20. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 80. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 24. Juni 2024, 14:00 Uhr
Konrad-Adenauer-Str. 1, 10557 Berlin
Paul-Löbe-Haus, Raum E 600

Vorsitz: Petra Pau, MdB

Tagesordnung - Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

BT-Drucksache 20/10859

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Rechtsausschuss
Ausschuss für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
Ausschuss für Digitales

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Carmen Wegge [SPD]
Abg. Marc Henrichmann [CDU/CSU]
Abg. Misbah Khan [BÜNDNIS 90/DIE GRÜNEN]
Abg. Manuel Höferlin [FDP]
Abg. Steffen Janich [AfD]
Abg. Martina Renner [Die Linke]

Inhaltsverzeichnis

Dem Ausschuss sind die vorliegenden Stellungnahmen teilweise in nicht barrierefreier Form zugeleitet worden.

Anwesende Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
SPD	Wegge, Carmen	
CDU/CSU	Henrichmann, Marc	
BÜNDNIS 90/DIE GRÜNEN	Khan, Misbah	
FDP	Höferlin, Manuel	
AfD	Janich, Steffen	
Die Linke	Pau, Petra	
BSW	Ernst, Klaus	
fraktionslos		

Liste der Sachverständigen
Öffentliche Anhörung am Montag, 24. Juni 2024, 14.00 Uhr
„Bundesdatenschutzgesetz“

Prof. Ulrich Kelber[5)]
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn

Matthias Marx[3)]
Chaos Computer Club, Hamburg

Johannes Müller[1)]
Verbraucherzentrale Bundesverband e. V., Berlin

Prof. Dr. Boris P. Paal, M.Jur. (Oxford)[2)]
Lehrstuhl für Law and Regulation of the Digital Transformation
TUM School of Social Sciences and Technology, München

Prof. Eike Richter[4)]
Akademie der Polizei Hamburg
Professur für Öffentliches Recht, insbesondere Recht der Digitalisierung und IT-Sicherheitsrecht Netzwerk Digitale

Prof. Dr. Alexander Roßnagel[1)]
Hessischer Beauftragter für Datenschutz und Informationsfreiheit,
Vorsitzender der Datenschutzkonferenz

Dr. Simone Ruf[3)]
Gesellschaft für Freiheitsrechte e. V., Berlin

Prof. Dr. Meinhard Schröder[2)]
Universität Passau
Lehrstuhl für Öffentliches Recht, Europarecht und Informationstechnologierecht

Prof. Dr. Luisa Specht-Riemenschneider[1)]
Universität Bonn
Lehrstuhl für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz

Prof. Dr. Gregor Thüsing, LL.M. (Harvard)[2)]
Universität Bonn
Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit

---
1) Vorschlag: SPD
2) Vorschlag: CDU/CSU
3) Vorschlag: BÜNDNIS 90/DIE GRÜNEN
4) Vorschlag: FDP
5) Gemäß § 69a Abs. 3 GO BT

Gesetzentwurf der Bundesregierung

Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

BT-Drucksache 20/10859

AVors. **Petra Pau** (Die Linke): Liebe Kolleginnen und Kollegen, sehr geehrte Damen und Herren, ich eröffne die 80. Sitzung des Ausschusses für Inneres und Heimat und begrüße Sie alle sehr herzlich. Mein Name ist Petra Pau. Ich bin die amtierende oder Altersvorsitzende des Ausschusses für Inneres und Heimat und werde die öffentliche Anhörung von Sachverständigen leiten.

Ich danke Ihnen allen, sehr geehrte Sachverständige, dass Sie unserer Einladung nachgekommen sind und uns mit Ihrer Expertise zur Verfügung stehen, um die Fragen der Kolleginnen und Kollegen aus dem Ausschuss für Inneres und Heimat und der mit-beratenden Ausschüsse zu beantworten. Daher begrüße ich zunächst die von den Fraktionen benannten und hier anwesenden Sachverständigen: Herrn Professor Ulrich Kelber, Herrn Matthias Marx, Herrn Johannes Müller, Herrn Professor Eike Richter, Herrn Professor Dr. Alexander Roßnagel, Frau Dr. Simone Ruf, Frau Professorin Dr. Luisa Specht-Riemenschneider und Herrn Professor Dr. Gregor Thüsing. Ich begrüße außerdem die per Videokonferenz zugeschalteten Sachverständigen: Herrn Professor Dr. Boris P. Paal und Herrn Professor Dr. Meinhard Schröder. Und zugeschaltet sollte die Kollegin Mechthilde Wittmann sein, was aber bisher noch nicht der Fall ist. Für die Bundesregierung darf ich dann Herrn Ministerialdirigenten Dr. Andreas Mom aus dem Bundesministerium des Innern und für Heimat willkommen heißen.

Die gesamte Sitzung wird live im Parlamentsfernsehen und auf der Homepage des Deutschen Bundestages übertragen und ab morgen über die Mediathek für die Öffentlichkeit zum Abruf bereitgestellt.

Wir hatten schriftliche Stellungnahmen erbeten, für die eingegangenen Stellungnahmen bedanke ich mich bei den Sachverständigen herzlich, sie sind an die Ausschussmitglieder verteilt worden und werden auch dem Protokoll unserer Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur Durchführung der öffentlichen Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamt-drucksache umfasst. Von der heutigen Anhörung wird ein Wortprotokoll erstellt und Ihnen, werte Sachverständige, zur Korrektur übersandt. Im Anschreiben werden Ihnen Details zur Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus Protokoll und schriftlichen Stellungnahmen, wird im Übrigen dann auch ins Internet eingestellt.

Für die Anhörung ist die Zeit von 14:00 bis 16:00 Uhr vorgesehen. Einleitend möchte ich jedem Sachverständigen die Gelegenheit geben, in einer kurzen Einleitung, die drei Minuten nicht über-schreiten sollte, zum Beratungsgegenstand Stellung zu beziehen. Ich bitte Sie ausdrücklich, sich angesichts der Vielzahl von Sachverständigen an dieses Zeitfenster zu halten, damit ausreichend Zeit für Fragen durch die Abgeordneten besteht. Ihre umfassenden schriftlichen Stellungnahmen sind den Ausschussmitgliedern zugegangen und damit bekannt. Nach den Eingangsstatements werden wir orientiert an Fraktionsrunden mit der Befragung der Sachverständigen beginnen. Ich bitte, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die sie die Fragen richten wollen. Zu den Frageregeln gilt: In der ersten Fraktionsrunde kann jeder Fragesteller entweder zwei Fragen an einen Sachverständigen oder je eine Frage an zwei Sachverständige richten. Für die Fragen gilt eine Zwei-Minuten-Zeitbegrenzung. Die Auskunftsperson antwortet unmittelbar auf die Frage. Für die Antwort auf jede Frage stehen ebenfalls zwei Minuten zur Verfügung. In der zweiten Fraktionsrunde werde ich angesichts der dann verbrauchten Zeit situativ entscheiden, ob das Zeitfenster weiterhin zwei oder nur noch eine Frage zulässt. Wenn Sie damit einverstanden sind, werden wir so verfahren. Das ist offensichtlich der Fall, danke. Dann darf ich entsprechend alphabetischer Reihenfolge Herrn Professor Kelber um sein Eingangsstatement bitten.

SV **Prof. Ulrich Kelber** (BfDI): Sehr geehrte Frau Vorsitzende, meine sehr geehrten Damen und Herren Abgeordnete, herzlichen Dank für die Möglichkeit, heute zum Gesetzentwurf Stellung nehmen zu können. Der Gesetzentwurf zielt darauf ab, die im Koalitionsvertrag getroffenen Vereinbarungen zur Institutionalisierung der Datenschutzkonferenz sowie zur besseren Durchsetzung und Kohärenz des Datenschutzrechtes sicherzustellen. Dieses Vorhaben begrüße ich natürlich und ich konnte in der Ressortabstimmung, an der ich frühzeitig und umfassend beteiligt worden bin, viele Vorschläge bereits einbringen. Ein Beispiel: Die erforderliche Klarstellung in § 18 Absatz 2 BDSG, dass die Aufsichtsbehörden in Deutschland bereits in Kooperations- und Dringlichkeitsverfahren auf europäischer Ebene koordiniert vorgehen – das sichert ein einheitliches Auftreten. Ich kann Ihnen erzählen, dass es vor fünf Jahren einmal leider einen anderslautenden Fall gab, der die

deutsche Position damals nachhaltig geschädigt hat und lange aufgearbeitet werden musste. Nicht berücksichtigt wurde unter anderem mein Vorschlag, die Aufsichts-zuständigkeit des BfDI für Verstöße durch Beschäftigte von Bundesbehörden vorzusehen, die zum Beispiel personenbezogene Daten der Behörden für eigene Zwecke missbrauchen – den sogenannten Mitarbeiterexzess. Wo ist das Problem? Nach aktueller Rechtslage ist der BfDI Aufsichtsbehörde für die Bundesbehörde und die jeweiligen Landesdatenschutzbehörden für den den Exzess begehenden Mitarbeiter der gleichen Behörde. Eine einheitliche Aufsicht könnte aber in einem neuen Absatz 2 in § 9 BDSG erfolgen. Damit würde vermieden, dass mehrere Datenschutzaufsichtsbehörden die Datenbestände der Bundesverwaltung kennenlernen, damit in Berührung kommen – darunter natürlich auch sensible Daten und Bereiche der Sicherheitsbehörden. Meine Kolleginnen und Kollegen aus den Ländern unterstützen diese Regelung.

Es gibt die Evaluierung des Bundesdatenschutzgesetzes aus dem Jahr 2021, dazu auch eine Stellungnahme der Datenschutzkonferenz. Dort sind noch zwei weitere Punkte schwerpunktmäßig als Beispiel angesprochen: Der erste ist, dass es eine bereichsspezifische Ausnahmeregelung für die Datenschutzaufsichtsbehörde geben muss, um Zwangsmittel gegen andere Behörden und juristische Personen des öffentlichen Rechtes einsetzen zu können, wenn diese den entsprechenden Anordnungen nicht folgen. Das Fehlen dieser Möglichkeit widerspricht aus unserer Sicht auch den europäischen Rechtssetzungen.

Noch wichtiger wäre die Streichung des § 20 Absatz 7 BDSG. Mit der Streichung würde die Möglichkeit geschaffen, als Aufsichtsbehörde gegenüber einer Behörde oder deren Rechtsträgern die sofortige Vollziehung der Maßnahme anordnen zu können. So wie es im Augenblick geltende Rechtslage ist, setzen sich auch schwerwiegendste Datenschutzverstöße über Jahre fort, wenn denn eine Klage eingereicht wird.

Ansonsten darf ich auf die umfangreiche Stellungnahme verweisen.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Nun erhält Matthias Marx das Wort.

SV **Matthias Marx** (CCC): Guten Tag, Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete. Ich spreche heute als Vertreter des Chaos Computer Clubs, werde dabei aber auch ganz persönliche Erfahrungen teilen. Ich möchte über biometrische Fernidentifikationssysteme sprechen, kurz: Gesichtserkennung. Wir fordern ein unmissverständliches Verbot von Gesichtserkennung im öffentlichen Raum. Und genau das fehlt in dem Entwurf. Seit mehr als vier Jahren treibt mich dieses Thema um. Damals wurde Clear View AI bekannt, eine Gesichter-Suchmaschine aus den USA. Ich kann eine App öffnen, ich kann Sie oder jede andere Person, deren Foto im Internet zu finden ist und die ich stalken möchte, identifizieren. Nur dank eines Auskunftsersuchens konnte ich damals heraus-finden, dass Clear View AI Bilder meines Gesichtes gespeichert hat. In der Folge verhängten Datenschutzbehörden in Italien, Griechenland, Frankreich und Großbritannien hohe Bußgelder, da das Unternehmen rechtswidrig biometrische Daten von Millionen Europäer*innen verarbeitete. Ohne Auskunftsersuchen hätte es diesen Erfolg nicht gegeben. Ich hatte mich damals in Hamburg beschwert – dort wurde kein Bußgeld verhängt. Dies scheiterte unter anderem daran, dass die Behörde sich fürchtete, eine Strafe „nur“ für Hamburg auszusprechen. Mit einem für alle Länder bindenden Beschluss der Datenschutzkonferenz sähe das heute vielleicht anders aus.

Zum grundsätzlichen Risiko von Gesichtserkennung: Vor der Gesichtserkennung können wir uns nicht verstecken. Ob ich mich schminke, älter werde, eine Grimasse ziehe oder eine Brille aufsetze – so leicht lassen sich die Algorithmen heute nicht mehr täuschen. In einer frühen Phase der AI-Act-Verhandlungen war ich in Brüssel im Parlament und habe den zweitbesten Schutz gegen Gesichtserkennung präsentiert – eine Papiertüte! Aber das ist aus offensichtlichen Gründen unpraktisch, besser wäre eine strenge Regulierung. Deshalb gibt es jetzt die im AI-Act explizit vorgesehene Möglichkeit der nationalen Verschärfung europäischer Regeln sowohl für Echtzeit-, als auch für nachträgliche biometrische Fernidentifizierung zu nutzen und das Verbot von biometrischer Überwachung im BDSG zu verankern. Denn es sind nicht nur private Unternehmen, die Recht und Gesetz gelegentlich ignorieren, in letzter Zeit häufen sich die Fälle missbräuchlicher Anwendung biometrischer Überwachungssysteme durch Strafverfolgungsbehörden. Und bei allen dieser Versuche müssen wir leider davon ausgehen, dass die Landes- beziehungsweise der Bundesdatenschutzbeauftragte nicht zufällig nicht eingebunden wurden. Das jüngste Beispiel sind Versuche verdeckter Gesichtserkennung aus Transportern am Straßenrand in Sachsen, die Weitergabe von fast fünf Millionen ImpulZ-Gesichtsbildern vor wenigen Monaten an das Fraunhofer-Institut, um Software zu testen – wieder ohne Rechtsgrundlage, und schließlich der Einsatz einer

Gesichtserkennungssoftware im Rahmen von G20 mit mehr als 100 000 Betroffenen. Die Polizei ignorierte eine Löschanordnung und wieder fehlten offenbar Zwangsmittel. Daher: Nutzen Sie die Chance, die sich gerade ergibt! Denken Sie an Ihren Koalitionsvertrag und verhindern Sie, dass bald mehr Leute mit Papiertüten über dem Kopf herumlaufen.

AVors. **Petra Pau** (Die Linke): Der nächste Sachverständige ist Herr Johannes Müller. Bitte.

SV **Johannes Müller** (vzbv): Vielen Dank, Frau Vorsitzende, sehr geehrte Damen und Herren. Ich möchte zuerst den Hinweis geben, dass der Verbraucherzentrale Bundesverband e.V. sich nur zu den §§ 34 Absatz 1 und 37a BDSG geäußert ha, weswegen ich auch nur dazu Stellung nehmen und Fragen beantworten kann. Bonitäts-Scoring durch Wirtschaftsauskunfteien erfüllt grundsätzlich eine legitime Funktion in unserer Wirtschaftsordnung, indem es ein aktives Risikomanagement für Unternehmen ermöglicht. Für Verbraucher*innen besteht allerdings die Gefahr, dass sie durch einen Mangel an Transparenz und eine ausufernde Nutzung gruppenbezogener Datenverarbeitung diskriminiert oder benachteiligt werden, ohne überhaupt etwas davon mitzubekommen und sich dementsprechend wehren zu können. Der vzbz begrüßt daher die Initiative der Bundesregierung, den Rechtsrahmen des Bonitäts-Scorings an das aktuelle Urteil des EuGHs anzupassen und zusätzlich ein höheres Level an Transparenz und fairer Datenverarbeitung anzustreben.

Der Entwurf geht unserer Meinung nach einige Schritte in die richtige Richtung. Der Ausschluss der verschiedensten Datenkategorien wie Daten aus sozialen Medien oder Kontoinformationen tragen dazu bei, die Privatsphäre von Verbraucher*innen zu schützen und besonders der Ausschluss von Adressdaten dient einer fairen Datenverarbeitung, da so sichergestellt werden kann, dass trotz eines guten individuellen Zahlungsverhaltens der Score nicht schlecht ist, nur weil die Nachbarn ihre Rechnungen nicht bezahlen.

Auch in Sachen Transparenz der Scoring-Verfahren lässt der Gesetzentwurf einerseits auf Fortschritte hoffen, enthält allerdings auch Unklarheiten, die beseitigt werden sollten. Die Verpflichtung von Wirtschaftsauskunfteien, die wichtigsten Einfluss-faktoren mit ihrer Gewichtung darzustellen trägt dazu bei, dass Scoring-Ergebnis nachvollziehbar darzustellen und zeichnet das Ende des viel zitierten Blackbox-Scorings vor. Allerdings ist der Entwurf an dieser Stelle nicht eindeutig, was die Zahl der Einflussfaktoren angeht, die beauskunftet werden sollen. Aus unserer Sicht würde es auch möglich sein, dass nur zwei Einflussfaktoren offenbart werden, was zu wenige sind. Außerdem ist nicht klargestellt, wie die Begriffe „Kriterien“ und „Kategorien“ zu verstehen sind. Und die vorgeschlagene Änderung des § 34 Absatz 1 BDSG droht außerhalb des Scorings dazu, pauschale Ablehnungen von Auskunftsersuchen durch Unternehmen zu ermöglichen. Hier sind noch wichtige und bedeutende Klarstellungen und Änderungen notwendig. Danke.

AVors. **Petra Pau** (Die Linke): Vielen Dank – auch für die Zeitdisziplin. Als Nächstes hat Professor Paal das Wort. Bitte.

SV **Prof. Dr. Boris P. Paal** (TUM): Zunächst noch einmal ganz herzlichen Dank für die Einladung und die Gelegenheit, auch aus der Entfernung hier aus München Stellung zu nehmen, da ich heute universitäre Verpflichtungen habe. Ich würde mich gern auf drei grundsätzliche Bemerkungen konzentrieren, jetzt in meinem Eingangsstatement – vielleicht unter der Überschrift „zu wenig“, „zu viel“ und „leider gar nicht“.

„Zu wenig“ bezieht sich auf den § 16a, also die Institutionalisierung der DSK (Datenschutzkonferenz). Hier wäre aus meiner Sicht wünschenswert gewesen, hinsichtlich der Bedeutung der Institution und der Unabhängigkeit der Datenschutzbehörden, mehr ins Gesetz aufzunehmen. Aus meiner Sicht ist das, was niedergelegt, im Wesentlichen ein rein symbolischer Akt. Zusätzliche Regelungen sollten sich meines Erachtens beziehen auf Ziele, Struktur, Arbeitsweise und insbesondere auf die Einrichtung einer gemeinsamen Geschäftsstelle. Mir leuchtet wohl ein und erschließt sich natürlich, dass das Verbot der Mischverwaltung hier ein Hindernis darstellen kann und dass verfassungsrechtliche Grenzen bestehen. Ich meine aber, das sind Hindernisse, die jedenfalls teilweise überwunden werden können.

Wenn wir über Grenzen reden, dann bin ich bei der nächsten Bemerkung, die ich überschreiben würde mit „zu viel“. Da geht es um die unionsrechtlichen Grenzen, mit Blick auf den § 37a BDSG, sprich auf das Scoring. Positiv ist, denke ich, dass hier eine neue Regelung geschaffen werden soll, die den wohl unionsrechtswidrigen, geltenden § 31 BDSG ersetzen soll. Ich meine aber, die Neukonzeption läuft ebenfalls Gefahr, unionsrechtswidrig zu sein. Es handelt sich ja, um das in Erinnerung zu rufen, um eine Ausnahmevorschrift zum Artikel 22 Absatz 1 DSGVO, der durch das Urteil des EuGH aus dem vergangenen

Dezember besondere Aufmerksamkeit erfahren hat. Es ist aber gerade nicht möglich, eine generelle datenschutzrechtliche Erlaubnis im Sinne der Artikel 5 und Artikel 6 DSGVO vorzunehmen. Und die jetzige Ausgestaltung der Vorschrift von ihrer Konzeption nach ihrem Wortlaut droht Missverständnisse hervorzurufen, droht Rechtsunsicherheiten hervorzurufen, indem sie beispielsweise Erstellung und Verwendung in den Blick nimmt. Aus meiner Sicht ist die Vorschrift zu beschränken auf dasjenige, was im Artikel 22 DSGVO als Ausnahme überhaupt vorgesehen ist, und das sind automatisierte Entscheidungen – hier sagt der EuGH, dass eine Maßgeblichkeit erforderlich ist. Und in diesem Sinne ist aus meiner Sicht im jetzigen Gesetzesvorschlag zu viel drin. Der Gesetzgeber droht hier, seine Kompetenzen zu überschreiten und damit droht auch die künftige Vorschrift, sollte sie so kommen, unionsrechtswidrig zu sein.

Und schließlich mein letzter Punkt, „leider gar nicht“ – die offenen Fragen. Mir ist bewusst, dass das ein umstrittenes Thema ist, aber der Beschäftigtendatenschutz beispielsweise bedarf auch noch der gesetzgeberischen nationalen Ausgestaltung. Ich danke Ihnen zunächst für Ihre Aufmerksamkeit und freue mich auf Fragen im Nachgang.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Und nun ist Professor Richter dran.

SV **Prof. Eike Richter** (AdP): Vielen Dank. Ich danke natürlich auch für die Möglichkeit der Stellungnahme. Ich kann da gleich anschließen und würde mich auf zwei Punkte konzentrieren: Einmal die Datenschutzkonferenz und einmal das Verbot biometrischer Gesichtserkennung, das schon angesprochen worden ist. Bei der Datenschutzkonferenz kann ich gleich anschließen an die Vorredner und will mich da konzentrieren auf die Frage der verfassungsrechtlichen Zulässigkeit.

Vorab aber ein Punkt: Das Interesse an Kohärenz ist auch ein Interesse an der Wirksamkeit von Recht, das heißt, es geht auch darum, die Wirksamkeit und die Steuerungskraft von Recht zu schützen, indem es eben auch kohärent wird. Das heißt, es ist auch ein eigenes Interesse des Datenschutzrechts. Und deswegen ist auch wichtig, wie das Recht in seiner Interpretation, in seiner Auslegung organisiert wird – das vorab.

Ich will an dieser Stelle konzentriert auf das Verbot der Mischverwaltung eingehen. Meines Erachtens wird das Verbot der Mischverwaltung häufig zu pauschal verwendet, also es wird zu pauschal gesagt, es gäbe ein Verbot. Wichtig ist, dass es das als solches eigentlich gar nicht gibt, in der Normativität, sondern es ist eine Bezeichnung, eine deskriptive Bezeichnung für die Frage, wie weit etwas mit der geltenden Kompetenzordnung im Grundgesetz vereinbar ist. Und so wird das auch vom Bundesverfassungsgericht regelmäßig gesagt. Das läuft zwar unter der Überschrift, aber es wird konkret gefragt, inwieweit bestimmte Verwaltungskooperationen mit den Vorgaben im Grundgesetz vereinbar sind. Und wenn Sie als Parlament selbst dort quasi Relativierungen vornehmen wollen, dann ist eine solche Relativierung auch grundsätzlich rechtfertigbar – also ein pauschales Verbot steht gar nicht im Raum. Das ist auch vollkommen undenkbar, weil wir dann in vielen Verwaltungsbereichen überhaupt nicht arbeiten könnten.

Ich will an der Stelle fragen, was ist eigentlich genau der Rechtfertigungsgrad? Und der ist eigentlich relativ deutlich beschrieben, nämlich in der Frage: Liegt eigentlich ein sachlicher Grund vor, um eine Kooperation vorzunehmen? Und: geht es um eine eng begrenzte Verwaltungsmaterie? Dazu muss man vorausschicken, dass es auch die Frage ist, um welche Art von Relativierung es sich handelt. Da kann von Eingriff in die Kompetenzordnung überhaupt nicht die Rede sein. Wir reden hier von vornherein von Fragen der verbindlichen Beschlussfassung – *intern*. Also nicht nach außen. Das ist schon einmal sehr, sehr wichtig. Das heißt, die Kooperationsgegenstände, die Relativierungen, sind darauf beschränkt. Das hat was damit zu tun, welchen Rechtfertigungsmaßstab man ansetzt an die beiden erwähnten Kriterien, die vom Bundesverfassungsgericht immer wieder genannt werden.

Ich konzentriere mich auf diese beiden Kriterien. Der sachliche Grund ist hier natürlich darin zu sehen, dass man versuchen will und ggf. muss, ein kohärenteres, abgestimmteres Verständnis datenschutzrechtlicher Vorschriften zu bekommen. Das ist im föderalen System natürlich ein ständiges Thema, weil wir tendenziell immer 17 verschiedene Ein- bzw. Vorstellungen haben. Man könnte an der Stelle einwenden: letztendlich schaffen dann eben die Gerichte eine gemeinsame Auslegung.

Nur würde man da verkennen, dass die Gerichte nicht die Aufgabe haben, in ihrer Kontrollfunktion das Recht allein zu konkretisieren, sondern es ist eine originäre Aufgabe auch der Verwaltung, Gesetze in der Auslegung zu konkretisieren. Die Ausführung der Gesetze liegt bei der Exekutive. Das ändert nicht, dass in der Kontrollperspektive der Gerichte Recht vereinheitlicht werden kann, aber es ist eben auch

eine originäre Aufgabe der Exekutive. So gesehen, finde ich, liegt da auch ein sachlicher Grund vor, dass man diese Kohärenz verfolgt, indem man versucht, die Datenschutzkonferenz anders zu organisieren, nämlich etwas stärker auf Kohärenz auszurichten.

Es ist auch eine eng umgrenzte Verwaltungsmaterie. Ach so, die Zeit. Einen letzten Halbsatz, wenn Sie den mir noch gönnen, zu dem letzten Punkt? Zu den Bereichen der Mischverwaltung kann ich gerne noch zwei, drei Beispiele nachliefern, die sich in diesem Spektrum bewegen. Ich wollte ergänzend zu dem Beitrag von Herrn Marx noch sagen, dass bezüglich eines Verbots biometrischer Gesichtserkennung, wenn man sich politisch dafür entscheidet – und das ist eine politische Frage – meines Erachtens verfassungsrechtlich keine Bedenken bestehen, im Gegenteil, verfassungsrechtlich sogar eine Überlegung besteht, tatsächlich genau das zu tun, vor dem Hintergrund des bis jetzt unwirksamen Vorbehalt des Gesetzes.

AVors. **Petra Pau** (Die Linke): Wir werden nachher sehen, wie wir in der Gesamtrechnung mit der Zeit rauskommen. Das Wort hat nun Professor Roßnagel.

SV **Prof. Dr. Alexander Roßnagel** (DSK): Vielen Dank, Frau Vorsitzende, meine sehr verehrten Damen und Herren. Als Vorsitzender der DSK begrüße ich die Institutionalisierung der DSK. Sie ist das entscheidende Instrument, um die Zusammenarbeit der Aufsichtsbehörden zu koordinieren und eine einheitliche Anwendung des Datenschutzrechts zu fördern. Das Ziel wird von der DSK seit 2018, seit Geltungsbeginn der Datenschutzgrundverordnung, intensiv und erfolgreich verfolgt. Dieses Ziel sollte auch im Gesetzestext festgehalten werden. Seine Erfüllung bedarf aber der organisatorischen Unterstützung durch eine Geschäftsstelle, deren Notwendigkeit im Gesetzestext aufgegriffen werden sollte. Bei zunehmenden Anforderungen an die DSK kann nur durch sie, durch die Geschäftsstelle, das künftig notwendige Maß an Professionalität und Kontinuität erreicht werden. Die Regelungen in den §§ 19 und 40 BDSG, nach denen bei fehlender Niederlassung des Verantwortlichen in Deutschland eine federführende Aufsichtsbehörde bestimmt werden soll, sollte gestrichen werden. Ohne eine Niederlassung gibt es keine federführende Aufsichtsbehörde und keinen One Stop Shop. Die Regelungen in den §§ 34 BDSG und 83 SGB X sollen Geschäfts- und Betriebsgeheimnisse gegen Auskunftsansprüche schützen. Sie verstoßen gegen Artikel 15 Absatz 4 DSGVO, weil sie weitergehende Einschränkungen des Auskunftsrechts enthalten, als Artikel 15 DSGVO vorsieht.

Es ist zu begrüßen, dass der Entwurf zu § 37 BDSG viele Handlungsempfehlungen der DSK aufgenommen hat. Dennoch sind einige Klarstellungen notwendig: Zum einen ist in Absatz 2 Nr. 1b der Begriff „soziale Netzwerke“ so zu präzisieren, dass auch aus Nutzersicht nicht-kommerzielle Angebote wie X oder Telegram erfasst sind.

Der Verweis auf die Verbraucherkreditrichtlinie geht fehl, weil dort keine Definition enthalten ist.

Zweitens ist der Begriff der Zahlungseingänge und Ausgänge in Buchstabe c so zu präzisieren, dass er auch Verwendungszweck, Beteiligte, Zeitpunkte und Orte umfasst. Diese Präzisierungen könnten auch in der Gesetzesbegründung erfolgen. In Absatz 2 sollte auch die Nutzung von Daten zum Alter und Geschlecht ausgeschlossen werden. In Absatz 2 sollte außerdem auch ein Verfahren gefordert werden, um richtige und aktuelle Daten für das Scoring sicher-zustellen. Und schließlich fordert die DSK für das Scoring eine Zertifizierung des wissenschaftlich anerkannten, mathematisch-statistischen Verfahrens. Dieses wäre mit einem großen Mehrwert für die Aufsichtsbehörden verbunden. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank. Das Wort hat Frau Dr. Ruf.

SV **Dr. Simone Ruf** (GFF): Sehr geehrte Abgeordnete, ich möchte drei Aspekte in meinem Eingangsstatement ansprechen. Als ersten Punkt, und hierauf möchte ich auf den Fokus legen, schlage ich vor, ein umfassendes Verbot für den Einsatz biometrischer Fernidentifikationssysteme im öffentlichen Raum ins Bundesdatenschutzgesetz aufzunehmen. In unserer schriftlichen Stellungnahme finden Sie dazu auch einen Formulierungsvorschlag. Warum? Aus grundrechtlicher Perspektive ist es notwendig, dass solche Systeme verboten sind und auch verboten bleiben. Der Einsatz geht nämlich mit erheblichen Risiken und Gefahren für Grund- und Menschenrechte einher. Erstens kann man dadurch umfassende Bewegungs- und Persönlichkeitsprofile erstellen und gerade der Kontext eines Aufenthaltsortes ermöglicht vielfache Rückschlüsse auf andere sensible Daten, wie zum Beispiel politische Einstellungen, die sexuelle Orientierung und so weiter. Das heißt, Anonymität im öffentlichen Raum droht verloren zu gehen, sowohl gegenüber dem Staat als auch gegenüber Privaten. Außerdem sind mit dem Einsatz erhebliche Abschreckungseffekte verbinden – Menschen trauen sich dann zum Beispiel nicht mehr, an Ver-

sammlungen teilzunehmen oder sich vertraulich mit Journalist*innen zu treffen. Besonders herausstellen möchte ich aber auch die Fehleranfälligkeit der Systeme. Gerade nicht-weiße Menschen werden häufig falsch identifiziert. Die Folgen könnten dann weitere grundrechtsbeschränkende Maßnahmen sein. Das ist letztendlich auch nicht im Sinne einer effektiven Polizeiarbeit, wenn die Polizei Systeme nutzt, die gar nicht richtig funktionieren.

Wir haben auch ein großes Risiko in der Datensicherheit – die Konsequenzen sind letztlich erheblich, wenn Unberechtigte Zugriff auf biometrische Datenbanken erhalten. Biometrische Daten sind fix einer Person zugeordnet und können eben nicht wie ein Passwort oder eine Kreditkartennummer einfach geändert werden.

Ich möchte noch zwei weitere Punkte herausstellen: Einmal die enorme Streubreite. Es sind letztlich alle Betroffenen, deren Gesichter oder andere biometrische Daten abgeglichen werden, also auch Menschen, die nicht in Referenzdatenbanken gespeichert sind. Hier verweise ich auf die verfassungsgerichtliche Rechtsprechung: Auch sogenannte Nicht-Treffer sind jeweils Grundrechtseingriffe. Dadurch, dass die Maßnahmen heimlich stattfinden, haben wir auch nur ganz beschränkte oder gar keine Rechtsschutzmöglichkeiten, was auch für ein erhebliches Eingriffsgewicht spricht. Und gerade vor dem Hintergrund, wir haben es jetzt schon gehört, dass einige Bundesländer derartige Systeme bereits zu Strafverfolgungszwecken einsetzen, meine ich, dass es hier unbedingt einer Klarstellung durch den Gesetzgeber bedarf.

Der zweite Punkt betrifft die Einschränkung des Auskunftsanspruchs zugunsten von Betriebs- und Geschäftsgeheimnissen. Hier empfehlen wir, die Norm zu streichen. Zum einen bestehen da schon erhebliche Zweifel, ob die Ausnahme mit Unionsrecht vereinbar und überhaupt erforderlich ist. Dazu werden aber wahrscheinlich noch andere hinreichend Stellung nehmen. Deshalb möchte ich hier nur ergänzend noch ein Argument einbringen, nämlich, dass ein Auskunftsanspruch der erste Schritt ist, um Rechtsschutz zu erlangen. Wenn man Auskunftsansprüche einschränkt, dann schränkt man auch mittelbare Rechtsschutzmöglichkeiten ein.

