichtsbehörden geschaffen werden, die denen vergleichbar sind, die die DSGVO für die europäischen Datenschutzaufsichtsbehörden im Kapitel VII getroffen hat. Die aktuellen Regelungen der §§ 40 Absatz 2, 18 Absatz 2 BDSG sind hierfür nicht ausreichend, weil aus ihnen insbesondere eine Verpflichtung zur Zusammenarbeit auf nationaler Ebene nicht abgeleitet werden kann. Des Weiteren sollte das Gesetz die Einrichtung einer permanenten Geschäftsstelle der DSK vorsehen.

V. Betroffenenrechte

Zusammenfassung:
Die Regelungen sind in wesentlichen Punkten nicht sachgerecht.

Mit den Regelungen in den §§ 32 bis 37 wird das BDSG den europarechtlichen Vorgaben nicht gerecht und stellt bestehende datenschutzrechtliche Standards in Frage. Die Rechte der betroffenen Personen (Information, Auskunft, Löschung, Widerspruch, automatisierte Einzelentscheidung/Profiling) werden in unzulässigem Maße eingeschränkt. Diese Einschnitte in die Betroffenenrechte stellen im Wesentlichen lediglich eine Arbeitserleichterung für die Daten verarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Daten der DSGVO diametral entgegen. Die DSGVO gestattet dem nationalen Gesetzgeber nur in sehr engem Rahmen weitere Einschränkungen der Betroffenenrechte vorzusehen. Entsprechend der Intention der DSGVO haben die Verantwortlichen vielmehr primär durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Der nationale Gesetzgeber sollte auf eine weiter gehende Beschneidung der Betroffenenrechte verzichten. Wo er aus besonders wichtigen Gründen, die in Artikel 23 DSGVO aufgelistet sind, dennoch Beschränkungen vornimmt, muss er sich strikt in den Grenzen der Tatbestände des Art 23 Absatz 1 lit. a-j DSGVO halten und die Erforderlichkeit und Verhältnismäßigkeit der Beschränkung im Hinblick auf diese erlaubten Zwecke genau prüfen (so auch insbes. Absatz 42 der am 15. 12. 2020 vom EDSA beschlossenen Leitlinien „Guidelines 10/2020 on restrictions under Article 23 GDPR“, die sich derzeit in der öffentlichen Konsultation befinden). Außerdem soll der Gesetzgeber die Verbindung zwischen der Beschränkung und dem verfolgten Zweck im Gesetz oder einem begleitenden Dokument klar herausarbeiten (ebda, Absätze 19 und 21). Wie unten gezeigt wird, werden die §§ 32 bis 37 BDSG diesen Anforderungen, auch unter Heranziehung der Gesetzesbegründung, an mehreren Stellen nicht gerecht und bedürfen daher der Überarbeitung.

Auch die Regelungen in §§ 56-58 BDSG sind überarbeitungsbedürftig. In § 56 Absatz 3 und § 57 Absatz 4 BDSG sollten Voraussetzungen geregelt werden, nach denen die dort genannten Behörden ihre Zustimmung zur Benachrichtigung oder Auskunftserteilung an betroffene Personen versagen dürfen. Die in § 57 Absatz 2 und 7 BDSG sowie die in § 58 Absatz 1 Satz 5 und Absatz 3 BDSG getroffenen Regelungen sind nicht mit den Vorgaben der JI-RL vereinbar und entsprechend anzupassen. § 57 Absatz 3 BDSG sollte aufgrund von Anwendungsschwierigkeiten in eine Ermessensnorm umgewandelt werden.

1. Sind die Regelungen zu den Betroffenenrechten in den §§ 32 bis 37 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

a) Zu § 32 BDSG

(1) Zu § 32 Absatz 1 BDSG

Artikel 23 Absatz 1 DSGVO kennt eine mit dem Ursprungszweck zu vereinbarende Weiterverarbeitung analoger Daten nicht als Ausnahmegrund. Da sich die Regelung auf Verarbeitungen bezieht, bei denen „sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet“, ist schon deshalb nicht ersichtlich, warum in solchen Fällen keine angemessene Information erfolgen soll. Zudem ist die Regelung in hohem Maße unbestimmt. Unklar bleibt insbesondere, wann „das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalles, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist“.

Es wird daher vorgeschlagen, Artikel 32 Absatz 1 Nr. 1 BDSG zu streichen.

Die Ordnungsmäßigkeit der Aufgabenerfüllung kann schon bei zeitlichen Verzögerungen tangiert sein kann. In § 23 Absatz 1 Nr. 2 BDSG fehlt jedoch die notwendige Klarstellung, dass die bloße zeitliche Verzögerung der Aufgabenerfüllung den Ausschluss der grundrechtlich gebotenen Informationsverpflichtung nur in begründeten Ausnahmefällen zu rechtfertigen vermag.

Daher sollte zur Klarstellung in § 23 Absatz 1 Nr. 2 BDSG nach dem Wort „überwiegen" das Komma gestrichen, durch einen Punkt ersetzt und die Worte „Zeitliche Verzögerungen stellen nur in begründeten Ausnahmefällen Gefährdungen der ordnungsgemäßen Erfüllung im Sinne dieser Vorschrift dar." eingefügt werden.

Die Formulierung des § 33 Absatz 2 Nummer 6 BDSG, die von der Bundesregierung noch in der Version der 2. Ressortabstimmung (11.11.2016) für § 31 Absatz 1 Nummer 2 lit. b BDSG vorgeschlagen worden war, wurde in der Kabinettsfassung bedauerlicher Weise gestrichen. Sie gewährleistet im Vergleich zur jetzigen Fassung des § 32 Absatz 1 Nr. 3 BDSG jedoch, dass die zuständige öffentliche Stelle beurteilt, ob eine Gefährdung der öffentlichen Sicherheit vorliegt und diese Beurteilung nicht der verantwortlichen, gegebenenfalls also auch nicht-öffentlichen Stelle zugemutet wird. Zudem wird in der aktuellen Fassung nicht dem Umstand Rechnung getragen, dass die DSGVO im Gegensatz etwa zu Artikel 36 AEUV bewusst nicht die öffentliche Ordnung als Ausnahmetatbestand nennt.

Folglich sollten in § 32 Absatz 1 Nr. 3 BDSG die Worte „die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten" vorangestellt und die Worte „oder Ordnung" gestrichen werden.

Vom Wortlaut des § 32 Absatz 1 Nr. 4 BDSG wird die Einschränkung der Informationspflicht zur Durchsetzung aller „rechtlichen" Ansprüche ermöglicht. Artikel 23 Absatz 1 lit. j DSGVO bestimmt jedoch, dass das Recht auf Information nach Artikel 13 DSGVO durch nationalstaatliches Recht allenfalls dann eingeschränkt werden darf, wenn bestimmte Voraussetzungen erfüllt sind und zusätzlich die gesetzliche Regelung der Durchsetzung „zivilrechtlicher" Ansprüche dient. Die DSGVO ermöglicht daher nicht die Einschränkung der Informationspflicht zur Durchsetzung aller „rechtlichen" Ansprüche.

Zudem könnte nach der aktuellen Fassung eine bloße Beeinträchtigung der Durchsetzung von Ansprüchen etwa schon in Fällen gesehen werden, in denen die Anspruchsdurchsetzung sich nur minimal verzögern würde. Dies würde der geforderten strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung in Bezug auf die Einschränkung nicht gerecht. Danach muss die auf Artikel 23 Absatz 1 lit. j DSGVO gestützte Einschränkung erforderlich sein, um die Durchsetzung des zivilrechtlichen Anspruchs zu gewährleisten.

In § 32 Absatz 1 Nr. 4 BDSG sollte mithin das Wort „rechtlicher" durch das Wort „zivilrechtlicher" und vor das Wort „beeinträchtigen" ein „erheblich" hinzugefügt werden.

Nach dem Wortlaut des § 32 Absatz 1 Nr. 5 BDSG gibt es ein allgemein vorrangiges Interesse an einer gegenüber der betroffenen Person geheim zu haltenden, sie betreffenden Kommunikation mit Behörden. Dies ist mit der DSGVO jedoch nicht vereinbar. Danach muss eine entsprechende Ausnahme von der in Artikel 13 DSGVO statuierten Informationspflicht auf die in Artikel 23 Absatz 1 DSGVO genannten Ziele begrenzt werden. Zudem muss eine Beschränkung dieser Ausnahme für den Fall vorgesehen werden, dass der Verantwortliche wissentlich falsche Anschuldigungen gegen die betroffene Person erhebt (vgl. Artikel 23 Absatz 2 lit. c und g DSGVO).

Es wird daher vorgeschlagen, den Punkt in § 32 Absatz 1 Nr. 5 BDSG durch ein Komma zu ersetzen und die Worte „die dem Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679

genannten Ziele dient, soweit dadurch keine schutzwürdigen Interessen der betroffenen Person beeinträchtigt werden.“ anzufügen.

(2) Zu § 32 Absatz 2 BDSG

Artikel 23 Absatz 1 DSGVO macht es zur Voraussetzung nationaler Artikel 13 einschränkender Rechtsvorschriften, dass die Beschränkung den Wesensgehalt der Grundrechte achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Verantwortliche Stellen in den Fällen der Nummern 3 und 4 des Absatzes 1 pauschal von der Verpflichtung zum Ergreifen der Maßnahmen nach Absatz 2 zu entbinden, wie es von § 32 Absatz 2 Satz 3 BDSG geregelt wird, verstößt gegen diese Prinzipien. Eine ersatzweise Bereitstellung der Informationen nach Artikel 13 Absatz 1 und 2 für die Öffentlichkeit, wie sie § 32 Absatz 2 Satz 1 vorsieht, könnte nur in allgemeiner, nicht personenbezogener Form erfolgen. Es ist nicht nachvollziehbar, weshalb dies einschließlich der Begründungspflicht nach § 32 Absatz 2 Satz 2 in den genannten Fällen nicht angewendet werden soll.

