



Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

per E-Mail:
innenausschuss@bundestag.de

Landesbeauftragte für Datenschutz
Schleswig-Holstein
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Dr. h.c. Marit Hansen
Durchwahl: 988-1289
E-Mail: dsk2024@datenschutz.de
Aktenzeichen: 01.03/01.001

Kiel, 12. April 2024

Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BR-Drs. 72/24; BT-Drs. 20/10859)

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) vom 12. April 2024

Sehr geehrte Damen und Herren Abgeordnete,

mit dem oben genannten Gesetzentwurf soll das Bundesdatenschutzgesetz in einigen Punkten geändert werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder stimmt diesen Änderungsvorschlägen teilweise zu. Aus Sicht der DSK sprechen jedoch gegen einige der Änderungen grundlegende Bedenken, zum Beispiel gegen die Beschränkung des Auskunftsanspruchs betroffener Personen durch Betriebs- und Geschäftsgeheimnisse. Die DSK sieht zudem weitergehenden Änderungsbedarf im Hinblick auf das Bundesdatenschutzgesetz, der in dem vorliegenden Gesetzentwurf nicht aufgegriffen wird.

Die DSK hat ihre Kritikpunkte an dem Gesetzentwurf und den darüber hinaus bestehenden Änderungsbedarf in einer Stellungnahme erläutert, die ich Ihnen im Anhang übersende.

Ich würde mich freuen, wenn Sie die Positionen der DSK im weiteren Gesetzgebungsverfahren berücksichtigen würden. Gern stehe ich für einen Austausch hierzu zur Verfügung.

Mit freundlichen Grüßen


Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein
Vorsitz der DSK im Jahr 2024

Stellungnahme

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. April 2024

zum Gesetzentwurf der Bundesregierung: Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BR-Drs. 72/24; BT-Drs. 20/10859)

I.	Vorbemerkung	2
II.	Zu den einzelnen Regelungsvorschlägen	2
1.	Institutionalisierung der Datenschutzkonferenz (§ 16a BDSG-E).....	2
2.	Ergänzende Zuständigkeitsregelungen (§§ 19, 40 BDSG-E)	4
3.	Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen betroffener Personen (§ 34 Abs. 1 Satz 2 BDSG-E, § 83 SGB X-E)	5
4.	Scoring (§ 37a BDSG-E)	5
5.	Länderübergreifende Datenverarbeitungsvorhaben (§ 40a; § 27 Abs. 5 BDSG-E)	10
III.	Weitergehender Änderungsbedarf.....	11
1.	Sofortige Vollziehbarkeit von Verwaltungsakten gegenüber öffentlichen Stellen (§ 20 Abs. 7 BDSG).....	11
2.	Anwendbare Vorschriften des Ordnungswidrigkeitengesetzes und des Gesetzes gegen Wettbewerbsbeschränkungen für Verstöße nach Art. 83 DS-GVO (§ 41 BDSG)	12
3.	Aufnahme einer Befugnis zur Einziehung von Gegenständen in § 41 BDSG	15
4.	Streichung des § 43 Abs. 3 BDSG (Verhängung von Geldbußen auch gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Abs. 1 BDSG)	17
5.	Bedarf einer bereichsspezifischen Ausnahmeregelung i. S. v. § 17 VwVG	18
6.	Anwendbarkeit des für nichtöffentliche Stellen geltenden Rechts für Religionsgemeinschaften	18

I. Vorbemerkung

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder nehmen als Datenschutzkonferenz (DSK) gemeinsam zu dem Vorschlag der Institutionalisierung der DSK sowie weiterer im Gesetzentwurf der Bundesregierung enthaltener Vorschläge Stellung.

Über den vorliegenden Gesetzentwurf hinaus besteht aus Sicht der DSK weiterer Änderungsbedarf. Diesen hat die DSK in einer Stellungnahme zur Evaluierung des BDSG vom 2. März 2021¹ ausführlich beschrieben. Auf diese Stellungnahme wird verwiesen. In der vorliegenden Stellungnahme beschränkt sich die DSK daher auf diejenigen Punkte, in denen der Änderungsbedarf am dringlichsten ist.

II. Zu den einzelnen Regelungsvorschlägen

1. Institutionalisierung der Datenschutzkonferenz (§ 16a BDSG-E)

Mit der Vorschrift des § 16a BDSG-E wird die in der Koalitionsvereinbarung vorgesehene Institutionalisierung der DSK vollzogen. Die DSK wird so als wichtiges, national und international geachtetes Datenschutz-Gremium anerkannt, unbeschadet der insbesondere nach Maßgabe der Datenschutz-Grundverordnung (DS-GVO) bestehenden Zuständigkeiten, Aufgaben und Befugnisse. Die gesetzliche Verankerung der Datenschutzkonferenz und die Festlegung der Geschäftsordnung als wesentliches Instrument zur Regelung ihrer Tätigkeit (§ 16a S. 2 BDSG-E) tragen der Bedeutung der DSK und der Unabhängigkeit der Datenschutzaufsichtsbehörden des Bundes und der Länder angemessen Rechnung.

Allerdings enthält der neue § 16a BDSG-E nicht viel Neues: Die DSK arbeitet bereits seit mehreren Jahren auf Basis einer sich selbst gegebenen Geschäftsordnung. Darin sind auch Anwendungsbereich und Verfahren von Mehrheitsentscheidungen definiert. Diese Festlegung erzeugt eine Selbstbindung der DSK-Mitglieder und hat sich als tragfähig erwiesen. Die völlige Unabhängigkeit der Datenschutzaufsichtsbehörden wird gewahrt; zugleich werden die in der Geschäftsordnung genannten Ziele verfolgt, die Koordinierung und Zusammenarbeit ihrer Mitglieder und die einheitliche Anwendung des Datenschutzrechts zu fördern.

¹ https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf.

Zusätzliche Regelungen im § 16a BDSG-E könnten dies unterstützen. So wäre von Vorteil, die **Ziele der DSK** in dieser gesetzlichen Regelung aufzunehmen, z. B. durch den Satz:

„Die Datenschutzkonferenz fördert die Koordinierung und die Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder sowie eine einheitliche Anwendung des Datenschutzrechts.“

Für die Aufgabe der einheitlichen Anwendung des Datenschutzrechts ist die DSK in der Vergangenheit dadurch aktiv geworden, dass sie eine konsistente Datenschutzaufsicht verwirklicht, die Verantwortlichen, Auftragsverarbeitern und betroffenen Personen Rechtssicherheit bietet. Dazu hat sie zahlreiche Materialien herausgegeben. Hinzu kommen abgestimmte Stellungnahmen zu Gesetzentwürfen oder Praxisfragen der Verarbeitung in Deutschland und Europa, die regelmäßig in kurzer Frist von der DSK erwartet werden.