Und der dritte Punkt betrifft die Institutionalisierung der Datenschutzkonferenz. Die Norm begrüßen wir. Allerdings hätte man hier auch noch in Erwägung ziehen können, noch weiterzugehen, insbesondere die Einrichtung einer Geschäftsstelle zu normieren und festzuschreiben, dass die Datenschutzkonferenz im Endeffekt verbindliche Beschlüsse treffen kann. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Nun hat Herr Professor Schröder das Wort.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank, Frau Vorsitzende. Sehr geehrte Damen und Herren Abgeordnete, vielen Dank für die Gelegenheit, meine Stellungnahme hier im Gesetzgebungsverfahren einbringen zu dürfen. Grundsätzlich ist es richtig, das BDSG in einigen Punkten zu überarbeiten. Diese Änderungen müssen aber mit dem Unionsrecht und mit dem Grundgesetz vereinbar sein, und das ist aus meiner Sicht beim vorliegenden Entwurf nicht überall der Fall. Ich möchte zu zwei Punkten Stellung nehmen, zu den beiden zentralen Punkten „Institutionalisierung der Datenschutzkonferenz" und „Neuregelung des Scoring": Zur Institutionalisierung der Datenschutzkonferenz kann ich keine Gesetzgebungskompetenz des Bundes erkennen, auf die man diesen vorgeschlagenen § 16a BDSG stützen könnte. Informell können Bund und Länder oder auch die Länder untereinander vieles machen, ohne dabei verfassungsrechtlichen Vorgaben zu unterliegen – man denke da nur an die Ministerpräsidentenkonferenz und Ähnliches, aber sobald man den Weg eines formellen Gesetzes gehen will, muss es dafür auch eine Gesetzgebungskompetenz geben. Die sehe ich nicht. Mit dem vorgeschlagenen Gesetz werden nämlich die Datenschutzaufsichtsbehörden der Länder zum Mitmachen in der Datenschutzkonferenz gezwungen. Die machen das vielleicht auch gern freiwillig, aber trotzdem ist es rechtlich ein Zwang und das ist eine Vollzugsangelegenheit und könnte meines Erachtens nur auf Artikel 84 Grundgesetz gestützt werden. Dann dürfte sich aber die bundesrechtlich institutionalisierte DSK nicht mit Fragen der Aufsicht über öffentliche Stellen der Länder befassen, also mit dem Vollzug von deren Datenschutzrecht. Das ist aber, glaube ich, nicht das Bild, was man von einer Datenschutzkonferenz in der bisher etablierten Form hat.

Zur Neuregelung des Scoring: Die ist ebenfalls grundsätzlich zu begrüßen, ist aber in der konkreten Ausgestaltung mit Europarecht, wie es ja auch schon gesagt wurde, wohl nicht ganz vereinbar.

Zunächst möchte ich darauf hinweisen, dass der vorgeschlagene § 37a BDSG, indem er allgemein das Scoring regeln will, wohl über die Öffnungsklausel des Artikel 22 Absatz 2 Buchstabe b DSGVO hinausgeht und schon deshalb europarechtswidrig ist. Es

wird nämlich das Verbot weiter gefasst, als es überhaupt europarechtlich vorgesehen ist. Nicht jede Erstellung von Wahrscheinlichkeitswerten, wie es da im Entwurf steht, fällt darunter. Und Scoring, das sich unter die anderen Varianten des Artikel 22 Absatz 2 DSGVO subsummieren lässt – Vertragserfüllung, Einwilligung – kann sowieso nicht verboten werden.

Zweitens erscheinen im Anwendungsbereich der Öffnungsklausel die vorgeschlagenen Verwendungsverbote für bestimmte Daten durchaus bedenklich. Man kann sie zwar grundsätzlich als Schutzmaßnahmen im Sinne des Artikel 22 Absatz 2 Buchstabe b DSGVO qualifizieren, aber die konkrete Ausgestaltung ist zu beanstanden: Das Totalverbot der Verwendung besonderer Kategorien, besonderer Daten beim Scoring ist so, glaube ich, nicht von einer Öffnungsklausel gedeckt. Artikel 22 Absatz 4 DSGVO hat abschließend geregelt, inwieweit das zulässig ist. Und das kann der nationale Gesetzgeber nicht verschärfen.

Andererseits geht der vorgeschlagene pauschale Ausschluss von Daten zu weit. Die sind, wenn sie offen sind, nicht anders zu behandeln als Daten aus dem offenen Internet und die dürften auch verwendet werden. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Das Wort geht weiter an Frau Professor Specht-Riemenschneider.

SV **Prof. Dr. Luisa Specht-Riemenschneider** (Universität Bonn): Vielen Dank, Frau Vorsitzende, sehr geehrte Damen und Herren. Ich möchte zwei Punkte machen, entsprechend meinen Forschungsschwerpunkten, ich stehe aber natürlich gern für weitere Fragen dann zur Verfügung. Ich rege erstens an, die Gesetzesänderung in § 34 BDSG zu streichen, weil sie über Artikel 15 Absatz 4 DSGVO hinausgeht, Frau Ruf und Herr Rossnagel hatten das bereits angesprochen. Ich möchte noch ein paar Worte dazu verlieren, warum das der Fall ist: Wir haben bereits heute eine Beschränkung des Auskunftsrechts in Artikel 15 Absatz 4 DSGVO. Da ist das Auskunftsrecht beschränkt durch die Rechte und Freiheiten anderer Personen und andere Personen sind dabei eben auch der Verantwortliche und nicht nur dritte Person. Warum geht die Änderung in Artikel 34 BDSG über Artikel 15 Absatz 4 DSGVO hinaus? Die Gesetzesänderung sieht vor, dass das Auskunftsrecht von vornherein nicht besteht, wenn ein Betriebs- oder Geschäftsgeheimnis betroffen ist. Und wenn ein solches Auskunftsrecht von vornherein nicht besteht, dann muss es auch nicht durch Teilschwärzung befriedigt werden, wie das aber heute der Fall ist, wenn Betriebs- und Geschäftsgeheimnisse der Beauskunftung entgegenstehen. Damit geht §34 in der vorgeschlagenen Fassung zugunsten des Verantwortlichen über Artikel 15 Absatz 4 DSGVO hinaus und stellt Betroffene damit schlechter, als es nach heutiger Rechtslage der Fall ist. Und deswegen ist Artikel 15 Absatz 4 DSGVO ein milderes Mittel und § 34 BDSG würde in dieser konkreten Formulierung mit Artikel 23 DSGVO nicht vereinbar sein.

Zweiter Punkt, zu § 37a BDSG: Ich möchte dazu insbesondere einen Punkt starkmachen. Sie haben nach dem Schufa-Urteil des EuGH die Gesetzgebungskompetenz für die Regulierung des Scorings, wenn dieses Scoring einer automatisierten Entscheidung maßgeblich zugrunde gelegt wird, wir haben es gerade gehört, die Öffnungsklausel findet sich in § 22 Absatz 1b BDSG. § 37a BDSG ist aus meiner Perspektive eine ausgewogenere Regulierung, die auch nicht unionsrechtswidrig ist, darauf kann ich in den Nachfragen gern eingehen.

Sie werden das Problem eines unausgewogenen Scorings aber mit § 37a allein nicht in den Griff bekommen, und diesen Punkt möchte ich hier machen, denn der Elefant im Gesetzgebungsraum, das sind die Zahlungsdiensteanbieter – PayPal, Klarna –, die Sie mit § 37a BDSG nicht erfassen. Warum nicht? Weil sich die Zahlungsdienste-Anbieter auf § 22 Absatz 1a BDSG berufen können und § 37a BDSG aber nur greift, wenn Sie als Öffnungsklausel § 22 Absatz 1b BDSG haben. Wie kriegen wir den Elefant aus dem Raum? Ich glaube zwei Dinge sind heute aus Betroffenenperspektive wichtig: § 37a BDSG muss erstens schnell kommen, um die Betroffenen jedenfalls gegenüber Auskunfteien hinreichend vor einem unrechtmäßigen Scoring, einem unfairen Scoring zu schützen und auch um eine Vorbildregelung für das Scoring durch andere Anbieter zu haben. Wir haben die Möglichkeit, Artikel 18 der Verbraucherkreditrichtlinie umzusetzen und dabei können wir uns aus meiner Perspektive so weit wie möglich an § 37a BDSG orientieren. Warum? Denken Sie einmal darüber nach, man müsste das vielleicht noch einmal ausführlicher diskutieren, Artikel 18 der Verbraucherkreditrichtlinie könnte eine Rechtspflicht im Sinne von Artikel 6 Absatz 1c DSGVO sein, das heißt wir könnten hier ein nationales Gesetz erlassen, was sich auch an Artikel 6 Absatz 3 DSGVO orientiert. Dann haben wir zwar keine Regelung, die identisch mit § 37a BDSG ist, die wir hier in Umsetzung von Artikel 18 Verbraucherkreditrichtlinie erlassen

könnten, die aber ähnlich sein könnte und die dann eben auch Zahlungsdienste-Anbieter, wie PayPal und Klarna mit im Anwendungsbereich hat. Dabei will ich es belassen. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen und das Wort geht an Professor Thüsing.

SV **Prof. Dr. Gregor Thüsing** (Universität Bonn): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren, herzlichen Dank, hier eingeladen worden zu sein und für Ihr Interesse an meiner juristischen Meinung. 120 Sekunden – ich habe eine Minute dem Kollegen überlassen. Ich werde nicht der Versuchung erliegen, 17 Seiten Stellungnahme zu referieren, sondern ich nehme zwei Punkte heraus, vielleicht auch nur, um Mut zu machen. Das, was Sie getan haben, halte ich dort, wo ich mich geäußert habe, weder für verfassungswidrig noch für europarechtswidrig. Die Einführung des § 16a BDSG wurde von einem Kollegen als „zu weit gehend“ und von einem anderen Kollegen als „zu wenig weit gehend“ kritisiert – der eine sieht keine Gesetzgebungskompetenz, der andere fürchtet eine Mischverwaltung. Ich glaube, Sie sind einen guten Weg dazwischen gegangen, es ist wenig mehr übriggeblieben als „weiße Salbe“. Aber das ist eben der Kompromiss, wenn man deutlich machen will, wir brauchen eine solche Konferenz, sehen aber die Gefahr der Mischverwaltung und wollen diese nicht realisieren. Insofern halte ich das für gut, auch im Hinblick auf mögliche Verfassungswidrigkeitserwägungen.

Zum Zweiten, es wurde darauf hingewiesen, auch von meiner sehr geehrten Frau Kollegin Specht-Riemenschneider, dass Ihre Regelung zum Geheimnisschutz ganz sicher europarechtswidrig wäre. Zwei Minuten reichen nicht, um Irrlehren zu bekämpfen, die prominente Fürsprecher haben. Aber ich glaube, man sollte doch deutlich machen, dass das, was Sie momentan niedergeschrieben haben, letztlich nicht viel mehr als eine Konkretisierung des Artikel 15 Absatz 4 DSGVO ist. Es ist deutlich gemacht, dass der Geheimnisschutz nur insoweit nicht besteht, als dem Geschäftsgeheimnisse entgegenstehen. Und insofern ist auch die weitere Argumentation möglich, hier zu sagen: … insoweit eben auch nur, als es nicht durch Schwärzungen realisiert werden kann.

Zum Dritten: § 37a BDSG ist eine überaus gelungene Norm. Sie ist ja nichts anderes als eine Öffnungsklausel im Sinne des Artikel 22 DSGVO; sie sagt nichts über die Prüfung, die nach Artikel 6 DSGVO weiterhin erforderlich ist und der deutsche Gesetzgeber kann diese Öffnung gänzlich verweigern – das wäre nicht klug, das will er auch nicht und das ist richtig, dass er das nicht tut – aber er kann sie auch an Bedingungen knüpfen und diese Bedingungen kann er nahezu beliebig wählen. Insofern ist das, was er hier getan hat, sicherlich nicht europarechtswidrig, aber, auch das hat Frau Kollegin Specht-Riemenschneider schon gesagt, es befasst andere Bereiche nicht, die sich auf andere Rechtfertigungsgründe im Hinblick auf Artikel 22 DSGVO berufen können. Aber es ist auch hier zu hoffen, dass das eine gewisse Vorbildfunktion mit Modellcharakter ist und deswegen ist es auch unter diesen Gesichtspunkten gut, das zu tun.

AVors. **Petra Pau** (Die Linke): Gut. Erst einmal herzlichen Dank an alle Sachverständigen. Wir kommen jetzt in die erste Fragerunde. Für alle noch einmal durchschaubar: Die Fragesteller*innen haben zwei Minuten Zeit, entweder zwei Fragen an einen Sachverständigen oder je eine Frage an zwei Sachverständige zu stellen. Es wird unmittelbar geantwortet. Für jede Antwort stehen auch jeweils zwei Minuten zur Verfügung. Noch einen Hinweis: In der ersten Runde werden nach den Fraktionen auch die Gruppen mit dem Fragerecht berücksichtigt, in der zweiten Runde aber nicht – das waren die Regeln, die im Innenausschuss in der Obleuterunde festgelegt wurden. Ich werde nachher kreativ klären, wie die Gruppe Die Linke ihr Fragerecht hier wahrnehmen kann oder ob die Gruppe das an die Vorsitzende abtritt. Das zum Prozedere, wir beginnen mit der Kollegin Wegge.

Abg. **Carmen Wegge** (SPD): Vielen Dank, Frau Vorsitzende. Ich hätte zwei Fragen an einen Sachverständigen, und zwar an Herrn Professor Dr. Roßnagel. Die erste Frage zu § 40a, der jetzt neu ins BDSG hinein kommen soll: In der Stellungnahme der DSK begrüßen Sie zunächst die vorgeschlagene Regel bei länderübergreifender Datenverarbeitung von Unternehmen, Sie schreiben aber auch, dass diese Regelung gegebenenfalls zu Rechtsunsicherheit führen kann, weil aktuell eine Anzeigepflicht vorgesehen ist und man zunächst klären müsste, ob überhaupt eine gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO vorläge und Sie schlagen vor, statt einer Anzeige der Unternehmen einen Antrag an die Aufsichtsbehörden zur geänderten Zuständigkeit vorzusehen. Die erste Frage, die ich eben dazu hätte, wäre, ob Sie noch einmal erläutern können, warum Sie aus Sicht der Aufsichtsbehörden für eine solche Regelung sind, also konkret, warum sie notwendig erscheint.

Und die zweite Frage wäre: Wir haben es ja jetzt schon oft gehört, wir schreiben die DSK als

Institution ins Gesetz. Welche weiteren Möglichkeiten sehen Sie denn, um die Zusammenarbeit der DSK weiter zu stärken in diesem Spannungsfeld, was heute schon häufig angeklungen ist?

AVors. **Petra Pau** (Die Linke): Danke. Sie haben das Wort zur Beantwortung.

SV **Prof. Dr. Alexander Roßnagel** (DSK): Vielen Dank für die zwei Fragen. Zu § 40a und § 27 Absatz 5 BDSG: Da geht es ja darum, dass die Zuständigkeit bei einer Aufsichtsbehörde konzentriert wird. Das wird grundsätzlich begrüßt von der DSK, nur der Satz 5, mit dem haben wir Probleme, weil darin geregelt ist, dass die Adressaten selbst bestimmen, ob die Voraussetzungen vorliegen. Und das ist für öffentliches Recht äußerst ungewöhnlich und sollte abgeändert werden. Man wird auch nichts gewinnen dadurch. Das Ziel ist ja, dass man rechtssichere und bürokratiearme Gestaltung gewinnt, aber wenn die Antragsteller, also die Unternehmen, die behaupten, sie hätten eine gemeinsame Verantwortung, dies selbst feststellen können und das einfach nur anzeigen, dann führt das dazu, das die Aufsichtsbehörde, die nach Recht und Gesetz vorgehen muss, prüfen muss, ob die Voraus-setzungen erfüllt sind. Und solange sie das nicht geprüft hat, wird die Anzeige keine Wirkung haben. Das kann dazu führen, dass sie nach einem Vierteljahr, nach einem halben Jahr mit ihrer Prüfung durch ist und dann entweder Nachforderungen stellt an Unterlagen oder mitteilt, dass sie gar nicht zuständig ist, weil ihrer Meinung nach keine gemeinsame Verantwortung vorliegt. Die Idee, eine gemeinsame Verantwortung als Grundlage zu nehmen für solch eine Zuordnung der Aufsicht ist richtig, aber gemeinsame Verantwortung ist auch ein äußerst schillernder Begriff: Wir haben drei Urteile des EuGH zu diesem Thema, die mehr Fragen hinterlassen als sie geklärt haben und die Abgrenzung von gemeinsamer Verantwortung / ihre Feststellung ist äußerst umstritten und anspruchsvoll. Deswegen unser Vorschlag: Statt eine Anzeige, die dann in irgendeiner Weise verbindlich sein soll aber nicht kann, lieber eine moderate Prüffrist. Das würde dann innerhalb kürzester Zeit für alle Beteiligten Rechtssicherheit bewirken und die Aufsichtsbehörden und die betroffenen Unternehmen wüssten, woran sie sind. Diese Prüffrist kann ja damit verbunden werden, dass, wenn die Frist vorbei ist, man dann annimmt, dass es zutreffend ist, was angezeigt wurde. Man hätte dann die Möglichkeit, aber auch die Notwendigkeit, dass die Aufsichtsbehörden das rechtzeitig prüfen. Also insofern denke ich, wäre das von Vorteil für alle Beteiligten und auch viel rechtssicherer und bürokratieärmer.

Zu dem Thema DSK: Die DSK ist ja bisher ein freiwilliger Zusammenschluss, der auf freiwilligem Zusatzengagement des jeweiligen Vorsitzes beruht. Es ist äußerst schwierig, wenn der Vorsitz jedes Jahr wechselt, Erfahrungsbildung und Erfahrungs-weitergabe sicherzustellen. Deswegen brauchen wir dafür, dass wir Kontinuität und Professionalität gewährleisten können, eine ständige Geschäftsstelle. Die muss nicht sehr umfangreich sein, aber sie könnte technisch, organisatorisch die DSK oder den jeweiligen DSK-Vorsitz unterstützen. Wir würden dies gern im Gesetz festgelegt sehen, das hätte den Vorteil, dass diese Geschäftsstelle unabhängig von einem Bundesland ist, das vielleicht nicht mitwirken will. Und vor allen Dingen, weil das auf einer Zeitschiene schnell zu einem Ergebnis führen könnte.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank. Die nächsten Fragen stellt die Union, Herr Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Ich habe zwei Fragen, an Herrn Professor Thüsing und an Herrn Professor Schröder. Herr Professor Thüsing, Sie hatten vorhin im Rahmen des § 16a BDSG den Begriff „weiße Salbe“ genannt und hatten umgekehrt, wenn ich Sie richtig verstanden habe, es so erklärt, dass wir hier zwei „Extremmeinungen“ hätten und in der Mitte läge dann der gute Kompromiss. Die Frage, was genau meinen Sie mit „weißer Salbe“, weil ob weiße Salbe da ein guter Kompromiss ist, ist die Frage. Und konkretisierend eben – wir haben ja schon im Rahmen der föderalen Struktur bei uns einige zumindest zeitliche Verzögerungen in der Anwendung, auch gelegentlich Unsicherheiten, was stringente Entscheidungen, was schnelle Entscheidungen zum Beispiel bei bundesweit tätigen Unternehmen und so weiter angeht. Die Frage: Welche konkreten Verbesserungen sehen Sie jetzt durch diesen Gesetzentwurf, außer, dass es jetzt eine Geschäftsstelle oder sonst so etwas gibt? Wo sehen Sie hier die Verbesserungen und sehen Sie gegebenenfalls in irgendeiner Form noch zusätzliche gestalterische Möglichkeiten, hier weiter nach vorne zu kommen?

Und die zweite Frage, Professor Schröder, Sie hatten vorhin gesagt, Verwendungsverbote für bestimmte Daten seien bedenklich und hatten sich da auf die abschließende Regelung des Artikel 22 Absatz DSGVO bezogen. Wenn Sie nochmal netterweise konkretisieren könnten, ob Sie das jetzt sozusagen für sämtliche Regelungen bezüglich der Einschränkungen, die jetzt vorgenommen werden, sehen oder

ob Sie da unterscheiden? Wenn Sie das nochmal näher ausführen, wäre ich Ihnen dankbar.

AVors. **Petra Pau** (Die Linke): Dann hat Professor Thüsing als erstes das Wort.

SV **Prof. Dr. Gregor Thüsing** (Universität Bonn): Sehr herzlichen Dank. Ich habe einen Fachbegriff aus der Medizin verwendet: „Weiße Salbe“ meint ein Placebo, welches dem Patienten ein gutes Gefühl gibt, etwas gegen seine Schmerzen, seine Krankheit getan zu haben, ohne dass das tatsächlich mit einem wirkbaren Medikament verbunden ist. Das heißt also, man macht deutlich, dass man die Konferenz haben will, ohne aber tatsächlich substanzielle Regelungen zu finden. Denn dass es eine Geschäftsstelle gibt, dass man sich eine Geschäftsordnung geben kann, das sind Regeln, für die es eine gesellschaftliche Ermächtigung wohl auch nicht bräuchte, wenn verbindliche Entscheidungen mit dieser Konferenz eben nicht verbunden sind. Das ist das Entscheidende, was eben nicht vorgesehen ist und meines Erachtens zu Recht nicht vorgesehen ist, weil dann würden die ja bereits angemerkten verfassungs-rechtlichen Kompetenzprobleme durchaus sehr viel stärker wahrnehmbar sein, wir wären in der Gefahr einer Mischverwaltung. Es wurde eben lange ausgeführt, warum man hier keine unzulässige Mischverwaltung sehen würde. Ich glaube, niemand bestreitet, dass es eine Mischverwaltung wäre und die, die sagen, es ginge trotzdem, hoffen auf einen sachlichen Grund. Man kann sich da die Rechtsprechung des Bundesverfassungsgerichts näher angucken, Rand-Nr. 169 ff. der Entscheidung zu den Arbeitsgemeinschaften, da wird man feststellen, dass der sachliche Grund doch sehr, sehr eng gefasst ist. Und gerade da, wo ein Land verbindliche Beschlüsse bekommen würde, also in seiner Verwaltungspraxis, Vorschriften von der Mehrheit der übrigen Länder bekommen kann, ist das tatsächlich ein ganz massiver Eingriff in die Eigenständigkeit der Verwaltung. Und dann müsste man sich auch fragen, wie sollen denn die Stimmen gewichtet werden in den Ländern? Nach Einwohnern? Oder soll es nur qualifizierte Mehrheiten geben? Braucht es die Einstimmigkeit? All das ist nicht geregelt und es ist gut, dass es nicht geregelt ist, weil es keine Verbindlichkeit geben kann.

Der sachliche Grund, auch die in der Stellungnahme des Kollegen ausgeführten Gründe, überzeugen mich nicht und überzeugen viele nicht, deswegen glaube ich, sollte man sich auf dieses verfassungsrechtliche Experiment nicht einlassen.

AVors. **Petra Pau** (Die Linke): Ich muss Sie auf die zwei Minuten aufmerksam machen.

SV **Prof. Dr. Gregor Thüsing** (Universität Bonn): Dann höre ich auf.

AVors. **Petra Pau** (Die Linke): Wir können ja für die nächsten Anhörungen noch einmal schauen, welche Modelle da denkbar sind, da können Sie das klären, aber jetzt hat erst einmal Professor Schröder das Wort.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank für die Frage. Der Artikel 22 Absatz 4 DSGVO schließt ja die Verwendung besonderer Kategorien personenbezogener Daten in solchen automatisierten Einzelfallentscheidungen aus, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g DSGVO gilt. Der Unionsgesetzgeber hat sich also von vornherein, und zwar ohne zu differenzieren, welcher Fall des Artikel 22 Absatz 2 jetzt gerade einschlägig ist, Gedanken darüber gemacht, in welchem Umfang besondere Kategorien personen-bezogener Daten verwendet werden dürfen und ich sehe nicht, dass man hier als nationaler Gesetzgeber darüber hinausgehen darf und einfach sagen kann, es dürfen überhaupt keine verwendet werden. Das scheint mir zu weit zu gehen. Das gilt nur für die, die in diesem Gesetzesvorschlag in § 37a Absatz 2 Nummer 1 Buchstabe a genannten Daten.

Bei den anderen stellt sich die Frage, ob die Verbote angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sind – das würde ich jetzt so pauschal nicht für alles sagen können in der Kürze der Zeit, da braucht man eine ausführliche Verhältnismäßigkeitsprüfung. Ich hatte nur Bedenken angedeutet im Hinblick auf die Daten aus sozialen Netzwerken. Mir leuchtet unmittelbar ein, dass was man in geschlossenen sozialen Netzwerken teilt, besonders schutzbedürftig ist, also wo ich zuerst mit einem anderen Nutzer einen Kontakt herstellen muss. Wenn ich aber Daten auf eine öffentlich zugängliche und durch Google auffindbare Facebook-Seite stelle, dann sehe ich nicht, dass diese Daten schutzbedürftiger wären als Daten, die ich auf einer ganz normalen Website außerhalb eines sozialen Netzwerks online stelle und die da auch auffindbar sind. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen und jetzt geht das Fragerecht an die Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Ich würde gern zwei Sachverständige befragen. Die erste Frage geht an Herrn Marx und danach an Frau Ruf. Bitte können

Sie noch einmal darstellen, welche Risiken Sie mit den KI-Systemen zur biometrischen Fern-überwachung im öffentlichen Raum verbinden und inwieweit Sie die bisherigen Versuche durch Sicherheitsbehörden, diese Möglichkeiten zu nutzen, als problematisch einstufen? Sie haben da schon Beispiele genannt. Und welche Risiken sehen Sie in Bezug auf den Grundrechtsschutz?

Und die Frage an Frau Ruf: Sie haben einen Formulierungsvorschlag schon erwähnt. Da würde ich Sie bitten, diesen noch einmal zu erläutern, um Bezug zu nehmen auf folgende Aspekte. Erstens: Wieso eignet sich das BDSG als Regelungsort? Und Zweitens: Warum ist eine nationale Regelung mit europarechtlichem Blick auf die KI-Verordnung möglich und sinnvoll? Beziehungsweise, wieso ist es aus Ihrer Sicht auch sachgerecht, da ein Verbot national festzuschreiben? Man könnte ja auch einfach darauf verzichten, nur ermöglichende Rechtsgrundlagen zu nutzen. Danke.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen und die erste Antwort kommt von Herrn Marx.

SV **Matthias Marx** (CCC): Biometrische Überwachung greift fundamental, massiv in unsere Grundrechte ein, die informierte Selbstbestimmung und Meinungsfreiheit werden angegriffen, denn bereits Menschen, die sich nur überwacht fühlen, ändern ihr Verhalten und zwar so, dass sie sich vermeintlich konform verhalten. Sie könnten sich zum Beispiel gegen die Teilnahme an einer Demo gegen rechts entscheiden, weil sie befürchten, erfasst und gespeichert zu werden. Wir hörten bereits, die Systeme sind nicht diskriminierungsfrei und wir können sie auch nicht nur auf schwere Straftäter anwenden, denn es liegt in der Natur der Technik, dass zunächst alle biometrisch erfasst werden müssen, bevor ich mir die heraussuche, an denen ich ein weiteres Interesse habe. Insbesondere an hochfrequentierten Orten, wie zum Beispiel Flughäfen oder Bahnhöfen, wo sich zum Teil mehrere hunderttausend Menschen pro Tag aufhalten, dort muss ich davon ausgehen, dass immer eine gesuchte Person in der Nähe ist – eine dauerhafte biometrische Überwachung aller Passagiere wäre also die Folge. Die bisherigen Versuche sind problematisch, weil die Polizei sich wahrscheinlich mit Absicht einer demokratischen Kontrolle entzieht. Die Polizei Sachsen operierte zuletzt im Geheimen und erst durch eine parlamentarische Anfrage wurde bekannt, was dort passiert. Und das kann sich die Polizei wahrscheinlich auch erlauben, weil offenbar den Datenschutzbehörden Zwangsmittel fehlen, um bestehende Regeln durchzusetzen. Das Ganze ist schlecht für unsere Grundrechte, denn wir ziehen in Richtung einer Überwachungsgesellschaft ohne Anonymität in der Offline-Welt. Gesichtserkennung ist ein hervorragendes Werkzeug in einer dystopischen Zukunft, um politische Gegner zu verfolgen.

AVors. **Petra Pau** (Die Linke): Danke schön. Und die zweite Frage geht an Frau Dr. Ruf.

SV **Dr. Simone Ruf** (GFF): Ich fange damit an, warum es mit Blick auf EU-Recht überhaupt möglich ist: Im EU-Recht gibt es Öffnungsklauseln in der KI-Verordnung, sowohl für den retrograden Abgleich als auch für den Echtzeitabgleich. Die könnte man nutzen und restriktivere Regelungen treffen. Restriktivere Regelung wäre auch ein Verbot. Die DSGVO erlaubt in Artikel 9 Absatz 4, restriktivere Regelungen zu treffen – also auch hier kein Problem und auch die JI-Richtlinie gibt nur Mindeststandards vor.

Dann die zweite Frage: Vielleicht zuerst, wieso es sachgerecht ist, ein Verbot festzuschreiben und nicht nur einfach nicht die Regelungsspielräume auszunutzen. Das stimmt natürlich in Bezug auf Sicherheitsbehörden, wir haben es mehrfach gehört, es wird trotzdem gemacht. Es gibt keine Rechtsgrundlagen, weder in der StPO noch woanders, die das erlauben würden – hier ist auf jeden Fall eine Klarstellung angezeigt. Aber auch was Private betrifft – das ist zwar momentan schwer vorstellbar, dass es einen Fall gibt, wo die Voraussetzungen von Artikel 6 und 9 DSGVO vorliegen würden – aber auch hier wäre es angezeigt, klarzustellen, dass es nicht möglich sein kann. Insbesondere auch mit Blick darauf, dass vielleicht solch ein Fall einmal vor Gericht kommt. Und wenn man dann ein explizites Verbot in den Gesetzen findet, ist es natürlich viel einfacher, als sich dann noch einmal mit den Tatbestandsvoraussetzungen von verschiedenen Regelungen befassen zu müssen. Es wird dann oft angeführt, dass es schon das Verbot des sogenannten Image-Scrapings geben würde in der KI-Verordnung und das quasi ausreichend wäre. Dazu lässt sich klar sagen: Das betrifft zum einen nur die Gesichts-erkennung; es gibt aber auch andere biometrische Daten, man kann Personen auch eindeutig identifizieren, zum Beispiel am Gang oder den Augenbewegungen. Außerdem betrifft dieses Verbot nur das ungezielte Auslesen aus Videoüberwachungsaufnahmen und würde einfach nicht weit genug greifen.

Wieso eignet sich das BDSG jetzt besonders gut? Es gibt da schon Rechtsregelungen, die an die Verarbeitung biometrischer Daten anknüpfen, die könnte man hier erweitern.

Für wen gilt das BDSG? Einmal für nicht öffentliche Stellen, die hätte man damit abgedeckt, für öffentliche Stellen des Bundes, für öffentliche Stellen der Länder nur subsidiär, wenn da im eigenen Datenschutzrecht was nicht oder nicht abschließend geregelt ist und sie Bundesrecht ausführen.

An der Stelle will ich auch auf § 500 StPO hinweisen: Der erweitert den Anwendungsbereich für die Länder. Das heißt, wenn die Polizei repressiv tätig wird, egal ob Bund oder Land, dann gilt letztendlich immer das BDSG. Das wäre hier noch besonders wichtig hervorzuheben. Im Verhältnis zu den Fachgesetzen kann man feststellen, dass es hier darum geht, dass man kein bereichsspezifisches Verbot festlegen, sondern klarstellen will, dass es übergreifend ist und deswegen ist es besonders gut, das im BDSG zu verankern.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Dann geht das Fragerecht an die AfD-Fraktion, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Auch vielen Dank für die beiden Beiträge, die jetzt gerade gekommen sind. Die haben mich sehr interessiert. Ich möchte mir allerdings zum Thema Gesichts-erkennung auch noch einmal eine andere Position anhören. Herr Professor Richter, Sie haben dort in Ihrem letzten Satz gesagt, dass Sie bezüglich der Gesichtserkennung keine Problematik im Verfassungsrecht sehen. Vielleicht können Sie das noch einmal aus Ihrer Position darstellen und insbesondere auch auf sicherheitsrelevante Problematiken bei unseren Sicherheitsdiensten mit eingehen.

Meine zweite Frage würde an Herrn Professor Schröder gehen. Sie sagten, dass Sie § 37a BDSG für europarechtswidrig halten – Frau Professor Dr. Specht-Riemenschneider hatte das ja schon wieder in einem anderen Licht gesehen. Vielleicht können Sie uns noch einmal erklären, wie Sie Ihre Position dort entsprechend sehen. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke. Professor Richter.

SV **Prof. Eike Richter** (AdP): Vielen Dank. Ich würde nur dazu Position beziehen, ob ich da verfassungsrechtliche Probleme sehe. Wenn man sich den Ausgangspunkt überlegt: Es geht um eine Verbotsnorm. Das ist ja etwas Besonderes. Normalerweise regeln wir im öffentlichen Recht Befugnisse und keine Verbote. Das muss man bedenken, wenn wir das Verbot grundrechtlich prüfen. Da wäre zum Beispiel die Unternehmerfreiheit und sind Leute, die gern arbeiten mit solchen Systemen arbeiten usw. Dann wäre die Frage, ob ein solcher Grundrechtseingriff – wenn man den in einem Verbot sehen würde – ob ein solches explizites Verbot rechtfertigbar wäre. Ich sehe da ganz klar die Möglichkeit durch die Hinweise, die auch schon vorgetragen wurden: die starken Beeinträchtigungen der informativen Selbstbestimmung plus deren Folgen, Sekundäreffekte, die wir haben. Das wäre, glaube ich, überhaupt kein Problem an der Stelle. Wie gesagt: Man kommt von der anderen Seite, nicht von einer *Gebots*norm, sondern von einer *Verbots*norm. Deswegen muss man auch diesen Aspekt berücksichtigen.