Mithin sollte § 32 Absatz 2 Satz 3 ersatzlos gestrichen werden.

b) Zu § 33 BDSG

Die Ordnungsmäßigkeit der Aufgabenerfüllung kann schon bei zeitlichen Verzögerungen tangiert sein kann. In § 33 Absatz 1 Nr. 1 lit. a BDSG fehlt jedoch die notwendige Klarstellung, dass die bloße zeitliche Verzögerung der Aufgabenerfüllung den Ausschuss der grundrechtlich gebotenen Informationsverpflichtung nur in begründeten Ausnahmefällen zu rechtfertigen vermag.

Daher wird vorgeschlagen, bei § 33 Absatz 1 Nr. 1 lit. a BDSG nach dem Wort „würde“ einen Punkt einzufügen und die Worte „Zeitliche Verzögerungen stellen nur in begründeten Ausnahmefällen Gefährdungen der ordnungsgemäßen Erfüllung im Sinne dieser Vorschrift dar.“ anzufügen.

Aus den zu § 32 Absatz 1 Nr. 3 BDSG genannten Gründen (s.o.) sollten ferner in § 33 Absatz 1 Nr. 1 lit. b BDSG die Worte „die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten“ vorangestellt und die Worte „oder Ordnung“ gestrichen werden.

§ 33 Absatz 1 Nr. 2 lit. a BDSG verlangt lediglich eine Beeinträchtigung der Durchsetzung von Ansprüchen. Eine Beeinträchtigung der Durchsetzung von Ansprüchen könnte jedoch schon in Fällen gesehen werden, in denen die Anspruchsdurchsetzung sich nur minimal verzögern würde, siehe auch oben bei § 32 Absatz 1 Nr. 4 BDSG.

Daher wird angeregt, in § 33 Absatz 1 Nr. 2 lit. a BDSG vor das Wort „beeinträchtigen“ das Wort „erheblich“ hinzuzufügen.

Die DSGVO nennt im Gegensatz etwa zu Artikel 36 AEUV bewusst nicht die öffentliche Ordnung als Ausnahmetatbestand. Gleichwohl ist ein solcher in § 33 Absatz 1 Nr. 2 lit. b BDSG geregelt.

In § 33 Absatz 1 Nr. 2 lit. b BDSG sollten daher die Worte „oder Ordnung“ gestrichen werden.

c) Zu § 34 BDSG

Die Regelung des § 34 Absatz 1 Nr. 2 BDSG kann für Fälle von Speicherungen aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften und zum Zwecke der Datensicherung und Datenschutzkontrolle nicht mit der Gefährdung eines oder mehrerer der

in Art 23 Absatz 1 DSGVO genannten abschließenden Schutzziele begründet werden. So hat auch der Gesetzgeber an dieser Stelle, anders als für andere Ausnahmeregelungen, keine der in Artikel 23 Absatz 1 lit. a-j DSGVO gelisteten Ausnahmemöglichkeiten benannt. Auch aus der Begründung zu Artikel 33 DSGVO, auf die verwiesen wird, geht keine Ausnahmemöglichkeit für § 34 Absatz 1 Nr. 2 BDSG hervor. Der europäische Gesetzgeber hat die Abwägung des Interesses an der Ausübung der Betroffenenrechte mit dem damit verbundenen Aufwand für den Verantwortlichen bereits in seine Entscheidung einfließen lassen (vgl. Artikel 12 Absatz 5, 14 Absatz 5 lit. b DSGVO).

Auch zeigen die Erfahrungen der Aufsichtsbehörden, dass Unternehmen in vielen Fällen ihrer Pflicht zur Sicherung der Zweckbindung bzw. Einschränkung der Verarbeitung nicht nachkommen, was nicht selten zu einer zweckwidrigen Weiterverwendung führt, die dann von den Betroffenen nicht angegriffen werden kann, wenn ihnen nicht auf Antrag mitgeteilt werden muss, dass ihre personenbezogenen Daten weiter gespeichert sind. Auch könnte jedes Auskunftsersuchen gegenüber Telekommunikationsunternehmen zur Rechtmäßigkeit der Speicherung von Verkehrsdaten nach den Vorschriften zur Vorratsdatenspeicherung pauschal zurückgewiesen werden.

Es wird daher vorgeschlagen, § 34 Absatz 1 Nr. 2 BDSG zu streichen.

d) Zu § 35 BDSG

(1) Zu § 35 Absatz 1 BDSG

Die in § 35 Absatz 1 BDSG erlaubte Beschränkung des Löschungsanspruchs ist nicht durch Artikel 23 Absatz 1 DSGVO gedeckt, da dort kein Ausnahmetatbestand der Vermeidung eines unverhältnismäßig hohen Aufwandes normiert ist, sondern in diesem Zusammenhang nur die in Artikel 23 Absatz 1 lit. i und j DSGVO genannten Tatbestände Einschränkungen der Betroffenenrechte rechtfertigen können. Auch bestünde bei der Entbindung von der Löschpflicht aufgrund der besonderen Art der Speicherung die Gefahr, dass das Recht auf Löschung dadurch umgangen würde, dass entsprechende Speicherungsarten gewählt würden, um die Löschungsverpflichtung zu verhindern.

Folglich sollte § 35 Absatz 1 BDSG gestrichen werden.

(2) Zu § 35 Absatz 2 BDSG

Nur die betroffene Person weiß, ob die Vermutung des Verantwortlichen, eine Löschung würde ihre schutzwürdigen Belange beeinträchtigen, tatsächlich zutreffend ist. Daher muss sie davon erfahren, dass der Verantwortliche diese Vermutung hegt. Die in § 35 Absatz 2 BDSG geregelten Beschränkungen können vor der DSGVO keinen Bestand haben. Artikel 17 Absatz 3 lit. e DSGVO enthält bereits Beschränkungen der Löschungsverpflichtung, soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Soweit die im BDSG enthaltenen Beschränkungen hierüber hinausgehen, sind sie nicht durch den Schutz eines Zieles des Artikels 23 Absatz 1 DSGVO gerechtfertigt. So hat auch der Gesetzgeber an dieser Stelle, anders als für andere Ausnahmeregelungen, keine der in Artikel 23 Absatz 1 lit. a-j DSGVO gelisteten Ausnahmemöglichkeiten benannt.

Für § 35 Absatz 2 BDSG wird daher folgende Formulierung vorgeschlagen:
„Der Verantwortliche unterrichtet die betroffene Person, sofern die Löschung deshalb unterbleibt, weil der Verantwortliche Grund zu der Annahme hat, dass anderenfalls schutzwürdige Interessen der betroffenen Person beeinträchtigt würden."

(3) Zu § 35 Absatz 3 BDSG

Auch die in § 35 Absatz 3 BDSG geregelten Beschränkungen können vor der DSGVO keinen Bestand haben. Artikel 17 Absatz 3 lit. b DSGVO enthält bereits Beschränkungen der Löschungsverpflichtung, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Soweit die Beschränkungen hierüber hinausgehen, sind sie nicht durch den Schutz eines Zieles des Artikels 23 Absatz 1 DSGVO gerechtfertigt. Auch hierfür hat der Gesetzgeber, anders als für andere Ausnahmeregelungen, keine der in Artikel 23 Absatz 1 lit. a-j DSGVO gelisteten Ausnahmemöglichkeiten benannt.

Folglich sollte § 35 Absatz 3 BDSG gestrichen werden.

e) Zu § 36 BDSG

§ 36 BDSG erweitert den Ausschluss des Widerspruchsrechts über Artikel 21 Absatz 1 der DSGVO hinaus in einem Maße, das durch Artikel 23 Absatz 1 DSGVO nicht gerechtfertigt ist. Nach Artikel 21 Absatz 1 Satz 2 DSGVO ist es dem Verantwortlichen möglich, die personenbezogenen Daten trotz Widerspruchs zu verarbeiten, wenn er zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. In diesen Fällen nicht nur die durch den Widerspruch angegriffene Verarbeitung ausnahmsweise zu erlauben, sondern das Recht auf Widerspruch sogar ganz auszuschließen, kann nicht als dem Wesensgehalt des Grundrechts achtende und in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikel 23 DSGVO angesehen werden.

Es wird daher vorgeschlagen, § 36 BDSG zu streichen.

2. Sind die Regelungen zu den Betroffenenrechten in den §§ 55 bis 61 BDSG aus Ihrer Sicht normenklar? Sind sie aus Ihrer Sicht sachgerecht und praktikabel, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen?

a) Zu § 56 und § 57 BDSG

In § 56 Absatz 3 und § 57 Absatz 4 BDSG sollten Voraussetzungen geregelt werden, nach denen die dort genannten Behörden ihre Zustimmung zur Benachrichtigung oder Auskunftserteilung an betroffene Personen versagen dürfen. Dass die Benachrichtigung oder Auskunft nur mit Zustimmung dieser Stellen zulässig ist, impliziert, dass die Behörden ihre Zustimmung auch verweigern können. Hierfür gibt es keine gesetzlichen Voraussetzungen. Somit fehlt nicht nur für die beteiligten Behörden ein Entscheidungsmaßstab. Auch die aufsichtliche Kontrolle läuft insoweit ins Leere, weil es keinen Prüfmaßstab gibt, um in Fällen, in denen die Zustimmung nicht erteilt wurde, die Rechtmäßigkeit des Absehens von der Benachrichtigung oder Auskunft zu prüfen.