Die organisatorische Unterstützung dieser Harmonisierungsmaßnahmen durch eine Geschäftsstelle wird im Gesetzentwurf bisher nicht geregelt. Gerade angesichts der gestiegenen und weiter steigenden Erwartungen an die DSK hemmt dies eine kontinuierliche Weiterverfolgung der einheitlichen Anwendung des Datenschutzrechts. Aus diesem Grund bekräftigt die DSK die Notwendigkeit der Errichtung einer **Ständigen Geschäftsstelle**, die im § 16a BDSG-E geregelt sein sollte, beispielsweise in der folgenden Form:

„Bund und Länder errichten eine Ständige Geschäftsstelle, die die Datenschutzkonferenz bei der Erfüllung ihrer Aufgaben unterstützt. Sie dient als Kontaktstelle für andere Behörden und Institutionen zur Datenschutzkonferenz und zu ihren Mitgliedern. Einzelheiten der Errichtung und Finanzierung der Geschäftsstelle werden von Bund und Ländern in Abstimmung mit der Datenschutzkonferenz gemeinsam festgelegt. Sie arbeitet nach Beschlusslage und auf Anweisung der Datenschutzkonferenz.“

Eine Ständige Geschäftsstelle bringt einen Gewinn an Professionalität und eine Steigerung der Kontinuität im Handeln der DSK. Die Wahrung dieser Kontinuität bei gleichzeitiger effektiver Aufgabenwahrnehmung wird auch vor dem Hintergrund der fortschreitenden Technologien auf Dauer eine Herausforderung bleiben, die einen eigenen, überschaubaren aber angemessenen Verwaltungsunterbau erfordert. Der jeweilige Vorsitz wird unterstützt und zugleich insbesondere von administrativen Aufgaben entlastet. Ein Aufbau von Routinen wird durch den in bundesstaatlicher Tradition etablierten kontinuierlichen Wechsel im Vorsitz erschwert.

Vor diesem Hintergrund ist eine Geschäftsstelle angesichts der Institutionalisierung der DSK und der damit an sie gerichteten Ansprüche unerlässlich.

2. Ergänzende Zuständigkeitsregelungen (§§ 19, 40 BDSG-E)

Die Änderungen des § 19 BDSG sind laut der Gesetzesbegründung klarstellender Natur und sollen keine inhaltlichen Änderungen zur Folge haben. Nach § 19 Abs. 1 S. 4 BDSG-E ist das Verfahren nach § 18 Abs. 3 BDSG auch dann anzuwenden, wenn eine Aufsichtsbehörde bestimmt werden muss aufgrund der Tatsache, dass ein Verantwortlicher oder Auftragsverarbeiter keine inländische Niederlassung hat.

Die ergänzende Regelung der Zuständigkeit in Fällen der Zusammenarbeit, bei denen es keine inländische Niederlassung gibt (§ 19 Abs. 1 S. 4 BDSG-E), geht jedoch fehl und sollte gestrichen werden. § 19 BDSG dient dazu, die federführende Behörde in Deutschland zu bestimmen. Federführende Behörde i. S. d. DS-GVO ist in einem grenzüberschreitenden Fall die Behörde am Ort der Haupt- oder einzigen Niederlassung (Art. 56 Abs. 1 DS-GVO). Gibt es keine Niederlassung in Deutschland, kann es denklogisch auch keine federführende deutsche Aufsichtsbehörde geben. Es hat daher keinen Sinn, für diesen Fall eine federführende Behörde zu bestimmen.

Gleiches gilt für § 40 Abs. 2 S. 3 BDSG-E, nach dem die Aufsichtsbehörden gemeinsam eine zuständige Behörde nach dem Verfahren des § 18 Abs. 3 BDSG-E bestimmen, wenn ein Verantwortlicher keine Niederlassung in der Bundesrepublik Deutschland hat. Es wird aus dem Entwurf nicht ausreichend klar, welche Fälle damit gemeint sind und für welchen Zweck eine Zuständigkeit bzw. Federführung in Deutschland als erforderlich angesehen wird. Nach Auffassung der Datenschutzaufsichtsbehörden der Länder kann die Regelung nicht den Marktortfall (Art. 3 Abs. 2 DS-GVO) betreffen. Denn es gibt im Marktortfall auch nach der DS-GVO kein One-Stop-Shop-Verfahren, sondern es sind alle Aufsichtsbehörden der EU-Mitgliedstaaten zuständig. Außer dem Marktortfall ist kein Anwendungsbereich für den Fall ersichtlich, dass es keine inländische Niederlassung gibt.

Die Regelung sollte daher gestrichen werden.

3. Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen betroffener Personen (§ 34 Abs. 1 S. 2 BDSG-E, § 83 SGB X-E)

Die Regelungen des § 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB X-E sollen die Wahrung des Geschäfts- und Betriebsgeheimnisses bei der Durchsetzung von Auskunftsansprüchen sicherstellen. Allerdings ist ihre Vereinbarkeit mit Art. 23 DS-GVO zweifelhaft. Derartige Zweifel werden bereits gegenüber dem bestehenden § 34 Abs. 1 Nr. 2 BDSG geäußert, wenn und soweit kein Ausnahmetatbestand ersichtlich ist. Die Einschränkungen der Betroffenenrechte nach Art. 23 DS-GVO sind eng auszulegen. Als Ausnahmetatbestand für die Wahrung des Geschäfts- und Betriebsgeheimnisses kommt Art. 23 Abs. 1 lit. i DS-GVO in Betracht, wonach eine Beschränkung zum Schutz von Rechten und Freiheiten anderer Personen zulässig ist. Darüber hinaus sind die in § 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB X-E adressierten Aspekte bereits in Art. 15 Abs. 4 DS-GVO, konkretisiert durch Erwägungsgrund 63 S. 5 zur DS-GVO, berücksichtigt.

Vor dem Hintergrund der Regelung des Art. 15 Abs. 4 DS-GVO, der nur hinsichtlich des Rechts auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DS-GVO vorsieht, dass dieses Recht die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf, sind § 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB X-E zu weit gefasst. Der deutsche Gesetzgeber würde ansonsten eine weitergehende Beschränkung schaffen als der europäische Gesetzgeber im Verordnungstext. Nach Ansicht des EDSA gilt die Einschränkung des Art. 15 Abs. 4 DS-GVO nicht für die Informationen nach Art. 15 Abs. 1 lit. a bis h DS-GVO (vgl. EDSA, Guidelines 01/2022 on data subject rights – Right of Access, Version 2.0, Adopted on 28 March 2023, Rn. 169).