Andererseits kann man darüber nachdenken, ob man grundrechtlich verpflichtet wäre, ein solches Verbot sogar tatsächlich einzuführen, auch das wäre denkbar. Aber ich denke, diese verfassungsrechtlichen Grenzen, bei denen der Gesetzgeber tatsächlich verpflichtet ist, aus den Grundrechten heraus ein Verbot zu statuieren, sind sehr eng und hier auch nicht erreicht. Das heißt, es bleibt Sache der politischen Einschätzung, das zu machen. Aber ich würde dazusagen, was dafür spricht, ist schon angedeutet worden: Denn eigentlich ist es jetzt schon verboten, nämlich weil und solange es nicht erlaubt ist. Das ist der Vorbehalt des Gesetzes. Es gibt keine Rechtsgrundlagen für den Einsatz. Deswegen stelle ich die Frage, ob man nicht auch als Gesetzgeber tatsächlich berücksichtigen muss, wenn der Vorbehalt des Gesetzes so gesehen nicht greift, also nicht wirksam wird, ob man dann nicht tatsächlich den Vorrang des Gesetzes, sprich ein explizites Verbot statuieren müsste. Wir haben eine Parallele, zum Beispiel das Folterverbot in der StPO, was auch ausdrücklich formuliert ist. Das könnte an dieser Stelle in dem Sinne auch geboten sein. Aber es ist eine politische Einschätzung. Verfassungsrechtliche Bedenken für eine Einführung eines Verbots sehe ich jedenfalls nicht.

AVors. **Petra Pau** (Die Linke): Danke. Dann geht das Wort an Professor Schröder.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank. Meine Annahme, dass § 37a BDSG, wie er geplant ist, europarechtswidrig ist, basiert im Wesentlichen auf zwei Punkten: Der eine Punkt ist, dass das Verbot, so wie ich es im 37a Absatz 1 lese, das Verbot, das der Artikel 22 Absatz 1 DSGVO aufstellt, letztlich erweitert, indem gesagt wird: Das Recht gemäß Artikel 22 Absatz 1, keiner solchen automatischen Einzelfallentscheidung unterworfen zu werden, besteht über die Ausnahmen hinaus nicht – die werden anerkannt –, wenn zu einer natürlichen Person Wahrscheinlichkeitswerte erstellt oder verwendet werden. Im § 37a BDSG geht es um

die Erstellung oder Verwendung von Wahrscheinlichkeitswerten, der Artikel 22 Absatz 1 DSGVO sagt aber überhaupt nur: Verboten ist, wenn man eine Entscheidung trifft, die gegenüber der Person rechtliche Wirkung entfaltet und sie in ähnlicher Weise erheblich beeinträchtigt. Ob das jetzt in jedem Fall so ist, wenn ich nur einen Wahrscheinlichkeitswert erstelle, das scheint mir doch fraglich. Der zweite Punkt ist dann die Frage, wie diese Ausnahme nach Artikel 22 Absatz 2 DSGVO auszusehen hat. Da dürfen die Mitgliedstaaten ja angemessene Maßnahmen – – Sie müssen sogar angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Person vorsehen. Das ist soweit in Ordnung, aber speziell für das, was hier gemacht werden soll, nämlich ein Verbot der Verwendung besonderer Kategorien personenbezogener Daten – das ist meines Erachtens in Artikel 22 Absatz 4 DSGVO geregelt und die anderen muss man genau auf ihre Angemessenheit überprüfen. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Das Fragerecht geht an den Kollegen Höferlin.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Zunächst einmal höre ich natürlich oft, dass wenn so viele Experten aus dem Bereich des Rechts sind, sie alle einer Meinung sind, nein, Spaß beiseite. Man sieht: Es gibt wieder viele unterschiedliche Haltungen und trotzdem finde ich sie sehr spannend. Ich habe zwei Fragen an einen Experten, nämlich an Herrn Professor Richter. Einmal zum Thema der Datenschutzkonferenz. Sie haben dazu bereits ausgeführt, wie andere auch. Vielleicht können Sie nochmal das vorgebrachte Argument, dass das nicht ginge, weil das eine Mischverwaltung sei, ausführen? Das ist das eine Argument und das allein spräche schon gegen die Einrichtung einer Geschäftsstelle. Sie schreiben aber auch in Ihrer Bewertung etwas zu „kohärenteren Entscheidungsverfahren“, und zwar zu abstrakten Rechtsthemen, nicht zu konkreten Einzelfällen. Das ist ein zweiter Kontext, den ich auch sehr spannend finde, der aber bisher noch nicht so richtig zur Sprache gekommen ist. Wir haben die Situation, dass manchmal, das ist auch angeklungen hier in der Runde, es abstrakte Rechtsfragen gibt, unter-schiedliche Gerichtsurteile, die mehr Fragen hinterlassen als sie Antworten liefern und dann wäre es hilfreich, wenn es bundesweit eine gemeinsame Auslegung gäbe. Vielleicht können Sie nochmal was zur Kohärenz der Entscheidungen sagen. Der zweite Fragekomplex geht auch noch mal zum Thema Gesichtserkennung. Wir haben ja in § 4 des neuen Entwurfs des BDSG jetzt nur noch eine Adressierung an öffentliche Stellen. Wir sprechen aber über die biometrische Gesichtserkennung sowohl für öffentliche Stellen als auch für private. Das heißt, der § 4 wäre eine nicht passende Stelle, um das zu normieren, weil dort ausschließlich öffentliche Stellen adressiert sind. Ist es Ihrer Meinung nach notwendig, im BDSG auch nochmal eine zweite Stelle aufzumachen, um die biometrische Gesichtserkennung für den privaten Bereich zu machen oder muss da unterschieden werden, auch vielleicht vom Normcharakter oder Inhalt her?

AVors. **Petra Pau** (Die Linke): Bitte, Sie haben das Wort.

SV **Prof. Eike Richter** (AdP): Vielen Dank. Zur Mischverwaltung. Wie der Kollege Thüsing auch schon gesagt hat, ist es ist total wichtig, sich genau anzuschauen: Was genau ist der Kooperationsgegenstand? Tatsächlich ist das genau die Frage. Hier geht es nur um die verbindliche Beschlussfassung bezüglich der abstrakten Auslegung von Datenschutzvorschriften. Es geht nicht um die Einzelfallbehandlung. Das ist von vornherein klar. Genau da liegt der Mehrwert der Kohärenz. Wenn man sich anschaut, wie die Mischverwaltung in Deutschland aussieht, kann man sehen, dass es tatsächlich gar nicht ein so enges Verständnis davon gibt. Ein Beispiel: Der IT-Planungsrat, den wir alle kennen, fasst auch verbindliche Beschlüsse. Dafür hat man damals die Notwendigkeit gesehen, einen Staatsvertrag zu machen, also Gesetzesänderung plus Verfassungsänderung. Warum war das so? Weil in dem Staatsvertrag in der ersten Nummer des Aufgabenkatalogs gleich drinsteht, dass man außenwirksame Beschlüsse über Standards machen wollte. Das war der entscheidende Punkt: *außenwirksam*. Deswegen hatte das eine ganz andere Wucht. Vorliegend steht aber gar keine Außenwirkung in dem Sinne in Rede. Sondern tatsächlich nur, was man gesetzlich regeln müsste, dass es nur um die Innenwirkung geht.

Dann ein Gegenbeispiel: Wenn Sie sich die Polizeidienstvorschriften in Deutschland angucken, werden die ja in der Innenministerkonferenz als Muster abgestimmt und sind im Kern auch verbindlich, indem sie über den Erlasswege verbindlich gemacht werden. In diesem Bereich gibt es – trotz Verbindlichkeit – noch nicht einmal ein Gesetz. Ich frage mich immer, auf welcher Grundlage das funktioniert – wahrscheinlich auf der Geschäftsordnung. Jedenfalls hat das eine hohe Verbindlichkeit und ganz ehrlich: Ich komme aus diesem Bereich – auch wenn aus dem Bildungsbereich in der Polizei –, aber ohne diese

Abstimmung über Polizeidienstvorschriften könnten wir zum Beispiel Einsätze wie jetzt während der EM überhaupt nicht organisieren. Das ist vollkommen klar. Natürlich muss es eine Koordination geben, und da geht es genau um diese Ebene der abstrakten Festlegung, losgelöst vom Einzelfall. Wenn man sich auf diesen Gegenstand beschränkt, dann ist meines Erachtens eine ganz andere Frage, was dann an Rechtfertigungslast für die Rechtfertigung einer sogenannten Mischverwaltung entsteht. So gesehen finde ich, wenn man immer an den Fall einer neuen, große Aufsichtsbehörde im Kolleg denkt – das wäre etwas ganz anderes, aber das ist hier gar nicht der Fall. Sondern es soll tatsächlich viel weniger gemacht werden: nämlich Verwaltungsvorschriften im Grunde deutschlandweit zu koordinieren; und das passiert in vielen Bereichen bereits. Das wäre der Punkt dazu. Deswegen glaube ich, ist es sehr wichtig – ich habe das auch im Gutachten ausgeführt –, dass man den Gegenstand der Kooperation in der Wirkung gesetzlich genau festlegt. Dadurch entsteht überhaupt erst die Last der verfassungsrechtlichen Rechtfertigung, die dann dementsprechend auch niedriger ist und der, finde ich, mit guten Gründen Rechnung getragen werden kann. So gesehen finde ich das immer zu pauschal, wenn man von *dem* Verbot der Mischverwaltung spricht.

Zum zweiten Punkt: Das ist eine ganz entscheidende Frage, eine wichtige Frage. Kann man ein solches Verbot für eine biometrische Gesichtserkennung eigentlich für alle Bereiche festlegen? Daran kann man seine Zweifel haben, wenn man sich die Intentionen des § 4 BDSG zur Videoüberwachung ansieht, der ja auf Grundlage der Rechtsprechung des Bundesverwaltungsgerichts modifiziert werden muss. Man kann an der Stelle tatsächlich überlegen, ob nicht da genau eine Parallele ist, dass man den privaten Bereich auch von dem Gesichtserkennungsverbot herausnehmen muss. Ein Aspekt, der dann nachdenkenswert ist, das habe ich vorhin angedeutet: Das Bundesdatenschutzgesetz hat die Verarbeitung personenbezogener Daten, also die Verarbeitung biometrischer Daten als Gegenstand. Die KI-Verordnung kommt aber eigentlich von der Technikregulierung. Sie reguliert Systeme und wenn Sie von der biometrischen Gesichtserkennung sprechen, dann fragt man sich: Was genau ist jetzt gemeint? Die KI-Systeme? Da geht es um die Öffnungsklauseln der KI-VO, da kann man Systeme anders regeln. Oder geht es um die Verarbeitung biometrischer Daten? Da wäre ja dann die Frage: Kommen die Öffnungsklauseln aus dem Datenschutzrecht? So gesehen würde ich sagen: Darüber könnte man noch mal nachdenken, weil man ja eigentlich am Instrument bzw. an der Tätigkeit insgesamt ansetzt, an der biometrischen Gesichtserkennung, die sowohl das Datenschutzrecht als auch die KI-Verordnung berührt. Das wäre eine Überlegung wert, aber die würde ich jetzt erst einmal nur in den Raum stellen wollen. Ansonsten ist die Parallele zu § 4 BDSG, der Videoüberwachung, nachvollziehbar.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Jetzt habe ich eine Frage an Herrn Kelber. Sie sind am Anfang Ihrer schriftlichen Stellungnahme vom April dieses Jahres kurz darauf eingegangen, dass Sie ja im Falle einer Auskunftsverweigerung durch öffentliche Stellen des Bundes Vorgänge einsehen dürfen, in die den Betroffenen nach § 34 Absatz 3 BDSG die Einsicht verweigert wird. Sie haben das als „Ersatzrecht für die betroffenen Personen“ bezeichnet. Wäre denn ein solches Ersatzrecht auch im Zusammenhang mit Auskunfteien und dem Scoring ein gangbarer Weg, wenn also der Schutz von Betriebs- und Geschäftsgeheimnissen vorgebracht wird, um ein Auskunftsbegehren abzuwehren? Und wenn ja, wie könnte der Bundesgesetzgeber hier vorgehen, wenn es dann ein gangbarer Weg wäre, um so etwas zu installieren, weil ja für die nicht öffentlichen Stellen nun wiederum die Länder zuständig sind?

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank, Frau Vorsitzende. Zumindest in diesem Bereich sind in der Tat die Länder die aufsichtsführenden Organe. Im Gegensatz zu Herrn Professor Roßnagel habe ich also keine Auskunftei unter meiner Aufsicht, aber wir haben natürlich genau solche Punkte auch in anderen Zusammenhängen schon besprochen. Selbst in Augenblicken, wo Geschäftsgeheimnisse oder die Daten Dritter nicht offenbart werden können, ist auch in diesem Bereich natürlich die federführende Aufsicht in der Lage, die Daten auf Plausibilität zu prüfen.

AVors. **Petra Pau** (Die Linke): Ja, dann kommen wir zügig in die zweite Runde und die Kollegin Wegge hat das Wort.

Abg. **Carmen Wegge** (SPD): Genau, ich habe jeweils eine Frage an zwei Sachverständige. Zum einen an Herrn Müller. Sie hatten in Ihrem Eingangsstatement schon erwähnt, dass sich auch die VZBV mit dem Geschäftsgeheimnisschutz in § 34 BDSG beschäftigt, hatten aber nicht ausgeführt. Vielleicht könnten Sie nochmal konkret sagen, welche Probleme Sie aus verbraucherrechtlicher Perspektive sehen?

Meine zweite Frage würde an Professor Dr. Luisa Specht-Riemenschneider gehen. Dadurch, dass Sie schon so zum § 34 BDSG umfassend ausgeführt

haben, würde mich jetzt interessieren, wie Sie denn zum Anwendungsbereich und auch insgesamt zum § 37a BDSG ausführen können. Sie haben ja vorhin im Eingangsstatement gesagt, Sie sehen die Europarechtswidrigkeit eigentlich nicht. Vielleicht können Sie dazu nochmal Stellung nehmen.

SV **Johannes Müller** (vzbv): Es wurde ja schon viel zu dem Punkt gesagt. Ich will das kurz halten und dann noch was anderes einschieben. Das größte Problem, was ich sehe, ist, dass Verbraucher*innen außerhalb des Scorings – also im Scoring, glaube ich, findet § 34 Absatz 1 BDSG nach dem aktuellen Stand sowieso keine Anwendung – die Auskunft mit der Begründung, es liege ein Geschäftsgeheimnis vor, was geschützt werden soll, verwehrt wird und dann quasi der Weg über die Datenschutzbehörden gegangen werden muss, was sehr lange dauert und im Endeffekt dazu führt, dass dann vielleicht auch der lange Atem nicht reicht, um das Recht auf Auskunft auch wirklich geltend zu machen.

Zu der Frage, die jetzt noch angesprochen wurde: Sind die ausgeschlossenen Datenkategorien eine geeignete Maßnahme zum Schutz der Verbraucher*innen im Sinne von Artikel 22 Absatz 2 lit. b) DSGVO? Da würde ich ganz klar sagen: Ja, und will da einen Gedanken mit hineinbringen; und zwar, wenn Sie die Transparenz bei diesem Verfahren erhöhen und Verbraucher zum Beispiel keine Kredite oder keine Telekommunikationsverträge bekommen, dann werden sie sich an dieser Transparenz, also an der geöffneten Logik der Datenverarbeitung, orientieren. Dann ist es extrem wichtig, dass bestimmte Datenkategorien nicht verarbeitet werden, weil Verbraucher sich sonst an diesen Datenkategorien orientieren, um ein besseres Scoring-Ergebnis zu erzielen. Also wenn wir an Kontoinformationen denken, das Einkaufen in bestimmten Einkaufsläden oder das Verhalten in sozialen Netzwerken oder die Anschrift, wo ich wohne – all das kann dann von Verbrauchern als Ziel identifiziert werden, um die Bonität zu verbessern. Diesen Einfluss von diesen Systemen auf unser Leben sollten wir auf jeden Fall verhindern!

AVors. **Petra Pau** (Die Linke): Danke, Sie haben das Wort.

SV **Prof. Dr. Luisa Specht-Riemenschneider** (Universität Bonn): Ja, vielen Dank, Frau Wegge. Meinhard, entschuldige bitte, wenn ich dir an dieser Stelle widerspreche. Ich würde auf die beiden Argumente eingehen: Artikel 22 1a DSGVO Regelungsbereich insgesamt und Ausschluss in Artikel 22 Absatz 4 DSGVO. Erstens: Der Regelungsbereich ist sicherlich nicht optimal formuliert, da würde ich dir zustimmen. Ich glaube aber, dass man beim § 37a BDSG durch Auslegung dazu kommen kann, dass er nur im Bereich Artikel 22 1a DSGVO Anwendung findet, also nur dann, wenn das Scoring auch maßgeblich der Entscheidung zugrunde gelegt wird.

Zweiter Punkt, den habe ich mir tatsächlich noch ein bisschen genauer angeguckt, dass der Artikel 22 Absatz 4 DSGVO sagt, die Entscheidungen dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 DSGVO beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g DSGVO gilt. Ja, das stimmt, da geht der Gesetzgeber darüber hinaus, aber in Artikel 9 Absatz 2 Buchstabe a DSGVO steht auch explizit drin, dass er Regelungen erlassen darf, die auch ein Scoring mit Einwilligung oder eine Datenverarbeitung mit Einwilligung nicht zulassen und in Buchstabe g steht auch, dass ich eine gesetzliche Regelung erlassen kann. Insofern würde ich hier unter Zugrundelegung dessen, was in Artikel 9 Absatz 2 Buchstaben a und g DSGVO drinsteht, dazu kommen, dass der § 37a BDSG auch in diesem Sinne nicht unions-rechtswidrig ist.

AVors. **Petra Pau** (Die Linke): Danke schön. Dann gehen wir weiter zu Herrn Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank. Zwei Fragen an Herrn Professor Paal würde ich gern stellen, und zwar das Thema DSK nochmal aufrufen, § 16a BDSG. Sie hatten vorhin unter der Rubrik „mehr“ gesagt, dass die Institutionalisierung grundsätzlich zu begrüßen sei, sie sich aber in Bezug auf Ziele, Struktur und Arbeitsweise mehr vorstellen könnten. Da die Frage: Welche Maßnahmen wären das, um Effektivität und Arbeitsweise zu stärken? Und Punkt zwei. Sie haben in Ihrer schriftlichen Stellungnahme drei Blöcke aufgemacht und Sie haben neben DSK und Scoring einen Punkt besonders hervorgehoben: den Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen. Da möchte ich gerne nochmal nachfragen. Sie haben geschrieben, dass Sie mit der jetzt geplanten Regelung, insbesondere was die Abwägung angeht, vielleicht auch die neu eingeführte Abwägung zwischen dem Auskunfts-interesse und dem Geschäfts- und Betriebsgeheimnis, unionsrechtliche Bedenken haben. Wo sehen Sie da Kritikpunkte und wo vor allem auch Änderungs-bedarf bzw. wie sähen Ihre Änderungsvorschläge hier aus? Danke.

AVors. **Petra Pau** (Die Linke): Danke. Professor Paal, Sie haben das Wort.

SV **Prof. Dr. Boris P. Paal** (TUM): Vielen Dank für Ihre beiden Fragen. Ich würde mit der zweiten Frage beginnen wollen, die bereits von meinen Vorrednerinnen und Vorrednern adressiert worden ist, wenn ich es recht sehe, nämlich die Frage, ob hier überhaupt noch Raum für eine Regelung im Lichte der unionsrechtlichen Vorgaben besteht. Nach meinem Dafürhalten – ich habe es in meiner Stellungnahme ausgeführt – würde ich anraten und empfehlen, die vorgeschlagenen Änderungen in § 34 BDSG und § 83 SGB X zu streichen, weil ich hier keinen Raum mehr sehe – in Übereinstimmung mit jedenfalls einigen, meiner Vorredner und unions-rechtliche Kompetenz oder unionsrechtliche Vorgaben, hier keinen zusätzlichen Regelungsspielraum mehr lassen, sondern vielmehr die Regelungen, die bereits im Artikel 15 Absatz 4 DSGVO und in seiner Konkretisierung durch den Erwägungsgrund § 63 Satz 5 DSGVO Ausdruck gefunden haben, das abschließend regeln und zusätzlichen nationalen Regelungen deswegen aus meiner Sicht kein Raum eröffnet ist.

Dann zu Ihrer ersten Frage – vielen Dank auch hierfür – betreffend den § 16a BDSG. In der Tat, und ich habe auch das in meiner schriftlichen Stellungnahme etwas weiter ausführen dürfen, wäre mein Petitum, insbesondere, und auch da kann ich an einiges anknüpfen, was die Vorredner bereits ausgeführt haben: Es ist wichtig, sollte man die Hindernisse der Grenzen der verfassungs-rechtlichen Vorgaben zur Mischverwaltung überwinden, eine auskömmlich finanzierte ständige Geschäftsstelle zu etablieren, um die DSK praktisch möglichst arbeitsfähig zu machen. Ich hielte es auch für sinnvoll, das durch eine Festschreibung der Ziele der DSK im BDSG und eine gesetzliche Festlegung zu der organisatorischen Unterstützung zu ergänzen, nochmal konkret, in Ausgestaltung einer solchen auskömmlich finanzierten ständigen Geschäftsstelle. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke schön. Dann geht es weiter mit der Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Danke schön. Ich würde auch gern zwei Sachverständige befragen. Meine erste Frage geht an Professor Kelber. Es geht um die Stärkung der Aufsicht. In ihrer Stellungnahme fordert der BfD ja unter anderem die Möglichkeit, bei Datenschutzverstößen von öffentlichen Stellen die Entscheidung für sofortige Vollziehbarkeit zu erklären und da werden auch Mittel vorgeschlagen, zum Beispiel die Zwangsvollstreckung oder Zwangsgelder, um das durchsetzen zu können. Können Sie bitte noch einmal erläutern, warum die Möglichkeit erforderlich ist und bitte auch darauf eingehen, inwiefern sich die öffentlichen Stellen bei sofort vollziehbaren Anordnungen im Wege des Eilrechtsschutzes wehren können?

In dem ganzen Bezug geht es auch um Bußgelder und da frage ich mich: Sie fordern auch die Möglichkeit, Bußgelder gegen öffentliche Stellen zu verhängen und das gerade in dem Bereich der hochsensiblen Daten. Ich formuliere es anders: In dem ganzen hochsensiblen Bereich, wenn es da rechtswidrigen Umgang mit Sozialdaten gibt, gibt es ja eine Spezialnorm, § 85a Absatz 3 des SGB X, der das ausschließt. Mich interessiert, wie Sie diesen Zustand bewerten. Können Sie vielleicht auch anhand von Beispielen darlegen, weshalb es hier besonders wichtig ist, auch gegen öffentliche Stellen mit Bußgeldern vorgehen zu können?

Das ist die erste Frage und die zweite Frage, da würde ich gern nochmal auf Frau Ruf und auf das, was der Sachverständige Richter zu dem Verbot der Nutzung von biometrischen Fernidentifikationen durch Private ausgeführt hat, Bezug nehmen. Sie haben in Ihrer eigenen Stellungnahme ja auch noch etwas dazu gesagt. Ich würde Sie dahingehend nochmal befragen: Ließe sich ein Verbot der biometrischen Fernidentifikationen im öffentlichen Raum für Private nicht auch auf Artikel 9 Absatz 4 der DSGVO stützen? Denn es handelt sich ja nicht nur um eine formale Verarbeitung von personen-bezogenen Daten, sondern es geht ja gerade auch um geschützte biometrische Daten und hierfür eröffnet der Artikel 9 Absatz 4 der DSGVO ja einen nationalen Regelungsspielraum, der sowohl durch Private als auch durch öffentliche Stellen umfasst würde.

AVors. **Petra Pau** (Die Linke): Professor Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank. Es gibt ja oft die Argumentation, es müsste doch zwischen Behörden eigentlich ausreichen, dass die Position eingenommen wird und man sich dort einigt. Das ist erfahrungsgemäß nicht der Fall. Umgesetzt werden muss das europäische Recht der Abhilfemaßnahmen nach Artikel 58 Absatz 1 und 2, aber Absatz 2 sagt auch, sie müssen vollumfänglich und umfassend sein und es stellt sich eben heraus, dass, wenn man zum Beispiel bei sehr schwerwiegenden Datenschutzverstößen mit einer Weisung oder einer Untersagung arbeitet und dagegen Rechtsschutz gesucht wird, die unrechtmäßige Datenverarbeitung eventuell sehr weitreichend ist und sich noch über Jahre hinziehen kann. Von daher wäre wie in anderen Bereichen zum Beispiel gegenüber privaten Stellen die Möglichkeit, den sofortigen Vollzug anzuordnen,

relevant, um diese Datenschutzverstöße abzuschaffen, zu mindern. Natürlich gibt es auch hier die Möglichkeit den entsprechenden Rechtsschutz einzulegen, also das Gericht entscheiden zu lassen, welche Variante jetzt auch im Eilrechtsschutz die bessere ist.

Zum Thema Bußgelder: Insbesondere ist es dort wichtig, wo Sozialdaten zunehmend wettbewerblich zum Einsatz kommen. Der Gesetzgeber hat durchaus dafür gesorgt, dass zum Beispiel gesetzliche Krankenversicherungen tatsächlich häufiger im Wettbewerb zueinander auftreten. Da gehört die Geldbuße dann als Rechenmittel im Hinterkopf dazu. Ich will ein Beispiel nennen: Bei Krankengeld dürfen die gesetzlichen Krankenversicherungen eigentlich nicht auf die Versicherten zugehen und Druck ausüben. Wir erleben allerdings, dass regionale Manager zur Verbesserung ihrer eigenen Zahlen diese Regelung umgehen, tatsächlich Druck ausüben, direkt oder indirekt, weil sie eben nicht damit rechnen müssen, dass wenn es eine Beschwerde gibt, eine Geldbuße folgt, das heißt jeder erfolgreiche Fall, in dem jemand nicht mehr das Krankengeld bezieht, ist ein positiver Punkt für die eigenen Zahlen. Die Geldbuße folgt nicht. Das würde sich umdrehen, wenn hier ganz sinnvollerweise die Möglichkeit der Geldbuße eingeführt würde.

AVors. **Petra Pau** (Die Linke): Frau Dr. Ruf.

SV **Dr. Simone Ruf** (GFF): Ja. Also es gibt den Artikel 9 Absatz 4 DSGVO, der in meinen Augen eben schon hier erlaubt, restriktivere Voraussetzungen auch im Sinne eines Verbots zu treffen. Klar, die KI-Verordnung regelt natürlich vor allem Systeme, weist aber an vielen Stellen auch darauf hin, dass das Datenschutzrecht gilt und dass auch im Bereich der Verarbeitung biometrischer Daten die einschlägigen Vorschriften aus DSGVO und JI-Richtlinie gelten. In der DSGVO ist es grundsätzlich nicht erlaubt, die biometrischen Daten zu verarbeiten. Es werden aber auch die Ausnahmen aufgezählt. Gleichzeitig können die Mitgliedstaaten aber, weil es sich um hochsensible Daten handelt, Einschränkungen treffen. Da sehe ich eigentlich kein Problem.

Ich finde, der Vergleich mit der Videoüberwachung geht in meinen Augen so ein bisschen fehl, weil Videoüberwachung natürlich schon nochmal etwas anderes ist. Da werden nicht per se biometrische Daten erhoben. Natürlich könnte man darüber nachdenken, danach biometrische Templates aus Videoaufnahmen herauszuziehen, aber es ist vom Grundsatz her nochmal etwas anderes und einfache Videoaufnahmen fallen – jedenfalls meines Wissens – noch nicht unter Artikel 9 DSGVO. Es macht schon Sinn, im vorderen Teil des Bundesdatenschutz-gesetzes, der ja gerade die nichtöffentlichen Stellen betrifft, auch eine Regelung für Private zu schaffen. Ich hatte eingangs schon auf die Risiken und Gefahren hingewiesen, die in verschiedenen Nuancen sowohl für den Einsatz durch den Staat, aber auch für Private gelten, insbesondere, wenn man darauf blickt, dass biometrische Datenbanken auch von Privaten aufgebaut werden können. Und wenn Unberechtigte Zugriffe erhalten, eben erhebliche Konsequenzen drohen, finde ich, macht es schon Sinn, auch dafür ein Verbot aufzunehmen und es spricht, wie gesagt, auch aus unionsrechtlicher Perspektive nichts dagegen.

AVors. **Petra Pau** (Die Linke): Danke schön. Das Fragerecht geht an Herrn Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Ich habe Fragen an zwei Sachverständige. Die erste Frage richtet sich an Herrn Professor Roßnagel: Sie hatten die DSK und dass sie jetzt hier im § 16a BDSG ins Gesetz kommen soll, ausdrücklich begrüßt. Meine Frage ist: Welche praktischen Änderungen ergeben sich dadurch, dass die Datenschutzkonferenz jetzt in das Gesetz eingebracht wird? Aus welchen Gründen war es notwendig, die DSK ins Gesetz einzubringen? Hätte es nicht auch in der bisherigen Form gereicht?

Die zweite Frage geht an Herrn Professor Kelber: Gehen Sie davon aus, dass es zu Rechts-unsicherheiten kommen könnte oder kann, wenn die Regelungen zur Videoüberwachung durch Private nicht länger im Bundesdatenschutz geregelt sind, sondern deutlich abstrakter im Artikel 6 der DSGVO? Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke. Dann hat das Wort erst einmal Professor Roßnagel.

SV **Prof. Dr. Alexander Roßnagel** (DSK): Ja, vielen Dank für die Frage. Ich würde gern darauf hinweisen, weil das mehrfach angesprochen worden ist: Die DSK braucht verbindliche Mehrheitsentscheidungen. Wir haben eine Geschäftsordnung und in der steht seit zwei Jahren drin, dass wir Mehrheitsentscheidungen verbindlich treffen können, und das tun wir auch. Also insofern ist die Antwort auf die Frage, was es bringt, so etwas gesetzlich zu regeln, wenn es in der Geschäftsordnung, die ja im Gesetz vorgesehen ist, schon drinsteht und auch praktiziert wird, dass die DSK im BDSG anerkannt wird den Vorteil hat, dass diese freiwillige Arbeitsgemeinschaft jetzt eine entsprechende Stärkung erhält, dass sie eine Anerkennung erhält. Und wir erhoffen uns daraus, dass das Ziel der Kohärenz der Datenschutzpraxis, dann auch gelebt wird, weil das voraussetzen wird, dass

für die Gesetze, die dann einen kohärenten Vollzug erfordern, die DSK auch mit einbezogen wird, wenn solche Gesetze im Bundestag diskutiert/erörtert werden. Wir bieten da, wenn man so will, einen Dialog an oder unsere Expertise an – jahrelange Erfahrung mit der Umsetzung von Datenschutzrecht in unterschiedlichen Anwendungsfeldern. Dieser Erfahrungsschatz wäre, denke ich, wenn der genutzt würde, auch für den Gesetzgeber von Vorteil. Insofern erhoffen wir uns durch die gesetzliche Anerkennung auch einen stärkeren Dialog zwischen Gesetzgeber und DSK.

AVors. **Petra Pau** (Die Linke): Danke. Herr Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Dankeschön. Also erstmal: Die Änderung im BDSG, Herr Abgeordneter, ist natürlich aufgrund der entsprechenden europäischen Rechtsprechung notwendig. Die Regelung in der DSGVO selbst ist abstrakter. Die DSGVO soll ja auch zukunftsfest sein, aber natürlich gibt es längst Aufsichtspraxis. Es gibt entsprechende Guidance-Papiere, sowohl national als auch des Europäischen Datenschutzausschusses und auch bereits erste Gerichtsurteile zu dem Thema. Das heißt, zusätzlich zu der abstrakten rechtlichen Regelung entsteht mehr aus der Praxis und der Rechtsprechung heraus, sodass ich das durchaus nicht für rechtsunsicher halte.

Wichtig ist natürlich auch zu wissen: Die KI-Verordnung wird ebenfalls die Auswertung von Videoüberwachung, zumindest im Bereich der Hochrisikosysteme, regeln. Dementsprechend wird es dort dann auch nochmal Abklärung miteinander geben. Die Datenschutzaufsichtsbehörden sind natürlich besonders erfahren, das auch in diesem Bereich vorzunehmen.

AVors. **Petra Pau** (Die Linke): Danke. Kollege Höferlin.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Ich würde meinen letzten Frageblock nochmal auf zwei Experten/Expertinnen, splitten. Die erste Frage geht an Frau Specht-Riemenschneider und betrifft nochmal den Themenkomplex der kohärenteren Entscheidungen der Datenschutzkonferenz. Wir haben jetzt gehört, dass Herr Professor Richter das Vorliegen eines sachlichen Grundes als verfassungsrechtliche Rechtfertigung genannt hat. Herr Thüsing hat das, glaube ich, explizit in Zweifel gezogen. Jetzt würde mich interessieren, was man Ihrer Meinung nach an „mehr“ tun kann, um diese Kohärenz herzustellen. Geschäftsstelle? Grundlagenentscheidungen in abstrakten Sachfragen? Da würde mich Ihre Position nochmal interessieren.

Die zweite Frage würde ich an Herrn Professor Roßnagel stellen: Sie hatten – das ist noch gar nicht zur Frage gekommen, meine ich – in Ihrer Stellungnahme vorgeschlagen, dass Datenschutz-beauftragte, Sie haben es „Tatmittel“ genannt – ein strafrechtlicher Begriff – beschlagnahmen können und haben beispielsweise von Dashcams gesprochen. Im datenschutz-rechtlichen Kontext könnte man aber durchaus auch ganze Serverfarmen vielleicht einziehen oder beschlagnahmen, weil Datenschutzverstöße im Cloud-Computing nicht eingehalten wurden. Ich gebe offen zu, dass mich diese zusätzliche Befugnis für Datenschutzbeauftragte, die von Ihnen vorgeschlagen wird, noch nicht überzeugt hat. Deswegen wollte ich Sie fragen, wie Sie dazu kommen, dass ein solch starker Eingriff, da man ja eher in anderem behördlichen Kontext von Tatmitteln spricht als bei den Datenschutzbeauftragten bisher – – Wie Sie dazu stehen und vielleicht überzeugen Sie mich dann doch noch, mich dem positiver zu nähern. Vielleicht aber auch nicht.

AVors. **Petra Pau** (Die Linke): Danke. Bitte Frau Professor, Sie haben das Wort.