Die Regelungen des § 57 BDSG entsprechen nicht in allen Punkten den Vorgaben der JI-RL.
Artikel 15 Absatz 3 Satz 1 JI-RL sieht die Unterrichtung über das Absehen oder die Einschränkung der Auskunft vor. Satz 2 sieht Ausnahmen hiervon vor. Nach Satz 3 sind die Mitgliedstaaten verpflichtet zu regeln, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. Diese Vorschrift ist noch nicht umgesetzt. Insbesondere § 57 Absatz 7 Satz 2 BDSG widerspricht Artikel 15 Absatz 3 Satz 3 JI-RL. Der Verantwortliche hat stets (ggfs. mit der Eingangs- oder Zwischennachricht) über die Beschwerdemöglichkeit oder den gerichtlichen Rechtsbehelf zu unterrichten, nicht nur im Falle der Unterrichtung nach § 57 Absatz 7 S. 1 BDSG.

Die fehlende Umsetzung führte auch bei den verantwortlichen Stellen zu erhöhtem Beratungsbedarf.

§ 57 Absatz 2 BDSG ist nicht mit den Vorgaben der JI-RL vereinbar. Nach § 57 Absatz 2 BDSG besteht kein Auskunftsrecht, wenn Daten nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungspflichten nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und durch geeignete technische und organisatorische Maßnahmen (TOM) sichergestellt ist, dass eine Verarbeitung zu anderen Zwecken ausgeschlossen ist. Als Leitgedanke dieser Ausnahmen erscheint das geringere Gefährdungspotential der betreffenden Datenverarbeitungen für betroffene Personen. Allerdings ist dieser Ausnahmetatbestand nicht mit Artikel 15 Absatz 1 JI-RL vereinbar, der die zulässigen Zwecke einer Einschränkung abschließend auflistet. Die Vorschrift sollte gestrichen werden.

Die Regelung des § 57 Absatz 3 BDSG führt zu Anwendungsschwierigkeiten. Danach ist von der Auskunft abzusehen, wenn die betreffende Person keine Angaben macht, die das Auffinden der Daten ermöglichen (unbestimmter Auskunftsantrag) und mangels entsprechender Angaben der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem gelten gemachten Informationsinteresse steht. Diese Einschränkung erscheint von Artikel 15 Absatz 1 JI-RL noch gedeckt (Schutz vor Beeinträchtigung der Aufgabenerfüllung im Sinne der JI-RL), ist aber äußerst restriktiv auszulegen. Sie sollte nur Anwendung finden, wenn die Aufgabenerfüllung nicht mehr im gebotenen Maß möglich ist. Der Wortlaut „ist abzusehen“ ist insoweit allerdings missverständlich und wird in der Praxis von Verantwortlichen teilweise als Konkretisierungspflicht der betroffenen Person aufgefasst. In Fällen etwa, in denen die Verwechslung einer Person zu einer Speicherung geführt hat, ist es der betroffenen Person gar nicht möglich, etwaige Anknüpfungspunkte zu benennen. Kommt der Betroffene dieser Pflicht nicht nach, erteilen die Stellen gar keine Auskunft, nicht einmal eine ggf. mit geringem Aufwand mögliche Teilauskunft. Eine vollständige Beschränkung des Auskunftsanspruches erscheint hier jedoch nicht durchweg erforderlich. Deshalb sollte die Vorschrift in eine Ermessensnorm umgewandelt werden.

Nach § 57 Absatz 4 BDSG bestehen Einschränkungsmöglichkeiten unter den gleichen Voraussetzungen wie bei Benachrichtigungspflichten, d.h. solange bei Auskunftserteilung die Erfüllung von Aufgaben nach § 45 BDSG, die öffentliche Sicherheit oder Rechtsgüter Dritter konkret gefährdet wäre und das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt. Das bedeutet aber nicht, dass zwangsläufig kein Auskunftsanspruch besteht, wenn zuvor die Benachrichtigung unterblieben ist. In der Praxis wird dieser Rückschluss jedoch von einigen Verantwortlichen gezogen. Hier sollte klargestellt werden, dass aufgrund des Auskunftsantrages das Vorliegen der Voraussetzungen zu diesem Zeitpunkt immer erneut geprüft werden muss. Vor einer vollständigen Beschränkung des Auskunftsanspruchs ist zunächst in Betracht zu ziehen, ob das Ziel auch durch mildere Mittel erreicht werden kann. Die Auskunft könnte etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden.

§ 57 Absatz 6 Satz 2 BDSG ermöglicht es den Verantwortlichen, bei einem Absehen von oder der Einschränkung einer Auskunft unter bestimmten Voraussetzungen auch davon abzusehen, den Antragsteller hiervon zu unterrichten.

Absatz 6 Satz 2 ermöglicht theoretisch zwei grundsätzliche Fallgestaltungen: 1. Teilauskunft/Teilunterrichtung bei gleichzeitigem Absehen von weiterer Auskunft/Unterrichtung über das Absehen oder die Einschränkung der Auskunft, und 2. Vollständiges Absehen von Auskunft und Unterrichtung.

In beiden Fallgestaltungen wäre eine Antwort an die betroffene Person, die vorgibt, dass keine (weiteren) personenbezogenen Daten verarbeitet werden – entweder bei 1. durch das Verschweigen des Absehens von weitergehender Auskunft/Unterrichtung oder bei 2. durch die Behauptung, dass überhaupt keine personenbezogenen Daten verarbeitet werden –, einen falschen Eindruck vermitteln bzw. schlichtweg unwahr sein und wäre rechtsstaatlich nicht hinnehmbar.

Im Hinblick auf 1. hat darüber hinaus eine Teilauskunft/Teilunterrichtung bei gleichzeitigem Absehen von weiterer Auskunft/Unterrichtung in Form einer sog. „neither confirm nor deny"-Antwort für die Praxis neben der Möglichkeit einer Verweigerung und Unterrichtung nach Absatz 6 Satz 1 (i.V.m. Satz 3 – auch ohne Begründung) keinen Mehrwert, da beides einen Rückschluss auf die behördliche Intention der Verweigerung zulässt.

Als einzige praxistaugliche Möglichkeit der Anwendung von Absatz 6 Satz 2 könnte daher die (vorübergehende) Untätigkeit des Verantwortlichen auf ein Auskunftsersuchen angesehen werden. Dies ist jedoch nur bei der zweiten Fallgestaltung eines vollständigen Absehens denkbar, so dass letztlich Absatz 6 Satz 2 bei einer Teilauskunft/Teilunterrichtung keine (sinnvolle) Anwendung findet. Eine „neither confirm nor deny"-Antwort anstelle der vollständigen Untätigkeit würde im Übrigen ebenfalls einen Rückschluss auf die behördliche Intention zulassen und hat damit in keiner der Fallgestaltungen einen Mehrwert.

Die betroffene Person sollte zudem – etwa mit der Eingangs- oder Zwischennachricht – auf die Möglichkeit von gerichtlichem Rechtsschutz oder der Anrufung des/der Bundes- oder Landesdatenschutzbeauftragten (Artikel 15 Absatz 3 Satz 3 JI-RL) hingewiesen werden.
Da bei Anwendung von Absatz 6 Satz 2 die Transparenz für die betroffenen Personen (fast) vollständig ausgeschlossen wird, sollte im Wortlaut der Vorschrift zudem deutlich zum Ausdruck gebracht werden, dass diese Möglichkeit nur als ultima ratio in Betracht kommt.
An dieser Stelle zeigt sich besonders deutlich, dass die konkrete Vorgehensweise bei dieser Evaluierung nicht zielführend ist. Es wäre nämlich zuerst Sachverhaltsarbeit zu leisten und darzustellen, wie die Sicherheitsbehörden das Auskunftsverfahren in der Praxis ausgestalten. Zu klären wäre insbesondere:

- Wie viele Auskunftsersuchen gab es, aufgeschlüsselt nach Behörden und Bereichen?
- Wie viele wurden abgelehnt?
- Bei wie vielen wurde von der Beantwortung abgesehen?
- Jeweils: Mit welchen Gründen?
- Wie viele Rechtsbehelfe und mit welchem Ergebnis?
- Wie viele datenschutzrechtliche Kontrollergebnisse?
- War bei einer Verweigerung bzw. dem Absehen von der Auskunft die Begründung ausreichend dokumentiert?
- War die dokumentierte Begründung ausreichend substantiiert?

In § 57 Absatz 7 Satz 3 sollte der 2. Halbsatz BDSG „soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde" gestrichen werden.

Artikel 17 JI-RL schränkt das Auskunftsrecht über die Aufsichtsbehörde nicht ein. Insofern muss diese Einschränkung gestrichen werden, um Artikel 17 JI-RL umzusetzen und das Auskunftsrecht über die Aufsichtsbehörde, hier der BfDI, nicht zu unterlaufen.

Der BfDI wird nach dem Sicherheitsüberprüfungsgesetz sicherheitsüberprüft und hat auch ebenso Personal, welches sicherheitsüberprüft ist, so dass auch den Aspekten der Sicherheit des Bundes oder eines Landes durch die verpflichtende Sicherheitsüberprüfung Rechnung getragen wird.

Die Systematik mit § 57 Absatz 7 Satz 4 BDSG erfordert ebenso die Streichung. § 57 Absatz 7 Satz 4 BDSG geht davon aus, dass dem BfDI immer Auskunft zu gewähren ist: Der BfDI darf diese Auskunft prüfen, aber nicht an die betroffene Person weitergeben, soweit und solange gemäß Artikel 15 JI-RL die Auskunft eingeschränkt oder von der Auskunft abgesehen werden darf.