Die Änderung des § 34 BDSG und des § 83 SGB X sollte daher gestrichen werden.

4. Scoring (§ 37a BDSG-E)

Die erstmals nach der Verbändebeteiligung im Regierungsentwurf aufgenommene Regelung gibt aus grundsätzlichen Erwägungen genauso wie aus einer Reihe von Einzelgesichtspunkten Anlass zu Kritik:

4.1 Allgemeines

a) Regelungsnotwendigkeit

Nach der Entscheidung des EuGH vom 7. Dezember 2023 (C-634/21) stellt Art. 22 Abs. 1 DS-GVO ein grundsätzliches Verbot dar, betroffene Personen einer

ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung zu unterwerfen. Mitgliedstaatliche Regelungsspielräume bestehen insoweit zunächst nur für solche Bestimmungen, die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person im Sinne von Art. 22 Abs. 2 lit. b DS-GVO vorsehen. Wegen der übergeordneten Geltung der Grundsätze des Art. 5 DS-GVO weist der EuGH außerdem darauf hin, dass die Mitgliedstaaten nach Art. 22 Abs. 2 lit. b DS-GVO keine Rechtsvorschriften erlassen dürfen, nach denen ein Profiling unter Missachtung der Anforderungen von Artt. 5 und 6 DS-GVO in deren Auslegung durch die Rechtsprechung des Gerichtshofs zulässig wäre und stellt klar, dass die Mitgliedstaaten gleichzeitig nicht befugt sind, nähere Vorschriften für die Anwendung der Bedingungen der Rechtmäßigkeit für Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. a, b und f DS-GVO zu erlassen (EuGH, C-634/21, Rn. 68 und 72).

Allerdings hatte der EuGH im Hinblick auf die ihm vorgelegten Fragen des Ausgangsgerichts keinen Anlass zur abschließenden Erörterung über Art. 22 DS-GVO hinausgehender Anforderungen an nationale Ausnahmeregelungen im Sinne von Art. 22 Abs. 2 lit. b DS-GVO. Da Art. 22 DS-GVO in den Anforderungen des Art. 23 DS-GVO an mitgliedstaatliche Beschränkungen der Pflichten und Rechte von Verantwortlichen und Auftragsverarbeiter ausdrücklich erwähnt wird, müssen aus Sicht der DSK die dort festgelegten Schranken nationaler Regelungsbefugnisse systematisch neben den in Art. 22 Abs. 2 lit. b DS-GVO genannten Einzelanforderungen beachtet werden. Eine Regelung wie die vorliegende muss daher wie andere Regelungen zur Beschränkung der Betroffenenrechte des 3. Abschnitts der DS-GVO insbesondere darlegen, auf welche der in Art. 23 Abs. 1 DS-GVO abschließend genannten Ausnahmegründe sie gestützt wird und ob sie insoweit eine notwendige und verhältnismäßige Maßnahme darstellt. Aussagen hierzu sind dem vorliegenden Entwurf an keiner Stelle zu entnehmen und auch aus dem Gesamtzusammenhang nicht ersichtlich.

Insbesondere kann die Entscheidung des EuGH selbst nicht als zwingender Anlass und Begründung der Notwendigkeit einer nationalen Regelung nach Art. 22 Abs. 2 lit. b DS-GVO betrachtet werden, da für die Nutzung von Scorewerten weiterhin Gestaltungen verbleiben, die außerhalb des durch den EuGH präzisierten Anwendungsbereichs des Art. 22 DS-GVO liegen.

Die DSK hält es daher für erforderlich, im weiteren Gesetzgebungsverfahren zu prüfen, ob § 37a BDSG-E mit den weitergehenden Anforderungen des Art. 23 DS-GVO an nationale Beschränkungen des mit Art. 22 DS-GVO gewährleisteten Betroffenenrechts in Einklang steht.

b) Anwendungsbereich

Entgegen seiner Überschrift kann sich § 37a BDSG-E nach o. g. Rechtsprechung des EuGH alleine auf Art. 22 Abs. 2 lit. b DS-GVO stützen, mangels nationaler Regelungsbefugnis nicht aber als umfassende Ausgestaltung sonstiger Scoring-Sachverhalte auf Grundlage von Art. 22 Abs. 2 lit. a und c DS-GVO verstanden werden. Zur Vermeidung von Rechtsunsicherheiten sollte daher von vornherein die Überschrift den Anwendungsbereich so klar als möglich abgrenzen.

Die DSK schlägt hierzu folgende Änderung der Paragraphenbenennung vor:

„Ausnahmen vom Verbot automatisierte Entscheidungen im Einzelfall bei Scoring“

c) Sachverständigenanhörung

Angesichts der grundlegenden Bedeutung einer rechtssicheren Regelung von Kreditwürdigkeitsprüfung durch Scoringverfahren für Verbraucherinnen und Verbraucher genauso wie für Unternehmen der Kreditwirtschaft, des Online-Handels und zahlreicher weiterer Branchen sowie im Hinblick darauf, dass der Regelungsvorschlag zu § 37a BDSG-E nicht Gegenstand der Verbändeanhörung zum Referentenentwurf des BMI vom Sommer 2023 war, empfiehlt die DSK, die Regelung im Rahmen einer Sachverständigenanhörung im weiteren Gesetzgebungsverfahren umfassend zu analysieren.

4.2 Einzelheiten

Die DSK stellt fest, dass der Regelungsvorschlag eine größere Zahl ihrer Handlungsempfehlungen zum Datenschutz bei Scoringverfahren vom 11.05.2023 berücksichtigt hat, auch wenn diese zum damaligen Zeitpunkt nicht als Maßnahmen zur Wahrung der Rechte und Freiheiten im Rahmen einer Verbotsausnahme nach Art. 22 Abs. 2 lit. b DS-GVO bestimmt waren. Unbeschadet dessen verbleiben noch nachfolgende Nachbesserungs- beziehungsweise Ergänzungserfordernisse:

a) § 37a Abs. 2 Nr. 1 lit. b BDSG-E – Klärung des Begriffs „soziale Netzwerke“

Im Interesse der Rechtssicherheit empfiehlt die DSK, eine über die Begründung hinausgehende gesetzliche Präzisierung des Begriffs „sozialer Netzwerke“ im Kontext von Scoring aufzunehmen, die sich auch auf aus Nutzersicht nicht kommerzielle Angebote wie „X“ (vormals „Twitter“) oder „Telegram“ erstreckt.

b) § 37a Abs. 2 Nr. 1 lit. c BDSG-E – Klärung der Begriffe „Zahlungseingänge und -ausgänge“

Die im BDSG nicht anderweitig vorgeprägte Begrifflichkeit „Zahlungseingänge und -ausgänge“ sollte jedenfalls in der Gesetzesbegründung angesichts der Sensibilität dieser Daten konkretisiert werden. Zur Vermeidung von Rechtsunsicherheiten ist klarzustellen, dass davon nicht nur Salden oder der Nennwert von Gutschriften und Belastungen umfasst sind, sondern auch Verwendungszweck, Anweisende, Zahlungsempfänger, Zeitpunkt und ggf. Ort oder Zahlungsmittel, an dem oder durch das Buchungen ausgelöst wurden.