SV **Prof. Dr. Luisa Specht-Riemenschneider** (Universität Bonn): Vielen Dank. Hinsichtlich der Frage, was geht mehr – so lege ich jetzt Ihre Frage aus – was geht mehr? Es geht das mehr, was Herr Richter hier vorgeschlagen hat und Herr Roßnagel, all das, was Sie in Ihrer Frage schon angesprochen haben. Also Geschäftsstelle, aber auch Mehrheits-beschlüsse, die sich auf abstrakte Entscheidungen beziehen, aus meiner festen Überzeugung heraus. Es wurde eigentlich alles schon gesagt, aber ich möchte dem trotzdem noch einmal Nachdruck verleihen: Wir haben im Wesentlichen zwei Argumente, die dagegengehalten werden. Das ist einmal die völlige Unabhängigkeit der Datenschutzaufsicht. Da haben wir noch nicht so explizit drüber gesprochen, und einmal das Verbot der Mischverwaltung. Beides wird eigentlich wie so ein Damoklesschwert über die Frage gehalten, was können wir mit der DSK machen. Lassen Sie mich zu beiden Punkten kurz etwas sagen.

Bei der völligen Unabhängigkeit geht es um eine institutionelle Unabhängigkeit, also um eine Unabhängigkeit von Regierung und Verwaltung. Es geht nicht um die Unabhängigkeit der Datenschutzaufsichtsbehörden untereinander, solange die Erweiterung der Kooperationsregelung eben auf abstrakte Sachverhalte, zum Beispiel Auslegungshilfen, beschränkt bleibt. Dann haben wir das in der Geschäftsordnung, aber das ist natürlich was anderes, wenn ich es ins Gesetz schreibe. Die Geschäftsordnung kann ich aber

jederzeit wieder aufheben. Zweiter Punkt, Verbot der Mischverwaltung, auch das wird als Totschlagargument gebracht. Das Bundesverfassungsgericht, das haben wir schon mehrfach gehört, hat niemals entschieden, dass wir das Verbot der Mischverwaltung überhaupt nicht durchbrechen können, sondern wir brauchen den sachlichen Grund und wir brauchen einen hinreichend umgrenzten Anwendungsbereich – und was denn, wenn nicht die effiziente Durchsetzung des Datenschutzrechts, was ist denn dann ein hinreichend begrenzter Anwendungsbereich und ein sachlicher Grund? Man kann sagen – und ich will mich da gar nicht politisch zu äußern: Wir machen das nicht. Aber dann ist das aus meiner Perspektive keine rechtliche Entscheidung, sondern eine politische Entscheidung, und dann klagen Sie bitte nie wieder über eine uneinheitliche Auslegung des Datenschutzrechts. Denn dann, also ab jetzt, ist das Ihre Sache! Jetzt haben wir nichts mehr mitzutun. Danke.

AVors. **Petra Pau** (Die Linke): Professor Roßnagel.

SV **Prof. Dr. Alexander Roßnagel** (DSK): Wenn eine Beschlagnahme nicht möglich ist, dann besteht ja die Gefahr, dass das Tatmittel, was auch immer das ist, also von einem Laptop bis hin zu einer Serverfarm – ja wieder zurückgegeben werden muss. Also selbst wenn man es nimmt, um es zu untersuchen, um forensische Prüfungen durchzuführen – man muss es dann wieder zurückgeben, und dann wird es direkt für den gleichen Zweck noch einmal verwendet. Also, wenn diese Gefahr besteht, ist es sinnvoll, die Möglichkeiten für die Verletzung von Datenschutzrecht – wenn das zu erwarten ist – unterbindet.

AVors. **Petra Pau** (Die Linke): Danke schön. Liebe Kolleginnen und Kollegen, wie Sie sehen, hätten wir die Chance, wenn Sie noch Fragen drängen, jeweils eine Frage und eine Antwort für jede Fraktion hier zuzulassen. Kollegin Wegge? Bitte.

Abg. **Carmen Wegge** (SPD): Vielen Dank. Dann hätte ich eine Frage an Professor Kelber: Wir haben ja gerade gehört, die DSK, möglicherweise ist da was möglich, wenn man mutig ist, wenn man hinreichende Gründe dafür anführt. Meine Frage geht deswegen auch in Ihre Richtung: Wie sehen Sie das denn? Inwieweit hätte der Gesetzgeber den Spielraum? Vor allem, wenn man aber jetzt sagen würde: Das mit der Mischverwaltung, das ist uns zu heikel. Was hätten wir als Gesetzgeber oder auch als Parlament möglicherweise noch für andere Möglichkeiten bzw. wie steht es zum Beispiel um eine Verwaltungsvereinbarung zwischen Bund und Ländern? Ist das eine weitere Option, die im Raum steht, um so eine Geschäftsstelle hinzubekommen?

AVors. **Petra Pau** (Die Linke): Professor Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank. Also den Argumenten, die vorgetragen wurden von Frau Professor Specht-Riemenschneider, von Herrn Professor Roßnagel und anderen, warum es möglich ist, brauche ich nichts mehr hinzuzufügen. Ich glaube auch, das ist noch einmal ein besonderer Mehrwert auch gegenüber dem, was die DSK aus eigener Not und eigenem Wollen heraus mit der Geschäftsordnung natürlich bereits vorgetragen hat. Die Geschäftsstelle könnte an vielen Stellen extreme Verbesserungen und Beschleunigungen erreichen, allein indem sie auch Zusammenarbeitsverfahren im technischen Bereich pflegt. Sie dürfen aber auch nicht die unterschiedliche Größe der Aufsichtsbehörden vergessen, und natürlich kann es als Vorsitz auch sehr kleine Behörden geben, die in der Aufsicht dann den gesamten Bereich bis hin zu den europäischen Gremien mit abdecken müssen. In der Tat könnten Sie natürlich als Bundesgesetzgeber herantreten, es erstens festlegen und sich zweitens, auch schon um die Geschäftsstelle kümmern. Das zweite wäre natürlich über die Institutionalisierung, die ja schon drinnen steht, und auch einer entsprechenden Aufführung einer Geschäftsstelle dann auf eine Verwaltungsvereinbarung zwischen Bund und Ländern auf die Einrichtung einer solchen Geschäftsstelle dann hinzuwirken und sie möglichst schnell zu etablieren. Kleiner Hinweis, es folgen eher kleinere Länder in dem Vorsitz nach Hessen.

AVors. **Petra Pau** (Die Linke): Danke schön. Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Ja, mit einer Abschlussfrage an den Professor Schröder. Sie hatten ja die gesetzgeberische Kompetenz für die Institutionalisierung der DSK infrage gestellt. Jetzt haben wir gerade gehört, es gäbe durchaus Spielraum für den Gesetzgeber in irgendeiner Form anderweitig tätig zu werden. Wie schätzen Sie die Situation ein und welchen gesetzgeberischen Spielraum für Veränderungen sehen Sie im Rahmen von Verbesserungen der Effizienz? Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ja, bitte, Herr Professor Schröder.

SV **Prof. Dr. Meinhard Schröder** (Universität Passau): Vielen Dank für die Frage. Ich sehe durchaus einen gewissen Spielraum, der hier besteht. Man muss bei der gesetzlichen Regelung als

Bundesgesetzgeber darauf achten, dass man sich von Bereichen fernhält, die in die Kompetenz der Länder fallen. Das ist das Problem bei dieser DSK: dass die Zuständigkeit zumindest nach derzeitigem Stand ja völlig unklar ist. Ich glaube, ein wesentlicher erster Schritt wäre, dass man mal klar sagt, was diese DSK eigentlich darf und was sie nicht darf, und dann kann man auch viel klarer beurteilen, ob das, was vorgesehen ist, hier noch unter dem Begriff Ausführung von Bundesgesetzen zu subsumieren ist oder insbesondere den Bereich des Datenschutzrechts für nichtöffentliche Stellen betrifft. Das klarer darzustellen ist, glaube ich, die zentrale Aufgabe. Und wenn man dann zu dem Ergebnis kommt, das sind alles unbedenkliche Bereiche, das kann man alles gestützt auf den Artikel 84 Grundgesetz so regeln, dann gehört da selbstverständlich auch eine Geschäftsstelle dazu. Das ist alles kein Problem, auch Mehrheits-entscheidungen würde ich dann nicht als problematisch erachten. Aber man muss ganz klar erst einmal sagen, wofür diese DSK zuständig sein soll. Dass das politisch sinnvoll sein mag, will ich gar nicht in Abrede stellen. Mir scheint das im Datenschutzrecht immer ein bisschen überproblematisiert zu werden, diese uneinheitliche Auslegung. Natürlich, sie findet statt, aber Recht wird sonst auch uneinheitlich ausgelegt. Auch das Bundesrecht wird mitunter uneinheitlich ausgelegt. Ich will gar nicht das Beispiel nennen, weil das eher so in den Bereich Justiz geht, was ja nochmal was anderes ist, aber im Strafrecht, schauen Sie sich die Strafzumessung an, die ist auch in jedem Bundesland anders. Das gibt es eben einfach. Warum jetzt gerade im Datenschutzrecht jenseits der europäischen Mechanismen ein besonderes Vereinheitlichungs-bedürfnis bestehen soll, hat mir auch noch niemand erklären können. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Dankeschön, Kollegin Khan.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Meine Frage geht an Professor Roßnagel. Es geht um Scoring und ich würde mich dafür interessieren: Wie bewerten Sie die bisherigen aufsichtsrechtlichen Befugnisse im Hinblick auf die gängigen Scoring-Algorithmen etwa bei der Schufa und welche Vorteile könnte es darüber hinaus haben, eine verpflichtende formale Zertifizierung für die dem Scoring zugrunde liegenden wissenschaftlich anerkannten mathematisch-statistischen Verfahren im BDSG vorzuschreiben? Danke schön.

SV **Prof. Dr. Alexander Roßnagel** (DSK): Also ganz einfach: In den Aufsichtsbehörden sind Juristen und Informatiker. Das sind keine Statistiker und solche, die Spezialkenntnisse haben, was die angewendeten Scoring-Verfahren angeht. Für die Aufsichtsbehörden wäre es ein großer Mehrgewinn, wenn jetzt eine Zertifizierung stattfinden würde, wenn eine unabhängige Stelle, die auf solche Fragen spezialisiert ist, prüft, ob denn die Verfahren, die da beim Scoring verwendet werden, ob die denn den Anforderungen, die der EuGH und andere Gerichte jetzt gestellt haben, genügen. Das ist eine Frage, eine Prüfungsfrage, die die Aufsichtsbehörden stark belastet, für die sie eigentlich das Personal nicht haben, für die das auch nicht darstellbar ist, dass man dafür eigene Personen einbezieht. Wie in vielen anderen Fällen wäre eine externe Begutachtung an der Stelle mit verbindlichem Ergebnis sehr hilfreich.

AVors. **Petra Pau** (Die Linke): Danke. Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Herr Professor Kelber, Sie hatten in Ihrem Eingangsstatement den Begriff „Mitarbeiterexzess“ verwendet. Könnten Sie mir erklären, was sich dahinter verbirgt?

SV **Prof. Ulrich Kelber** (BfDI): Wir haben ja die Situation, dass bei bestimmten Datenschutz-verstößen, dass das Mitarbeiterinnen und Mitarbeiter in dem Umfang, wo sie eigentlich ihrer Aufgabe nachkommen sollten, getan haben. Dann ist das ein Verstoß, den wir der Behörde oder dem Privatunternehmen zuordnen. Jetzt bei Behörden und bei Bundesbehörden kann es aber passieren, dass jemand Daten für eigene Zwecke verwendet, die nie vorgesehen waren. Also er nimmt Daten aus einer Datenbank, weil er an der Stelle etwas über seine Nachbarn wissen möchte. Das ist natürlich nicht der Behörde zuzuordnen, außer wenn sie unzureichende Sicherheitsmaßnahmen ergriffen hat, also jemand auf die Daten zugreifen konnte, der auf diese Daten nie hätte zugreifen dürfen. Was ist aber, wenn der Mensch, der auf diese Daten für dienstliche Zwecke hätte zugreifen können, sie einfach für private Zwecke missbraucht? Das ist das, was wir als „Mitarbeiterexzess“ benennen und dort müssen wir dann aber, weil die Aufsicht über Privatpersonen im Datenschutzrecht nicht beim BfDI liegt, die Landesdatenschutzbehörden des Wohnsitzes der Personen hinzuordnen. Das ist meistens eine, könnten aber auch mehr sein. Die müssen dann den gleichen Tatbestand noch einmal angehen. Wir können bestimmte Dinge natürlich bereits überprüfen und weitergeben, aber insbesondere, wenn es nachher zu einem Bußgeld kommt, muss die Landesdatenschutzbehörde natürlich nachweisen, dass sie eigene Untersuchungen vorgenommen hat, also auch an diesen Datenbeständen arbeiten, die ja sensibel sein können. Außerdem haben wir leider in der

Vergangenheit erlebt, dass sich Bundesbehörden geweigert haben, dann noch einmal mit einer weiteren Datenschutzbehörde zusammenzuarbeiten, sodass bestimmte Datenschutzverstöße, die durch Mitarbeiterinnen und Mitarbeiter als Mitarbeiterexzess begangen wurden, nicht geahndet wurden.

AVors. **Petra Pau** (Die Linke): Danke. Kollege Höferlin.

Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Meine letzte Frage geht nochmal an Herrn Professor Richter. Wir haben jetzt viel über die Datenschutzkonferenz, ihre Geschäftsstelle, ihre kohärentere Entscheidungsfindung in abstrakten Fragen gesprochen und über das Wort „Mischverwaltung“ gesprochen. Dem folgt ja noch ein viel wichtigeres Wort, gerade wenn es im Bund-Länder-Verhältnis eine Rolle spielt, nämlich die Mischfinanzierung. Da geht es ums Geld und deswegen meine Frage: Wie sieht es denn mit den Möglichkeiten einer Mischfinanzierung, zum Beispiel bei einer Geschäftsstelle und bei der Zusammenarbeit zwischen Bund und Ländern aus? Gibt es denn da verfassungsrechtliche Grenzen, die das unmöglich machen?

AVors. **Petra Pau** (Die Linke): Professor Richter.

SV **Prof. Eike Richter** (AdP): Ja, vielen Dank. Die gibt es natürlich dort im Grunde auch, in den Artikeln 104a ff. Um es auf den Punkt zu bringen: An der Stelle gilt der Grundsatz, dass auch die Lasten, die aus den Aufgaben, die die einzelnen Ebenen wahrzunehmen haben, also Länder oder Bund, für sich zu tragen sind. Da haben wir ein altes Problem generell bei der Frage der Kooperation von Verwaltungsebenen, nämlich das Grundgesetz setzt an der Stelle voraus, dass man die Aufgaben, die man gemeinsam wahrnimmt, in der Last tatsächlich auch zuteilen kann. Es regelt aber nicht was gilt, wenn man etwas zusammen macht. Und hier haben wir das Problem. Wenn wir darüber sprechen, was die Datenschutzkonferenz machen soll, ist das ja das gemeinsame Auslegen, das gemeinsame Finden der Interpretation. Da kann man kaum sagen: Wer hat denn jetzt wie viel davon gemacht? Das ist der klassische Fall, worauf die Einteilung der Kompetenzordnung im Grundgesetz nicht zugeschnitten ist, und deswegen gibt es dann diese Lösung, die jeder kennt, nämlich die Verteilung über den Königsteiner Schlüssel, dass man dann versucht, das entlang der Verantwortungsbeteiligungen aufzuteilen. Das muss man an der Stelle aber auch gesetzlich regeln. Wenn ich an der Stelle die Gelegenheit noch mal nutzen kann: Ich glaube, es ist wirklich wichtig, dass man sich klar macht, was genau eigentlich der Gegenstand der Kooperation sein soll. Es ist *nicht* die Beratung an Gesetzen. Das, würde ich sagen, sollte bei der Datenschutzkonferenz immer gefragt werden, wenn da neue Datenschutzgesetze gemacht werden – das ist eine gesetzgeberische Beratung. Es geht um die Interpretation unterhalb des Gesetzes, nämlich die Auslegung solcher Rechtsvorschriften. Auch das Beispiel mit den Gerichten, bei allem Respekt, greift nicht so ganz, weil Gerichte unabhängig sind. Vergleichbarer wäre die Staatsanwaltschaft und da haben wir die RiStBV (Richtlinien für das Straf- und Bußgeldverfahren), die auch genau das wieder machen, nämlich deutschlandweit im staatsanwaltlichen Verfahren Standards zu setzen. Weil es nämlich fatal wäre, wenn da jeder Staatsanwalt etwas anderes machen würde. Bei den Richtern gibt es das nicht, da haben wir die richterliche Unabhängigkeit. Deswegen, glaube ich, hinkt dieser Vergleich an der Stelle. Deswegen muss man wirklich genau definieren, wo der Kooperationsbereich liegt. Erst dann kann man über die verfassungsrechtliche Last sprechen. Das gilt auch für die Finanzierung.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen und ich danke auch, trotz einiger Irritationen am Anfang, für die Zeitdisziplin aller Beteiligten. Ich sehe, wir sind am Ende der Befragung. Wie am Anfang schon erläutert, wird Ihnen, den Sachverständigen, das Protokoll der heutigen Anhörung zugestellt, einschließlich der Hinweise zum weiteren Verfahren. Sie werden dann die Veröffentlichung der Drucksache des Ausschussprotokolls und natürlich auch die Veröffentlichung des Videos entsprechend wahrnehmen können. Ich danke allen Beteiligten und schließe die 80. Sitzung des Innenausschusses.

Schluss der Sitzung: 15:50 Uhr

Petra Pau, MdB
Altersvorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)414

DSK
DATENSCHUTZKONFERENZ
Vorsitz 2024
Landesbeauftragte für Datenschutz
Schleswig-Holstein

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

[redacted]

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

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 2021[1] 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 Reglung 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 11.05.2023[2] 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 Personenvereinigung 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 Verantwortungskreis 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 gewährleitet 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 abzuhelfen, 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.

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)416

Bonn, den 10.04.2024

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BT-Drs. 20/10859)

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Der vorliegende Gesetzesentwurf soll Vereinbarungen des Koalitionsvertrags 2021 – 2025 aufgreifen sowie Ergebnisse umsetzen, die sich aus der Evaluierung des Gesetzes durch das Bundesministerium des Innern und für Heimat (BMI) ergeben haben.

Er enthält einige notwendige Klarstellungen, u.a. zum Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder nach § 18 BDSG. Allerdings sind insbesondere viele Vorschläge des BfDI und der Datenschutzkonferenz (DSK), die u.a. auf den im Rahmen der Evaluierung des BDSG durch die DSK im Jahr 2021 gewonnen Ergebnissen basieren, in dem Gesetzesentwurf nicht bzw. nicht ausreichend aufgegriffen worden.

Der BfDI übersendet daher die nachstehenden Änderungsvorschläge zum BDSG-E und zum BDSG.

Unabhängig von dieser Stellungnahme hat auch die Datenschutzkonferenz (DSK), deren Mitglied ich bin, eine Stellungnahme an den Bundesgesetzgeber adressiert. In der folgenden Stellungnahme finden sich einige Punkte, die ich aus der Stellungnahme der DSK übernommen habe, weil sie mir besonders wichtig erscheinen. Dies ist dann entsprechend gekennzeichnet.

I. Anmerkungen zum BDSG-E

1. 34 BDSG-E

a.) Zu Nummer 12 Buchstabe a Doppelbuchstabe bb:

Es wird gemeinsam mit der DSK vorgeschlagen, § 34 Absatz 1 Satz 2 BDSG-E zu streichen.

Begründung:

Die Regelungen des § 34 Absatz 1 Satz 2 BDSG-E und § 83 Absatz 1 Satz 2 SGB X-E sollen die Wahrung des Geschäfts- und Betriebsgeheimnisses bei der Durchsetzung von Auskunftsansprüchen sicherstellen. Allerdings ist ihre Vereinbarkeit mit Art. 23 DSGVO zweifelhaft. Derartige Zweifel werden bereits gegenüber dem bestehenden § 34 Absatz 1 Nr. 2 BDSG geäußert, wenn und soweit kein Ausnahmetatbestand ersichtlich ist. Die Einschränkungen der Betroffenenrechte nach Art. 23 DSGVO sind eng auszulegen. Als Ausnahmetatbestand für die Wahrung des Geschäfts- und Betriebsgeheimnisses kommt Art. 23 Absatz 1 lit. i DSGVO in Betracht, wonach eine Beschränkung zum Schutz von Rechten und Freiheiten anderer

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Personen zulässig ist. Darüber hinaus sind die in § 34 Absatz 1 Satz 2 BDSG-E und § 83 Absatz 1 Satz 2 SGB X-E adressierten Aspekte bereits in Art. 15 Absatz 4 DSGVO, konkretisiert durch Erwägungsgrund 63 Satz 5 zur DSGVO, 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 Satz 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).

b.) Zu Nummer 12 Buchstabe b:

Ergänzend zu der in § 34 Absatz 3 Satz 3 BDSG neu geregelten Pflicht wird vorgeschlagen, klarzustellen, dass sich § 34 Absatz 3 BDSG auch auf den Ausschlusstatbestand des § 29 Absatz 1 Satz 2 BDSG bezieht.

Begründung:

In der Praxis haben sich Unklarheiten im Hinblick auf die Reichweite des § 34 Absatz 3 BDSG, dergestalt gezeigt, ob diese Sonderregelung aufgrund ihrer Stellung in § 34 BDSG ausschließlich die in § 34 Absatz 1 Nr. 1 und Nr. 2 BDSG geregelten Ausschlusstatbestände von Art. 15 DSGVO erfasst oder sie auch den Ausschlusstatbestand des § 29 Absatz 1 Satz 2 BDSG mit einbezieht.

Nach Auffassung des BfDI umfasst die Vorschrift nicht nur die in § 34 Absatz 1 Nr. 1 und Nr. 2 geregelten Ausschlusstatbestände, sondern bezieht sich aus den folgenden Erwägungen auch auf den Ausschlusstatbestand des § 29 Absatz 1 Satz 2 BDSG:

- Nach dem Wortlaut des § 34 Absatz 3 BDSG greift die Auskunftspflicht an mich in den Fällen, in denen „der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft“ erteilt wird. Die Vorschrift kann trotz ihrer Stellung mithin auch so gelesen werden, dass die Auskunftspflicht an mich für alle Fälle der Auskunftsverweigerung durch öffentliche Stellen des Bundes, mithin auch in den An-wendungsfällen des § 29 Absatz 1 Satz 2 BDSG, gilt.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

- § 34 Absatz 3 BDSG regelt eine Maßnahme zum Schutz der Rechte und Freiheiten der betroffenen Person. Die Intention des Gesetzgebers war es, durch Einführung dieser Regelung ein Ersatzrecht für die betroffenen Personen zu schaffen, denen gegenüber eine Auskunfterteilung u.a. aus den inzwischen in § 34 Absatz 1 Nr. 1 und Nr. 2 BDSG und in § 29 Absatz 1 Satz 2 BDSG aufgeführten Gründen abgelehnt wurde. Ihnen wird so grundsätzlich die Möglichkeit gegeben, durch mich prüfen zu lassen, ob sie in ihren Rechten beeinträchtigt worden sind. Entsprechende Schutzvorschriften sind grundsätzlich weit auszulegen. Es ist nicht erkennbar, warum die Pflicht zur Auskunftserteilung an mich nach Anpassung des BDSG an die DSGVO in Abweichung zur alten Rechtslage in den ergänzend durch Art. 34 Absatz 1 geregelten Fällen bestehen soll, in den Fällen des § 29 Absatz 1 Satz 2 BDSG hingegen nicht. Die Schutzbedürftigkeit der betroffenen Person, die dieses Ersatzrecht bedingt, ist in den Fällen des § 29 Absatz1 Satz 2 BDSG ebenso gegeben.

- Da § 34 Absatz 3 BDSG nach der Vorstellung des Gesetzgebers an die bisherige Regelung des § 19 Absatz 6 BDSG a.F. anknüpfen soll und die Altregelung auch den heutigen Beschränkungsgrund des § 29 Absatz 1 Satz 2 BDSG umfasste (vgl. § 19 Absatz 4 Nr. 3 BDSG a.F.), ist auch nach einer historischen Auslegung von einer Einbeziehung des § 29 Absatz 1 Satz 2 BDSG auszugehen.

Da der Wortlaut aber auch dahingehend interpretiert werden kann und teilweise auch so interpretiert wird, dass sich § 34 Absatz 3 BDSG nur auf die in § 34 Absatz 1 Nr. 1 und Nr. 2 geregelten Ausschlusstatbestände bezieht, wird eine entsprechende Klarstellung im Gesetz angeregt.

2. § 37a BDSG-E

Die nachfolgenden Ausführungen beinhalten eine Wiedergabe der Stellungnahme der DSK, der ich mich anschließe.

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

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

2.1. 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 Absatz 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.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Ich halte 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.

Ich schlage 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, empfehle ich mit der DSK, die Regelung im Rahmen einer Sachverständigenanhörung im weiteren Gesetzgebungsverfahren umfassend zu analysieren.

2.2. 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:

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

a) § 37 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 empfehle ich mit der 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.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

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

In ihrer Stellungnahme vom 11.05.2021 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 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.“

[1] https://www.datenschutzkonferenz-online.de/media/st/DSK-Handlungsempfehlungen_Verbesserung_des_Datenschutzes_bei_Scoringverfahren.pdf.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

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.

Ich schlage 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.

Ich schlage 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.“

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

II. Weiterer Regelungsbedarf im BDSG

1. Erweiterung der Aufsichtszuständigkeit des BfDI für Verstöße durch Beschäftigte öffentlicher Stellen des Bundes, die sich selbst als Verantwortliche gerieren (sog. Mitarbeiterexzess)

Es wird vorgeschlagen, in § 9 BDSG folgenden neuen Absatz 2 einzufügen:

„Die oder der Bundesbeauftragte ist ebenfalls zuständig für die Aufsicht über Beschäftigte, soweit diese gelegentlich ihrer dienstlichen oder betrieblichen Tätigkeit für Stellen, die ihrer oder seiner Aufsicht unterliegen, personenbezogene Daten aus deren Datenbeständen oder Erhebungsverfahren ausschließlich für dienst- oder betriebsfremde eigene Zwecke oder Zwecke eines Dritten verarbeiten (Exzess) und hierdurch selbst zu einem Verantwortlichen im Sinne des Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 werden."

Der bisherige Absatz 2 wird dann Absatz 3.

Begründung:

Soweit Beschäftigte gelegentlich ihrer dienstlichen oder betrieblichen Tätigkeit für Stellen, die der Aufsicht des BfDI unterliegen, personenbezogene Daten aus deren Datenbeständen ausschließlich für dienst- oder betriebsfremde eigene Zwecke oder Zwecke eines Dritten verarbeiten und hierdurch selbst zu einem Verantwortlichen im Sinne des Artikel 4 Nummer 7 DSGVO werden, ist nach geltender Rechtslage nicht BfDI für die Aufsicht über die Verarbeitung personenbezogener Daten durch den Beschäftigten, der den Exzess begangen hat, sondern die jeweilige Datenschutzaufsichtsbehörde des Landes zuständig. Ihre Aufsichtszuständigkeit ergibt sich hier aus den Zuständigkeitsabgrenzungen zwischen BfDI und den Aufsichtsbehörden der Länder in § 9 und § 40 BDSG. Für die entsprechende Verarbeitung personenbezogener Daten durch den Mitarbeiter, der den Exzess begangen hat, ist nach § 40 BDSG die jeweilige Datenschutzaufsichtsbehörde des Landes zuständig, in dem der Mitarbeiter seinen Wohnsitz hat, da der Mitarbeiter als Privatperson nicht die Voraussetzungen der in § 9 Absatz 1 BDSG genannten Stellen erfüllt, sondern als nichtöffentliche Stelle i. S. v. § 2 Absatz 4 Satz 1 BDSG handelt.

Die Zuständigkeit der Aufsichtsbehörde des Landes ist vor dem Hintergrund der in § 9 BDSG geregelten sachlichen Zuständigkeit des BfDI jedoch nicht sachgerecht und führt in der Praxis zu unnötigen Schwierigkeiten. Dem BfDI gelangt jährlich eine niedrige zweistellige Zahl von Fällen des Mitarbeiterexzesses seitens Beschäftigter von Bundesbehörden

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

zur Kenntnis. Die von den Beschäftigten begangenen Datenschutzverstöße werden sehr häufig gegenwärtig nicht geahndet, da die insoweit zuständigen Landesdatenschutzaufsichtsbehörden aus unterschiedlichen Gründen die notwendigen Ermittlungen nicht durchführen und zum Teil – etwa wenn es um Sachverhaltsermittlungen bei den Bundesbehörden selbst geht – auch nicht durchführen können.

BfDI sollte daher in diesen Fällen auch für die Aufsicht über entsprechende Datenverarbeitungen der Beschäftigten zuständig sein. Durch die Erweiterung seiner Zuständigkeit für Mitarbeiterexzesse könnten einheitliche Lebenssachverhalte bei einer Aufsichtsbehörde gebündelt werden. Dadurch könnte insbesondere auch vermieden werden, dass Landesdatenschutzbehörden bei Ermittlung des Sachverhaltes mittelbar auch mit Datenbeständen oder Verfahren der Bundesverwaltung gerade auch im Sicherheitsbereich in Berührung kommen. Zudem bliebe BfDI auch bei solchen Vorfällen der alleinige Ansprechpartner für die Bundesverwaltung. Die Aufsichtsbehörden der Länder sind mit diesem Vorschlag einverstanden.

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

Es wird vorgeschlagen, im Sinne der zweiten Alternative des § 17 VwVG „etwas anderes bestimmt“ § 16 BDSG dahingehend zu ergänzen, dass auch dem BfDI die Anwendung von Zwangsmitteln im Fall des Nichtnachkommens von Anordnungen durch öffentliche Stellen ausdrücklich erlaubt wird.

Begründung:

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 DSGVO und der JI-RL 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 Absatz 1 Satz 3 FinDaG, § 22 Absatz 3 Satz 4 ArbSchG).

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

3. Streichung des § 20 Absatz 7 BDSG

Es wird vorgeschlagen, § 20 Absatz 7 BDSG zu streichen.

Begründung:

Die Aufsichtsbehörde muss gemäß Art. 58 Absatz 2 DSGVO über umfassende Abhilfebefugnisse verfügen. Durch die Vorgaben des § 20 Absatz 7 BDSG ist jedoch in vielen Fällen keine durch Art. 58 Absatz 2 vorgesehene wirksame Abhilfe bei datenschutzrechtlichen Verstößen möglich. Eine rechtswidrige Datenverarbeitung oder ein sonstiger Verstoß gegen datenschutzrechtliche Bestimmungen kann dadurch 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.

Wie insbesondere die Erfahrungspraxis meines Hauses zeigt, gibt es auch im öffentlichen Bereich Fälle, in denen die Anordnung der sofortigen Vollziehung notwendig ist, um die Rechte der Betroffenen zu wahren.

Gegen Abhilfemaßnahmen des BfDI sind bislang 25 Anfechtungsklagen erhoben worden. Die Anzahl der Klagen zeigt, dass es nicht selbstverständlich ist, dass die Abhilfemaßnahmen durch öffentliche Stelle umgesetzt werden. Aufgrund der aufschiebenden Wirkung von Anfechtungsklagen werden die Maßnahmen erst einmal nicht umgesetzt. Für Eilfälle wäre es daher entscheidend, dass die sofortige Vollziehung angeordnet werden kann, um in der Zwischenzeit irreversible Folgen für betroffenen Personen im Einzelfall zunächst abwenden zu können.

Die derzeitige Regelung in § 20 Absatz 7 BDSG ist ferner auch zum Schutz der öffentlichen Stellen nicht erforderlich, weil diese in ihrem Handeln ihrerseits durch § 80 Absatz 5 Verwaltungsgerichtsordnung (VwGO) geschützt sind, wonach sie wie jeder andere Adressat der aufsichtsbehördlichen Maßnahme jederzeit die Möglichkeit haben, gerichtlich durch Beantragung der Wiederherstellung der aufschiebenden Wirkung nach § 80 Absatz 5 VwGO eine Anordnung der sofortigen Vollziehung überprüfen zu lassen. Die verbindliche Entscheidung trifft demnach auch in einem solchen Fall allein das Verwaltungsgericht.

Zudem werden auch im Bereich der Richtlinie (EU) 2016/680 durch Artikel 47 die Mitgliedstaaten verpflichtet, wirksame Abhilfebefugnisse für die Aufsichtsbehörden vorzusehen. Hierzu gehört nach hiesiger Auffassung etwa auch die Möglichkeit der Anordnung der sofortigen Vollziehung, die § 20 Absatz 7 BDSG derzeit noch ausschließt. Für effektiven Grundrechtsschutz wäre eine solche Befugnis aber von großer Bedeutung. Da der Wortlaut und die Zielsetzung des § 20 Absatz 7 BDSG eindeutig sind, ist eine unionsrechtskonforme

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Auslegung dieser Norm nicht möglich. Im Ergebnis wird dadurch dem Aufsichtsinstrument der Anordnung seine in Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 vorausgesetzte Wirksamkeit genommen.

Die Frage der Durchsetzung aufsichtsbehördlicher Entscheidungen stellt sich aus hiesiger Sicht in jedem Fall, nicht zuletzt, weil eine effektive Durchsetzung aufsichtsbehördlicher Entscheidungen auch ein Mittel zur Prävention von Datenschutzverstößen sein kann.

4. Streichung des § 43 Absatz 3 BDSG

Es wird vorgeschlagen, § 43 Absatz 3 BDSG zu streichen.

Begründung:

Gemäß § 43 Absatz 3 BDSG sollen gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 BDSG keine Geldbußen verhängt werden. Der nationale Gesetzgeber hat hier von der Öffnungsklausel des Art. 83 Absatz 7 DSGVO 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. 57 DSGVO eingeräumten Befugnisse die am meisten abschreckende Wirkung und dienen folglich der Sicherstellung der Einhaltung der Bestimmungen der DSGVO, indem insbesondere 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 meiner Ansicht 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,

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

dass (durch die damit einhergehende Motivation zur Einhaltung der datenschutzrechtlichen Bestimmungen) vermieden wird, dass öffentliche Mittel für mögliche Schadensersatzansprüche von Betroffenen gemäß Art. 82 DSGVO verwendet werden müssen.