Ein erheblicher Anteil der Beschwerden im Sinne des § 60 BDSG betrifft die oftmals unverhältnismäßige lange Bearbeitungsdauer von Auskunftsverlangen durch das Bundeskriminalamt. Dies hat regelmäßig zur Folge, dass die Betroffenen keine Kenntnis über mögliche Speicherungen ihrer personenbezogenen Daten durch die Polizeibehörden erhalten. Dadurch wird zugleich eine effektive Geltendmachung weiterer Rechte durch die Betroffenen verhindert. Dem Betroffenen sollte im Verfahren nach § 57 BDSG ein Recht analog § 61 Absatz 2 BDSG gegenüber dem Verantwortlichen eingeräumt werden.

b) Zu § 58 BDSG

In § 58 Absatz 1 Satz 5 BDSG sollte die Einschränkung „wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist“ gestrichen werden. Die Regelung birgt die Gefahr, dass ein Antrag einer betroffenen Person auf Vervollständigung von Daten aus Gründen des Verwaltungsaufwands abgelehnt wird. Der Aufwand ist kein Kriterium nach der JI-Richtlinie, um Betroffenenrechte einzuschränken.

§ 58 Absatz 3 BDSG (wortgleich zu § 37 Absatz 3 Nr. 3 GwG (FIU)) betrifft die Möglichkeit, statt der Löschung die Verarbeitung einzuschränken, wenn sie für den Verantwortlichen einen unverhältnismäßig hohen Aufwand bedeutet. § 58 Absatz 3 Nr. 3 BDSG geht über den Gestaltungsspielraum des Artikels 16 Absatz 3 JI-RL hinaus.

Die Anwendung der Vorschrift ist nicht praktikabel. Gestaltet der Verantwortliche seine Verarbeitung so, dass nur mit unverhältnismäßig hohem Aufwand gelöscht werden kann, gewährleistet er u.a. die Intervenierbarkeit nicht und verarbeitet damit die Daten ohnehin rechtswidrig. Wer rechtswidrig verarbeitet, kann sich aber nicht auf einen Ausnahmetatbestand berufen.

VI. Pflichten der Verantwortlichen und Auftragsverarbeiter

Zusammenfassung:
Bei der Anwendung dieser Vorschriften in der Praxis zeigen sich Unsicherheiten, die auf begrifflichen Abweichungen von der JI-RL beruhen. Hier sollte zur Klarstellung eine sprachliche Anpassung an die JI-RL erfolgen. Das Konzept für die Anforderungen an die Datensicherheit sollte auf die in anderen Bereichen bereits etablierten „Gewährleistungsziele" umgestellt werden. Die Anwendung des Instruments der Datenschutz-Folgenabschätzung führt in der Praxis zu Schwierigkeiten, die durch klarere gesetzliche Regelungen ausgeräumt werden könnten. Die Regelung des § 70 BDSG ist nicht normenklar. Ergänzungs- und Klarstellungsbedarf besteht zudem bei der Protokollierungspflicht des § 76 BDSG.

1. Sind die Regelungen über die Auftragsverarbeitung in § 62 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

keine Anmerkungen

2. Sind die Regelungen über gemeinsam Verantwortliche in § 63 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

keine Anmerkungen

3. Sind die Bestimmungen über die Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten in den §§ 64 bis 66 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hin-ausgehen, sachgerecht und praktikabel?

a) Zu § 64 BDSG

§ 64 Absatz 1 BDSG sollte an die Terminologie der JI-RL und der unmittelbar anwendbaren DSGVO angepasst werden. Daher sollte anstelle des Begriffs „Gefahren" der Begriff „Risiken" (dazu näher bei den Erläuterungen zu § 67 BDSG) und anstelle des Begriffs „Rechtsgüter der betroffenen Personen" der europarechtliche Begriff der „Rechte und Freiheiten natürlicher Personen" verwendet werden. Zudem sollte der Verantwortliche verpflichtet werden, „die geeigneten technischen und organisatorischen Maßnahmen" anstelle der „erforderlichen technischen und organisatorischen Maßnahmen" zu ergreifen.

In § 64 Absatz 1 Satz 2 BDSG sollte der Verantwortliche verpflichtet werden, die einschlägigen Standards, Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik „einzuhalten", anstatt sie nur zu „berücksichtigen". Zudem sollten dort neben den bereits erwähnten „Technischen Richtlinien" und „Empfehlungen" auch die „Standards" des BSI aufgenommen werden.

Im BDSG sollte außerdem eine dem Artikel 32 Absatz 1 lit. d DSGVO entsprechende Regelung eingefügt werden, nach der Verantwortliche ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten haben. § 64 Absatz 3 BDSG sieht nur Maßnahmen der Gewährleistung vor, eine Überprüfung fehlt dort. Zwar ist die Überprüfung und Evaluierung in der JI-Richtlinie nicht zwingend vorgeben, aber eine Vereinheitlichung dieser Anforderungen ist erforderlich.

§ 64 Absatz 2 und 3 BDSG enthält eine Vermischung von „neuen Gewährleistungszielen" und „alten Kontrollmaßnahmen", die von den mittlerweile durch die DSGVO etablierten Standards der Datensicherheit abweichen. Die in Absatz 2 aufgezählten Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit folgen dem Grundgedanken der technikunabhängigen Formulierung von Sicherheitsanforderungen, decken jedoch noch nicht alle erforderlichen Aspekte der Datenverarbeitung ab. Stattdessen sollten insgesamt sieben Gewährleistungsziele normiert werden. Diese sieben Gewährleistungsziele bilden auch die Basis für das Standard-Datenschutzmodell. Sie beschreiben die Schutzrichtung des Datenschutzes und sind sowohl in Artikel 4 der JI-RL und in Artikel 5 der Verordnung als auch in den Datenschutzgesetzen einiger Länder bereits vorgebildet und haben ihre Praxistauglichkeit bewiesen. Sie sind zudem in verschiedenen Dokumenten des IT-Planungsrates verankert (etwa in der Nationalen E-Government-Strategie).

§ 64 Absatz 3 BDSG kann bei einer entsprechenden Änderung des § 64 Absatz 2 Satz 2 BDSG gestrichen werden.

b) Zu § 65 und § 66 BDSG

§ 65 BDSG führt trotz des klaren Wortlautes zu einigen Umsetzungsproblemen in der Praxis. Die Vorschrift regelt eindeutig, dass der Verantwortliche Datenschutzverletzungsmeldungen unverzüglich abzugeben hat. Die verantwortliche Stelle ist also selbst für die Meldung verantwortlich. Die Meldung an eine übergeordnete Dienststelle zur Weitermeldung an die Datenschutzaufsichtsbehörde ist hierfür nicht ausreichend. Dies wurde in der Praxis jedoch beobachtet. Ebenso wenig kann die Meldung in anderer Form delegiert werden z.B. von einer Polizeibehörde an die Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens". Auch solche Überlegungen sind in der Praxis jedoch schon aufgekommen.

Die Meldung an die zuständige Datenschutzaufsichtsbehörde hat außerdem unabhängig von der Anzeige eventueller Ordnungswidrigkeiten zu erfolgen, die im Zusammenhang mit der Datenschutzverletzung z.B. von Behördenmitarbeitern begangen wurden. Da die OWi-Zuständigkeit für den sog. Mitarbeiterexzess bei Bundesbediensteten derzeit nicht klar geregelt ist, können die zuständigen Behörden in der Praxis auseinanderfallen.

In §§ 65 und 66 BDSG sollte ebenfalls der Begriff „Gefahr" durch den Begriff „Risiko" ersetzt werden (siehe Ausführungen zu § 67 BDSG).

4. Sind die Regelungen über die Datenschutz-Instrumente (Datenschutz-Folgenabschätzung, Anhörungsverfahren, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung) in den §§ 67, 69, 70 und 76 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

a) Zu § 67 und § 69 BDSG

§ 67 BDSG (Datenschutz-Folgenabschätzung (DSFA)) setzt Artikel 27 der JI-RL um. Im Gegensatz zur Richtlinie setzt § 67 BDSG dem Wortlaut nach keine Prognose eines hohen Risikos, sondern eine voraussichtliche "erhebliche Gefahr" für die Rechtsgüter betroffener Personen voraus. Bei richtlinienkonformer Auslegung darf im Hinblick auf die Intensität kein Unterschied bestehen. Es droht dennoch die Gefahr, dass der Begriff "erhebliche Gefahr" im polizei- und ordnungsrechtlichen Sinne verstanden wird und diese Missverständnisse dazu führen, dass die rechtlichen Vorgaben des § 67 BDSG nicht eingehalten werden.

Bei der DSFA handelt es sich inhaltlich um kein neues Instrument des Datenschutzes. Vor in Krafttreten des BDSG n.F. waren die Ziele der DSFA in der Vorabkontrolle § 4d Absatz 5 und 6 BDSG a.F. geregelt. Für die damalige Vorabkontrolle war der Datenschutzbeauftragte zuständig. Die Durchführung der DSFA obliegt nunmehr der verantwortlichen Stelle und hebelt daher eine datenschutzrechtliche Schwelle aus. Der Gesetzgeber hat die Voraussetzungen für eine DSFA mit Blick auf die JI-RL erweitert und sich dabei an Artikel 35 DSGVO orientiert; eine Konkretisierung, in welchen Fällen eine DSFA durchzuführen ist, wie es zum Beispiel Artikel 35 Absatz 3 DSGVO vorsieht, enthält § 67 BDSG nicht. Das Erfordernis einer DSFA soll nach der Gesetzesbegründung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen bestehen (BT-Drs. 18/11325, S. 117). Aufgrund der mangelnden Konkretisierung ist die derzeitige Regelung über die Durchführung einer DSFA anfällig für Fehlinterpretationen und weist daher Mängel in der Praktikabilität auf.