Das Verhältnis zu besonderen gesetzlichen Vorgaben, insbesondere der Kreditwürdigkeitsprüfung (z. B. §§ 18, 18a KWG; §§ 505a, 505b BGB) durch Kreditinstitute, ist nicht im Gesetzestext geregelt und erschließt sich systematisch allenfalls über die allgemeine Regelung zum Vorrang bereichsspezifischer Datenschutzregelungen. Angesichts der Besonderheiten einer Ausnahmeregelung auf Grundlage von Art.22 Abs. 2 lit. b DS-GVO empfiehlt die DSK, eine Klarstellung im Normtext zu prüfen.

c) § 37a Abs. 2 Nr. 1 BDSG-E – fehlende Diskriminierungsverbote

Unbeschadet künftiger Anforderungen der KI-Verordnung hält es die DSK anknüpfend an ihre bisherigen Handlungsempfehlungen für erforderlich, in § 37a Abs. 2 Nr. 1 BDSG-E in Anlehnung an das AGG, ein Verbot der Nutzung von Daten zum Alter (für Wahrscheinlichkeitswerte im Sinne von § 37a Abs. 1 Nr. 1 BDSG-E) und zum Geschlecht der betroffenen Person als Grundlagen der Erstellung oder Verwendung eines Wahrscheinlichkeitswertes zu prüfen.

d) § 37a Abs. 2 BDSG-E – fehlende Anforderungen an Datenrichtigkeit und -aktualität

In ihrer Stellungnahme vom 11.05.2023² hatte die DSK empfohlen, Verfahren zur Sicherstellung richtiger und aktueller Daten für das Scoring zu implementieren. Diese Empfehlung hat keinen Eingang in § 37a BDSG-E gefunden. Die Richtigkeit und Aktualität der für die Berechnung herangezogenen Daten stellt indes ein entscheidendes Kriterium für eine valide und aussagekräftige Wahrscheinlichkeitsberechnung dar, deren Bedeutung für die Interessenabwägung auch der EuGH unterstreicht (Urt. v. 7.12.2023, Rs. C 26/22, Rn. 93 [Hervorhebung

² https://www.datenschutzkonferenz-online.de/media/st/DSK-Handlungsempfehlungen_Verbesserung_des_Datenschutzes_bei_Scoringverfahren.pdf.

durch Verf.]: „Zur Abwägung der verfolgten berechtigten Interessen ist festzustellen, dass die Analyse einer Wirtschaftsauskunftei insoweit, als sie eine objektive und zuverlässige Bewertung der Kreditwürdigkeit der potenziellen Kunden der Vertragspartner der Wirtschaftsauskunftei ermöglicht, Informationsunterschiede ausgleichen und damit Betrugsrisiken und andere Unsicherheiten verringern kann.“)

Dementsprechend sollten entsprechende Anforderungen übergreifend in § 37a BDSG-E festgelegt werden.

e) § 37a Abs. 2 Nr. 3 lit. a BDSG-E – fehlendes Zertifizierungserfordernis für die zu Grunde zu legenden wissenschaftlich anerkannten mathematisch-statistischen Verfahren

Abweichend von den DSK-Handlungsempfehlungen verzichtet der Gesetzentwurf bislang darauf, in § 37a Abs. 2 Nr. 3 lit. a BDSG-E eine formale Zertifizierung für die dem Scoring zu Grunde zu legenden wissenschaftlich anerkannten mathematisch-statistischen Verfahren zu fordern. Das Merkmal der Nachweisbarkeit schafft dazu zwar Anknüpfungspunkte, verzichtet aber auf eine rechtssichere und operable Anforderung.

§ 37a Abs. 2 Nr. 3 lit. a BDSG-E sollte daher durch folgenden Satz ergänzt werden:

„Die Erheblichkeit eines bestimmten Verhaltens für die Berechnung der Wahrscheinlichkeitswerte ist durch eine unabhängige Stelle im Rahmen eines anerkannten Zertifizierungsverfahrens zu bestätigen.“

f) § 37a Abs. 4 BDSG-E – proaktive Transparenzpflichten; Präzisierung der maßgeblichen Kriterien

(1) Die Informationen nach § 37a Abs. 4 BDSG-E sollten den betroffenen Personen nicht nur antragsabhängig, sondern proaktiv bei Übermittlung eines Scorewertes mitgeteilt werden.

Die DSK schlägt daher vor, in § 37a Abs. 4 BDSG-E die Wörter „auf Antrag“ zu streichen.

(2) § 37a Abs. 4 Nr. 2 BDSG-E verlangt eine Beauskunftung der Kriterien, die den Wahrscheinlichkeitswert „am stärksten beeinflussen“ und greift damit grundsätzliche Handlungsempfehlungen der DSK zur Verbesserung der Betroffeneninformationen auf. Allerdings sollte der unbestimmte Rechtsbegriff zumindest im Rahmen der Begründung über die bisherigen Aussagen hinaus konkretisiert werden oder anknüpfend an den Schlussantrag des Generalanwalts in der Rechtssache C-634/21 (Rn. 58) jedenfalls das Ziel der Information benennen, nämlich der betroffenen Person

die für eine etwaige Anfechtung der „Entscheidung“ maßgeblichen und dienlichen Informationen bereitzustellen.

g) § 37a Abs. 6 BDSG-E – Präzisierung spezifischer Betroffenenrechte

Um die Effektivität der Schutzrechte für betroffene Personen zu stärken, sollte anknüpfend an Art. 21 Abs. 4 DS-GVO eine Anforderung aufgenommen werden, die zum Hinweis auf diese Schutzrechte in verständlicher und von anderen Informationen getrennter Form verpflichtet.