5. § 41 Absatz 1 BDSG

Es wird mit der DSK vorgeschlagen,

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

Um sicherzustellen, dass § 30 Absatz 2a Satz 1 und 3 OWiG anwendbar bleiben (Bußgeld gegen Gesamtrechtsnachfolger) und das Verfahrensrecht des GWB nachgebildet wird, sollte in § 41 Absatz 1 BDSG folgender Satz 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 über 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 Absatz 1 BDSG folgender Satz 5 ergänzt werden:

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

Begründung:

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.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

§ 30 Absatz 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 Absatz 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 DSGVO entgegensteht. So heißt es konkret im Tenor zu 1 der zuvor genannten Entscheidung: „Art. 58 Absatz 2 Buchst. i und Art. 83 Absatz 1 bis 6 der [DSGVO] sind dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Absatz 4 bis 6 DSGVO 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 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 Absatz 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. Vw. auf Gassner/Seith, Ordnungswidrigkeitengesetz, 2. Aufl. 2020 § 30 Rn. 13). Folglich fallen alle Personen, die im Rahmen der unternehmerischen Tätigkeit handeln, in den abstrakten Verantwortungskreis 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 Absatz 1 OWiG über § 41 Absatz 1 Satz 1 und 2 BDSG den Vorgaben der DSGVO zuwider. Die Aufsichtsbehörden sind aufgrund des Anwendungsvorrangs des EU-Rechts derzeit verpflichtet, § 41 Absatz 1 Satz 1 und 2 BDSG in Bezug auf die Weitergeltung des § 30 Absatz 1 OWiG unangewendet zu lassen (vgl. EuGH, Urteil vom 22. Juni 1989 C-103/88, Rn. 28 ff.).

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

§ 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 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 DSGVO dem des Kartellrechts gleich ist um „die in Art. 83 Absatz 1 DSGVO 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 Absatz 2 DSGVO 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 DSGVO zu verhängen, nach Art. 83 im Licht des 150. Erwägungsgrundes der DSGVO verpflichtet, bei der Berechnung der Geldbußen für die in Art. 83 Absatz 4 bis 6 DSGVO 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).

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

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

- § 81e: Ausfallhaftung bei Erlöschen eines Unternehmens
- § 81f: Verzinsung der Geldbuße
- § 81g Absatz 2: Unterbrechung der Verjährung durch Auskunftsverlangen
- § 82b: Anwendungsbefehl zu §§ 59 bis 59b GWB im Bußgeldverfahren

In Anlehnung an § 83 Absatz 2 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.

6. Streichung von § 29 Absatz 3 Satz 1 BDSG

Es wird vorgeschlagen, § 29 Absatz 3 Satz 1 BDSG zu streichen.

Begründung:

§ 29 Absatz 3 Satz 1 BDSG regelt aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten. Die Vorschrift schließt die Untersuchungsbefugnisse der Aufsichtsbehörden nach Art. 58 Absatz 1 lit. e und f DSGVO gegenüber den in § 203 Absatz 1, 2 und 3 des StGB genannten Personen aus, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Person führen würde.

§ 29 Absatz 3 Satz 1 BDSG stützt sich auf Art. 90 DSGVO, um das Spannungsverhältnis zwischen den aufsichtsrechtlichen Befugnissen der Aufsichtsbehörden einerseits und den Schutz von Berufsgeheimnissen andererseits aufzulösen. Nach Art. 90 DSGVO können die Befugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern durch den nationalen Gesetzgeber geregelt werden, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.

Da § 29 Absatz 3 Satz 1 BDSG die gesamte Datenverarbeitung von Berufsgeheimnisträgern ausschließt, obgleich dies nach der Vorgabe des Art. 90 DSGVO nur für die Fälle durch die Mitgliedstaaten geregelt werden kann, in denen dies notwendig und verhältnismäßig ist, um das um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen, überspannt diese Regelung den in Artikel 90 Absatz 1 DSGVO eröffneten Spielraum.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Eine Abwägung im Hinblick auf die Frage der Notwendig- und Verhältnismäßigkeit findet durch § 29 Absatz 3 Satz 1 BDSG nicht statt. Informationen, die einer Geheimhaltungspflicht unterliegen, lassen sich jedoch nicht per se durch nationale Regelungen einer aufsichtsbehördlichen Kontrolle entziehen, sondern ihnen kann im Einzelfall nur dann durch nationales Recht Vorrang eingeräumt werden, wenn die Pflicht zur Wahrung des Berufsgeheimnisses tatsächlich mit dem Recht auf Datenschutz in Kollision tritt und das Bestehen einer aufsichtsbehördlichen Eingriffs-kompetenz das Recht tatsächlich unterläuft.

Die Streichung des § 29 Absatz 3 Satz 1 BDSG würde zudem nicht zu einem unbeschränkten Datenzugriff durch die Aufsichtsbehörden führen, da durch Artikel 58 Absatz 1 lit. e DSGVO sichergestellt wird, dass Aufsichtsbehörden nur den Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, verlangen können.

7. Überprüfung des Anwendungsbereichs oder Streichung von § 22 BDSG

Es wird vorgeschlagen, § 22 Absatz 1 BDSG im Hinblick auf seinen Anwendungsbereich zu überprüfen oder zu streichen.

Begründung:

Die Regelung des § 22 Absatz 1 BDSG wird in ihrer Form als Generalklausel den Anforderungen der in Art. 9 Absatz 2 DSGVO, der Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Absatz 1 DSGVO ermöglicht, enthaltenen Öffnungsklauseln nicht gerecht. Durch die Öffnungsklausel darf kein Auffanggesetz mit abstrakten Verarbeitungstatbeständen und entsprechend unspezifischen Garantien für die Grundrechte und Interessen der betroffenen Person geschaffen werden. Dies ist aber mit § 22 Absatz 1 BDSG der Fall.

In den einzelnen Regelungen des § 22 Absatz 1 BDSG wird der Wortlaut der Spezifizierungsklauseln des Art. 9 Absatz 2 DSGVO nahezu unverändert übernommen. § 22 Absatz 1 Nr. 2 BDSG begrenzt zwar zusätzlich den Anwendungsbereich auf öffentliche Stellen und verlangt eine Güterabwägung. Letztere wir aber ohnehin bereits durch Art. 9 Absatz 2 lit. g DSGVO, d.h. der § 22 Absatz 1 Nr. 2 BDSG zugrundeliegenden Öffnungsklausel, gefordert. Sinnvolle Konkretisierungen durch nationales Recht sind diesen Regelungen nicht zu entnehmen.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

§ 22 Absatz 1 BDSG gestaltet sich überdies in der Praxis schwierig, da die hierin getroffenen Regelungen insbesondere in Konflikt mit den bereichsspezifischen Regelungen des jeweiligen Fachrechts, welches in großen Teilen bereits eine Verarbeitung besonderer Kategorien personenbezogener Daten explizit regelt und den Regelungen des § 22 Absatz 1 insoweit vorgeht, geraten. So differenziert § 22 BDSG im Gegensatz zu den vorhandenen bereichsspezifischen Regelungen beispielweise nicht nach einzelnen Verwendungszwecken.

Insbesondere, da die durch Art. 9 DSGVO geschützten besonders sensiblen Daten nach dem Verordnungsgeber einen besonderen Schutz verdienen, weil im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können, müssen die Ausnahmetatbestände des Artikel 9 Absatz 2 DSGVO, die einer nationalen Regelung zugänglich sind, in dieser Regelung umfassend berücksichtigt werden.

8. Streichung von § 23 Absatz 1 Nr. 2 BDSG sowie § 23 Absatz 1 Nr. 3 Var. 1 und 5 BDSG

Es wird vorgeschlagen, § 23 Absatz 1 Nr. 2 BDSG zu streichen und § 23 Absatz 1 Nr. 3 Var. 1 und 5 BDSG im Hinblick auf den jeweiligen Anwendungsbereich zu überprüfen und ggf. zu streichen.

Begründung:

Nach dem in Art. 5 Absatz 1 lit. b DSGVO geregelten Grundsatz der Zweckbindung müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht mit einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Nach dem in Art. 5 Absatz 1 lit. a DSGVO geregelten Grundsatz der Transparenz müssen diese Daten zudem in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Art. 6 Absatz 4, Art. 23 Absatz 1 DSGVO ermöglichen es den Mitgliedstaaten, durch nationale Rechtsvorschriften die Verarbeitung zu anderen Zwecken als denjenigen, zu denen die personenbezogenen Daten erhoben wurden, zu erlauben.

Beschränkungen nach Art. 23 DSGVO müssen den Wesensgehalt der Grundrechte beachten, notwendig und verhältnismäßig sein. Nach der ständigen Rechtsprechung des EuGH müssen sich Ausnahmen von den unionrechtlichen Vorgaben auf das absolut Notwendige beschränken. Um die Verhältnismäßigkeit zu wahren, muss die Beschränkung u.a. die Ziele benennen, deren Sicherung sie dienen soll, die Beschränkung muss zudem diesen Zielen dienen und zu ihrer Umsetzung geeignet sein.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Die durch § 23 Absatz 1 Nr.2 BDSG vorgenommene Beschränkung erfüllt diese Voraussetzungen nicht.

Nach § 23 Absatz 1 Nr. 2 BDSG ist eine zweckändernde Weiterverarbeitung personenbezogener Daten in den Fällen, in welchen die Angaben einer Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, zulässig. Es ist nicht erkennbar, auf welches der in Art. 23 Absatz 1 lit. a-j genannten Ziele diese ausnahmsweise erlaubte Sekundärverarbeitung Bezug nimmt. Zudem enthält die Vorschrift keine Einschränkungen, welche sicherstellen, dass der normierte Datenabgleich tatsächlich zum Schutz dieser Ziele stattfindet. Ferner ergibt sich bereits aus dem ebenfalls in Art. 5 Absatz 1 lit. a DSGVO geregelten Grundsatz der Richtigkeit die Pflicht des Verantwortlichen, lediglich richtige personenbezogene Daten zu verarbeiten.

Auch die Regelungen in § 23 Absatz 1 Nr. 3 Var. 1 (Abwehr erheblicher Nachteile für das Gemeinwohl) und 5 (Wahrung erheblicher Belange des Gemeinwohls) BDSG erfüllen aufgrund ihrer zu unbestimmten Formulierung nicht die Voraussetzungen der Art. 6 Absatz 4, Art. 23 Absatz 1 DSGVO und können den Verantwortlichen in ihrer aktuellen Fassung nicht von der in der DSGVO grundsätzlich vorgesehenen Zweckvereinbarkeit befreien. Es ist insbesondere nicht klar, welche Sachverhalte unter diese beiden vom nationalen Gesetzgeber - entgegen der in Art. 23 DSGVO geforderten Konkretisierung- lediglich generalklauselmäßig benannten Zwecke zu subsumieren sind. Abgrenzungsprobleme ergeben sich zudem u.a. zu § 23 Absatz 1 Nr. 3 Var. 2 BDSG der bereits die Abwehr einer Gefahr für die öffentliche Sicherheit regelt.

9. Überarbeitung von § 27 Absatz 2 BDSG und § 28 Absatz 4 BDSG

Es wird eine unionsrechtkonforme Überarbeitung von § 27 Absatz 2 BDSG und § 28 Absatz 4 BDSG vorgeschlagen.

Begründung:

§ 27 Absatz 2 BDSG und § 28 Absatz 4 BDSG beschränken wesentliche Betroffenenrechte bei der Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken bzw. bei der Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Die beiden Vorschriften erschöpfen sich dabei nahezu wortgleich in der Wiedergabe der jeweils zugrundeliegenden Öffnungsklausel der DSGVO (§ 27 Absatz 2 BDSG stützt sich auf Art. 89 Absatz 2 DSGVO und § 28 Absatz 4 BDSG auf Art. 89 Absatz 3 DSGVO) und stehen auch aufgrund ihrer pauschalen Formulierung nicht im Einklang mit diesen. Darüber hinaus fehlt in beiden Vorschriften der in den jeweiligen Öffnungsklauseln 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 (Sicherung des Grundsatzes der Datenminimierung durch geeignete technische und organisatorische Maßnahmen) zu gewährleisten sind. Ferner werden beide Vorschriften den Anforderungen der qualifizierten Erforderlichkeit aus Artikel 89 Absatz 2 und 3 DSGVO nicht gerecht.

Insbesondere mangels Aufnahme von Spezifikationen, wann die Betroffenenrechte ausnahmeweise eingeschränkt werden dürfen, haben die Verantwortlichen durch die derzeitigen Fassungen des § 27 Absatz 2 BDSG und § 28 Absatz 4 BDSG einen zu weiten, nicht mit dem Unionsrecht zu vereinbarenden Entscheidungsspielraum.

10. Überarbeitung von § 32 Absatz 1 BDSG und § 33 Absatz 1 BDSG

Es wird vorgeschlagen, § 32 Absatz 1 BDSG zu streichen und §§ 32 Absatz 1 Nr. 2 – 5, 33 Absatz 1 Nr. 1 lit. a, Absatz 1 Nr. 1 lit. b, Absatz 1 Nr. 2 lit. a und Absatz 1 Nr. 2 lit b BDSG zu überarbeiten.

Begründung:

Zwar können die Mitgliedstaaten nach Art. 23 Absatz 1 DSGVO auch Beschränkungen der Informationspflichten nach Art. 13 DSGVO und Art. 14 DSGVO regeln, jedoch stehen die vom Bundesgesetzgeber auf diese Öffnungsklausel gestützten Normen des § 32 Absatz 1 BDSG und des § 33 Absatz 1 BDSG (teilweise) nicht im Einklang mit der DSGVO.

§ 32 Absatz 1 Nr. 1 BDSG verstößt aus mehreren Gründen gegen Unionsrecht. Die DSGVO schränkt zwar ihren Anwendungsbereich nach Art. 2 Absatz 1 für bestimmte Formen der nicht-automatisierten Verarbeitung ein, sie differenziert im Übrigen jedoch nicht zwischen analoger und digitaler Datenverarbeitung. Auch Artikel 23 Absatz 1 DSGVO nennt eine mit dem Ursprungszweck zu vereinbarende Weiterverarbeitung analoger Daten nicht als Ausnahmegrund. Insbesondere handelt es sich hierbei nicht um eine Maßnahme, durch die

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Rechte und Freiheiten anderer Personen i. S. v. Art. 23 Absatz 1 lit. i Var. 2 DSGVO sicherstellt werden. Zudem verstößt die Regelung gegen das Bestimmtheitsgebot. Unklar ist 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“. Die Vorschrift ist daher zu streichen.

Auch die in §§ 32 Absatz 1 Nr. 2 – 5, 33 Absatz 1 Nr. 1 lit. a, Absatz 1 Nr. 1 lit. b, Absatz 1 Nr. 2 lit. a und Absatz 1 Nr. 2 lit b BDSG geregelten Ausnahmetatbestände begegnen unionsrechtlichen Bedenken, da sie teilweise über die Öffnungsklausel des Art. 23 Absatz 1 DSGVO hinausgehen. So schränkt beispielsweise § 32 Absatz 1 Nr. 2 BDSG die Informationspflicht mangels Konkretisierung über die ihr zugrundeliegende Öffnungsklausel des Art. 23 Absatz 1 lit. h DSGVO hinaus bei einer Gefährdung der Erfüllung sämtlicher in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben unzulässig ein. Obgleich Art. 23 DSGVO lediglich die öffentliche Sicherheit als Schutzgut kennt, führen §§ 32 Absatz 1 Nr. 3, 33 Absatz 1 Nr. 1 lit.b und Nr. 2 lit. b hingegen (auch) eine Gefährdung der öffentlichen Ordnung als Grund für die Ausnahme von der jeweiligen Informationspflicht an. Diese Vorschriften sollten mithin überarbeitet werden.

11. Streichung von § 35 Absatz 3 BDSG

Es wird vorgeschlagen, § 35 Absatz 3 BDSG zu streichen.

Begründung:

Nach § 35 Absatz 3 BDSG soll die Löschungsverpflichtung ergänzend zu Art. 17 Absatz 3 lit. b DSGVO nicht bestehen, wenn einer Löschung „satzungsgemäße oder vertragliche Aufbewahrungsfristen“ entgegenstehen.

Art. 17 Absatz 3 lit. b DSGVO, auf den diese Ausnahmeregelung gestützt wird, sieht jedoch bereits Beschränkungen der Löschungsverpflichtung für die Fälle, in denen die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, vor.

Die in § 35 Absatz 3 BDSG benannten vertraglichen sowie einseitig vom Verantwortlichen übernommene Verpflichtungen können folglich keine Rechtspflichten i. S. d. Art. 17 Absatz 3 lit. b DSGVO begründen. In Betracht kommen mithin allenfalls hoheitlich begründete Rechtspflichten.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Bestehen die in § 35 Absatz 3 BDSG benannten satzungsmäßigen oder vertraglichen Aufbewahrungsfristen könnte man zudem darauf abstellen, dass die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, weiter notwendig bleiben und folglich der Löschgrund nach Art. 17 Absatz 1 lit. a DSGVO ohnehin nicht greift.

Da eine Einschränkung der Betroffenenrechte durch private Satzungen nicht möglich ist, müsste § 35 Absatz 3 BDSG selbst für den Fall, dass keine Streichung erfolgen sollte, dahingehend geändert werden, dass das Wort „satzungsmäßiger" durch „von in öffentlich-rechtlichen Satzungen vorgesehenen" ersetzt wird (vgl. auch die mit dem Gesetzesentwurf entsprechend vorgenommene Änderung zu § 34 Absatz 1 Nr. 2 BDSG).

12. Ergänzung des § 9 BDSG um die Aufsichtszuständigkeit des BfDI für Stellen, die für den Bund Dienstleistungen der Informationstechnik erbringen oder informationstechnische Infrastrukturen betreiben

Es wird vorgeschlagen, § 9 Absatz 1 BDSG um folgenden Satz 3 zu ergänzen:

„(1) … [3]Satz 2 gilt auch für nichtöffentliche Stellen, soweit sie für den Bund Dienstleistungen der Informationstechnik erbringen oder informationstechnische Infrastrukturen betreiben"

Begründung:

In der Aufsichtspraxis des BfDI haben sich im Hinblick auf für den Bund zu erbringende Dienstleistungen der Informationstechnik bzw. zu betreibende informationstechnische Infrastrukturen Fälle ergeben, in denen eine Auftragsverarbeitung dergestalt vorliegt, dass der Verantwortliche eine öffentliche Stelle des Bundes und das (nichtöffentliche) Betreiberunternehmen (Unter-)Auftragsverarbeiter ist. Das Betreiberunternehmen darf als (Unter-)Auftragsverarbeiter personenbezogene Daten nur aufgrund der Weisungen des Verantwortlichen verarbeiten. Dadurch, dass die öffentlichen Stellen als Verantwortliche nach § 9 BDSG der Aufsicht des BfDI unterliegen, ist mittelbar zunächst sichergestellt, dass sämtliche in diesem Zusammenhang durch das Betreiberunternehmen durchgeführte Verarbeitungen ebenfalls der Aufsicht des BfDI unterliegen. Dies gilt unabhängig von der Rechtsform des Betreiberunternehmens und einer etwaigen Beherrschung durch den Bund.

Die Betreiberunternehmen unterliegen gem. § 9 Abs. 1 Satz 2 BDSG als nichtöffentliche Stellen auch dann der Aufsicht durch den BfDI, wenn dem Bund die Mehrheit der Anteile

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

gehört oder ihm die Mehrheit der Stimmen zusteht. Ist eine solche Beherrschung durch den Bund jedoch nicht gegeben, unterliegen die Betreiberunternehmen der Aufsicht der zuständigen Landesdatenschutzaufsichtsbehörde. Dieser obliegt damit die konkrete Aufsicht, ob das Betreiberunternehmens die Vorschriften der DSGVO einhält. In der Folge unterliegt die Betreibergesellschaft gegenüber dem BfDI keinen Mitwirkungspflichten. Dadurch ist seitens BfDI aufgrund Eingriffs in die Aufsichtsbefugnisse der jeweiligen Landesdatenschutzaufsichtsbehörde keine Vor-Ort-Kontrolle möglich und er ist in diesen Fällen immer auf eine mittelbare Einwirkung über den Verantwortlichen (bzw. einem Auftragsverarbeiter) unter seiner Datenschutzaufsicht angewiesen.

Eine vollständige einheitliche Aufsicht durch den BfDI ist in den genannten Konstellationen somit allein auf Basis eines Auftragsverarbeitungsverhältnisses nicht gewährleistet, vielmehr erfolgt die Aufsicht über die Einhaltung der DSGVO bei der Verarbeitung personenbezogener Daten in der Erfüllung öffentlicher Aufgaben des Bundes teilweise durch die jeweils zuständige Landesdatenschutzaufsichtsbehörde.

Eine vollständige und uneingeschränkte Aufsicht durch den BfDI über das privatrechtlich organisierte Betreiberunternehmen wäre möglich, wenn dieses insoweit den vom Bund beherrschten Auftragsverarbeitern gleichgestellt wird. Zwar nimmt das Betreiberunternehmen in diesem Falle öffentliche Aufgaben des Bundes wahr, jedoch ist die weitere Voraussetzung, die Beherrschung durch den Bund im Sinne einer Mehrheitsbeteiligung oder eines auf andere Weise hergestellten alleinigen Einflusses des Bundes auf alle wesentlichen Entscheidungen der Geschäftstätigkeit, nicht zwangsläufig gegeben. Die vorgeschlagene Ergänzung des § 9 Abs. 1 schließt diese Lücke und stellt sicher, dass bei Anwendungen wie beispielsweise einer Bundescloud eine durchgehende Aufsicht durch den BfDI besteht. Führt das Betreiberunternehmen auch andere Verarbeitungsvorgänge außerhalb der Tätigkeit für den Bund durch, gelten weiterhin die Zuständigkeiten der Landesdatenschutzaufsichtsbehörden nach § 40 BDSG. Insofern entstünde eine geteilte, aber klar abgrenzbare Aufsichtszuständigkeit ähnlich wie bei Anbietern von Telekommunikations- oder Postdienstleistungen.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 A

Technische Universität München | Arcisstraße 21 | 80333 München
Professor Paal | Chair for Law and Regulation of the Digital Transformation

München, 19. Juni 2024

Stellungnahme für die öffentliche Anhörung des Deutschen Bundestages – Ausschuss für Inneres und Heimat – am 24. Juni 2024

zum Gesetzentwurf der Bundesregierung – Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes
BT-Drucksache 20/10859

Sehr geehrte Mitglieder des Ausschusses,

der Stellvertretende Vorsitzende des Ausschusses für Inneres und Heimat, Herr Prof. Dr. Lars Castellucci, MdB hat mich eingeladen, an der o.g. Anhörung als Sachverständiger teilzunehmen. Dieser Einladung komme ich sehr gerne nach. Nachstehend übersende ich zur Vorbereitung der Anhörung auf Aufforderung einige grundsätzliche Stellungnahmen zu ausgewählten Punkten des Gesetzesvorhabens. Wegen der Kurzfristigkeit der Einladung und weiterer Verpflichtungen konnten leider nur vergleichsweise knappe Ausführungen erfolgen. Ich danke Ihnen für die Kenntnisnahme meiner Stellungnahmen und freue mich darauf, in der öffentlichen Anhörung weitergehende Ausführungen vorzunehmen und Ihre Fragen zu beantworten.

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

Durch § 16a BDSG-E soll die Institutionalisierung der Datenschutzkonferenz (DSK) als des Gremiums der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder vollzogen werden. Die gesetzliche Verankerung der DSK und die Festlegung der Geschäftsordnung sind in Ansehung der Bedeutung der DSK und der Unabhängigkeit der Datenschutzaufsichtsbehörden des Bundes und der Länder uneingeschränkt zu begrüßen.

In materieller Hinsicht enthält § 16a BDSG-E allerdings über die Formalisierung hinaus kaum neue Impulse, so arbeitet die DSK bereits seit längerem auf der Grundlage einer von ihr selbst gegebenen Geschäftsordnung. Vor diesem Hintergrund wäre es wünschenswert, zusätzliche Regelungen in § 16a BDSG-E aufzunehmen, um die Arbeit der DSK zu erleichtern und die Stellung der Institution zu stärken.

TU München
School of Social Sciences and Technology (SOT)
Department of Governance

Prof. Dr. Boris P. Paal, M.Jur. (Oxon.)
Chair for Law and Regulation of the Digital Transformation
Zertifizierter Wirtschaftsmediator
Richter am LG Hamburg a.D.

Postadresse
Arcisstr. 21 . 80333 München
Besucheradresse
Richard-Wagner-Straße 1
80333 München

Kontaktdaten
Tel.: +49 89 907 793 240
Mobil: +49 151 571 46 846
boris.paal@tum.de
www.gov.sot.tum.de/lrd

Konkret empfehlen sich eine Festschreibung der Ziele der DSK und gesetzliche Festlegungen zu einer organisatorischen Unterstützung der Arbeit der DSK durch eine auskömmlich finanzierte ständige Geschäftsstelle.

II. Zur Neuregelung des Scoring (§ 37a BDSG-E)

1. Vorbemerkungen

Da an der Unionsrechtskonformität des aktuellen § 31 BDSG mit guten Gründen erhebliche Zweifel bestehen, ist im Ausgangspunkt uneingeschränkt zu begrüßen, dass der Gesetzgeber diesen Zustand zu beseitigen beabsichtigt. Ein Urteil des EuGH vom Dezember 2023 (Rs. C-634/21) hat diese Entwicklung weiter beschleunigt: Nach der einen Scoring-Sachverhalten betreffenden Vorabentscheidung des EuGH enthält Art. 22 Abs. 1 DS-GVO – anders als der Wortlaut dies nahelegt: „Recht“ – ein grundsätzliches Verbot, betroffene Personen einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung zu unterwerfen.

Nach Art. 22 Abs. 1 DS-GVO hat die betroffene Person das Recht, dass Entscheidungen, die für sie eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, nicht ausschließlich aufgrund einer automatisierten Datenverarbeitung getroffen werden. Nach Abs. 2 der Vorschrift gilt dieses Verbot allerdings nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist (lit. a), sie aufgrund einer unions- oder mitgliedstaatlichen Rechtsvorschrift zulässig ist (lit. b) oder wenn die betroffene Person ausdrücklich eingewilligt hat (lit. c). Voraussetzung ist hierfür stets, dass eine solche Entscheidung mit angemessenen Garantien zum Schutz der betroffenen Person verbunden ist. Mitgliedstaatliche Regelungsspielräume bestehen hier grundsätzlich (nur) für 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.

Art. 22 DS-GVO betrifft nur das Verfahren der automatisierten Einzelentscheidung. Demgegenüber trifft Art. 22 DS-GVO gerade keine Festlegungen betreffend die Rechtmäßigkeitsvoraussetzungen der konkreten Verarbeitung von der Entscheidung zugrundeliegenden Daten; es handelt sich also gerade nicht um einen Erlaubnistatbestand im Sinne des Art. 6 Abs. 1 DS-GVO. Der EuGH hat in der vorbezeichneten Entscheidung ausdrücklich darauf hingewiesen, dass die Mitgliedstaaten nach Art. 22 Abs. 2 lit. b DS-GVO keine Rechtsvorschriften erlassen dürfen, nach denen der Erlass einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unter Missachtung der Anforderungen von Art. 5 und 6 DS-GVO in deren Auslegung durch die Rechtsprechung des Gerichtshofs zulässig wäre; zudem hat der Gerichtshof klargestellt, dass die Mitgliedstaaten keine Legislativkompetenz haben, um näher ausgestaltende 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).

2. Zum Anwendungsbereich und der generellen Terminologie

Entgegen der aktuell vorgeschlagenen Überschrift („Scoring“) kann sich § 37a BDSG-E nach unionsrechtlichen Vorgaben und der vorbezeichneten Rechtsprechung des EuGH alleine auf den Ausnahmetatbestand des Art. 22 Abs. 2 lit. b DS-GVO betreffend automatisierte Entscheidungen im Einzelfall stützen. Eine darüber hinausgehende nationale Regelungsbefugnis im Sinne einer umfassenden Ausgestaltung sämtlicher Scoring-Sachverhalte ist dagegen nicht eröffnet.

Zur Vermeidung von Missverständnissen und Rechtsunsicherheiten daher die Überschrift den Anwendungsbereich möglichst klar und unmissverständlich benennen. Es empfiehlt sich daher eine konkretisierende Änderung der Benennung der Vorschrift, wonach es sich in § 37a BDSG-E um „Ausnahmen vom Verbot automatisierter Entscheidungen im Einzelfall bei Scoring” handelt.

Der vorbezeichnete Befund setzt sich in der Terminologie des § 37a Abs. 1 BDSG-E fort: § 37a Abs. 1 BDSG-E stellt auf die Erstellung oder Verwendung eines Wahrscheinlichkeitswerts ab und berücksichtigt nicht hinreichend die zusätzlichen Anforderungen, unter denen ein Scoring dem Art. 22 Abs. 1 DS-GVO unterfällt und die Regelungsbefugnis des deutschen Gesetzgebers eröffnet ist. Nach der Rechtsprechung des EuGH handelt es sich bei der Erstellung eines Wahrscheinlichkeitswerts gerade dann um eine Entscheidung im Sinne des Art. 22 Abs. 1 DS-GVO, wenn von diesem Wahrscheinlichkeitswert „maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet“ (EuGH, C-634/21, Rn. 73).

Es empfiehlt sich daher, in § 37a Abs. 1 BDSG darauf abzustellen, dass ebendieser Wahrscheinlichkeitswert nicht bloß erstellt, sondern gerade für die Entscheidung verwendet wird, ob ein Vertragsverhältnis mit der betroffenen Person begründet, durchgeführt oder beendet wird.

3. § 37a Abs. 2 Nr. 1 lit. a BDSG-E – Verbot der Verwendung besonderer Kategorien personenbezogener Daten

Art. 22 Abs. 4 DS-GVO statuiert ein Verbot, besondere Kategorien personenbezogener Daten den Entscheidungen im Sinne des Art. 22 Abs. 2 DS-GVO vorbehaltlich der in Art. 9 Abs. 2 lit. a und g DS-GVO genannten Ausnahmen zugrunde zu legen. Die Regelung in § 37a Abs. 2 Nr. 1 lit. a BDSG-E geht darüber hinaus, indem sie die Verwendung besonderer Kategorien personenbezogener Daten ausnahmslos untersagt.

Eine entsprechende Regelungskompetenz des deutschen Gesetzgebers erscheint zweifelhaft und dürfte sich insbesondere nicht (mehr) aus Art. 22 Abs. 2 lit. b DS-GVO ableiten lassen.

Es empfiehlt sich daher, die Regelung in § 37a Abs. 2 Nr. 1 lit. a BDSG-E ersatzlos zu streichen.

4. § 37a Abs. 2 Nr. 1 BDSG-E – Implementierung von Diskriminierungsverboten

Unbeschadet der rechtlichen Rahmungen durch – insbesondere – das Wettbewerbsrecht und die EU-KI-Verordnung sollte die Implementierung eines Verbot der Nutzung von Daten zum Alter (für Wahrscheinlichkeitswerte nach § 37a Abs. 1 Nr. 1 BDSG-E) und zum Geschlecht der betroffenen Person als Grundlagen der Erstellung oder Verwendung eines Wahrscheinlichkeitswertes erwogen werden.

5. § 37a Abs. 6 BDSG-E – Präzisierung der Rechte von betroffenen Personen

Um die Effektivität der Schutzrechte für betroffene Personen zu stärken, sollte eine Verpflichtung zum Hinweis auf die Rechte der betroffenen Personen in verständlicher und von anderen Informationen getrennter Form statuiert werden. Danach hätten die Verantwortlichen betroffene Personen in verständlicher und von anderen Informationen getrennter Form entsprechend zu unterrichten.

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

Die Regelungen des § 34 Abs. 1 S. 2 BDSG-E und des § 83 Abs. 1 S. 2 SGB X-E sollen die Wahrung des Geschäfts- und Betriebsgeheimnisses bei der Durchsetzung von Auskunftsansprüchen sicherstellen.

Hier bestehen nicht nur unerhebliche Zweifel an der Vereinbarkeit der vorgeschlagenen Änderungen mit dem höherrangigen Unionsrecht, konkret mit Art. 23 DS-GVO. 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.

Allerdings finden die in § 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB X-E adressierten Aspekte bereits einen gesetzlichen Niederschlag in Art. 15 Abs. 4 DS-GVO und werden zudem konkretisiert durch Erwägungsgrund 63 S. 5 DS-GVO. In Ansehung von Art. 15 Abs. 4 DS-GVO, der nur hinsichtlich des Rechts auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DS-GVO anordnet, dass die Rechte und Freiheiten anderer Personen nicht beeinträchtigen werden dürfen, ist zweifelhaft, ob § 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB X-E weiter gefasst werden dürfen als dies der Unionsgesetzgeber vorgesehen hat.

Es wird deshalb empfohlen, die vorgeschlagenen Änderungen des § 34 BDSG und des § 83 SGB X zu streichen.

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 B

verbraucherzentrale
Bundesverband

FAIRES UND TRANSPARENTES BONITÄTS-SCORING GESETZLICH VERANKERN

Stellungnahme des Verbraucherzentrale Bundesverbandes e.V. (vzbv) zum Regierungsentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG)

28. März 2024

Impressum

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Team Finanzmarkt
finanzen@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.