Nach derzeitigem Kenntnisstand wird von § 67 BDSG zudem kaum Gebrauch gemacht. Es fehlt insofern auch an einer zwingenden Vorgabe, die bereits bestehenden Verfahren an den Vorgaben des neuen Datenschutzrechts zu messen.

Da von der DSFA kaum Gebrauch gemacht wird, wirkt sich dieser Mangel auch spiegelbildlich auf das Anhörungsverfahren des BfDI nach § 69 BDSG aus.

Es gibt zudem unterschiedliche Auffassungen darüber, ob eine DSFA nach §§ 67, 69 BDSG erstellt werden muss, wenn die Behörde noch eine fachgesetzliche Pflicht zur Erstellung einer Errichtungsanordnung (EAO) trifft. Die Bundespolizei etwa vertritt im Gegensatz zum BfDI die Ansicht, dass im Fall der Erstellung einer EAO eine DSFA nicht mehr erforderlich ist. Der BfDI hat in den Hinweisen zu einem vom BfDI erstellten Muster zur DSFA ausdrücklich darauf hingewiesen, dass die EAO zwar im Zuge der Prüfung der Erforderlichkeit und ggfs. auch der Erstellung einer DSFA herangezogen werden kann, aber in der DSFA keine pauschale Verweisung auf die EAO erfolgen soll.

Für die Auslegung der Regelung und zur Erstellung des Musters und der Hinweise musste auf Hinweise der Art 29 WP zu DSGVO zurückgegriffen werden. Die Regelung ist nicht eindeutig genug, um sicherzustellen, dass die Behörden immer eine DSFA erstellen, wenn dies erforderlich ist. Eine Klarstellung im Gesetzestext wäre hilfreich.

Zudem wurden in einem anderen Fall die Anforderungen der Schwellenwertanalyse verkannt. Es wurde in diesem Zusammenhang u. a. die Auffassung vertreten, dass es sich nicht um „neue Technologien“ im Sinne von § 67 Absatz 1 BDSG handele, wenn diese bereits durch andere Branchen und Behörden genutzt würden.

Gleichzeitig bestand grundsätzlicher Beratungsbedarf bei der Erstellung und Durchführung einer DSFA. Unklar waren den die Vorschrift anwendenden Behörden insbesondere Umfang und Inhalt der Mindestvorgaben nach § 67 Absatz 4 BDSG.

b) Zu § 70 BDSG

§ 70 BDSG ist nicht normenklar. Aufgrund einer Anforderung des BfDI nach § 70 Absatz 4 BDSG bei einem Verantwortlichen wurde deutlich, dass bei der Auslegung der Vorschrift Beratungsbedarf besteht. Insbesondere hinsichtlich des Umfangs der Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten, dem Verhältnis auf daneben zu erstellende Errichtungsanordnungen und hinsichtlich mehrerer in § 70 Absatz 1 BDSG vorgesehener Pflichtangaben bestand Unsicherheit. BfDI hat daher ein Muster- und Hinweisblatt zu § 70 BDSG mit detaillierten Einzelerläuterungen erstellt.

Dem BfDI liegt aus dem Bereich des Bundeskriminalamts und der Bundespolizei bislang kein Verfahrensverzeichnis gemäß § 70 BDSG vor.

c) Zu § 76 BDSG

Die Regelung des § 76 BDSG erscheint erheblich verbesserungsbedürftig.

Der Begriff der Protokollierung in § 76 Absatz 1 BDSG ist nicht legal definiert. Gemeint ist, dass zu allen Datenverarbeitungsvorgängen systemseitig im Hintergrund bestimmte Transaktionsdaten in Form sogenannter Protokolldaten mitgeschrieben werden. Es sollte klargestellt werden, dass es sich hierbei um einen automatisierten Prozess handeln soll.

Inhaltliche Vorgaben enthält § 76 Absatz 2 BDSG entsprechend der Vorgaben der JI-RL lediglich für die Ereignisse der Abfrage (Nr. 3) und Offenlegung (Nr. 4). Diese Protokolle müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und soweit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Zur Sicherstellung einer effizienten Datenschutzkontrolle sollten die gleichen Protokollinhalte auch bei allen anderen Ereignissen verfügbar sein. Die entsprechende Einschränkung sollte gestrichen werden.

Die Einschränkung „soweit wie möglich“ in Bezug auf die Identität der abfragenden oder offenlegenden Person ist beim heutigen Stand der Technik nicht mehr nachvollziehbar. Schließlich dürfte jeder mit einer speziellen Nutzerkennung o.ä. individualisierbar im System angemeldet sein. Die eindeutige Identifizierbarkeit über personalisierte Nutzerkennungen dient nicht nur einer umfassenden datenschutzrechtlichen Kontrollierbarkeit, sondern auch dem Schutz aller korrekten Anwender. Die Einschränkung sollte gestrichen werden. Kernziel der Protokollierung ist die Nachvollziehbarkeit der Datenverarbeitungsvorgänge von der Erhebung bis zur Löschung. Diese Anforderung an die Ausgestaltung sollte im Gesetz ergänzt werden.

Soweit nach der JI-RL bzw. § 76 Absatz 3 BDSG Protokolldaten „für Strafverfahren“ verwendet werden dürfen, ist dies unbedingt restriktiv auszulegen. Danach dürfen die Protokolldaten in Strafverfahren nur verwendet werden, solange das jeweilige Strafverfahren im Zusammenhang mit den Verwendungszwecken Kontrolle der Rechtmäßigkeit der Verarbeitung, Eigenüberwachung oder Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten steht (vgl. Empfehlung der Artikel 29-Gruppe in ihrer Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680) vom 29. November 2017, WP 258). Diese Verwendung ist bereits von der originären Zweckbindung erfasst. Insoweit hat die Vorschrift rein deklaratorischen Charakter. Dies sollte im Gesetzestext klargestellt werden.

§ 76 Absatz 5 entspricht in der vorliegenden Form nicht den Anforderungen der Rechtsprechung des BVerfG. Danach muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzaufsichtsbehörden in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem

zu kontrollierenden Vorgang enthält. Hieraus sind in der Praxis folgende Anforderungen abzuleiten: Die Protokolldaten müssen in einem strukturierten, gängigen, maschinenlesbaren und maschinenauswertbaren Format vorliegen oder in ein entsprechendes Format exportierbar sein. Die verantwortliche Stelle muss die Daten in diesem Format der Datenschutzaufsichtsbehörde vorlegen können. Die Protokolldaten müssen zeitnah zur Verfügung gestellt werden können. Außerdem muss es möglich sein, die Protokolldaten für Zwecke der Datenschutzkontrolle auszuwerten und in ihnen zu recherchieren. Eine entsprechende Vorgabe sollte ergänzt werden. In der Praxis hat sich herausgestellt, dass nicht alle Verantwortlichen Protokolldaten regelmäßig für anlasslose Eigenkontrollen verwenden. Eine entsprechende Vorgabe erschiene sinnvoll.

5. Sind die Regelungen über die Unterscheidung bestimmter Personenkategorien sowie zwischen Tatsachen und persönlichen Einschätzungen in den §§ 72 und 73 BDSG aus Ihrer Sicht normenklar?

Die Regelungen erschöpfen sich in der Wiedergabe der Vorgaben der JI-RL und stellen keine Konkretisierung dar. Insofern ist der Mehrwert gering. Eine Konkretisierung muss zwingend im Fachrecht erfolgen.

6. Sind die Regelungen über das Verfahren bei Datenübermittlungen in § 74 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

Die Regelungen erscheinen sachgerecht und erforderlich.

7. Sind die Regelungen über die Pflicht zur Berichtigung und Löschung sowie die Einschränkung der Verarbeitung in § 75 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

§ 75 BDSG ist teilweise wortgleich zu 37 Absatz 2 GwG (FIU). In der Praxis erweist sich regelmäßig als Problem, dass die Prüfung der Löschvoraussetzungen nicht einzelfallbezogen erfolgt. Selbst beim Wegfall der Erforderlichkeit (z. B. Einstellung des Ermittlungsverfahrens) wird der Löschverpflichtung nicht nachgekommen

VII. Datenübermittlungen an Drittstaaten und an internationale Organisationen

Zusammenfassung:
Für diesen Bereich werden Ergänzungen vorgeschlagen, mit denen Anwendungsschwierigkeiten in der Praxis behoben werden können. Eine gesetzliche Konkretisierung der Anforderungen an geeignete Garantien und rechtsverbindliche Instrumente in § 79 BDSG würde Anwendungsschwierigkeiten in der Praxis verhindern. Zu Schwierigkeiten in der Praxis führte zudem die fehlende Berichtspflicht für Übermittlungen nach § 80 Absatz 1 BDSG.

1. Sind die allgemeinen Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen in § 78 BDSG normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

§ 78 BDSG setzt Artikel 35 der JI-RL um. Inhaltlich werden die allgemeinen Anforderungen an Datenübermittlungen geregelt. Die in Artikel 36 JI-RL genannten Voraussetzungen zur Prüfung des Schutzniveaus bei einem Angemessenheitsbeschluss werden hier nicht aufgeführt. Für den Regelungsbereich der JI-RL (im Gegensatz zu dem DSGVO-Bereich) liegen noch keine Angemessenheitsbeschlüsse vor. Daher ist die Regelung aktuell von geringer praktischer Relevanz.