Die DSK schlägt vor, § 37a Abs. 6 BDSG-E um folgenden Satz zu ergänzen:

„Verantwortliche haben die betroffene Person spätestens bei der Mitteilung ihrer Entscheidung über ihre Rechte nach Satz 1 in verständlicher und von anderen Informationen getrennter Form zu unterrichten.“

5. Länderübergreifende Datenverarbeitungsvorhaben (§ 40a; § 27 Abs. 5 BDSG-E)

Die Datenschutzaufsichtsbehörden der Länder unterstützen das Ansinnen des Gesetzgebers, die einheitliche und effektive Durchsetzung des Datenschutzes in Deutschland zu stärken. Neben anderen Maßnahmen, vor allem der Stärkung der DSK durch Institutionalisierung, kann die Festlegung einer (alleinigen oder federführenden) Aufsichtsbehörde für länderübergreifende Datenverarbeitungen nichtöffentlicher Stellen dafür eine geeignete Maßnahme sein, insbesondere um die Zahl der notwendigen Ansprechpartner für Unternehmen und Forschungseinrichtungen zu reduzieren und Parallelverfahren zu vermeiden.

Die Einführung solcher neuen Zuständigkeitszuweisungen bringt aber nur dann die angestrebte höhere Effektivität und Rechtssicherheit, wenn sie nicht selbst zur Rechtsunsicherheit beiträgt. In diesem Fall sind die in § 40a BDSG-E herangezogenen Tatbestandsmerkmale nicht so eindeutig, wie es erscheinen mag. Denn die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO ist in der Praxis immer wieder im Einzelnen umstritten, etwa im Kontext von konzerninterner Datenverarbeitung. Es bedarf daher zumindest einer vorgeschalteten Prüfung durch die beteiligten Aufsichtsbehörden, ob eine gemeinsame Verantwortlichkeit überhaupt vorliegt und wie eine gemeinsam verantwortete Verarbeitung sich von anderen Verarbeitungen der beteiligten Unternehmen abgrenzen lässt. Diese Feststellung kann nicht in der Hoheit der verantwortlichen Unternehmen liegen. So schlägt die DSK vor, statt einer Anzeige der Unternehmen einen Antrag an die Aufsichtsbehörden zur geänderten

Zuständigkeit vorzusehen. Innerhalb einer gesetzlich definierten Prüffrist ab Vorliegen aussagekräftiger Unterlagen müssten dann die Aufsichtsbehörden diesen Antrag bescheiden.

Die DSK weist darauf hin, dass die verlagerte Zuständigkeit dazu führen würde, dass die Aufsichtsbehörde, zu der sich Zuständigkeiten verlagert hätten, dann auch in anderen Ländern hoheitlich tätig werden müsste. Es wäre zu prüfen, ob die damit verbundenen Fragen der örtlich erweiterten Geltung weiteren Regelungsbedarf auslösen.

Verbesserungsfähig ist die Definition des Adressatenkreises der Regelungen: „Verantwortliche, die nicht oder nicht ausschließlich Unternehmen sind“ (§ 27 Abs. 5 BDSG-E) ist nicht hinreichend bestimmt. Beispielsweise sind öffentliche Stellen nicht ausreichend klar vom Anwendungsbereich der Regelung ausgenommen.

Zudem erscheint eine Beschränkung der Regelung des § 40a BDSG-E lediglich auf Verfahren von Unternehmen nicht schlüssig. Ein tatsächlich häufiger Anwendungsbereich von Verfahren mit gemeinschaftlicher Verantwortung ist auch bei anderen nichtöffentlichen Stellen, z. B. im Zusammenspiel von Vereinen und übergeordneten Verbänden, zu finden.

Zuletzt sei darauf hingewiesen, dass die Kohärenzregelungen zwar Vorteile für die beteiligten Verantwortlichen haben können; die Rechtsfolgen für die von der Datenverarbeitung betroffenen Personen dürfen aber nicht aus dem Blick geraten.

III. Weitergehender Änderungsbedarf

1. Sofortige Vollziehbarkeit von Verwaltungsakten gegenüber öffentlichen Stellen (§ 20 Abs. 7 BDSG)

Der gegenwärtige Ausschluss der sofortigen Vollziehung von Verwaltungsakten in § 20 Abs. 7 BDSG führt in der Praxis dazu, dass die Datenschutzaufsicht in dringlichen Fällen nicht effektiv ausgeübt werden kann.

Jede Aufsichtsbehörde kann gemäß Art. 58 Abs. 2 DS-GVO und Art. 47 Abs. 2 der Richtlinie (EU) 2016/680 verbindliche Anordnungen gegenüber öffentlichen Stellen treffen. Nach Art. 58 Abs. 4 DS-GVO und Art. 47 Abs. 4 der Richtlinie (EU) 2016/680 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 DS-GVO und der in der Richtlinie (EU) 2016/680 normierten Grundsätze behindert wird. Das ist allerdings derzeit der Fall.

Ein rechtliches Defizit liegt in § 20 Abs. 7 BDSG begründet, wonach die Aufsichtsbehörde gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Abs. 2 S. 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 Abs. 7 BDSG gegen die Vorgaben der DS-GVO: Die Aufsichtsbehörde muss gemäß Art. 58 Abs. 2 DS-GVO 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 Abs. 7 BDSG ist zudem auch zum Schutz der betroffenen Behörde nicht erforderlich, weil diese in ihrem Handeln ihrerseits durch § 80 Abs. 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.

§ 20 Abs. 7 BDSG sollte daher gestrichen werden.

2. Anwendbare Vorschriften des Ordnungswidrigkeitengesetzes und des Gesetzes gegen Wettbewerbsbeschränkungen für Verstöße nach Art. 83 DS-GVO (§ 41 BDSG)

Gemäß § 41 Abs. 1 S. 1 BDSG gelten für Verstöße nach Art. 83 Abs. 4 bis 6 DS-GVO, soweit das BDSG nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Nach § 41 Abs. 1 S. 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 Personenvereinigungen für Bußgeldverstöße Geltung haben sollen. Dies würde jedoch den Vorgaben der DS-GVO widersprechen.

§ 30 Abs. 1 OWiG basiert auf dem sog. Rechtsträgerprinzip und normiert, dass die Verhängung von Bußgeldern gegen juristische Personen davon abhängt, dass der

konkrete Verstoß einer in § 30 Abs. 1 OWiG benannten Leitungsperson festgestellt wird. Der EuGH hat durch Urteil vom 5. Dezember 2023 (C-807/21 – Deutsche Wohnen) nunmehr festgestellt, dass das deutsche Rechtsträgerprinzip der Harmonisierung der DS-GVO entgegensteht. So heißt es konkret im Tenor zu 1 der zuvor genannten Entscheidung: „Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 der [DS-GVO] sind dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DS-GVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde“.