INHALT

VERBRAUCHERRELEVANZ

Bonitäts-Scores drücken die geschätzte Wahrscheinlichkeit aus, mit der Verbraucher:innen ihre vertraglich vereinbarten Zahlungen erfüllen. Diese Wahrscheinlichkeitswerte nutzen Anbieter, die in finanzielle Vorleistung gehen, um zu entscheiden, ob sie Verträge mit Verbraucher:innen schließen. Typischerweise handelt es sich dabei um Kredit- oder Telekommunikationsverträge. Aber auch um online auf Rechnung bezahlen zu können, ist oft ein guter Score nötig. Ein schlechter Score führt schnell zu einer Vertragsablehnung oder schlechteren Konditionen. Eine Ablehnung solcher Verträge auf Grundlage eines Bonitäts-Scores hat starke Auswirkungen auf den Verbraucheralltag. Bonitäts-Scores zu erstellen und zu verwenden, sollte daher besonderen Vorschriften im Hinblick auf den Schutz vor Diskriminierung und Falschbewertungen sowie Nachvollziehbarkeit und Transparenz unterliegen.

Insbesondere für den Bereich des Bonitäts-Scoring, aber auch darüber hinaus, ist das Recht auf Auskunft für Verbraucher:innen wesentlich. Nur so ist Transparenz und Kontrolle über die verarbeiteten Daten möglich. Dies fördert Vertrauen und schafft einen Ausgleich zwischen individuellen Rechten und Unternehmensinteressen. Zudem erleichtert es die Rechtsdurchsetzung, indem bei Verstößen gegen Datenschutzbestimmungen rechtliche Schritte ergriffen werden können. Ein wirksames Auskunftsrecht liegt damit nicht nur im Interesse der Betroffenen, sondern gleichermaßen im Interesse aller Unternehmen, die sich an die rechtlichen Vorgaben halten.

ZUSAMMENFASSUNG

Grundsätzlich begrüßt der Verbraucherzentrale Bundesverband (vzbv) den vorliegenden Regierungsentwurf für ein Bundesdatenschutzgesetz (BDSG-E) und nimmt im Einzelnen folgende Bewertungen vor:

- § 37a BDSG-E kann – im Sinne des Urteils C-634/21 des Europäisches Gerichtshofes[1] – nur Anwendung finden, wenn ein Bonitäts-Score eine Vertragsentscheidung „maßgeblich“ beeinflusst. Im weiteren Gesetzgebungsverfahren sollte geprüft werden, ob einheitliche und objektive Kriterien in § 37a BDSG-E aufgenommen werden können, um diese Maßgeblichkeit im Einzelfall zweifelsfrei festzustellen.[2]
- Die neuen Regelungen (§ 37a Abs. 2 Nr. 1 und 2 BDSG-E) schließen sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO, den Namen der Verbraucher:innen, Daten aus der Nutzung von sozialen Netzwerken, Kontoinformationen sowie Anschriftendaten von der Score-Berechnung aus und verhindern, dass Minderjährige von der Verarbeitung betroffen sind. Diese Anforderungen stellen einen wichtigen Schritt hin zu einem fairen Bonitäts-Scoring dar und sollten vollumfänglich beibehalten werden.
- Die Anforderungen an die Auswahl der zu berücksichtigenden Daten nach § 37a Abs. 2 Nr. 3 a) BDSG-E und die Genauigkeit der Bonitäts-Scores sollten konkretisiert werden, damit ein einheitliches Qualitätsniveau erreicht wird. Die Erfüllung dieser Anforderungen sollte von einer unabhängigen Stelle verpflichtend zertifiziert werden.
- Unternehmen, die Scores einer Änderung oder Kündigung eines bestehenden oder Ablehnung eines gewünschten Vertrages zugrunde legen, sollten dazu verpflichtet werden, Verbraucher:innen aktiv über die Rolle des Scores in der Vertragsentscheidung, den Score an sich und das berechnende Unternehmen zu informieren. Nur so werden Verbraucher:innen dazu veranlasst, die Richtigkeit ihrer Daten zu prüfen, diese gegebenenfalls zu korrigieren oder von Eingriffsrechten nach § 37a Abs. 6 BDSG-E Gebrauch zu machen.
- Mittels einer klaren Definition der Begriffe „Kriterien“ und „Kategorien“ im § 37a Abs. 4 Nr. 2 BDSG muss sichergestellt werden, dass Verbraucher:innen die ihnen gegebene Auskunft auf ein konkretes Verhalten zurückführen können. Nur so kann sichergestellt werden, dass Verbraucher:innen die Korrektur von falschen Daten und die Bildung eines eigenen Standpunktes nach § 37a Abs. 6 BDSG-E möglich ist.
- Die Transparenzanforderungen nach § 37a Abs. 4 Nr. 2 BDSG-E sollten dahingehend konkretisiert werden, dass die Gewichtung der fünf wichtigsten Kriterien und der übergeordneten Kategorien untereinander dargestellt werden müssen.
- Die Absicherung des Auskunftsrechtes von Verbraucher:innen nach § 37a Abs. 5 BDSG-E sollte beibehalten werden. Es ist nicht gerechtfertigt, den Schutz von Betriebs- und Geschäftsgeheimnissen über die Transparenz von automatisierten Einzelfallentscheidungen zu stellen.
- Die Einräumung des Rechtes auf Anfechtung, Darlegung des eigenen Standpunktes und Entscheidung einer natürlichen Person nach § 37a Abs.6 BDSG-E ist wesentlich, damit Verbraucher:innen einer Bonitäts-Bewertung in Form eines Scores

[1] EuGH, Urteil vom 07.12.2023, Rs. C-634/21

[2] siehe auch BR-Drs. 72/1/24, 2024, 1655, 2017, S. 7f

nicht machtlos gegenüberstehen. Daher sollte diese Regelung beibehalten werden.

- Artikel 15 DSGVO sowie § 29 Abs. 1 BDSG berücksichtigen bereits angemessen den Schutz von Geschäftsgeheimnissen. Die unter § 34 BDSG-E vorgeschlagene darüber hinausgehende Einschränkung des Auskunftsrechts lehnt der vzbv ab. Diese weitere Einschränkung im nationalen Recht würde die Wahrnehmung des wichtigen Rechts auf Auskunft erschweren.

EINLEITUNG

Bonitäts-Scores drücken die geschätzte Wahrscheinlichkeit aus, mit der Verbraucher:innen vertraglich vorgesehene Zahlungen bedienen. Dafür werden Profile von Verbraucher:innen erstellt und mit personenbezogenen Daten angereichert. Anhand dieser Daten ordnen Wirtschaftsauskunfteien Verbraucher:innen Vergleichsgruppen zu und betrachten die Unterschiede im Hinblick auf das Zahlungsausfallrisiko. Es wird also von der Gruppe auf den oder die Einzelne geschlossen.[3]

Die enorme Bedeutung der Scores für den Zugang zu Verträgen und damit für die Teilhabe von Verbraucher:innen am Wirtschaftsverkehr, begründet den Bedarf an besonderen gesetzlichen Anforderungen an die Berechnung und Verwendung dieser Scores.

Die bisherigen Regelungen zum Bonitäts-Scoring im Bundesdatenschutzgesetz (BDSG) regelten die Zulässigkeit der „Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) (…)“.[4] Diese Zulässigkeit wurde an bestimmte Anforderungen geknüpft, die Verbraucher:innen grundlegenden Schutz vor einer willkürlichen Prognose ihres Zahlungsverhaltens boten.

Allerdings hat der Europäische Gerichtshof (EuGH) kürzlich in einem Urteil die Berechtigung Deutschlands, eigene Regelungen zu diesem Vorgehen zu treffen, die über die Datenschutz-Grundverordnung (DSGVO) hinausgehen, in Zweifel gezogen.[5] Auf diese Entscheidung hat die Bundesregierung reagiert und im Rahmen der Novellierung des BDSG einen Vorschlag für einen neuen § 37a vorgelegt, der die alten Anforderungen des § 31 BDSG-alt übernimmt und ausweitet, jedoch einen eindeutigen Bezug auf die nationale Öffnungsklausel des Art. 22 Abs. 2 lit. b) DSGVO zur Regulierung von automatisierten Einzelfallentscheidungen aufstellt. Außerdem setzt sie damit das Vorhaben ihres Koalitionsvertrags um, die Transparenz beim Bonitäts-Scoring zu erhöhen.

Grundsätzlich begrüßt der vzbv die neuen Bestimmungen des § 37a BDSG-E, da wichtige Fortschritte in Richtung eines transparenten und fairen Scoring-Verfahrens[6] erkennbar sind.

In ihrem Gesetzesentwurf schlägt die Bundesregierung ferner vor, § 34 BDSG zu ändern und das Auskunftsrecht zugunsten des Schutzes von Betriebs- und Geschäftsgeheimnissen einzuschränken. Da Artikel 15 DSGVO sowie § 29 Abs. 1 BDSG den Geschäftsgeheimnisschutz bereits angemessen berücksichtigen, lehnt der vzbv die Vorschläge ab.

Im Folgenden werden die Bestimmungen einzeln bewertet und weiterer Verbesserungsbedarf im Interesse der Verbraucher:innen aufgezeigt.

---

[3] Sachverständigenrat für Verbraucherfragen: Gutachten Verbrauchergerechtes Scoring, 2018, https://www.zu-daily.de/daily-wAssets/pdf/SVRV_Verbrauchergerechtes_Scoring.pdf, S. 51, zuletzt abgerufen am 01.03.2024

[4] siehe §31 Abs. 1 Nr. 2 BDSG

[5] EuGH, Urteil vom 07.12.2023, Rs. C-634/21, Rn. 71

[6] siehe Verbraucherzentrale Bundesverband e.V.: Verbrauchergerechtes Bonitäts-Scoring, 2023, https://www.vzbv.de/sites/default/files/2023-12/FIN-23-12-04_Positionspapier_vzbv_Verbrauchergerechtes%20Bonit%C3%A4tsscoring.pdf, zuletzt abgerufen am 12.03.2024

KOMMENTIERUNG IM EINZELNEN

1. ZU § 37A BDSG-E – SCORING

Absatz 1 des neuen § 37a BDSG-E definiert den Anwendungsbereich der Regelung. Diese umfasst demnach jene automatisierten Einzelfallentscheidungen, die nach Art. 22 Abs. 1 DSGVO grundsätzlich verboten sind, allerdings durch eine nationale Bestimmung unter Berücksichtigung der beteiligten Interessen erlaubt werden können.[7] Der §37a BDSG-E stellt eine solche nationale Ausnahmeregelung für die Erstellung oder Verwendung von Wahrscheinlichkeitswerten im Sinne einer automatisierten Einzelfallentscheidung nach Art. 22 DSGVO dar.

Vor dem Hintergrund des EuGH-Urteils zu der Frage, inwiefern ein durch eine Wirtschaftsauskunftei berechneter Score, der in der Kreditvergabeentscheidung eines Kreditinstitutes berücksichtigt wird, eine automatisierte Einzelfallentscheidung nach Art. 22 DSGVO darstellt und damit den Anforderungen des § 37a BDSG-E unterliegen würde, herrscht jedoch Unklarheit. Der EuGH stellt keine objektiven Kriterien für die Einordung des Scores unter den Anwendungsbereich von Art. 22 DSGVO auf, sondern nennt nur die nicht näher beschriebene Bedingung, dass die Vertragsentscheidung „maßgeblich“ vom Bonitäts-Score abhängen muss.[8] Für Verbraucher:innen mündet dieser Umstand in der Unklarheit, ob sie die Einhaltung der erweiterten Anforderungen des § 37a BDSG-E für die Erstellung und Verwendung ihres persönlichen Scoring-Wertes zukünftig erwarten können.

> Im weiteren Gesetzgebungsverfahren sollte geprüft werden, ob einheitliche und objektiv überprüfbare Kriterien zur Feststellung der Maßgeblichkeit in § 37a BDSG-E aufgenommen werden können.[9] Alternativ müssten solche Kriterien für Verbraucher:innen und Aufsichtsbehörden durch die Gerichte oder eine weitere europäische Gesetzgebung eingeführt werden. Dies würde allerdings sehr viel länger dauern und damit eine längere Unsicherheit für Verbraucher:innen bedeuten.

1.1 Zu § 37a Abs. 2 Nr. 1 und 2 BDSG-E – Ausschluss bestimmter Daten und Schutz Minderjähriger

Absatz 2 des neuen § 37a BDSG-E nennt bestimmte Datenkategorien, die nicht in die Score-Berechnung einfließen dürfen. Die Einführung einer Negativliste für die Datenverarbeitung stellt einen echten Fortschritt für ein faires Bonitäts-Scoring dar. Der vzbv unterstützt die Regelungen des § 37a Abs. 2 Nr. 1 BDSG-E.

Der Ausschluss von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO, Informationen aus der Nutzung sozialer Netzwerke oder Kontoinformationen ist eine effektive Möglichkeit, um den Missbrauch dieser Daten, die die persönlichste Lebensführung von Verbraucher:innen betreffen und ein hohes Diskriminierungspotential bergen, zu verhindern. Insbesondere bei Daten über das Zahlungsverhalten (Kontoinformationen) oder die Selbstdarstellung in sozialen Medien ist davon auszugehen, dass Verbraucher:innen bei einem Wissen über die Berücksichtigung in der Datenverarbeitung ihr Verhalten bewusst an eine bekannte oder vermutete Verarbeitungslogik anpassen würden. So kann es beispielsweise dazu kommen, dass Verbraucher:innen in bestimmten Läden (nicht mehr) einkaufen oder bestimmte Hobbys in

[7] siehe Art. 22 Abs. 2 lit. b DSGVO

[8] EuGH, Urteil vom 07.12.2023, Rs. C-634/21, Rn. 73

[9] siehe auch Stellungnahme des Bundesrats, BR-Drs. 72/24(B), 2024, Nr. 7 lit. c), S. 8

sozialen Medien (nicht mehr) darstellen, um ihren Score zu verbessern. Diese Rückkopplung des Scoring-Verfahrens muss ausgeschlossen werden, weil dies einen zu starker Einfluss auf die persönliche Lebensführung der Verbraucher:innen ausüben würde.

Der Name der Verbraucher:innen, aber auch Informationen über die Herkunft oder biometrische Daten, liegen nicht in der Einflusssphäre von Verbraucher:innen. Sie sind also nicht verhaltensabhängig, sondern vorbestimmt. Die Bestimmung eines negativen Einflusses dieser Merkmale auf den Bonitäts-Score würde also ohne eine aktive Handlung der Verbraucher:innen einen schlechteren Score erzeugen. Somit kann es zu einer großen Diskrepanz zwischen dem Verhalten einzelner zu scorender Verbraucher:innen und dem der anhand des Merkmals gebildeten Vergleichsgruppe kommen. Daher ist der Ausschluss von Daten nach Artikel 9 Abs. 1 DSGVO und dem Namen eine wichtige Vorschrift.

Die Verwendung von Adressdaten wurde bereits im § 31 BDSG eingeschränkt, wobei dort nur die Berechnung eines Bonitäts-Scores allein auf Basis von Anschriftendaten untersagt wurde. Der komplette Ausschluss dieser Datenkategorie, wie jetzt vorschlagen, ist von besonderer Bedeutung, da Verbraucher:innen durch sie – möglicherweise völlig grundlos – erheblich benachteiligt werden. Grund dafür ist die Art, wie Bonitäts-Scoring als statistische Methode die Prognose über die Zahlungswilligkeit der Verbraucher:innen berechnet. Dabei werden Verbraucher:innen anhand des berücksichtigten Merkmals in Gruppen eingeteilt und im Hinblick auf das Zahlungsverhalten mit anderen so gebildeten Gruppen verglichen. Im Fall von Adressdaten werden also alle Verbraucher:innen der gleichen Straße oder mit der gleichen Postleitzahl einem Zahlungsverhalten zugeordnet. Das Problem daran ist, dass Verbraucher:innen, die ein tadelloses Zahlungsverhalten aufweisen, schlechter bewertet werden, wenn ihre Nachbarn ihre Rechnungen oder Kreditraten nicht bezahlen. Diese unfaire Praxis der Datenverarbeitung wird durch den Ausschluss dieser Datenkategorie unterbunden.

§ 37a Abs. 2 Nr. 2 BDSG-E untersagt die Erstellung oder Verwendung von Scores, die Minderjährige betreffen. Der Ausschluss von automatisierten Einzelfallentscheidungen, die Minderjährige betreffen, ist in der DSGVO festgelegt. Kinder sind eine besonders schützenswerte Verbrauchergruppe, daher ist ihr Ausschluss vom Bewertungssystem des Bonität-Scorings zu begrüßen.

> Der Ausschluss bestimmter Datenkategorien gemäß § 37a Abs. 2 Nr. 1 und 2 BDSG-E wird vom vzbv vollumfänglich unterstützt und muss beibehalten werden. Dies stellt einen echten Fortschritt hin zu einem fairen Bonitäts-Scoring dar.

1.2 Zu § 37a Abs. 2 Nr. 3 a) BDSG-E – Qualitätsanforderungen

§ 37a Abs. 2 Nr. 3 BDSG-E stellt besondere Anforderungen an die personenbezogenen Daten, die für die Berechnung oder Verwendung der Bonitäts-Scores nach Abs. 1 dieser Norm verwendet werden dürfen.

Unter lit. a) wird die alte Regelung des § 31 BDSG übernommen, wonach die für die Berechnung verwendeten personenbezogenen Daten unter Verwendung eines mathematisch statistischen Verfahrens nachweisbar erheblich sein müssen. Diese Anforderung ist grundsätzlich zu begrüßen, da sie die komplett willkürliche Auswahl von Kategorien personenbezogener Daten ausschließt.

Sie ist allerdings nicht ausreichend, um ein einheitlich hohes Maß an Qualität der Scores in Bezug auf Prognosegenauigkeit und Aussagekraft sicherzustellen. Die Formulierung eines „anerkannten mathematisch-statistischen Verfahrens“ lässt eine ganze

Bandbreite möglicher Methoden zu. Es besteht das Risiko, dass qualitativ schlechte Scores über den Zugang zu Verträgen entscheiden. Hier sollten konkrete Qualitätsanforderungen an die Prognosegenauigkeit und Aussagekraft der Scores festgelegt und im Rahmen von verpflichtenden Zertifizierungsverfahren geprüft werden müssen. Es muss deutlich werden, welche Bedingungen gelten, damit personenbezogene Daten für die Berechnung der Wahrscheinlichkeitswerte erheblich sind und welche Genauigkeit Bonitäts-Scores vorweisen müssen. Die Einhaltung dieser Anforderungen muss über ein verpflichtendes Zertifizierungsverfahren durch eine unabhängige Stelle geprüft werden, die durch die zuständigen Aufsichtsbehörden anerkannt wurde oder den Maßgaben des Artikel 43 DSGVO entspricht.[10] So kann sichergestellt werden, dass die Verantwortlichen, die Wahrscheinlichkeitswerte im Sinne des Absatzes 1 erstellen, keine mathematisch-statistischen Verfahren anwenden, die diskriminierenden, fehlerhaften oder ungerechtfertigten Ergebnisse produzieren. Vertragsschlüsse dürfen nicht durch ungenaue Scores verhindert werden.

> Die Anforderungen an die Verarbeitung von personenbezogenen Daten nach § 37a Abs. 2 Nr. 3 a) BDSG-E müssen konkretisiert werden. Es bedarf konkreter Qualitätsanforderungen an die Prognosegenauigkeit und Aussagekraft der Scores. Nur so können Verbraucher:innen vor ungenauen, diskriminierenden, fehlerhaften oder ungerechtfertigten Scores geschützt werden. Damit diese Qualitätsanforderungen in der Praxis eingehalten werden, müssen Verantwortliche dazu verpflichtet werden, ihre Scores durch eine unabhängige Stelle regelmäßig zertifizieren zu lassen.

1.3 Zu § 37a Abs. 4 BDSG-E (neu) – Informationspflichten

Die Verwendung und Berechnung von Bonitäts-Scores läuft für Verbraucher:innen in vielen Fällen im Verborgenen ab, solange sie nicht aktiv Auskunft verlangen.[11] Eine Beeinträchtigung der Verbraucher:innen durch das Verfahren ist so oft nicht wahrnehmbar. Deshalb sollten Unternehmen, die den Bonitäts-Score zum Anlass einer Änderung, Kündigung oder Ablehnung eines Vertrages genommen haben, aktiv über den Score an sich, seine Rolle in der Vertragsentscheidung und das Unternehmen, das den Score berechnet hat, informieren.[12] Erst wenn klar ist, dass der eigene Bonitäts-Score einen negativen Einfluss auf die Vertragsentscheidung genommen hat, sind Verbraucher:innen veranlasst, die Richtigkeit ihrer Daten zu prüfen und gegebenenfalls eine Korrektur zu verlangen oder ihre Rechte nach § 37a Abs. 6 BDSG-E wahrzunehmen.

> Es sollte ein neuer Absatz in § 37a BDSG-E eingefügt werden, der eine Informationspflicht der Verwender von Wahrscheinlichkeitswerten nach § 37a Abs. 1 BDSG-E für den Fall vorsieht, dass der Wert als Anlass für eine Änderung, Kündigung oder Ablehnung eines bestehenden oder vorgesehenen Vertrages genommen wurde. Für diesen Fall sollten Verbraucher:innen über den Score-Wert an sich, seine Bedeutung für die Vertragsentscheidung und das Unternehmen, das den Bonitäts-Score bereitgestellt hat, informiert werden.

[10] siehe auch Stellungnahme des Bundesrats, BR-Drs. 72/24(B), 2024, Nr. 6, S. 6

[11] Im Fall der Ablehnung eines Verbraucherdarlehensvertrages oder eines Vertrages über eine entgeltliche Finanzierungshilfe müssen Verbraucher:innen bereits nach § 30 Abs. 2 BDSG proaktiv über die Berücksichtigung des Scores und den Score unterrichtet werden.

[12] siehe auch Stellungnahme des Bundesrats, BR-Drs. 72/24(B), 2024, Nr. 7 lit. b), S. 7

Formulierungsvorschlag § 37a Abs. 4 BDSG-E (neu):
(4) Verantwortliche, die Wahrscheinlichkeitswerte im Sinne des Absatzes 1 verwenden und daraus eine Änderung oder Kündigung eines bestehenden Vertrages oder eine Ablehnung eines vorgesehenen Vertrages folgt, müssen der betroffenen Person unverzüglich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache Folgendes mitteilen:

1. die Bedeutung der Wahrscheinlichkeitswerte für die Vertragsentscheidung,
2. die konkreten Wahrscheinlichkeitswerte und
3. das Unternehmen, das die Wahrscheinlichkeitswerte erstellt hat.

Die hierfür erforderlichen Informationen sind für ein Jahr zu speichern.

1.4 Zu § 37a Abs. 4 BDSG-E - Transparenzanforderungen

§ 37a Abs. 4 BDSG-E stellt mehrere Anforderungen an die Art, wie Verantwortliche dem Auskunftsersuchen von Verbraucher:innen entsprechen müssen, die so im §31 BDSG nicht enthalten waren. Alle Anforderungen des Absatzes sind sinnvolle Ergänzungen und tragen dazu bei, die Score-Berechnung für Verbraucher:innen nachvollziehbar zu gestalten. Dies ist besonders dann wichtig, wenn Fehler in der Verarbeitung auftreten, Verbraucher:innen daraufhin beispielsweise Verträge gekündigt werden oder keine neuen Verträge erhalten. Dann ist es dringend erforderlich, genau zu erfahren, welche personenbezogenen Daten mit welcher Gewichtung verarbeitet wurden, um die Korrektur von falschen Daten zu erwirken oder Fehler in der Verarbeitungslogik erkennen zu können. Zudem sind diese Informationen essentiell, um die Eingriffsrechte nach Abs. 6 effektiv wahrnehmen zu können.

Um die Überprüfbarkeit sicherzustellen, muss vorgeschrieben werden, dass die Gewichtung von Informationen über ein konkretes Verhalten von Verbraucher:innen aufgezeigt werden muss. Es muss ersichtlich sein, wie sich eine einzelne, nicht bediente Forderung im Sinne des § 37a Abs. 3 BDSG-E oder ein einzelner laufender Kreditvertrag auf den individuellen Bonitäts-Score auswirkt. Die fehlende Definition der Begriffe „Kriterien“ und „Kategorien“ in § 37a Abs. 4 Nr. 2 BDSG-E und der dazugehörigen Gesetzesbegründung birgt die Gefahr, dass Verbraucher:innen die ihnen erteilte Auskunft nicht für die Prüfung und mögliche Korrektur oder Beanstandung von falschen Daten oder Rückschlüssen nutzen können.

Um die Überprüfbarkeit des Scoring-Ergebnisses durch Verbraucher:innen sicherzustellen, muss der Wortlaut von § 37a Abs. 4 Nr. 2 BDSG-E dahingehend konkretisiert werden, dass ein konkretes individuelles Verhalten der Person als „Kriterium“ definiert wird, das mit seiner Gewichtung dargestellt werden muss. Als „Kategorie“ sollte ein Obergriff für die einzelnen Kriterien definiert werden.

Neben den genauen Begriffserklärungen, ergibt sich eine weitere Schutzlücke im § 37a Abs. 4 Nr. 2 BDSG-E. Es wird nicht klargestellt, wie viele „Kategorien von Kriterien, die den Wahrscheinlichkeitswert am stärksten beeinflussen“, schlussendlich offengelegt werden sollen. Daraus könnte die Beauskunftung von lediglich zwei beeinflussenden Kriterien resultieren. Wenn eine weitergehende Vielzahl von Kriterien in der Berechnung berücksichtigt wurde, sind diese Einflussfaktoren für Verbraucher:innen nicht ersichtlich. Auch so könnte die Möglichkeit der Verbraucher:innen, ihr Scoring-Ergebnis nachvollziehen und so effektiv prüfen zu können, stark eingeschränkt werden. Um dies

zu vermeiden, sollte gesetzlich eine konkrete Anzahl der nachweislich einflussstärksten Kriterien vorgeschrieben werden. Denkbar wäre es, konkret vorzuschreiben, dass die fünf einflussreichsten Kriterien mit ihrer Gewichtung dargestellt werden müssen.

§ 37a Abs. 4 BDSG-E wird grundsätzlich vom vzbv unterstützt. Nr. 2 sollte jedoch dahingehend konkretisiert werden, dass die fünf nachweislich einflussstärksten Kriterien, die auf den Score gewirkt haben, in ihrer Gewichtung dargestellt werden müssen.

Formulierungsvorschlag § 37 a Abs. 4 Nr. 2 BDSG-E

„2. die Gewichtung von ~~Kategorien von~~ fünf Kriterien und ~~der einzelnen Kriterien zueinander~~ deren übergeordneten Kategorien, die den Wahrscheinlichkeitswert nachweislich am stärksten beeinflussen sowie der Einfluss der Kategorien untereinander,“

1.5 Zu § 37a Abs. 5 BDSG-E – Sicherstellung des Auskunftsrechtes bei Betriebs- und Geschäftsgeheimnissen

Absatz 5 des § 37a BDSG-E schließt das Bonität-Scoring vom Anwendungsbereich des § 34 BDSG aus. Nach § 34 BDSG haben Verbraucher:innen kein Auskunftsrecht, wenn die Auskunft die Offenbarung eines Betriebs- oder Geschäftsgeheimnisses beinhalten kann und die Interessen des Unternehmens denen der Verbraucher:innen überwiegen.

Nach Ansicht des vzbv werden Betriebs- und Geschäftsinteressen bereits ausreichend über Artikel 15 DSGVO sowie § 29 Abs. 1 BDSG gesichert (siehe dazu folgende Kommentierung zu § 34 BDSG-E). Sollten die Änderungsvorschläge für § 34 BDSG-E dennoch übernommen werden, muss aufgrund der besonderen Risiken des Bonitäts-Scorings auch § 37a Abs. 5 beibehalten werden, um eine Absicherung des Auskunftsrechtes zu ermöglichen. Ansonsten besteht die Gefahr, dass Unternehmen verstärkt versuchen, berechtigte Auskunftsinteressen mit Verweis auf diese Regelung abzuwehren. Verbraucher:innen würde das Auskunftsrecht erschwert und so insbesondere die besonderen Auskunftspflichten des Artikel 15 Abs. 1 lit. h) DSGVO für automatisierte Entscheidungen in der Praxis unterlaufen werden.

Die Absicherung des Auskunftsrechtes von Verbraucher:innen nach § 37a Abs. 5 BDSG-E sollte beibehalten werden.

1.6 Zu § 37a Abs. 6 BDSG-E – Eingriffsrechte der Verbraucher:innen

§ 37a Abs. 6 BDSG-E übernimmt die Anforderungen des Art. 22 Abs. 3 DSGVO auch für die Ausnahme vom Verbot einer automatisierten Einzelfallentscheidung auf Grundlage des § 37a BDSG-E. Dadurch erhalten Verbraucher:innen das „Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung“. Diese Vorgaben sind bedeutend, damit Verbraucher:innen einer automatisierten Einzelfallentscheidung nicht wehrlos gegenüberstehen und das Ergebnis akzeptieren müssen. Die Möglichkeit, eine Entscheidung anzufechten oder einen eigenen Standpunkt darzustellen, verstärkt die Bedeutung der Transparenzvorschriften aus Absatz 4, da erst diese Informationen eine Meinungsbildung der Verbraucher:innen über die Datenverarbeitung ermöglichen.

Die Einräumung des Rechtes auf Anfechtung, Darlegung des eigenen Standpunktes und Entscheidung einer natürlichen Person im Fall der Verarbeitung nach Absatz 1 wird seitens des vzbv unterstützt.

2. ZU § 34 ABS. 1 BDSG-E – AUSKUNFTSRECHT DER BETROFFENEN PERSON

In ihrem Gesetzesentwurf schlägt die Bundesregierung eine ausdrückliche Ausnahme vom Recht auf Auskunft gemäß Artikel 15 DSGVO vor. Die Ausnahme soll greifen, wenn das Interesse an der Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Verantwortlichen oder eines Dritten dem Interesse der betroffenen Person an der Information überwiegt. Die Bundesregierung stützt diesen Vorschlag auf die Öffnungsklausel des Artikel 23 Abs. 1 lit. i) DSGVO, die es dem nationalen Gesetzgeber erlaubt, Einschränkungen der Betroffenenrechte zum Schutz der Rechte und Freiheiten anderer Personen vorzunehmen.

Aus Sicht des vzbv ist unverständlich, warum eine solche Einschränkung im nationalen Recht erforderlich sein sollte – auch im Gesetzesentwurf wird der Vorschlag nicht inhaltlich begründet. Bereits Artikel 15 DSGVO sowie § 29 Abs. 1 BDSG sehen einen angemessenen Schutz von Geschäftsgeheimnissen vor.

So wird das Recht auf Auskunft nach Artikel 15 DSGVO nicht grenzenlos gewährt. In Artikel 15 Abs. 4 DSGVO wird etwa betont, dass das Recht auf Erhalt einer Kopie nicht die Rechte und Freiheiten anderer Personen beeinträchtigen darf. Auch Erwägungsgrund 63 stellt klar, dass das Auskunftsrecht die Rechte und Freiheiten anderer Personen nicht beeinträchtigen soll und nennt hierfür explizit Geschäftsgeheimnisse als Beispiel. Allerdings dürfe dies nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

In seinen Leitlinien zum Auskunftsrecht äußert sich der Europäische Datenschutzausschuss (EDSA) hierzu ausführlich[13] und erklärt, dass die Formulierung „anderer Personen“ den Verantwortlichen einschließt. Außerdem seien die Rechte und Freiheiten anderer auch dann zu berücksichtigen, wenn der Zugang zu den personenbezogenen Daten auf andere Weise als durch eine Kopie gewährt wird. Wichtig sei jedoch, dass der Verantwortliche versuchen müsse, die kollidierenden Rechte miteinander in Einklang zu bringen, etwa durch Maßnahmen zur Minderung des Risikos für die Rechte und Freiheiten anderer. Allerdings, so der EDSA, betrifft diese Einschränkung lediglich den Erhalt einer Kopie der Daten, nicht jedoch die Auskunft über die Datenverarbeitung nach Artikel 15 Abs. 1 lit. a)-h) an sich. Vielmehr warnt der EDSA davor, dass bei der Auslegung von Artikel 15 Abs. 4 DSGVO in Verbindung mit Artikel 23 DSGVO besondere Vorsicht geboten sei, um die bestehenden Einschränkungen des Auskunftsrechts nicht in ungerechtfertigter Weise auszuweiten. Solch eine Ausweitung sei nur unter strengen Voraussetzungen zulässig.

Diesem Umstand trug auch der deutsche Gesetzgeber Rechnung, als er im Jahr 2017 das Bundesdatenschutzgesetz an die DSGVO anpasste. Bereits der damalige Gesetzesentwurf der Bundesregierung enthielt den Vorschlag, das Auskunftsrecht einzuschränken, wenn „allgemein anerkannte Geschäftszwecke“ den Auskunftsinteressen der betroffenen Person überwiegen würden.[14] Allerdings, so unter anderem die Kritik des Bundesrats[15], war diese Einschränkung zu weitreichend und nicht durch Arti-

[13] EDPB Guidelines 01/2022, Version 2.0, 2023, Rn. 168-174.

[14] BT-Drs. 18/11325, 2017, § 34 Abs. 1 Nr. 1.

[15] BT-Drs. 18/11655, 2017, Rn. 45.

kel 23 Abs. 1 lit. i) gedeckt. Daher wurde das Auskunftsrecht in § 29 Abs. 1 BDSG allein in Fällen eingeschränkt, in denen Geheimhaltungspflichten des Verantwortlichen bestehen.

Eine über die aktuellen Regelungen hinausgehende Einschränkung des Auskunftsrechts für Fälle, in denen lediglich Geheimhaltungsinteressen von Unternehmen bestehen, widerspricht nach Ansicht des vzbv dem Willen des europäischen Gesetzgebers. Schließlich wurde in Artikel 15 Abs. 4 DSGVO eine Regelung beschlossen, welche die zulässige Einschränkung des Rechts auf Auskunft klar limitiert. Eine weitere Einschränkung im nationalen Recht würde außerdem in der Praxis ein Tor öffnen, zunehmend berechtigte Auskunftsinteressen mit Verweis auf diese Regelung abzuwehren und so den Betroffenen die Wahrnehmung des wichtigen Rechts auf Auskunft zu erschweren.[16]

> Artikel 15 DSGVO sowie § 29 Abs. 1 BDSG berücksichtigen bereits angemessen den Schutz von Geschäftsgeheimnissen. Die in § 34 Abs. 1 BDSG-E vorgeschlagene darüberhinausgehende Einschränkung des Auskunftsrechts lehnt der vzbv ab. Diese weitere Einschränkung im nationalen Recht würde die Wahrnehmung des wichtigen Rechts auf Auskunft erschweren.