2. Sind die weiteren Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen in den §§ 79 bis 81 BDSG normenklar?

Die Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen sollten auch weiterhin zentral im BDSG geregelt sein. Solange das einschlägige Fachrecht keine gleichwertigen Regelungen enthält, sind die Regelungen auch ohne ausdrückliche Verweisung ergänzend anzuwenden (Auffangfunktion des BDSG).
Soweit fachgesetzliche Regelungen vorhanden sind, sollten diese allerdings den Komplex der Drittstaatenübermittlungen abschließend und ohne Verweisungen regeln. Ansonsten kommt es – wie im BKAG – zu einem relativ unübersichtlichen Regelungsgeflecht.

§ 79 BDSG setzt Artikel 37 der JI-RL um und regelt die Datenübermittlung bei geeigneten Garantien, die entweder in einem rechtsverbindlichen Instrument (Nr. 1) oder nach Beurteilung aller Umstände (Nr. 2) einen Schluss auf eben diese Garantien zulässt. Das Fehlen von Legaldefinitionen in § 79 BDSG führt zu erheblichen Unsicherheiten und Anwendungsschwierigkeiten in der Praxis. Es stellt sich konkret die Frage, welche Anforderungen und Maßstäbe an geeignete Garantien und an ein rechtsverbindliches Instrument zu stellen sind. Es ist insoweit zwischen den formalen und den materiellen Anforderungen zu differenzieren. Weder Artikel 37 der JI-RL noch Artikel 46 DSGVO enthalten eine Legaldefinition des Begriffs geeigneter Garantien. Allerdings regelt Artikel 46 DSGVO, dass geeignete Garantien in einem rechtlich bindenden und durchsetzbaren Dokument, verbindlichen Datenschutzvorschriften oder Standarddatenschutzklauseln geregelt sein können. Für den Anwendungsbereich der JI-RL mangelt es an einer entsprechenden Regelung. Unmittelbar anwendbar ist Artikel 46 DSGVO allerdings nicht, sondern kann insoweit nur als Auslegungshilfe dienen. Auch lassen sich keine klar definierten Anforderungen an ein rechtsverbindliches Instrument aus Erwägungsgrund 71 JI-RL entnehmen. Dies können jedoch bilaterale Abkommen und Verträge sein, wenn sie in nationales Recht übernommen wurden und durchsetzbar sind.

Systematisch ist letztlich auf die Nähe und den Regelungszusammenhang des Artikel 37 zu Artikel 36 der JI-RL abzustellen. Die materiellen Anforderungen an das zu fordernde Schutzniveau enthält (allein) Artikel 36 Absatz 2 der JI-RL. Artikel 37 der JI-RL enthält hierzu keine abweichenden materiellen Vorgaben. Er will lediglich eine Möglichkeit zur Übermittlung schaffen, wenn es an der formalen Voraussetzung des Angemessenheitsbeschlusses fehlt. Statt eines formalen Angemessenheitsbeschlusses sieht daher Artikel 37 JI_RL (andere) „geeignete Garantien" vor. Diese müssen aber dieselben materiellen Vorgaben absichern wie der Angemessenheitsbeschluss. Aus Sicht der DSK müssen deshalb geeignete Garantien dem gleichen Maßstab wie das angemessene Schutzniveau i.S.d. Angemessenheitsbeschlusses unterliegen. Der Datenschutz würde sonst ausgehebelt werden (vgl. BeckOK Datenschutzrecht, Wolff/Brink, 33. Edition, § 79, Rn. 9).
Dieses Schutzniveau muss entsprechend rechtsverbindlich garantiert sein. § 79 BDSG setzt Artikel 37 der JI-RL zwar nahezu wortgleich um; bei der Umsetzung wäre aber eine Konkretisierung der Anforderungen an geeignete Garantien und rechtsverbindliche Instrumente wünschenswert gewesen, um Anwendungsschwierigkeiten in der Praxis zu verhindern.

Im Unterschied zu den Regelungen der JI-RL hat der nationale Gesetzgeber für alle Situationen einer Datenübermittlung (§§ 78 bis 80 BDSG) eine Einzelfallprüfung im Sinne des § 78 Absatz 2 BDSG vorgesehen. Demnach hat die Übermittlung personenbezogener Daten trotz des Vorliegens eines angemessenen Datenschutzniveaus zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegend schutzwürdige Interessen einer betroffenen Person entgegenstehen. Diese Regelung ist zwar dem Grunde nach nicht zu kritisieren, wirft jedoch systematische Fragen auf.

Bezüglich der Berichtspflichten an die Datenschutzaufsichtsbehörden ist aus der praktischen Erfahrung heraus zu kritisieren, dass für Übermittlungen nach § 80 Absatz 1 BDSG (ohne geeignete Garantien im Ausnahmefall) keine aktive Berichtspflicht an die Datenschutzaufsichtsbehörde besteht. Zwar hat die Datenschutzaufsichtsbehörde nach § 80 Absatz 3 BDSG das Recht, die Dokumentation entsprechender Übermittlungen anzufordern. Dieses Recht kann aber nur sinnvoll ausgeübt werden, wenn auf Anforderung auch zu Übermittlungen nach § 80 Absatz 1 BDSG die Anzahl der Übermittlungen je Empfängerstaat berichtet werden kann. Diese Informationen sind zur Aufgabenerfüllung des BfDI erforderlich und insoweit nach § 16 Absatz 4 Nr. 2 BDSG bereitzustellen und zu diesem Zwecke vorzuhalten. Anders als bei den aktiven Berichtspflichten zu anderen Übermittlungstypen war dies jedoch in der Praxis von den Verantwortlichen ursprünglich nicht vorgesehen sondern wurde erst auf Intervention des BfDI eingeführt.

Insgesamt erscheint es aus Sicht der Datenschutzaufsicht erforderlich, dass die verantwortliche Stelle einen Gesamtüberblick über die Anzahl von Datentransfers in Drittstaaten in den einzelnen Fallgruppen der §§ 79-81 BDSG hat und diesen auch belegen kann. Dies ergibt sich letztlich aus der allgemeinen Rechenschaftspflicht.

VIII. Haftung und Sanktionen

<u>Zusammenfassung</u>
Artikel 83 Absatz 8 DSGVO verpflichtet die Mitgliedstaaten, ordnungsgemäße Verfahren und Verfahrensgarantien für das Bußgeldverfahren festzulegen. Die bisher getroffenen Regelungen werden dem Willen des europäischen Gesetzgebers, eine harmonisierte Sanktionierung von Datenschutzverstößen zu schaffen, nicht gerecht.

Die normierten Verweise auf die Regelungen des OWiG zur Konkretisierung des Bußgeldverfahrens reichen nicht aus und sind zum Teil sogar europarechtswidrig. Dem deutschen Ordnungswidrigkeitenrecht ist das in der DSGVO normierte Verbandshaftungsrecht bisher fremd, sodass die Verweise zum Teil irreführend sind und dringend angepasst werden müssen. Insbesondere weil die Bußgeldtatbestände der DSGVO an das europäische Kartellrecht angelehnt sind, fordert die DSK, die Befugnisse der Datenschutzbehörden auch an das deutsche Kartellrecht anzugleichen und die bisherige Regelung des § 41 BDSG um Verweise in das GWB zu ergänzen.

Um dem Umfang von Bußgeldverfahren bei Datenschutzverstößen und der Bewertung der datenschutzrechtlichen Spezialmaterie gerecht zu werden, ist der Schwellenwert in § 41 Absatz 1 Satz 3 BDSG herabzusetzen. Auch der Vergleich zum Kartellrecht zeigt, dass Ordnungswidrigkeitenverfahren zu Spezialmaterie aufgrund der Komplexität vor einer Strafkammer verhandelt werden. So sieht § 83 GWB nicht ohne Grund für sämtliche Kartell-Ordnungswidrigkeitenverfahren die Zuständigkeit des Oberlandesgerichts geregelt.

Des Weiteren wird gefordert, die Abhilfemaßnahmen gegenüber öffentlichen Stellen entgegen der bisherigen Regelung des § 43 Absatz 3 BDSG weiter auszubauen und insbesondere Geldbußen auch gegenüber öffentlichen Stellen verhängen zu können um Datenschutzverstöße effektiv ahnden zu können.

Ferner wird mit der Formulierung „nach diesem Gesetz“ in § 83 Absatz 1 Satz 1 BDSG gegen das Wiederholungsverbot verstoßen.

1. Sind die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG aus Ihrer Sicht sachgerecht und normenklar?

a) Zu § 41 BDSG

Gemäß § 41 Absatz 1 Satz 1 BDSG gelten für Verstöße nach Artikel 83 Absatz 4 bis 6 DSGVO, soweit das BDSG nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Nach § 41 Absatz 1 Satz 2 BDSG finden lediglich die §§ 17, 35 und 36 OWiG keine Anwendung. Daraus könnte die falsche Schlussfolgerung geschlossen werden, dass die §§ 30, 130 OWiG zur Reichweite der Verantwortlichkeit von juristischen Personen und Personenvereinigung für Bußgeldverstöße Geltung haben sollen. Dies würde jedoch den Vorgaben der DSGVO widersprechen.