Damit stellt das Gericht klar, dass juristische Personen dafür verantwortlich sind, dass personenbezogene Daten im Rahmen ihrer unternehmerischen Tätigkeit rechtmäßig verarbeitet werden (vgl. Rn. 44). Erfasst sind deshalb nicht nur wie bisher die gesetzlichen Vertreter oder Leitungspersonen (§ 30 Abs. 1 OWiG), sondern sämtliche Mitarbeitende des Unternehmens oder der Unternehmensvereinigung (vgl. auch EuGH, Urteil vom 5. Dezember 2023 – C-807/21, Rn. 60, 77).

Das heißt, es wird die „soziale Einheit“ des Unternehmens sanktioniert, die mitunter fehlorganisiert sein könnte – nicht der Unternehmensträger (so KG, Beschl. v. 22. Januar 2024 – 161 AR 84/2, Rn. 14 m. Verweis auf Gassner/Seith, Ordnungswidrigkeitengesetz, 2. Aufl. 2020 § 30 Rn. 13). Folglich fallen alle Personen, die im Rahmen der unternehmerischen Tätigkeit handeln, in den abstrakten Verantwortungsbereich der juristischen Person (KG, Beschl. v. 22. Januar 2024 – 161 AR 84/2 mit Bezug zu EuGH, Urteil vom 5. Dezember 2023, – C 807/21).

Eine Kenntnis der Inhaber oder Geschäftsführer des Unternehmens von der konkreten Handlung ist für die Zuordnung der Verantwortlichkeit nicht erforderlich (EuGH, Urteil vom 5. Dezember 2023 – C-807/21, Rn. 77 m. w. N.), wobei Exzesse ausgenommen sind (vgl. EuGH, Urteil vom 5. Dezember 2023 – C-807/21, Rn. 44). Daher läuft eine Weitergeltung des § 30 Abs. 1 OWiG über § 41 Abs. 1 S. 1 und 2 BDSG den Vorgaben der DS-GVO zuwider. Die Aufsichtsbehörden sind aufgrund des Anwendungsvorrangs des EU-Rechts derzeit verpflichtet, § 41 Abs. 1 S. 1 und 2 BDSG in Bezug auf die Weitergeltung des § 30 Abs. 1 OWiG unangewendet zu lassen (vgl. EuGH, Urteil vom 22. Juni 1989 – C-103/88, Rn. 28 ff.).

§ 30 Abs. 2a S. 1 und 3 OWiG haben in § 81a Abs. 2 GWB eine Parallelvorschrift, sodass nicht unbedingt Teile des § 30 anwendbar gelassen werden müssen. Ohnehin müssten Normen des GWB zusätzlich Anwendung finden, damit das Kartellbußrecht besser

nachgebildet wird, bestehende Zurechnungslücken geschlossen werden und ein der Schwere der Bußgeldandrohung angemessenes Verfahren gewährleistet ist.

Dies auch, weil der EuGH in seinem o. g. Urteil explizit darauf verweist, dass der Umsatzbegriff der DS-GVO dem des Kartellrechts gleich ist um „die in Art. 83 Abs. 1 DS-GVO genannten Voraussetzungen [einer Geldbuße zu] erfüllen, sowohl wirksam und verhältnismäßig als auch abschreckend zu sein“ (EuGH, Urteil vom 5. Dezember 2023 – C-807/21, Rn. 58). So heißt es dort: „Daher ist eine Aufsichtsbehörde, wenn sie aufgrund ihrer Befugnisse nach Art. 58 Abs. 2 DS-GVO beschließt, gegen einen Verantwortlichen, der ein Unternehmen im Sinne der Art. 101 und 102 AEUV ist oder einem solchen angehört, eine Geldbuße gemäß Art. 83 DS-GVO zu verhängen, nach Art. 83 im Licht des 150. Erwägungsgrundes der DS-GVO verpflichtet, bei der Berechnung der Geldbußen für die in Art. 83 Abs. 4 bis 6 DS-GVO genannten Verstöße den Begriff ‚Unternehmen‘ im Sinne der Art. 101 und 102 AEUV zugrunde zu legen.“ (EuGH, Urteil vom 5. Dezember 2023 – C-807/21 Rn. 59).

In Anlehnung an § 83 Abs. 2 GWB sollte zumindest auch deklaratorisch § 41 Abs. 1 BDSG um eine spezifischere Festlegung ergänzt werden, der die funktionale Besetzung der Kammern bei den Landgerichten regelt.

Es wird daher empfohlen,

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

Um sicherzustellen, dass § 30 Abs. 2a S. 1 und 3 OWiG anwendbar bleiben (Bußgeld gegen Gesamtrechtsnachfolger) und das Verfahrensrecht des GWB nachgebildet wird, sollte in § 41 Abs. 1 BDSG folgender S. 3 ergänzt werden:

„§§ 59, 59b Absatz 3, 81 Absatz 2 Nr. 6 bis 11 i. V. m. § 81c, § 81a Absatz 2 bis 5, § 81b, § 81e, § 81f, § 81g Absatz 2, § 82b des Gesetzes gegen Wettbewerbsbeschränkungen sind entsprechend anwendbar; Geldbußen im Sinne jener Vorschriften sind solche wegen Verstößen gegen die Verordnung (EU) 679/2016, abweichend hiervon in den Fällen des § 81 Abs. 2 Nr. 6 bis 11 solche nach § 81c.“

Für die spezifische Festlegung der funktionalen Besetzung der Kammern bei den Landgerichten sollte in § 41 Abs. 1 BDSG folgender Satz 5 ergänzt werden:

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

Die für entsprechend anwendbar zu erklärenden Vorschriften des GWB umfassen:

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

3. Aufnahme einer Befugnis zur Einziehung von Gegenständen in § 41 BDSG

Die Bußgeldstellen der Aufsichtsbehörden benötigen die Befugnis zur Einziehung und zur erweiterten Einziehung von Gegenständen.