[16] siehe auch Stellungnahme des Bundesrats, BR-Drs. 72/24(B), 2024, Nr. 4, S. 5

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 C

UNIVERSITÄT BONN
Rechts- und Staatswissenschaftliche Fakultät Rechtswissenschaft

RHEINISCHE
FRIEDRICH-WILHELMS-
UNIVERSITÄT BONN

UNIVERSITÄT BONN · Prof. Dr. L. Specht · Adenauerallee 24-42, 53113 Bonn

An den
Deutschen Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Prof. Dr. Louisa Specht-Riemenschneider

Lehrstuhl für Bürgerliches Recht,
Informations- und Datenrecht

Adenauerallee 24-42
53113 Bonn

T 0228/73-4240
F 0228/73-5741
E Louisa.Specht@Forschungsstelle-Datenrecht.de

Sekretariat: Jacqueline Ostros

T 0228/73-4240
F 0228/73-5741
E sekretariat.specht@jura.uni-bonn.de

Bonn, 20.06.2024

Öffentliche Anhörung des Ausschusses für Inneres und Heimat zum Entwurf eines ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, BT-Drucksache 20/10859

Sehr geehrte Mitglieder des Ausschusses für Inneres und Heimat,

der stellvertretende Vorsitzende des Ausschusses für Inneres und Heimat, Herr Prof. Dr. Lars Castelluci, MdB, hat mich eingeladen, an der o.g. öffentlichen Anhörung als Sachverständige teilzunehmen. Dieser Einladung komme ich gerne nach. Im Folgenden möchte ich vorab schriftlich zum Thema der Anhörung Stellung nehmen. Auch wenn ich sämtliche Aspekte der Änderung des Bundesdatenschutzgesetzes mit erheblichem Interesse verfolge, berühren doch

v.a. §§ 34 und 37a BDSG n.F.-E den Schwerpunkt meiner Forschungstätigkeit. Ich erlaube mir daher nach Rücksprache, meine Stellungnahme auf diese Aspekte zu beschränken.

Ich wäre Ihnen dankbar, wenn Sie die nachfolgende Stellungnahme zur Kenntnis nehmen würden.

Mit freundlichen Grüßen

[redacted]

- Louisa Specht-Riemenschneider –

Stellungnahme zum ersten Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG n.F.-E)

A. Beschränkung des Auskunftsrechtes nach § 34 BDSG

I. Heutige Rechtslage

Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und weitere Informationen gem. Art. 15 Abs. 1 lit. a – h DSGVO. Nach Art. 15 Abs. 3 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Nach h.M. ist dieses Recht auf Erhalt einer Kopie gem. Art. 15 Abs. 4 DSGVO beschränkt durch die Rechte und Freiheiten anderer Personen, die durch den Erhalt einer Kopie nicht eingeschränkt werden dürfen. Nach h.M. erstreckt sich diese Einschränkung des Auskunftsrechts auch auf Art. 15 Abs. 1 DSGVO. „Andere Personen" sind dabei nicht nur dritte Personen, sondern auch der Verantwortliche. Zu den zu schützenden Rechten gehören auch Betriebs- und Geschäftsgeheimnisse, wobei dem Betroffenen die Auskunft auch bei Vorliegen eines Betriebs- und Geschäftsgeheimnisses nicht vollständig versagt werden darf, sondern der Verantwortliche angehalten ist, die Auskunft so weit wie möglich zu erteilen, z.B. indem relevante Passagen zu Betriebs- und Geschäftsgeheimnissen geschwärzt werden. Die Beweislast für das Vorliegen der Voraussetzungen des Art. 15 Abs. 4 DSGVO liegt bei demjenigen, der sich auf den Ausnahmetatbestand beruft, i.d.R. also bei demjenigen, der das Vorliegen von Geschäfts- und Betriebsgeheimnissen geltend macht. Weitere Ausnahmen ergeben sich aus §§ 27, 28 und 29 sowie aus § 34 BDSG, wobei diese Ausnahmen stets den Anforderungen des

Art. 23 DSGVO genügen müssen. Bereits heute ist das Auskunftsrecht also beschränkt.

II. Änderung des § 34 BDSG

Durch den Entwurf des ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BDSG n.F.-E) soll § 34 BDSG insoweit geändert werden, als Abs. 1 folgender Satz angefügt wird:

> „Das Recht auf Auskunft besteht auch insoweit nicht, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt."

Ich rege an, die Gesetzesänderung in § 34 BDSG n.F., soweit sie sich auf Betriebs- und Geschäftsgeheimnisse bezieht, zu streichen und stütze dies auf folgende drei Gründe:

1. § 34 BDSG n.F.-E. geht über die Einschränkung des Art. 15 Abs. 4 DSGVO hinaus

§ 34 BDSG n.F.-E. sieht seinem Wortlaut nach vor, dass das Auskunftsrecht von vornherein nicht besteht, wenn ein Betriebs- oder Geschäftsgeheimnis betroffen ist (*„besteht insoweit nicht"*). Besteht aber das Auskunftsrecht von vornherein nicht, muss es auch nicht durch Teilschwärzung befriedigt werden, wie es derzeit nach nahezu einhelliger Auffassung im Anwendungsbereich des Art. 15 Abs. 4 DSGVO der Fall ist. Damit geht § 34 BDSG n.F.-E. zugunsten der Verantwortlichen und Dritten über das bisherige Verständnis des Art. 15 Abs. 4 hinaus und stellt Betroffene damit schlechter als dies nach derzeitiger Rechtslage der Fall ist.

2. § 34 BDSG n.F.-E. steigert Transaktionskosten

Beweisrechtlich fordert § 34 BDSG außerdem von der betroffenen Person, ein Interesse an der Geltendmachung ihres Auskunftsrechtes darzulegen und ggf. zu beweisen. Art. 15 DSGVO soll aber als Grundlage der Ausübung sämtlicher anderer Betroffenenrechte dienen und hat damit elementare Bedeutung für die betroffene Person. Daher ist Art. 15 DSGVO bewusst gerade nicht an das Vorliegen weiterer Tatbestandsvoraussetzungen geknüpft, die die betroffene Person von der Geltendmachung ihrer Betroffenenrechte abhalten könnte. Ich weise darauf hin, dass von den Betroffenenrechten ohnehin aufgrund von Informationsasymmetrien, hohen Transaktionskosten und Rationalitätsdefiziten zu wenig Gebrauch gemacht wird. Weitere Voraussetzungen erhöhen den Aufwand für die betroffene Person zusätzlich und reduzieren gleichzeitig seine Erfolgsaussichten, wodurch rationale Entscheidungen mit noch höherer Wahrscheinlichkeit gegen eine Ausübung der Betroffenenrechte ausfallen werden.

3. Zweifel an der Vereinbarkeit von § 34 BDSG n.F.-E. mit Art. 23 DSGVO

Ich habe erhebliche Zweifel an der Vereinbarkeit des § 34 BDSG n.F.-E. mit den Vorgaben des Art. 23 DSGVO im Hinblick auf die Verhältnismäßigkeit, da mit der konkreten Formulierung über das mildeste Mittel zur Beschränkung der Betroffenenrechte zugunsten von Betriebs- und Geschäftsgeheimnissen hinausgegangen wird. Ein milderes, gleich geeignetes Mittel findet sich schon de lege lata mit Art. 15

Abs. 4 DSGVO. Über dessen Voraussetzungen sollte nicht hinausgegangen werden

B. Scoring-Vorschrift des § 37a BDSG

I. Heutige Rechtslage

Die DSGVO gewährt dem Betroffenen in Art. 22 das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Entscheidungen wie Kreditvergaben sollen also grundsätzlich von einer menschlichen Instanz getroffen werden müssen. Nur unter bestimmten vom Gesetz vorgegebenen Umständen ist auch schon heute eine automatisierte Entscheidung möglich. Mit Urteil vom 07.12.2023 erweitert der EuGH die Anwendbarkeit des Art. 22 DSGVO auf sogenannte vorbereitende automatisierte Entscheidungen, wie die Bildung von Score-Werten, die Verbraucherkreditentscheidungen häufig zugrunde gelegt werden. Derart automatisierte Vorfeldmaßnahmen sind zukünftig sogar gegebenenfalls verboten, ohne dass es einer Geltendmachung durch den Betroffenen bedarf. Der EuGH untersagt die automatisierte Scorewertberechnung aber tatsächlich nur, wenn die anschließende Kreditentscheidung „maßgeblich" auf dem Score-Wert beruht und ebenfalls nur dann, wenn der Gesetzgeber sie nicht doch gestattet (oder ein anderer Ausnahmetatbestand erfüllt ist). Denn Art. 22 DSGVO erfordert einen rechtlichen Nachteil oder eine ähnliche erheblich beeinträchtigende Wirkung der automatisierten Entscheidung (oder Vorfeldmaßnahme). Eine solche erheblich beeinträchtigende Wirkung hat der Score aber nur dann, wenn er die Kreditentscheidung maßgeblich in Richtung einer Kreditableh-

nung beeinflusst. Positive Scores sind also in Zukunft ebenso wenig untersagt wie Scores, die Kreditentscheidungen nicht maßgeblich zugrunde gelegt werden.

Durch die Gleichsetzung von automatisierten Entscheidungen und vorbereitenden Maßnahmen öffnet der EuGH die Tür, diese vorbereitenden Maßnahmen nationalen Regelungen zu unterstellen. Dies erlaubt die DSGVO in Art. 22 Abs. 1 lit. b DSGVO. Diese nationalen Regelungen müssen sich freilich im Rahmen der nach der DSGVO zulässigen Datenverarbeitungen halten und dürfen Abwägungsentscheidungen nicht abschließend vorgeben. Dass bestimmte Parameter beim Scoring aber, von Ausnahmefällen abgesehen, grundsätzlich berücksichtigt werden dürfen und andere eben nicht, dafür ist dem Gesetzgeber nun ein vormals jedenfalls streitiger Regelungsspielraum eröffnet worden. Das Argument, der Gesetzgeber dürfe auf nationaler Ebene keine Vorgaben für das Scoring selbst, sondern nur für die auf ihn beruhende Entscheidung treffen, verfängt nach der Gleichsetzung von Entscheidung und Vorfeldmaßnahme jedenfalls nicht mehr. Die Regelung des § 37a BDSG, die das Scoring nun zugunsten von Betroffenen an einheitlichen, nachvollziehbaren und fairen Kriterien orientieren will, ist daher zumindest im Grundsatz zu begrüßen. Im Einzelnen besteht aber Nachbesserungsbedarf insbesondere in folgenden drei Punkten:

1. Push- statt Pull-Informationen bei negativem Ersteintrag

§ 37a Abs. 4 BDSG n.F.-E. sieht vor, dass Verantwortliche, die Wahrscheinlichkeitswerte i.S.d. Abs. 1 erstellen, der betroffenen Person auf Antrag bestimmte Informationen zur Verfügung stellen müssen. Damit betroffene Personen ihre Rechte aber sinnvoll wahrnehmen können, sollten Sie proaktiv zumindest im Falle des ersten Negativeintrages i.S.d. Abs. 3 benachrichtigt werden. Dies sollte in einem neuen § 37a Abs. 4 S. 3 klargestellt werden.

Ein negativer Ersteintrag sollte auch ein solcher Negativeintrag i.S.d. Abs. 3 sein, der nach Ablauf von vier Jahren seit dem Schluss des Jahres des letzten Negativeintrages bekannt geworden ist.

Informationspflichten allein helfen dem Betroffenen aber wenig, da seit Jahrzehnten aus der Verbraucherforschung bekannt ist, dass mehr Information nicht zwingend zu mehr Informiertheit führt, sondern, ganz im Gegenteil, häufig zu einer Informationsüberlastung. In der Folge wird die Informationsaufnahme nicht selten abgebrochen, die betroffene Person ist also durch mehr Information häufig im Ergebnis weniger informiert. Daher sollte bei der Einführung von Informationspflichten stets auch über die Art und Weise der Information nachgedacht werden. Standardisierte Bildsymbole und abgestufte Informationskonzepte möchte ich hier nachdrücklich empfehlen.

2. § 37a Abs. 4 S. 2 BDSG n.F.-E. als Rechtsgrundlage für die Datenverarbeitung

Die Gesetzesbegründung enthält auf S. 23 den Passus, dass § 37a BDSG n.F.-E. keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellt. Das ist im Hinblick auf § 37a Abs. 4 S. 2 BDSG n.F.-E. nicht zutreffend. Ich rege daher an, die Gesetzesbegründung entsprechend anzupassen.

3. Regelung für Scoring von Zahlungsdiensteanbietern erforderlich

§ 37a BDSG n.F.-E. gilt für das Dreiecksverhältnis zwischen Kreditinstituten, Kreditauskunfteien und Betroffenen und unterwirft die Kreditauskunfteien in diesem Dreiecksverhältnis bestimmten einschränkenden Vorgaben. Sofern aber Zahlungsdiensteanbieter wie Paypal und Klarna selbst scoren, findet

die Regelung keine Anwendung. Derartige Zahlungsdiensteanbieter können sich vielmehr in vielen Fällen auf Art. 22 Abs. 2 lit. a DSGVO berufen. Für die Ausgestaltung des Art. 22 Abs. 2 lit. a DSGVO auf mitgliedstaatlicher Ebene besteht allerdings keine Öffnungsklausel, sodass § 37a BDSG für die Zahlungsdiensteanbieter keine Anwendung findet. Die neue Sektoruntersuchung des Bundeskartellamts zeigt aber, dass beim Scoring durch diese Zahlungsdiensteanbieter erhebliche Defizite bestehen. Gleichzeitig ist in Art. 18 der Verbraucherkreditrichtlinie, der derzeit in nationales Recht umzusetzen ist, normiert, dass Zahlungsdiensteanbieter Kreditwürdigkeitsprüfungen durchführen müssen und dass sie dabei entsprechende Vorgaben zu beachten haben. Diese Vorgaben sind allerdings allgemeiner gehalten als die Vorgaben des § 37a BDSG n.F.-E. Eine Öffnungsklausel, die die Konkretisierung dieser Anforderungen im nationalen Recht zulässt, besteht auch hier nicht. Es erscheint dringend angezeigt, die Vorgaben zum Scoring für Auskunfteien und Zahlungsdiensteanbieter in DSGVO, BDSG und Verbraucherkreditrichtlinie einander anzugleichen. Ein möglicher Weg dorthin ist die Verankerung derart einheitlicher Vorgaben in der EU-Verbraucheragenda 2025 – 2030, was ich nachdrücklich empfehle.

Prof. Dr. Meinhard Schröder

Lehrstuhl für Öffentliches Recht, Europarecht
und Informationstechnologierecht

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Herrn stv. Vorsitzenden
Prof. Dr. Lars Castellucci MdB

- per Email -

Telefon | Prof. Dr. Meinhard Schröder
0851 509-2381
Telefax | 0851 509-2382
E-Mail | Meinhard.Schroeder
@uni-passau.de

Datum | 20.6.2024

Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BT-Drucksache 20/10859)

Sehr geehrter Herr Professor Castellucci,

als Anlage übersende ich die erbetene Stellungnahme zum o.g. Gesetzentwurf. Aufgrund der kurzfristigen Anfrage konnte ich nur zu einigen ausgewählten Punkten Stellung nehmen. Fragen beantworte ich gerne in der Sitzung, an der ich leider aufgrund anderweitiger universitärer Verpflichtungen nur online teilnehmen kann.

Mit freundlichen Grüßen

[redacted]

Besucheradresse | Innstraße 39, Raum 114
Internetadresse | www.uni-passau.de/schroeder

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

(BT-Drucksache 20/10859)

Prof. Dr. Meinhard Schröder, Universität Passau

Vorbemerkung

Der Rahmen für Änderungen des Bundesdatenschutzgesetzes wird einerseits durch das Unionsrecht, andererseits durch die verfassungsrechtlichen Vorgaben des Grundgesetzes bestimmt.

Aus unionsrechtlicher Perspektive ist vor allem zu berücksichtigen, dass mit der Datenschutzgrundverordnung[1] grundsätzlich eine **Vollharmonisierung** des europäischen Datenschutzrechts bezweckt wird (insbes. Erwägungsgrund Nr. 10) und mitgliedstaatliches Datenschutzrecht insoweit nur noch zulässig ist, wo die Datenschutzgrundverordnung **Regelungsaufträge, Öffnungs- oder Spezifizierungsklauseln** enthält. Im Anwendungsbereich der sog. JI-Richtlinie[2] ist dagegen eine umfassende mitgliedstaatliche Gesetzgebung erforderlich, die den allgemeinen Anforderungen an die Umsetzung von europäischen Richtlinien genügen muss.

Aus verfassungsrechtlicher Sicht ist vor allem die **Kompetenzverteilung** zu beachten. Da das Grundgesetz dem Bund keine ausdrückliche Kompetenz für die Regelung des Datenschutzrechts zuweist und in Abwesenheit einer solchen Zuweisung die Gesetzgebungskompetenz bei den Ländern liegt (Art. 30, 70, 83 GG), besteht für den Bund nur dann eine Gesetzgebungskompetenz, wenn die Ausübung anderer Kompetenzen eine „Mitregelung" des Datenschutzrechts im Sinne einer **Kompetenz kraft Sachzusammenhangs** erfordert.[3]

Für das materielle Datenschutzrecht im Bereich **nicht-öffentlicher Stellen** wird seit jeher auf Art. 74 Abs. 1 Nr. 11 GG („Recht der Wirtschaft") zurückgegriffen; die Voraussetzungen des Art. 72 Abs. 2 GG erscheinen insoweit, wie auch die Entwurfsbegründung annimmt,[4] aus Gründen der Rechts- und Wirtschaftseinheit gegeben. Der **Vollzug** dieses Rechts liegt – genauso wie des an seine Stelle tretenden Unionsrechts – in den Händen der **Länder**, die daher Einrichtung und Verfahren der (Datenschutzaufsichts-) Behörden regeln müssen (Art. 83, 84 Abs. 1 S. 1 GG). Theoretisch wäre es hier möglich, den Ländern unter Berufung auf Art. 84 Abs. 1 S. 2 GG bundesrechtliche Vorgaben zu machen, von denen die Länder dann aber wieder abweichen könnten (Art. 84 Abs. 1 S. 3 GG). Soll die Abweichungsmöglichkeit ausgeschlossen werden, sind dafür nach Art. 83 Abs. 1 S. 5 GG rechtlich ein besonderes Bedürfnis nach bundeseinheitlicher Regelung und politisch nach Art. 83 Abs. 1 S. 6 GG die Zustimmung des Bundesrat erforderlich. Ob sich eine Konzentration der Aufsicht beim BfDI auf Art. 87 Abs. 3 S. 1 GG stützen ließe, ist unklar, weil dieser keine selbständige Bundesoberbehörde,[5]

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119/89.

[3] BVerfGE 125, 260 (314).

[4] BT-Drucksache 20/10859, S. 14.

[5] A.A. *Richter/Spiecker gen. Döhmann*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, 2022, S. 36.

sondern eine oberste Bundesbehörde darstellt (und aus Gründen der europarechtlich geforderten „völligen Unabhängigkeit“ wohl auch darstellen muss); eine entsprechende Anwendung der Vorschrift erscheint aber diskutabel.

Für das materielle Datenschutzrecht im Bereich **öffentlicher Stellen des Bundes** lässt sich eine Gesetzgebungskompetenz entweder kraft Natur der Sache oder über den Umweg der Verwaltungskompetenzen herstellen: Wo Behördenorganisation und Verfahren durch den Bund geregelt werden, muss Datenschutz mitgeregelt werden. Daraus ergibt sich eine Regelungsbefugnis des Bundes für das materielle Datenschutzrecht im Bereich der bundeseigenen Verwaltung (Art. 86 GG). Die Kompetenz zum **Vollzug** dieses Rechts – genauso wie des an seine Stelle tretenden Unionsrechts – liegt ebenfalls beim **Bund**, der hierfür (vgl. § 9 Abs. 1 BDSG) den BfDI als oberste Bundesbehörde eingerichtet hat.[6]

Für das materielle Datenschutzrecht im Bereich **öffentlicher Stellen der Länder** lässt sich eine Regelungszuständigkeit des Bundes praktisch nicht annehmen. Allenfalls wäre punktuell unter Berufung auf die Akzessorietät dieses Datenschutzrechts zum Verwaltungsverfahren eine Regelung möglich, soweit der Bund auch das Verwaltungsverfahren gem. Art. 84 GG vereinheitlichen kann (aber nur, soweit die Länder Bundesrecht ausführen und auch dann nur mit Abweichungsbefugnis der Länder, die sich nur mit Zustimmung des Bundesrates ausschließen ließe, s.o.). Für den **Vollzug** des Datenschutzrechts der **Länder** – genauso wie des an seine Stelle tretenden Unionsrechts – sind ausnahmslos diese zuständig (Art. 30 GG).

Zu beachten ist schließlich der Grundsatz der getrennten Verfassungs- und Verwaltungsräume im Bundesstaat, aus dem – auch aus demokratischen und rechtsstaatlichen Erwägungen – ein grundsätzliches **Verbot der Mischverwaltung** resultiert.[7] Ausnahmen davon – etwa in Form von Arbeitsgemeinschaften mehrerer Verwaltungsträger – sind nur zulässig, soweit sie in der Verfassung ausdrücklich vorgesehen sind oder aufgrund eines besonderen sachlichen Grundes und hinsichtlich einer eng umgrenzten Verwaltungsmaterie erforderlich erscheinen.[8]

Zu den konkret vorgeschlagenen Änderungen erscheinen – unter Berücksichtigung dieser Vorbemerkung – folgende Hinweise veranlasst:

Zur Neuregelung der Videoüberwachung (Artikel 1 Nr. 3 des Entwurfs)

Die Beschränkung des Anwendungsbereichs des § 4 BDSG-E auf öffentliche Stellen ist zu begrüßen. Die bisherige Regelung war aufgrund des Anwendungsvorrangs des Unionsrechts auf nichtöffentliche Stellen nicht anwendbar,[9] erweckte aber den gegenteiligen Eindruck. Sie stand daher im Widerspruch zu den rechtsstaatlichen Grundsätzen der Normenwahrheit und Normenklarheit[10]. Nichtöffentliche Stellen stützen ihre Videoüberwachung in aller Regel auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO (berechtigtes Interesse), der keine Öffnungs- oder Spezifizierungsklausel für die Mitgliedstaaten enthält und daher nicht durch Regelungen im BDSG eingeschränkt oder modifiziert werden kann.

Die vorgeschlagene neue Formulierung „nur zulässig, soweit sie zu ihrer Aufgabenerfüllung, einschließlich der Wahrnehmung ihres Hausrechts, erforderlich ist“ in § 4 BDSG-E versteht die Wahrnehmung des Hausrechts als Teil der Aufgabenerfüllung der Stellen. Die dem zugrundeliegende An-

[6] Grundlage ist wohl ebenfalls Art. 87 Abs. 3 GG (analog), wobei die Entwicklung von der Einrichtung „beim“ BMI hin zur obersten Bundesbehörde soweit ersichtlich nicht verfassungsrechtlich diskutiert wurde.
[7] BVerfGE 119, 331 (367, 370); 137, 108 (142 ff.); 139, 194 (226).
[8] Vgl. *F. Kirchhof*, in: Dürig/Herzog/Scholz, GG-Kommentar, 93. EL Juli 2020, Art. 83 Rn. 117.
[9] So schon vor längerer Zeit BVerwGE 165, 111.
[10] Dazu etwa BVerfG, 2 BvF 1/21, Rn. 81; BVerfGE 114, 196 Rn. 207.

nahme, „dass die Wahrnehmung des Hausrechts durch öffentliche Stellen Teil ihrer Aufgabenerfüllung ist“[11], trifft aber in dieser Pauschalität nicht zu und verkennt die in aller Regel dualistische Konstruktion des öffentlichen Sachenrechts[12]. Nach der inzwischen wohl überwiegenden Auffassung greift das *öffentlichrechtliche* Hausrecht nur dann ein, wenn die Stelle den öffentlich-rechtlichen Widmungszweck sichern, beispielsweise ihre Funktionsfähigkeit schützen möchte. Daneben gibt es aber weiterhin das *privatrechtliche* Hausrecht, das öffentlichen Stellen wie Privaten infolge ihrer Eigentümerstellung an einer öffentlichen Sache zusteht.[13] Letzteres unter den Begriff der „Aufgabenerfüllung“ zu subsumieren, erscheint kaum möglich. Damit ergibt sich (wenn man nicht davon ausgeht, dass eine Videoüberwachung immer auch dem Schutz der Aufgabenerfüllung dient), eine möglicherweise unbeabsichtigte Regelungslücke, denn ob eine öffentliche Stelle in dieser Situation auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zurückgreifen kann, ist angesichts von Art. 6 Abs. 1 UAbs. 2 DSGVO zweifelhaft. Mit der neuen Formulierung wird die Möglichkeit für Stellen des Bundes, von einer **Videoüberwachung** zum Zwecke der Ausübung des Hausrechts Gebrauch zu machen, daher möglicherweise zu einem gewissen Grad **verengt**. Es sollte geprüft werden, ob dieses Ergebnis beabsichtigt ist.

Zur Institutionalisierung der Datenschutzkonferenz (DSK) (Artikel 1 Nr. 1 lit. c und Nr. 4)

Die DSK verfügt über eine jahrzehntelange Tradition. Sie wird rechtlich als **Arbeitsgemeinschaft** qualifiziert, die sich im Rahmen der notwendigen Selbstorganisation eine **Geschäftsordnung** gegeben hat. Der vorgeschlagene § 16a BDSG kodifiziert diesen Bestand.

Der Regelungsgehalt der Vorschrift erschöpft sich darin, eine Abschaffung der DSK oder eine Aufhebung ihrer Geschäftsordnung zu verhindern – beides will soweit ersichtlich niemand. Daher handelt es sich jedenfalls um eine **überflüssige Regelung**, die noch dazu – **legistisch unschön** – die einzige Vorschrift eines eigenen Kapitels bildet. Dem ließe sich allerdings abhelfen, wenn § 16a BDSG-E **mit weiteren Vorschriften kombiniert** würde – der Koalitionsvertrag der die Bundesregierung tragenden Parteien spricht davon, der DSK „rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen“; gefordert wird auch immer wieder die Einrichtung einer Geschäftsstelle der DSK. Möchte der Gesetzgeber derartige Regelungen einführen, wäre Art. 16a BDSG-E als Einleitung eines ganzen Kapitels über die DSK sinnvoll.

Unabhängig davon stellt sich die Frage nach der **Vereinbarkeit von § 16a BDSG-E mit höherrangigem Recht**.

Die europäischen Vorgaben für die Organisation der Datenschutzaufsichtsbehörden lassen den Mitgliedstaaten ausdrücklich die Option, mehrere Datenschutzbehörden einzurichten (Art. 51 Abs. 1 DSGVO, Art. 41 JI-RL), so dass sich – unabhängig von der wohl zu verneinenden Frage, ob es sich bei der DSK überhaupt um eine Aufsichtsbehörde i.S.d. europäischen Datenschutzrechts handelt – bei der Institutionalisierung der DSK durch § 16a BDSG-E jedenfalls um eine **von der Verfahrensautonomie der Mitgliedstaaten gedeckte Konstruktion** handelt.

Verfassungsrechtlich ist allerdings zu berücksichtigen, dass die bisher völlig freiwillige Zusammenarbeit in der Arbeitsgemeinschaft DSK aufgrund des nun vorgeschlagenen § 16a BDSG verpflichtend wird. Auch wenn in der Praxis niemand eine Auflösung der DSK will, schreibt der Bund ihre Existenz nun verbindlich vor und zwingt die Länder zur Beteiligung an ihr. Die umfassende **Kompetenz des Bundes für diese Regelung** erscheint aber **zweifelhaft**. Die Annahme einer Annexkompetenz des Bundes zu Art. 23 Abs. 1 S. 2 GG, wie sie in einem Gutachten (bezogen auf verbindliche Beschlüsse

[11] So ausdrücklich die Begründung, BT-Drucksache 20/10859, S. 19.
[12] Vgl. statt vieler *Papier*, Recht der öffentlichen Sachen, 3. Aufl., 1998, S. 34 f.
[13] Vgl. OVG Münster NVwZ-RR 2019, 648; OVG Hamburg, NJW 2014, 1196 (1197); VGH Kassel, NJW 1990, 1250; BayVGH, DVBl. 1981, 1010 ff.

der DSK) vertreten wird,[14] überzeugt nicht. Sie würde gerade den anerkannten Grundsatz, dass die Europäisierung die innerstaatliche Kompetenzverteilung unberührt lässt und auch mit Blick auf die Vollzugskompetenzen zu fragen ist, welcher Hoheitsträger hypothetisch, d.h. nach den grundgesetzlichen Vorgaben, gesetzgebungskompetent wäre,[15] aushebeln. In letzter Konsequenz könnte die Berufung auf das zwar stets zu beachtende, in seinen konkreten Wirkungen aber unbestimmte und rein ergebnisbezogene Gebot des effektiven Vollzugs des Unionsrechts die innerstaatliche (Vollzugs-) Kompetenzverteilung aushebeln und zu einer Zentralisierung auf Bundesebene führen.[16] Im Ansatz überzeugender erscheint der (wieder im Kontext verbindlicher Beschlüsse der DSK) alternativ vorgeschlagene[17] Weg, die Institutionalisierung der DSK auf Art. 84 Abs. 1 S. 2 (und 5, 6) GG zu stützen (s.o.). Diese Gesetzgebung erfordert aber (wenn eine Abweichung der Länder ausgeschlossen werden soll) eine Zustimmung des Bundesrates (s.o.). Außerdem dürfte sich die so bundesrechtlich institutionalisierte DSK ohne freiwillige Zustimmung aller Beteiligten nicht mit Fragen der Aufsicht über öffentliche Stellen der Länder, also dem Vollzug von deren (hypothetischem) materiellem Datenschutzrecht befassen, da dieser Bereich gem. Art. 30 GG der alleinigen Vollzugskompetenz der Länder vorbehalten ist (s.o.). Ob das das (unausgesprochene) Bild ist, das der Bundesgesetzgeber von der in Art. 16a BDSG vorgesehenen DSK hat, erscheint aber zweifelhaft – realitätsgerecht ist, dass die institutionalisierte DSK dieselbe, umfassende Befassungskompetenz wie bisher haben soll. Für die Institutionalisierung einer solchen DSK besitzt der Bund aber **keine Gesetzgebungskompetenz**.

Was die noch weitergehende **Möglichkeit verbindlicher Entscheidungen der DSK** (im Sinne einer Bindung anderer deutscher Datenschutzbehörden an die Auslegung der DSK, nicht im Sinne eines Auftretens gegenüber Verantwortlichen, das soweit ersichtlich nirgends vorgeschlagen wird) anbelangt, stellt sich zunächst aus europarechtlicher Sicht die Frage, ob damit die „völlige Unabhängigkeit" der Aufsichtsbehörden, die Art. 52 Abs. 1 DSGVO verlangt, in Frage gestellt würde. Dafür könnte sprechen, dass die im konkreten Fall zuständige Behörde nicht mehr frei in ihren Entscheidungen ist, und zwar jenseits der Bindungen, die sich aus der DSGVO ergeben. Dort ist eine Bindung an die Entscheidungen anderer Datenschutzbehörden nur im Kohärenzverfahren vorgesehen (Art. 65 Abs. 2 S. 3 DSGVO). Diese Regelung ist allerdings im Kontext mit grenzüberschreitenden Auslegungskonflikten zwischen den Datenschutzbehörden zu sehen. Andere Bindungen, etwa solche an die Auslegung der DSGVO durch den EuGH, oder auch die innerhalb einer hierarchisch organisierten Behörde, werden als selbstverständlich vorausgesetzt. Es spricht daher viel dafür, dass die Unabhängigkeit nur gegen Einflussnahmen von außen schützen (vgl. auch Art. 52 Abs. 2 DSGVO), nicht hingegen Bindungen innerhalb des Netzwerks der Datenschutzbehörden[18] ausschließen soll. Zudem lässt die DSGVO erkennen, dass die Datenschutzbehörden eine einheitliche Auslegung der DSGVO anstreben sollen (insbes. Art. 51 Abs. 2 S 1, Art. 63 DSGVO). Eine innerstaatliche Organisation, die mehrere Aufsichtsbehörden dergestalt miteinander vernetzt, dass dieses Ziel gefördert wird, ohne dass es zu Einflüssen „von außen" kommt, erscheint daher **mit der DSGVO vereinbar**. Für die JI-Richtlinie gilt dasselbe.[19]

Verfassungsrechtlich stellen sich dagegen die oben bereits zur Institutionalisierung der DSK aufgeworfenen Fragen in verschärfter Form: Abgesehen von der **fehlenden Bundeskompetenz** zumindest

---

[14] Vgl. *Richter/Spiecker gen. Döhmann*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, 2022, S. 75 ff.
[15] Vgl. statt vieler *F. Kirchhof*, in: Dürig/Herzog/Scholz, GG-Kommentar, 93. EL Juli 2020, Art. 83 Rn. 166.
[16] Ablehnend zu einer Bundeskompetenz für den Vollzug von Unionsrecht daher auch *F. Kirchhof*, in: Dürig/Herzog/Scholz, GG-Kommentar, 93. EL Juli 2020, Art. 83 Rn. 163 f.
[17] Vgl. *Richter/Spiecker gen. Döhmann*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, 2022, S. 79 ff.
[18] Dazu etwa *v. Lewinski*, NVwZ 2017, 1483 ff.
[19] Vgl. Art. 41 ff. der JI-RL.

in Bereichen der Aufsicht über öffentliche Stellen der Länder erscheint bei einer Kooperation der Aufsichtsbehörden, die über Amtshilfe und unverbindlichen Austausch hinausgeht und der nach außen hin zuständigen Behörde Entscheidungselemente bindend vorgibt, ein **Verstoß gegen das Verbot der Mischverwaltung** naheliegend. Zwar kann eine Mischverwaltung nach der Rechtsprechung des Bundesverfassungsgerichts auch jenseits der in Art. 91a ff. und Art. 108 GG ausdrücklich vorgesehenen Formen verfassungsrechtlich gerechtfertigt werden.[20] Dafür müsste aber ein besonderer sachlicher Grund gegeben sein und das Datenschutzrecht eine „eng umgrenzte Verwaltungsmaterie" darstellen. Zweifelhaft ist schon das Vorliegen eines besonderen sachlichen Grundes. Dass die uneinheitliche Handhabung des Datenschutzrechts „in der ersten Instanz" ein Problem ist, wird durchaus bestritten,[21] und eine wirkliche Vereinheitlichung lässt sich ohnehin erst auf der unionsrechtlichen Ebene erreichen, und auch dies erst nach gerichtlicher Überprüfung durch den EuGH. Zudem ist zweifelhaft, ob es angesichts der nach der Kompetenzverteilung möglichen Alternativen, insbesondere einer Konzentration der Datenschutzaufsicht über den nicht-öffentlichen Bereich beim BfDI (s.o.), einen besonderen Grund gerade für eine Mischverwaltung gibt. Dass das Anliegen des Gesetzgebers sinnvoll ist, reicht jedenfalls nicht aus.[22] Schließlich erscheint es, selbst wenn man berücksichtigt, dass die DSK ihre möglichen Ingerenzrechte nur punktuell ausübt, zweifelhaft, ob das inzwischen ubiquitär relevante Datenschutzrecht wirklich eine „eng umgrenzte Verwaltungsmaterie" darstellt[23].