Gemäß EG 150 DSGVO gilt in Bußgeldverfahren der funktionale Unternehmensbegriff im Sinne der Artikel 101 und 102 AEUV. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff genügt für die Verantwortlichkeit eines Unternehmens bzw. einer Unternehmensvereinigung die Handlung einer Person, die berechtigt ist, für das Unternehmen bzw. die Unternehmensvereinigung tätig zu werden (EuGH, Urteil vom 7. Juni 1983, Rs. 100-103/80, Slg. 1983,1825, Rn. 97; EuGH, Urteil vom 29. April 2004, Rs. T-236/01, Slg. 2004, 1181, Rn. 278).

Erfasst sind deshalb nicht nur wie bisher die gesetzlichen Vertreter oder Leitungspersonen (§ 30 Absatz 1 OWiG), sondern sämtliche Bedienstete oder auch Beauftragte außerhalb des Unternehmens oder der Unternehmensvereinigung (vgl. auch EuGH, Urteil vom 7. Februar 2013, Rs. C-68/12, Rn. 25-28). Eine Kenntnis der Inhaber oder Geschäftsführer des Unternehmens von der konkreten Handlung oder eine Verletzung der Aufsichtspflicht (bisher gemäß § 130 OWiG notwendig) ist für die Zuordnung der Verantwortlichkeit nicht erforderlich, wobei Exzesse ausgenommen sind (vgl. KK OWiG Rogall, Rn. 249 zu § 30). Daher läuft eine Weitergeltung der §§ 30, 130 OWiG über § 41 Absatz 1 Satz 1 und 2 BDSG den Vorgaben der DSGVO zuwider. Entsprechend urteilte das Landgericht Bonn am 11. November 2020 (Az. 29 OWi 1/20 LG) in einem Verfahren. Es hat entschieden, dass die DSGVO, anders als in den §§ 30, 130 OWiG normiert, nicht erfordert, dass konkret festgestellt wird, dass eine Leitungsperson eines Unternehmens gegen bußgeldbewährte Regelungen verstößt, um ein Bußgeld verhängen zu können.

Die Aufsichtsbehörden sind aufgrund des Anwendungsvorrangs des EU-Rechts derzeit verpflichtet, § 41 Absatz 1 Satz 1 und 2 BDSG in Bezug auf die Weitergeltung der §§ 30, 130 OWiG unangewendet zu lassen (vgl. EuGH, Urteil vom 22. Juni 1989, Az. 103/88, Rn. 28 ff.).

Es wird daher empfohlen,

in § 41 Absatz 1 Satz 2 BDSG die Wörter „§§ 17, 35 und 36“ durch die Wörter „§§ 17, 30, 35, 36 und 130“ zu ersetzen.

Um sicherzustellen, dass § 30 Absatz 2a Satz 1 und 3 OWiG anwendbar bleiben (Bußgeld gegen Gesamtrechtsnachfolger), sollte in § 41 Absatz 1 BDSG folgender Satz 3 ergänzt werden:

„§§ 59, 59b Absatz 3, 81 Absatz 2 Nr. 6 bis 11, § 81a Absatz 2 bis 5, § 81b, § 81c Absatz 1 bis 3 und 5, § 81e, § 81f, § 81g Absatz 2, § 82b des Gesetzes über Wettbewerbsbeschränkungen sind entsprechend anwendbar; Geldbußen im Sinne jener Vorschriften sind solche wegen Verstößen gegen die Verordnung (EU) 679/2016.“

§ 30 Absatz 2a Satz 1 und 3 OWiG haben in § 81a Absatz 2 GWB eine Parallelvorschrift, sodass nicht unbedingt Teile des § 30 anwendbar gelassen werden müssen. Ohnehin müssten § 81a Absatz 3-5 GWB zusätzlich Anwendung finden, damit das Kartellbußrecht besser nachgebildet wird, bestehende Zurechnungslücken geschlossen werden und ein der Schwere der Bußgeldandrohung angemessenes Verfahren gewährleistet ist.

Zur Gewährleistung der ordnungsgemäßen Durchführung eines Bußgeldverfahrens nach Artikel 83 DSGVO sollte normiert werden, dass Unternehmen verpflichtet sind, über ihre wirtschaftlichen Verhältnisse gegenüber der Aufsichtsbehörde Auskunft zu geben sowie Unterlagen hierzu herauszugeben. Die bisherige Bußgeldpraxis hat gezeigt, dass es, soweit Unternehmen ihre Umsätze nicht offenlegen, für Aufsichtsbehörden zum Teil äußerst schwierig ist, auf sonstigen Wegen Informationen über die Umsätze zu erhalten oder diese zu schätzen. Der Umsatz ist aber bei Datenschutzverstößen von Unternehmen entscheidend für die Berechnung des Bußgeldrahmens und der darauf aufbauenden einzelfallbezogenen Bußgeldhöhe, da in diesen Fällen gemäß Artikel 83 Absatz 4 bis 6 DSGVO Geldbußen von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres des jeweiligen Unternehmens verhängt werden sollen. Da sich die DSGVO im Bereich der Sanktionsregelungen in vielen Teilen am Kartellrecht orientiert, bietet es sich an, eine Vorschrift entsprechend den Regelungen zur Auskunftspflicht von Unternehmen gegenüber Kartellbehörden nach § 59 GWB in das BDSG aufzunehmen. Zudem sollte auch eine ausdrückliche Vorschrift zur Befugnis der Schätzung wie § 81c Absatz 5 S. 2 GWB vorgesehen werden.

Die entsprechend anwendbaren Vorschriften des GWB umfassen:

- § 59: Auskunftsverlangen insb. zu wirtschaftlichen Kennzahlen
- § 59b Absatz 3: Enthält bei Satz 1 Nr. 3 eine Mitwirkungspflicht natürlicher Personen bei Durchsuchungen
- § 81 Absatz 2 Nrn. 6 bis 11: Materielle Bußgeldtatbestände, insbesondere, wenn verlangte Auskünfte nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt wurden
- § 81a Absatz 2 bis 5: Absatz 2 enthält insbesondere die notwendige Parallelvorschrift zu § 30 Absatz 2a Satz 1 und 3 OWiG. Absatz 3 enthält Regelungen zur wirtschaftlichen Nachfolge (nicht Gesamtrechtsnachfolge). Absatz 4 regelt insbesondere die Verjährung. Absatz 5 bestimmt eine die gesamtschuldnerische Haftung, wenn Geldbußen gegen mehrere Betroffene festgesetzt werden.
- § 81b: Geregelt werden Geldbußen gegen Unternehmensvereinigungen, insbesondere im Falle der fehlenden Zahlungsfähigkeit
- § 81c Absatz 1 bis 3, 5: Bußgeldrahmen für die Ordnungswidrigkeiten nach § 81 Absatz 2 Nrn. 6 bis 11 sowie Bestimmungen zum Verfahren (Gesamtumsatz der wirtschaftlichen Einheit, Schätzung des Umsatzes)
- 81e: Ausfallhaftung bei Erlöschen eines Unternehmens
- § 81f: Verzinsung der Geldbuße
- § 81g Absatz 2: Unterbrechung der Verjährung der Geldbuße durch Auskunftsverlangen
- § 82b: Anwendungsbefehl zu §§ 59 bis 59b GWB im Bußgeldverfahren

In Anlehnung an das GWB sollte zumindest auch deklaratorisch der § 41 Absatz 1 BDSG um eine spezifischere Festlegung ergänzt werden, der die funktionale Besetzung der Kammern bei den Landgerichten regelt:

„Das Landgericht entscheidet in der Besetzung von drei Mitgliedern mit Einschluss des Vorsitzenden Mitglieds."

b) Zu § 42 BDSG

Da die Datenschutzaufsichtsbehörden nicht für die Verfolgung von Straftaten zuständig sind, existieren keine praktischen Erfahrungen bei der Auslegung dieser Vorschrift. Gleichwohl fällt auf, dass der Begriff der „großen Zahl von Personen" in Absatz 1 Zweifel an der Bestimmtheit der Vorschrift begründen könnte. Daher erscheint eine Konkretisierung wünschenswert.

c) Zu § 43 BDSG

(1) Zu § 43 Absatz 3 BDSG

Gemäß § 43 Absatz 3 BDSG sollen gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 BDSG keine Geldbußen verhängt werden.

Die oder der BfDI sollte zukünftig unter Hinweis auf die Öffnungsklausel in Artikel 83 Absatz 7 DSGVO die Befugnis erhalten, gegen die vorgenannten Stellen Geldbußen zu verhängen. Dies ist insbesondere zur Sicherstellung der Einhaltung der Bestimmungen der DSGVO auch durch diese Stellen aufgrund drohender abschreckender Geldbußen sowie aus Gründen der Gleichbehandlung von öffentlichen und nicht-öffentlichen Stellen erforderlich.

Während bei nicht-öffentlichen Stellen datenschutzrechtliche Verstöße durch Verwarnung (bei geringeren Verstößen) und Bußgelder sanktioniert werden können, fehlt es bei öffentlichen Stellen an einer qualifizierten Sanktion im Verhältnis zu der Beanstandung, die die Schwere des Verstoßes im Vergleich zu den geringfügigeren Verstößen hinreichend ausdrückt.

Auch bei öffentlichen Stellen müssen sanktionsrechtliche Instrumente zur Verfügung stehen, um datenschutzrechtliche Verstöße ahnden und gleichzeitig spezial- und generalpräventiv wirken zu können. Der Sanktionscharakter eines Bußgeldes besteht aufgrund der eigenen Haushaltsbetroffenheit der jeweiligen Stelle uneingeschränkt. Darüber hinaus wären die vorgenannten Stellen aufgrund bestehender Bußgeldvorschriften motiviert, aktiv datenschutzrechtlichen Verstößen vorzubeugen und somit u.a. auch zu vermeiden, dass öffentliche Mittel für mögliche Schadensersatzansprüche von Betroffenen gemäß Artikel 82 DSGVO verwendet werden müssen.