Nach Art. 83 Abs. 8 DS-GVO muss die Ausübung der Befugnisse der Aufsichtsbehörden angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedsstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren unterliegen. Die Sanktionierung soll dabei nach Art. 83 Abs. 1 DS-GVO in jedem Fall wirksam, verhältnismäßig und abschreckend sein, um das von Erwägungsgrund 148 genannte Ziel der konsequenteren Durchsetzung der Vorschriften der Verordnung zu verfolgen. Aus den Erwägungsgründen zur DS-GVO ergibt sich dabei, dass der nationale Gesetzgeber auch Nebenfolgen zur Geldbuße

vorsehen kann (s. etwa die Erwähnung der Einziehung des Gewinns in Erwägungsgrund 149).

Gemäß § 41 Abs. 1 BDSG finden insoweit grundsätzlich die Regelungen des Ordnungswidrigkeitengesetzes (OWiG) Anwendung. Das Ordnungswidrigkeitengesetz sieht dabei allerdings die Einziehung von Gegenständen bei Ordnungswidrigkeiten nur dann vor, wenn eine spezialgesetzliche Regelung dies ausdrücklich zulässt (§ 22 Abs. 1 und § 23 OWiG). Bislang gibt es jedoch kein solches Androhungsgesetz (s. zum Begriff BeckOK OWiG/Sackreuther, 41. Ed. 1.1.2024, OWiG § 22 Rn. 16) für Ordnungswidrigkeiten im Sinne des Art. 83 DS-GVO.

Bereits der hohe Bußgeldrahmen des Art. 83 DS-GVO zeigt, dass aus Sicht des Gesetzgebers Datenschutzverstößen infolge der mit ihnen verbundenen Eingriffe in die Grundrechte betroffener Personen ein erhebliches Gewicht zukommen kann. Die gesetzliche Androhung einer Einziehung von Gegenständen kann schon deshalb nicht als generell unverhältnismäßig angesehen werden – unbeschadet der Notwendigkeit, die Verhältnismäßigkeit bei der Entscheidung über die Anordnung einer solchen Einziehung von Gegenständen im Einzelfall zu prüfen.

Auf der anderen Seite besteht allerdings ein dringender Bedarf, den Aufsichtsbehörden die Möglichkeit zur Einziehung von Gegenständen zu eröffnen, und zwar sowohl hinsichtlich der Tatmittel (z. B. einer beschlagnahmten, rechtswidrig eingesetzten Dashcam) als auch in Bezug auf Tatprodukte (wie beispielsweise einer SIM-Karte mit unrechtmäßig gespeicherten personenbezogenen Daten) sowie in Hinsicht auf Beziehungsgegenstände (z. B. unter Verstoß gegen die erforderlichen technischen und organisatorischen Maßnahmen entsorgte Akten oder sonstige Speichermedien).

Nach der derzeitigen Rechtslage müssen derartige Gegenstände, auch wenn sie beschlagnahmt oder sichergestellt wurden, grundsätzlich wieder an den letzten Gewahrsamsinhaber herausgegeben werden. Dies hat zur Folge, dass der Schutz der betroffenen Personen infolge der Rückgabe des Beweismittels nicht hinreichend gewährleistet ist. Vielmehr besteht derzeit in vielen Fällen weiterhin die Gefahr eines fortdauernden Datenschutzverstoßes.

Der „Verzicht“ auf die Nebenfolge der Einziehung von Gegenständen führt dazu, dass die Aufsichtsbehörden einem Datenschutzverstoß nicht gänzlich abhelfen können und das Bußgeld in der Gesamtschau an Wirksamkeit und Abschreckung durch die Rückgabe der rechtswidrig erlangten Tatprodukte, Tatmittel bzw. Beziehungsgegenstände verliert.

Um dem abzuwehren, besteht daher gesetzgeberischer Handlungsbedarf. Diesem sollte durch folgende Maßnahmen Folge geleistet werden:

In § 41 Abs. 1 sollten nach Satz 1 zwei neue Sätze eingefügt werden:
„Gegenstände, die zur Begehung oder Vorbereitung der Tat gebraucht worden sind, die durch die Tat hervorgebracht wurden oder auf die sich die Tat bezieht, können eingezogen werden. § 23 OWiG findet Anwendung.“

Zugleich bedarf es entgegen der bisherigen Rechtslage eines auf die Einziehung von Gegenständen gerichteten Verfahrensrechts. Dazu sollte die Regelung des § 87 OWiG zur Anwendung gebracht werden, deren Geltung bislang von § 41 Abs. 2 S. 2 BDSG ausgeschlossen wird.

Ergänzend ist daher in § 41 Abs. 2 S. 2 BDSG die Erwähnung von § 87 OWiG zu streichen.

4. Streichung des § 43 Abs. 3 BDSG (Verhängung von Geldbußen auch gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Abs. 1 BDSG)

Gemäß § 43 Abs. 3 BDSG sollen gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Abs. 1 BDSG keine Geldbußen verhängt werden. Der nationale Gesetzgeber hat hier von der Öffnungsklausel des Art. 83 Abs. 7 DS-GVO Gebrauch gemacht.

Wie sich auch in der Praxis gezeigt hat, besteht jedoch ein Bedarf, zur Möglichkeit der Verhängung von Geldbußen auch gegenüber diesen Stellen. Die Verhängung von Geldbußen kommt für leichte bis schwere Verstöße in Betracht. Mangels entsprechender Befugnis besteht gegenüber öffentlichen Stellen derzeit jedoch keine Möglichkeit, die Schwere des Verstoßes gegenüber der beaufsichtigten Stelle hinreichend deutlich zu machen. Darüber hinaus entfalten drohende Geldbußen im Hinblick auf die durch Art. 58 DS-GVO eingeräumten Befugnisse die am meisten abschreckende Wirkung und dienen folglich der Sicherstellung der Einhaltung der Bestimmungen der DS-GVO, indem Datenschutzverstößen aktiv vorgebeugt werden würde.

Die Möglichkeit zur Verhängung von Geldbußen ist zudem aus Gründen der Gleichbehandlung von öffentlichen und nichtöffentlichen Stellen erforderlich. Die Argumentation des Bundesministeriums für Inneres und für Heimat in seinem Bericht zur Evaluierung des BDSG aus dem Jahr 2021, nachdem die Verhängung von Geldbußen lediglich eine Verschiebung von Haushaltsmitteln des Bundes zwischen öffentlichen Stellen des Bundes zur Folge hätte und somit keine sachliche Vergleichbarkeit zu

nichtöffentlichen Stellen bestünde (S. 67), greift nach Ansicht der DSK zu kurz, denn der Sanktionscharakter eines Bußgeldes besteht aufgrund der eigenen Haushaltsbetroffenheit der jeweiligen Stelle uneingeschränkt. Die abschreckende Wirkung von drohenden Geldbußen führt letztlich auch dazu, dass (durch die damit einhergehende Motivation zur Einhaltung der datenschutzrechtlichen Bestimmungen) vermieden wird, dass öffentliche Mittel für mögliche Schadensersatzansprüche von betroffenen Personen gemäß Art. 82 DS-GVO verwendet werden müssen.