Es wird daher empfohlen, § 43 Absatz 3 BDSG wie folgt zu formulieren:

„(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 *können Geldbußgen gemäß Artikel 83 der Verordnung (EU)2016/679 verhängt werden*"

(2) Zu § 43 Absatz 4 BDSG

§ 43 Absatz 4 BDSG regelt, dass eine Meldung nach Artikel 33 DSGVO oder eine Benachrichtigung nach Artikel 34 Absatz 1 DSGVO in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 StPO bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden darf.

Nach dem Wortlaut gilt dieses Verwendungsverbot daher stets, sobald eine Meldung oder Benachrichtigung erfolgt ist und hinsichtlich aller Inhalte dieser Meldung oder Benachrichtigung. Insoweit stellt sich die Frage, wie mit folgenden Konstellationen zu verfahren ist:

a. Es erfolgt eine Meldung/Benachrichtigung, obwohl keine Pflicht hierzu besteht (bspw., weil keine „Verletzung des Schutzes personenbezogener Daten" i.S.d. Artikel 4 Nr. 12 DSGVO vorliegt, sondern ein Verstoß durch eine unrechtmäßige Datenverarbeitung)

b. Im Rahmen einer Meldung/Benachrichtigung werden auch Informationen erteilt, die über den Pflichtinhalt nach Artikel 33 bzw. 34 DSGVO hinausgehen.

In diesen Fällen liegt zwar eine Meldung/Benachrichtigung vor, so dass nach dem Wortlaut des § 43 Absatz 4 BDSG ein Verwendungsverbot gilt. Nach unserer Auffassung kann dieses Verbot bei freiwilligen Angaben jedoch nicht greifen. Dies gilt sowohl für irrtümliche Meldungen von (vermeintlichen) Verletzungen, die im Ergebnis keine Melde-/Benachrichtigungspflicht auslösen, wie auch für Meldungen/Benachrichtigungen, die über die in Artikel 33 bzw. 34 DSGVO genannten Informationen hinausgehen.

Anderenfalls bestünde für Verantwortliche die Möglichkeit, bei einem datenschutzrechtlichen Verstoß eine Meldung nach Artikel 33 DSGVO vorzunehmen – obwohl dies mangels Verletzung i.S.d. Artikel 4 Nr. 12 DSGVO gar nicht erforderlich ist – und sich somit gezielt die Privilegierung eines Verwendungsverbotes zu verschaffen und eine Sanktionierung des Verstoßes zu verhindern.

§ 43 Absatz 4 BDSG ist daher so auszulegen, dass sich das Verwendungsverbot ausschließlich auf Fälle mit einer Pflicht zur Meldung/Benachrichtigung bezieht und weiterhin nur auf die Pflichtangaben gemäß Artikel 33 bzw. 34 DSGVO.

Dies könnte zur Klarstellung in § 43 Absatz 4 BDSG explizit geregelt werden.

2. In wie vielen Fällen haben nach Ihrer Kenntnis Landgerichte gemäß § 41 Absatz 1 Satz 3 BDSG über einen Einspruch gegen einen Bescheid über ein Bußgeld von mehr als 100.000 (einhunderttausend) Euro wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 DSGVO entschieden? (Bitte nach Jahren und Landgerichten aufschlüsseln.)

Auch wenn die angefragte Statistik nicht geführt wird, stellt die Vorschrift des § 41 Absatz 1 Satz 3 BDSG (i. V. m. § 68 OWiG) nach welcher das Landgericht erst ab einer festgesetzten Geldbuße von einhunderttausend Euro zuständig ist, in der aufsichtsbehördlichen Praxis durchaus ein Problem dar. Zukünftig sollte der Schwellenwert für die Zuständigkeit der Landgerichte weiter herabgesetzt werden.

Hierfür spricht zum einen die gravierende Erhöhung des Bußgeldrahmens von dreihunderttausend Euro nach dem alten BDSG auf bis zu 20 Millionen Euro bzw. bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres im Falle eines Unternehmens gemäß Artikel 83 Absatz 4 bis 6 DSGVO, die der großen Bedeutung des Datenschutzrechts insbesondere in einer immer digitalisierten Welt und der damit verbundenen Komplexität der Rechts- und Technikmaterie und der enormen wirtschaftlichen Bedeutung der Verarbeitung personenbezogener Daten geschuldet ist. Eine vermehrte Zuweisung von datenschutzrechtlichen Fällen an die Landgerichte würde langfristig zu einer angemessenen Spezialisierung der zuständigen Richter und Richterinnen führen. Dies liegt sowohl im Interesse der Rechtsdurchsetzung als auch, soweit eine Verfolgung stattfindet, im Interesse der Beschuldigten,

Zum anderen legt dies auch die zuvor unter Ziffer 1 a) geschilderte Übernahme des kartellrechtlichen funktionalen Unternehmensbegriffs in der DSGVO nahe, da § 83 Absatz 1 GWB die Regelungen zur gerichtlichen Zuständigkeit in Kartellverfahren ohne Setzung einer Betragsgrenze bei gerichtlichen Verfahren wegen einer Ordnungswidrigkeit sogar das Oberlandesgericht als Eingangsinstanz bestimmt.

Keinesfalls darf die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen ab einer bestimmten Höhe hingegen abgeschafft werden. Das Sanktionsrecht der DSGVO ist mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Ordnungswidrigkeiten nach der DSGVO, die mit hohen Geldbußen einhergehen, bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind insoweit mit Wirtschaftsstrafsachen vergleichbar, die gemäß § 74c GVG ebenfalls den Landgerichten zugewiesen sind. Zudem würde eine breitere erstinstanzliche Zuständigkeit der Landgerichte die Amtsgerichte zukünftig entlasten.

3. Sind die Regelungen zu Haftung und Sanktionen in den §§ 83 und 84 BDSG aus Ihrer Sicht sachgerecht und normenklar?

a) Zu § 83 BDSG

Da Schadenersatz und Entschädigung nach § 83 BDSG auf dem Zivilrechtsweg einzuklagen sind, fehlt es den Datenschutzaufsichtsbehörden an praktischen Erfahrungswerten. Die Verweisung in § 83 Absatz 1 Satz 1 BDSG „nach diesem Gesetz“ dürfte sich richtigerweise nur auf den dritten Teil des BDSG beziehen. Denn sie kann sich nur auf denjenigen Teil des Gesetzes beziehen, welcher nicht vorrangig durch die unmittelbar anwendbare DSGVO geregelt wird, hier Artikel 82 DSGVO. Die aktuelle Formulierung verstößt somit gegen das Wiederholungsverbot. Zudem könnten sich

unterschiedliche Ergebnisse gegenüber der Anwendung von Artikel 82 DSGVO ergeben, so dass eine unzulässige Einschränkung der DSGVO das Resultat sein könnte.

b) Zu § 84 BDSG

Keine Anmerkungen.

IX. Allgemein zu den Regelungen des BDSG

1. Wie bewerten Sie das BDSG insgesamt in Bezug auf die Sachgerechtigkeit, Praktikabilität und Normenklarheit der Bestimmungen?

2. Bestehen in Ihrer datenschutzrechtlichen Praxis Schwierigkeiten mit der Auslegung und Anwendung des BDSG? Wenn ja, welche Schwierigkeiten sind das und auf welche Regelungen des BDSG beziehen sie sich?

Die Vorschriften § 47 BDSG und § 54 Absatz 2 BDSG sind zwar nicht im Fragenkatalog enthalten, haben sich jedoch aus folgenden Gründen als problematisch erwiesen:

a) Zu § 47 BDSG

Sowohl im Hinblick auf die Umsetzung der JI-RL als auch in der Anwendung des Datenschutzrechts in der Praxis gestaltet sich § 47 BDSG problematisch.

Artikel 4 Absatz 4 JI-RL, der die Rechenschaftspflicht des Verantwortlichen bekräftigt, ist dort nicht umgesetzt. Die Parallelvorschrift des Artikel 5 Absatz 2 DSGVO spielt in der Praxis eine wichtige Rolle. Zur Verdeutlichung der Pflichten der Verantwortlichen sollte die Regelung des Artikel 4 Absatz 4 JI-RL in das BDSG aufgenommen werden. Es handelt sich zwar nur um eine deklaratorische Regelung. Die Erfahrung in der Praxis hat jedoch gezeigt, dass gerade die Pflicht, die Einhaltung der Vorgaben nachzuweisen, nicht allen Verantwortlichen klar ist. Einige Verantwortliche gehen davon aus, dass die Datenschutzaufsichtsbehörde das Vorliegen von Verstößen gegen Datenschutzvorschriften positiv nachweisen müsse. Im Regelfall ist es jedoch umgekehrt: Der Verantwortliche muss gegenüber der Aufsichtsbehörde die Einhaltung der Vorgaben des Datenschutzrechts nachweisen. Gelingt dies nicht, muss die Aufsichtsbehörde davon ausgehen, dass das Datenschutzrecht nicht eingehalten ist und daraufhin prüfen, ob Maßnahmen erforderlich sind, um die Verarbeitung in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen.

b) Zu § 54 Absatz 2 BDSG

In § 54 Absatz 2 BDSG sollte als eine der Maßnahmen zum Schutz der betroffenen Personen das Recht auf persönliches Eingreifen durch den Verantwortlichen ausdrücklich aufgenommen werden. Dieses Recht ist sowohl in Artikel 11 JI-RL als auch in Artikel 22 Absatz 3 DSGVO ausdrücklich vorgesehen.