§ 43 Abs. 3 BDSG sollte daher gestrichen werden.

Alternativ sollte § 43 Abs. 3 BDSG dahingehend geändert werden, dass er wie folgt lautet:

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

5. Bedarf einer bereichsspezifischen Ausnahmeregelung i. S. v. § 17 VwVG

Nach § 17 VwVG sind Zwangsmittel gegen Behörden und juristische Personen des öffentlichen Rechts unzulässig, soweit nicht etwas anderes bestimmt ist. Das BDSG enthält keine Regelung i. S. v. § 17 VwVG. Ohne eine entsprechende Regelung können Anordnungen des BfDI entgegen den Vorgaben der DS-GVO und der Richtlinie (EU) 2016/680 zu deren Verbindlichkeit nicht vollstreckt werden. Die fehlende Vollstreckbarkeit von Anweisungen und Untersagungen durch Zwangsmittel gegenüber Behörden und juristische Personen des öffentlichen Rechts verstößt gegen das europäische Effektivitätsgebot. Für andere Aufsichtsbehörden gibt es teilweise bereits entsprechende Regelungen (vgl. § 17 Abs. 1 S. 3 FinDaG, § 22 Abs. 3 S. 4 ArbSchG). Nach Auffassung der DSK sollte im Sinne der zweiten Alternative des § 17 VwVG „etwas anderes bestimmt“ § 16 BDSG dahingehend ergänzt werden, dass auch dem BfDI die Anwendung von Zwangsmitteln im Fall des Nichtnachkommens von Anordnungen durch öffentliche Stellen ausdrücklich erlaubt wird.

6. Anwendbarkeit des für nichtöffentliche Stellen geltenden Rechts für Religionsgemeinschaften

Im BDSG sollte eine Regelung zu dem für Religionsgemeinschaften, Kirchen und weltanschauliche Gemeinschaften in der Rechtsform der Körperschaft des öffentlichen

Rechts geltenden Datenschutzrecht aufgenommen werden. Soweit die Körperschaften nicht nach Art. 91 DS-GVO eigene umfassende Datenschutzregeln anwenden, sind die DS-GVO und das nationale Datenschutzrecht anwendbar. Dabei ist jedoch unklar, ob sie als öffentliche oder als nichtöffentliche Stelle zu behandeln sind.

Das Verwaltungsgericht Hannover hat dazu im Urteil vom 30. November 2022, 10 A 1195/21 festgestellt:

„Insoweit ist allerdings problematisch, dass die Religionsgesellschaften, die – wie die Kl. – nach Art. 140 GG i. V. m. Art. 137 Abs. 5 WRV den Status einer Körperschaft des öffentlichen Rechts haben, einerseits schon in Ermangelung einer staatlichen Aufsicht (BVerfGE 139, 321 Rn. 91, mwN) jedenfalls keine öffentlichen Stellen des Bundes i. S. d. § 2 Abs. 1 bis Abs. 3 BDSG und auch keine öffentlichen Stellen des Landes i. S. d. § 1 Abs. 1 NDSG sind (Kühling/Buchner/Klar/Kühling, DS-GVO/BDSG, BDSG § 2 Rn. 5). Andererseits sind sie aber – anders als Religionsgesellschaften, die rein privatrechtlich (z. B. als Verein) organisiert sind – auch keine juristischen Personen des Privatrechts i. e. S. und damit grds. auch keine nicht-öffentlichen Stellen i. S. d. § 2 Abs. 4 BDSG. Die Gesetzgeber in Bund und Ländern ordnen die öffentlich-rechtlichen Religionsgesellschaften vielmehr weder dem einen noch dem anderen Bereich zu (Simitis/Hornung/Spiecker/Seifert, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 91 Rn. 3; Dammann NVwZ 1992, 1147 ff. (zum BDSG aF); vgl. ferner § 5 Abs. 1 S. 4 NDSG). Deswegen unterfallen die Religionsgesellschaften, die den Status einer Körperschaft des öffentlichen Rechts haben, aber – zumindest auf den ersten Blick – auch weder der Regelung über die Zuständigkeit des BfDI in § 9 Abs. 1 BDSG noch den für die Bekl. geltenden Zuständigkeitsregelungen in § 40 Abs. 1 und Abs. 2 BDSG und den §§ 18 ff. NDSG, weil diese jeweils an den Status der oder des zu Beaufsichtigenden als öffentliche oder nicht-öffentliche Stelle anknüpfen. Vielmehr fehlt es bei reiner Betrachtung des Wortlauts der Datenschutzgesetze in Deutschland insoweit an der nach Art. 51 Abs. 1 DS-GVO erforderlichen Bestimmung einer Aufsichtsbehörde. Eine solche Bestimmung kann auch nicht durch einen Rückgriff auf die DS-GVO ersetzt werden, weil diese zwar vorschreibt, dass es eine Aufsichtsbehörde geben muss, jedoch keine hier brauchbaren Direktiven für die Auswahl unter mehreren in einem Mitgliedstaat vorhandenen Aufsichtsbehörden enthält. Da die DS-GVO auch für die Verarbeitung personenbezogener Daten durch Religionsgesellschaften, die den Status einer Körperschaft des öffentlichen Rechts haben, Geltung beansprucht, wie sich aus Art. 91 DS-GVO unzweifelhaft ergibt, hätte Deutschland damit

insoweit seine unionsrechtliche Verpflichtung aus Art. 51 Abs. 1 DS-GVO verletzt.“

Dies hat das Verwaltungsgericht Hannover gelöst, indem es durch europarechtskonforme Auslegung der nationalen Zuständigkeitsregelungen die für nichtöffentlichen Stellen geltenden Vorschriften auch auf die Religionsgemeinschaften als Körperschaften des öffentlichen Rechts angewendet hat. Danach ist die Datenschutzaufsichtsbehörde des Landes die für die Körperschaft zuständige Datenschutzaufsichtsbehörde. Das Urteil ist nicht rechtskräftig. Ob andere Gerichte gleich entscheiden, ist ungewiss.

Die DSK spricht sich für eine gesetzliche Regelung der vom Verwaltungsgericht Hannover angewandten Lösung im BDSG aus, damit diese Frage innerhalb Deutschlands einheitlich geklärt wird.