Die **Institutionalisierung der DSK** im BDSG – und erst recht die Normierung von besonderen Befugnissen – sollte angesichts dieser Rahmenbedingungen ohne eingehende rechtliche Prüfung und präzise begrenzende Normierung ihrer Zuständigkeiten **unterbleiben**.

Zur Neuregelung des „Scoring" (Artikel 1 Nr. 11 und Nr. 14)

Die Neuregelung des Bereichs ist **grundsätzlich zu begrüßen**. Beim derzeit noch geltenden § 31 BDSG handelt es sich im Kern immer noch um den vor der europäischen Datenschutzreform geltenden §§ 28a und 28b BDSG-alt, der mit den Vorgaben der DSGVO kaum vereinbar ist und seit langem berechtigter Kritik ausgesetzt ist. Die Aufhebung der Vorschrift ist daher zu begrüßen.

Der als Ersatz vorgeschlagene § 37a BDSG ist als Ausnahme vom Verbot der vollständig automatisierten Einzelfallentscheidung (Art. 22 Abs. 1 DSGVO) konzipiert und soll damit die **Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO** ausnutzen. Der Vorschlag beschränkt sich aber nicht auf die Regelung eines weiteren Ausnahmetatbestands, sondern enthält darüberhinausgehende und nicht von Öffnungsklauseln in der DSGVO gedeckte Elemente.

Erstens erstreckt § 37a Abs. 1 BDSG-E das Verbot der vollständig automatisierten Einzelfallentscheidung über die in Art. 22 Abs. 1 DSGVO vorgesehenen Fälle. Verboten ist dort nur eine „auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende[…] Entscheidung, die [der betroffenen Person] gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Auch wenn der EuGH den Begriff des „Beruhens" in seiner Entscheidung vom 7. Dezember 2023[24] weit verstanden hat und einen maßgeblichen Einfluss ausreichen lässt, fällt die bloße Erstellung von Wahrscheinlichkeitswerten nicht darunter, genausowenig deren Verwendung zu anderen Zwecken. Mit der aktuellen Formulierung überschreitet der Gesetzgeber daher seinen verbleibenden Regelungsspielraum und schafft eine Norm, die von vornherein zumindest **teilweise europarechts-**

[20] BVerfGE 119, 331 (367, 370).
[21] Vgl. etwa *Thiel*, ZD 2021, 179.
[22] BVerfGE 119, 331 (370).
[23] A.A. *Richter/Spiecker gen. Döhmann*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, 2022, S. 49.
[24] Urteil vom 7.12.2023, Rs. C-634/21 – Schufa Holding, ECLI:EU:C:2023:957 Rn. 48 ff.

widrig ist. Hier sollte eine andere Formulierung gewählt werden, die nur den Spielraum der Öffnungsklausel ausnutzt und nicht versucht, jedwedes Scoring zu regeln.

Zweitens erscheinen die für § 37a Abs. 2 Nr. 1 BDSG-E vorgeschlagenen **Verwendungsverbote für bestimmte Daten** bedenklich. Im Grundsatz lassen sich die Einschränkungen zwar als „Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person" i.S.d. Art. 22 Abs. 2 lit. b DSGVO qualifizieren. Zweifelhaft erscheint aber, ob sie in dieser Pauschalität „angemessen" im Sinne der Vorschrift sind. Hier bedarf es einer detaillierten Verhältnismäßigkeitsprüfung, die im Rahmen dieser Stellungnahme nicht möglich ist. Schon auf den ersten Blick **unangemessen** erscheint beispielsweise der pauschale Ausschluss von Daten aus sozialen Netzwerken. Sind diese öffentlich zugänglich, sind sie nicht per se schutzbedürftiger als sonstige Inhalte im „offenen Internet", die aber nach § 37a Abs. 2 BDSG-E frei verwendet werden dürfen. Speziell zu § 37a Abs. 2 Nr. 1 lit. a) BDSG-E ist zudem zu berücksichtigen, dass der Unionsgesetzgeber in Art. 22 Abs. 4 DSGVO bereits (ohne Öffnungsklausel) geregelt hat, inwieweit besondere Kategorien personenbezogener Daten Eingang in Entscheidungen nach Art. 22 Abs. 2 DSGVO finden dürfen. Dass der deutsche Gesetzgeber zu einer Verschärfung in Form des vorgeschlagenen völligen Ausschlusses berechtigt ist, ist daher nicht anzunehmen; insofern hilft auch Art. 23 DSGVO nicht, der nur eine Einschränkung, aber keine Erweiterung von Betroffenenrechten ermöglicht. Auch **insoweit** ist der Vorschlag daher **europarechtswidrig**. § 37a Abs. 2 Nr. 1 lit. a BDSG-E sollte daher gestrichen und die übrigen Punkte auf ihre Verhältnismäßigkeit überprüft und ggf. durch andere Vorgaben zur Vermeidung diskriminierender Ergebnisse ersetzt werden.

Die in § 37a Abs. 4 BDSG-E vorgeschlagenen **Informationspflichten** lassen sich im Ansatz ebenfalls als „Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person" i.S.d. Art. 22 Abs. 2 lit. b DSGVO verstehen und bedürfen daher keiner besonderen Öffnungsklausel (Art. 23 DSGVO wäre dazu sowieso nicht geeignet, weil er nur eine Einschränkung der Betroffenenrechte ermöglicht, aber keine Erweiterung). Auch hier stellt sich aber die Frage, ob nicht die Auskunftspflichten des Verantwortlichen schon in der DSGVO abschließend geregelt sind, und zwar in diesem Fall in Art 15 Abs. 1 lit. h DSGVO, der sich speziell auf die automatisierte Entscheidungsfindung einschließlich Profiling bezieht. Allerdings ist dort nur von Art. 22 Abs. 1 und 4 die Rede, außerdem von „zumindest", was dafür spricht, dass in Ausnahmen nach Art. 22 Abs. 2 lit. b DSGVO weitergehende Pflichten des Verantwortlichen **unionsrechtskonform** normiert werden können, solange sie der Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person dienen.

Zur Behördenzuständigkeit bei gemeinsamer Verantwortlichkeit (Artikel 1 Nr. 16)

Der vorgeschlagene § 40a BDSG, nach dem gemeinsam verantwortliche Unternehmen i.S.d. Art. 26 DSGVO durch freiwillige Anzeige die Behördenzuständigkeit konzentrieren können sollen, erscheint zwar nicht rechtlich, aber **praktisch problematisch**.

Verfassungsrechtlich erscheint es grundsätzlich zulässig, die Behördenzuständigkeit von einer Erklärung des (potenziellen) Adressaten der Behördentätigkeit abhängig zu machen, solange die wesentlichen Kriterien für die Zuständigkeit gesetzlich festgelegt sind.[25] Auch europarechtlich bestehen keine Bedenken, da die Effektivität des Vollzugs der DSGVO dadurch wohl sogar gefördert, jedenfalls aber nicht gefährdet wird.

Problematisch erscheint aber, dass die Zuständigkeitskonzentration nicht nur von der Anzeige der gemeinsam verantwortlichen Unternehmen, sondern dazu noch von der Annahme des Vorliegens

[25] Zur ähnlichen Situation der Behördenzuständigkeit kraft Verwaltungsakts *Schröder*, in FS Streinz, 2023, S. 655 ff.

einer gemeinsamen Verantwortlichkeit durch alle beteiligten Behörden abhängig ist. Wann eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO gegeben ist, ist aber trotz (oder wegen) der Rechtsprechung des EuGH zu der Thematik im Einzelfall schwierig zu beurteilen, so dass es zu unterschiedlichen Auffassungen kommen kann. Damit erscheinen Streitigkeiten über den Ausschluss der Zuständigkeit der für das Unternehmen mit dem geringeren Jahresumsatz an sich zuständigen Aufsichtsbehörde vorprogrammiert.

Passau, den 20. Juni 2024

gez. Prof. Dr. Meinhard Schröder

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 E

PROF. DR. GREGOR THÜSING, LL.M. (HARVARD)

DIREKTOR DES INSTITUTS FÜR ARBEITSRECHT UND RECHT DER SOZIALEN SICHERHEIT

RHEINISCHE FRIEDRICH WILHELMS-UNIVERSITÄT BONN

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes BT-Drucks. 20/10859

Der Gesetzgeber hat am 27.3.2024 den Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes vorlegt (BT-Drs. 20/10859). Kernthemen der BDSG-Novelle sind vor allem die Institutionalisierung der Datenschutzkonferenz sowie eine neu eingefügte Vorschrift zum Kredit-Scoring durch Wirtschaftsauskunfteien.

I. Anlass und Ziel des Gesetzgebers

Im Zuge des Erlasses der Datenschutz-Grundverordnung (DSGVO) fasste der deutsche Gesetzgeber das Bundesdatenschutzgesetz (BDSG) neu, das parallel mit der Anwendbarkeit der DSGVO am 25.5.2018 in Kraft trat. Das Verhältnis und Zusammenspiel zwischen europäischem und nationalem Recht im Bereich des Datenschutzes ist komplexer geworden.[1] Dies führt dazu, dass hin und wieder eine Neujustierung des nationalen Rechts erforderlich ist. So auch im Falle des Scorings durch Wirtschaftsauskunfteien. Denn in einer weitreichenden Entscheidung des EuGH verweis dieser auf „durchgreifenden Bedenken" an der Wirksamkeit des § 31 BDSG des vorlegenden Gerichts.[2]

Das Thema Kredit-Scoring steht aber nicht erst seit der Entscheidung des EuGH auf der Agenda des Gesetzgebers. Die Bundesregierung führte es bereits in ihrem Koalitionsvertrag auf. Das gilt auch für die Institutionalisierung der Datenschutzkonferenz (DSK). Damit verfolgt sie das Ziel der „besseren Durchsetzung und Kohärenz des Datenschutzes".[3] Weitere Änderungen, die Gesetzesentwurf geplant sind, sind auf eine Evaluierung des Bundesministeriums des Innern und für Heimat zurückzuführen. Im Folgenden wird sich im Wesentlichen auf die Kernthemen, der

[1] Kühling/Buchner/*Kühling/Raab*, DS-GVO BDSG, 4. Aufl. 2024, A. Einführung Rn. 128 ff.
[2] EuGH, Urt. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905 Rn. 71.
[3] BT-Drs. 20/10859.

Institutionalisierung der DSK (II.) und dem Kredit-Scoring durch Wirtschaftsauskunfteien (III.) konzentriert. Dem schließen sich kurze Bemerkungen zu Vorschlägen, die es nicht in den Entwurf geschafft haben, an (IV.).

II. § 16a BDSG-E: Institutionalisierung der DSK ohne Ertrag?

Der geplante § 16a BDSG-E (Datenschutzkonferenz) verankert die aus den unabhängigen Datenschutzbehörden des Bundes und der Länder bestehenden DSK nun auch gesetzlich im BDSG. Damit verfolgt Gesetzgeber das Ziel der „besseren Durchsetzung und Kohärenz des Datenschutzes".[4] Ein Ziel, das mit dem vorlegten Entwurf wohl kaum erreicht wird – jedenfalls aber zu keiner Verbesserung des *status quo* führt. Die Begründung stellt klar, dass sich durch die Institutionalisierung der DSK nichts an ihrer Rechtsnatur ändert: „Sie ist eine Arbeitsgemeinschaft, die über keine eigene Rechtspersönlichkeit verfügt."[5] Entscheidend ist aber folgender Satz in der Begründung: „Eine Regelung zur rechtlichen Verbindlichkeit von Beschlüssen der DSK wird nicht getroffen, da damit wegen des Verbots der Mischverwaltung verfassungsrechtliche Grenzen berührt würden."[6]

Warum dann eine solche Regelung? Die DSK kann nach dem Gesetzentwurf keine rechtlich verbindlichen Beschlüsse fassen, mit der Konsequenz, dass einzelne Datenschutzaufsichtsbehörden trotz gemeinsamer Verständigung und Position der anderen Aufsichtsbehörden von Beschlüssen der DSK abweichen können. Das ist auch ihr gutes Recht, denn nach Art. 51 DSGVO sind die Aufsichtsbehörden unabhängig. Zudem ist das Argument des Verbots der Mischverwaltung, wie die Begründung sie anführt, ein sehr gewichtiges.[7] Fest steht jedenfalls, dass der derzeit geplante § 16a BDSG-E kaum zu einer besseren Durchsetzung und Kohärenz des Datenschutzes beiträgt. Schließlich hat sich die DSK auch ohne Verankerung im BDSG bereits eine Geschäftsordnung gegeben.[8] § 16a BDSG-E fehlt es an jeglichen Details zum Ziel der DSK, ihrer Struktur sowie Arbeitsweise. Auch findet sich z.B. keine Regelung zur Einrichtung einer gemeinsamen Geschäftsstelle.[9] Der Gesetzgeber muss sich ernsthaft die Frage stellen, ob es überhaupt den gesetzgeberischen Aufwand wert ist, § 16a BDSG-E in der derzeit geplanten Fassung zu erlassen. Sie führt jedenfalls zu keiner Verbesserung des *status quo*, die Institutionalisierung der DSK wäre in dieser Form ein rein symbolischer Akt.

[4] BT-Drs. 20/10859, S. 19.
[5] BT-Drs. 20/10859, S. 19.
[6] BT-Drs. 20/10859, S. 13.
[7] Hierzu näher *Martini/Botta*, DÖV 2022, 605, 610.
[8] Geschäftsordnung der DSK vom 5.9.2018, zuletzt geändert durch Beschluss vom 27.2.2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf.
[9] S. auch *Thiel*, ZD 2021, 179.

III. § 37a BDSG-E: Scoring durch Wirtschaftsauskunfteien

1. Warum es eine neue Norm braucht

Der bisherige § 31 BDSG (Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften) soll durch den neu geplanten § 37a BDSG-E (Scoring) ersetzt werden. Gut so! Anlass und Ausgangspunkt dieser Änderung ist die weitreichende Entscheidung des EuGH in der Rs. C-634/21, in der er zu dem Schluss kam, dass bereits die automatisierte Erstellung eines Wahrscheinlichkeitswerts über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung darstelle, die der betroffenen Person gegenüber rechtliche Wirkung entfalte oder sie in ähnlicher Weise erheblich beeinträchtige, wenn dieser mittels personenbezogener Daten der betroffenen Person ermittelte Wert von der Kreditauskunftei ein eine Bank übermittelt werde und jener Dritte diesen Wert seiner Entscheidung über die Begründung eines Vertragsverhältnisses mit der betroffenen Person „maßgeblich" zugrunde lege.

Wichtiger aber noch ist hier der Hinweis des EuGH auf die „durchgreifenden Bedenken" an der Wirksamkeit des § 31 BDSG des vorlegenden Gerichts. Das ist juristisch nachvollziehbar und wohl auch richtig, denn eine Öffnungsklausel für Scoring enthält die DSGVO nicht. Aber sie enthält eine Öffnungsklausel zur Rechtfertigung einer ausschließlich automatisierten Entscheidung im Einzelfall, Art. 22 Abs. 2 lit. b) DSGVO.

Eben diese will der deutsche Gesetzgeber jetzt angehen, weil er nicht dem Verbraucherschutz einen empfindlichen Rückschlag zumuten will. Denn fiele § 31 BDSG einfach ersatzlos weg, dann mag man zwar weniger ausschließlich automatisierte Entscheidungen bei der Scorenutzung haben, aber wo der Score nicht maßgeblich der Entscheidung zugrunde gelegt wird (und das werden wohl die meisten Fälle sein), dort würde es an den wichtigen Einschränkungen fehlen, die aktuell die Scoreerstellung und -verwendung binden.

Erste Reaktionen des Schrifttums auf den nun vorliegenden Entwurf machen deutlich, dass hier ganz grundlegende und weitgehende Feststellungen getroffen wurden, wobei sehr unterschiedlich beurteilt wird, ob man diese Feststellungen für richtig hält und begrüßt, oder das ein oder andere an der Argumentation für sperrig und systemwidrig hält.[10] Wichtig aber ist z.B. festzustellen, dass auch das Bundeskartellamt in seiner am Mittwoch veröffentlichten Abschlussbericht seiner

[10] S. *Blasek*, ZD 2024, 258; Heyer, ZVI 2024, 81; *Klein*, BB 2024, 266; *Langenbucher*, BKR 2024, 66; Menke, K & R 2024, 28; *Taeger*, BKR 2024, 41.

Sektoruntersuchung „Scoring im Onlinehandel“ am Scoring zwar allerlei zu kritisieren hat, den § 37a BDSG-E aber eben nicht kritisiert.[11] Das ist wichtig, und das ist richtig.

In der Tat: Es ist gut, dass der Gesetzgeber hier reagiert. Die geplante Neuregelung überführt den bisherigen § 31 BDSG in eine Ausnahmeregelung vom Verbot des Art. 22 Abs. 1 DSGVO und ergänzt ihn um weitere Bestimmungen zur angemessenen Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person gemäß Art. 22 Abs. 2 lit. b) DSGVO. In Absatz 1 und Absatz 2 wird dabei anknüpfend an der Formulierung des aktuellen § 37 Abs. 1 BDSG („Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag“) geregelt, dass diese beiden Absätze Ausnahmen von dem Verbot des Art. 22 Abs. 1 DSGVO festlegen, Personen nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu unterwerfen. Das Ziel ist klar: Die Bestimmung greift das zuvor bestehende Schutzniveau des ehemaligen § 31 BDSG auf und ergänzt diese Vorgaben in den Absätzen 1 bis 5 um materielle sowie formale Vorgaben, um das Schutzniveau an neue Rechtsprechung des EuGH anzupassen.

§ 37a BDSG stellt damit keine datenschutzrechtliche Erlaubnisnorm dar. Es gilt das allgemeine und besondere Datenschutzrecht, insb. Art. 6 DSGVO als Maßstab der Rechtmäßigkeit jeder Scoreerstellung.[12] Damit gilt auch: Die Übrigen Erlaubnisnormen des Art. 22 DS-GVO, insb. Art. 22 Abs. 2 lit. a) und lit. c) DS-GVO bleiben unberührt, unverändert und unbeeinflusst. Wer sich bislang hierauf berufen kann, der kann es auch künftig.

2. Einschränkungen der für Scoring nutzbaren Daten im Sinne des Verbraucherschutzes

Die Bedingungen, unter denen die Ausnahme eingreift, werden in den – gegenüber dem ehemaligen § 31 BDSG ergänzten – Vorgaben der Nummern 1 bis 7 ausgeführt. Darin sind insbesondere Daten genannt, die bei der Erstellung von Wahrscheinlichkeitswerten nicht berücksichtigt werden dürfen. All das dient dem Verbraucherschutz – ein legitimes Ziel auch bei der Ausgestaltung des Datenschutzrechts. Vorläufer gibt es dafür nicht, aber nachvollziehbar ist es allemal:

- Der ergänzte Absatz 2 Nr. 1 lit. a) macht zur Bedingung, dass bei der Erstellung und Verwendung eines Wahrscheinlichkeitswerts keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO genutzt werden. Mit dieser

[11] Abrufbar https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Scoring.pdf?__blob=publicationFile&v=2.
[12] Zurecht auch das Bundeskartellamt in seinem Abschlussbericht zur bereits erwähnten Sektoruntersuchung, S. 84.

Regelung wird auf den besonderen Schutzbedarf dieser Kategorie von Daten reagiert.[13] Der schon in Erwägungsgrund 71 der DSGVO erkannt wird („Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.“. Die Einbeziehung von Daten aus diesen Kategorien birgt in der Tat ein besonders Risiko für diskriminierende Ergebnisse, auch wenn sich an ihnen die Bonität beurteilen lassen sollte. Der so gewährleistete Schutz wurde auch von der DSK gefordert[14] und entspricht der Vorgabe des Art. 18 Abs. 3 Abs. 3 der Verbraucherkreditrichtlinie 2023/225/EU.

- Nr. 1 lit. b) macht zur Bedingung, dass bei der Erstellung und Verwendung eines Wahrscheinlichkeitswerts weder der Name der natürlichen Person noch personenbezogene Daten aus seiner Nutzung von sozialen Netzwerken genutzt werden. Soziale Netzwerke sind solche – so heißt es in der Gesetzesbegründung – im Sinne von Art. 18 Abs. 3 der Verbraucherkreditrichtlinie 2023/2225/EU[15] - freilich fehlt auch hier eine Definition. Eine Orientierung bietet insoweit § 1 Abs. 1 NetzDG, der eine – für die hiesige Betrachtung zwar nicht verbindliche, aber doch hilfreiche – Legaldefinition sozialer Netzwerke enthält: Danach versteht man hierunter „Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen“. Weitergehend noch ist die Forderung der DSK. Sie schlägt in ihrer Stellungnahme zum Gesetzesentwurf vor: „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.“[16] Das sind aber keine sozialen Netzwerke im Sinne des NetzDG. Das NetzDG unterscheidet zwischen privater und öffentlicher Kommunikation: In Abgrenzung zur zweiten Variante („der Öffentlichkeit zugänglich machen“) betrifft die Variante „teilen“ die Gruppenkommunikation innerhalb des sozialen Netzwerkes, also die Kommunikation zwischen registrierten Nutzern des Netzwerkes, die eine Kommunikationsgemeinschaft („Freundeskreis“) bilden. Die Bildung eines solchen „Freundeskreises“ setzt die

[13] BT-Drucks. 20/10859, S. 23.
[14] S. DSK, Stellungnahme v. 11.5.2023, Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren, S. 6, abrufbar abrufbar https://www.datenschutzkonferenz-online.de/media/st/DSK-Handlungsempfehlungen_Verbesserung_des_Datenschutzes_bei_Scoringverfahren.pdf.
[15] BT-Drucks. 20/10859, S. 23.
[16] Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. April 2024, S. 7 abrufbar https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf.

Registrierung im sozialen Netzwerk voraus.[17] „Teilen" von Inhalten erfasst keine Formen der Individualkommunikation. Dies folgt bereits aus der Genese des § 1 Abs. 1 S. 1 NetzDG. Die noch im Gesetzesentwurf enthaltene Differenzierung zwischen einem „Austausch" und einem „Teilen" von Inhalten wurde im Gesetzgebungsverfahren gestrichen, um zu verdeutlichen, „dass Dienste der Individualkommunikation (zB E-Mail- oder Messengerdienste) nicht unter das Gesetz fallen".[18] Eine solche Erweiterung mag man also erwägen, aber es fragt sich, ob *de lege lata* solche Informationen – die als nicht-öffentliche Informationen eben grds. dem Fernmeldegeheimnis unterliegen[19] – überhaupt verwendet werden könnten und wie die Auskunfteien diese Informationen erhalten könnten.

- Nr. 1 lit. c macht zur Bedingung, dass bei der Erstellung und Verwendung von Wahrscheinlichkeitswerten keine Informationen aus Zahlungseingängen und -ausgängen auf Geldkonten verwendet werden dürfen. Diese Zahlungsdaten sind besonders sensibel.[20] Umfasst von dieser Regelung sind sogenannte Kontotransaktionsdaten, die etwa über regulierte Kundeninformationsdienste nach dem Zahlungsdiensteaufsichtsgesetz ausgelesen und bereitgestellt werden können und Aufschluss über einzelne Zahlungsein- und -ausgänge einschließlich der jeweiligen Absender, Empfänger und Verwendungszwecke geben können. Die daraus ableitbaren Informationen bergen erhebliche Risiken für Betroffene, da sie im großen Umfang Erkenntnisse über persönliche und intime Aspekte der Lebensführung zulassen. Besondere gesetzliche Vorgaben, die etwa die Pflicht zur Einbeziehung von Informationen über Einkommensverhältnisse zur Risikobewertung betreffen, bleiben unberührt. Hier ist wiederum auf Art. 18 Abs. 3 der Verbraucherkreditrichtlinie hinzuweisen und seine Umsetzung: „Die Prüfung der Kreditwürdigkeit wird auf der Grundlage einschlägiger und genauer Informationen über Einkommen und Ausgaben des Verbrauchers sowie andere finanzielle und wirtschaftliche Umstände vorgenommen, die erforderlich sind und in einem angemessenen Verhältnis zu der Art, der Laufzeit, der Höhe und den Risiken des Kredits für den Verbraucher stehen. Zu diesen Informationen können Belege über Einkommen oder andere Quellen für die Rückzahlung, Informationen über Vermögenswerte und Verbindlichkeiten oder Informationen über andere finanzielle Verpflichtungen zählen".

[17] BeckOK InfoMedienR/*Hoven/Gersdorf*, 43. Ed. 1.8.2023, NetzDG § 1 Rn. 19.
[18] BeckOK InfoMedienR/*Hoven/Gersdorf*, 43. Ed. 1.8.2023, NetzDG § 1 Rn. 20 unter Hinweis auf BT-Drs. 18/12356, 7.
[19] Zu Reichweite und Grenzen *Wischmeyer* Dreier, Grundgesetz-Kommentar 4. Auflage 2023 Rn. 60-63: „Genaue Einzelfallprüfung"
[20] BT-Drucks. 20/10859, S. 24.

- Nr. 1 lit. d) ersetzt die bisher in § 31 Abs. 1 Nr. 3 BDSG vorgesehene Möglichkeit, Anschriftendaten für die Berechnung eines Wahrscheinlichkeitswerts zu nutzen, solange der Wert nicht ausschließlich auf Anschriftendaten beruht. Diese Rechtslage hat nach Auffassung der Entwurfsverfasser dem Diskriminierungsrisiko nicht hinreichend Rechnung getragen.[21] Zudem hat das Ausschließlichkeitsmerkmal Möglichkeiten zur Umgehung eröffnet. Im Anwendungsbereich des § 37a BDSG ist die Einbeziehung der Anschrift von natürlichen Personen nunmehr generell ausgeschlossen. Wiederum gilt: Die Zulässigkeit der Verarbeitung der Anschrift im Übrigen, etwa zu Zwecken der Kommunikation mit einer natürlichen Person, bleibt davon unberührt.[22] Gleiches gilt für den Zweck der Identifikation oder der bloßen Übermittlung der Adresse zur Betrugsprävention. Der Gesetzgeber würde damit eine Linie weiterverfolgen, die sich bereits in der Vergangenheit abzeichnete. Die BDSG-Reform 2009 führte den § 28 b Nr. 3 BDSG ein, der schon damals ursprünglich strenger gedacht war und der jetzt angestrebten Regelung entsprach.[23]2015 fassten Bündnis 90/Die Grünen nochmal nach und forderten das wiederum.[24] Die Banken machen davon nahezu ohnehin keinen Gebrauch[25] und in den USA wird das Geo-Scoring schon seit den 70er Jahren unter dem Stichwort „Redlining" als mögliche Diskriminierung.[26] Mit der neuen Regelung sollte die Praxis leben können.
- Nr. 2 macht zur Bedingung, dass die Erstellung und Verwendung von Wahrscheinlichkeitswerten keine minderjährigen Personen betreffen. Dies entspricht dem Regelungsgedanken des Erwägungsgrundes 71 Unterabsatz 1 S. 5 DSGVO („Diese Maßnahme sollte kein Kind betreffen.") – macht aus einem bloßen Erwägungsgrund freilich weitergehend „hard law". Die damit unmögliche Bonitätsbewertung Minderjähriger wäre in Anbetracht deren fehelenden Geschäftsfähigkeit ohnehin regelmäßig wenig sinnvoll. Die Regelung trifft keine Aussage darüber, ob ein Wahrscheinlichkeitswert über

[21] BT-Drucks. 20/10859, S. 24.
[22] Wiederum ausdrücklich BT-Drucks. 20/10859.
[23] BT-Drucks. 16/10529, S. 25 und Begründung S. 26.
[24] BT-Drucks. 18/4864, S. 7.
[25] So jedenfalls die Feststellung des ULD Schleswig-Holstein 2014 in seinem Abschlussbericht „Scoring nach der Datenschutznovelle 2009 und neuere Entwicklungen, S. 83: „Übereinstimmend berichten mit einer Ausnahme alle befragten Kreditinstitute, dass sie keine Daten zur Wohngegend bzw. Geo-Scoring verwenden. Als grundsätzliche Probleme von Geo-Scoring werden das Erlangen einer umfassenden Datenbasis, die Sicherstellung der Aktualität dieser Datenbasis und die Berücksichtigung der Dynamik der Stadtentwicklung genannt. Lediglich ein Kreditinstitut benutzt Infoscore-Daten zur Wohngegend bei der Score-Bildung. Da Infoscore Geo-Scoring-Daten verwendet, fließt der Wohnsitz als Variable indirekt in die Kreditentscheidung der Bank ein". Zur damaligen Praxis der Auskunfteien s. S. 72. Abrufbar https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2014/studie-scoring.pdf?__blob=publicationFile&v=1
[26] *Hsia*, Credit Scoring and the Equal Opportunity Act, Hastings Law Review Bd. 30/Vol. 2 [1978].

eine gerade volljährig gewordene Person erstellt werden darf, der auf Daten beruht, die sich auf das Verhalten der Person vor Erreichen der Volljährigkeit beziehen – es scheint aber naheliegend, dass das Verbot auch hier gilt. Auch hier will die DSK mehr. Sie hält es „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".[27] Nun nutzen die Auskunfteien schon bisher jedenfalls wohl nur selten das Alter und Geschlecht als Faktoren[28], obwohl das Alter aber durchaus kreditrelevant sein kann: Das Sterberisiko ist ein Kreditrisiko und der Gang in die Rente sicherlich auch. Die Regelungen des AGG sind keine absoluten Diskriminierungsverbote, sondern eine Benachteiligung wegen des Alters aus sachlichem Grund ist zulässig, s. § 20 Abs. 1 S. 1 AGG. Eben diese unterschiedliche Bonität, die an das Alter anknüpft, kann eine solche Rechtfertigung sein.[29] Man verzichtet also bereits aktuell weitergehender, als rechtlich erforderlich und systematisch geboten. Eine solcher Neuregelung bedarf es nicht.

- Nr. 3 lit. b) legt schließlich eine Zweckbindung der zur Erstellung und Verwendung genutzten Daten fest. Auf den ersten Blick erscheint das als problematisch, weil zumindest missverständlich, denn der Bezugspunkt der „anderen Zwecke" ist unklar, weil das Gesetz hier schweigt: Ist es der Zweck der Scoreerstellung oder der Zweck des Scores, der in Absatz 1 normiert ist? Nur letzteres kann richtig sein, weil nur dies der Systematik und dem Verbraucherschutz entspricht: Wenn man unter Zweck iSd. nicht den Zweck des Scores nach Absatz 1 versteht (Vertragsbegründung im weiteren Sinne und Bonitätsprüfung), sondern Zweck eben allein die Erstellung eines Scores selbst wäre dann wäre z.B. auch die Beauskunftung der Rohdaten selber, die in den Score einfließen, nicht mehr möglich. D.h. die Bank würde – anders als aktuell - einzig den Score bekommen, könnte aber im Austausch mit den Kunden ihn nicht Anhand der Daten, die in den Score eingeflossen sind, validieren. Das ist nicht im Sinne des Verbraucherschutzes. Dass das neue Recht wohl in der Tat so gelesen werden muss, macht auch die Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrats deutlich. Der Bundesrat meinte noch: „Aus der bisherigen Regelung geht nicht eindeutig hervor, auf welche Zwecke Bezug genommen wird. Gemeint sein könnten sowohl die Zwecke des § 37a Absatz 2 Nummer 3 Buchstabe

[27] aaO, S. 8.
[28] S. exemplarisch die SCHUFA AG: „Das Alter und das Geschlecht werden im SCHUFA-Scoring nicht berücksichtigt. Den Familienstand speichert die SCHUFA gar nicht erst." abrufbar https://www.schufa.de/scorechecktools/pt_einflussfaktoren.html.
[29] Hierzu ausführlich MüKoBGB/*Thüsing*, 9. Aufl. 2021, AGG § 20 Rn. 13-29.

a als auch die Zwecke des § 37a Absatz 1. Es bedarf daher der Klarstellung".[30] In seiner Ablehnung der vom Bundesrat geforderten Klarstellung betonte die Bundesregierung: „Der ausdrückliche Verweis auf Absatz 1 wird … als nicht erforderlich erachtet. Der jetzige Wortlaut ist in seiner Bezugnahme hinreichend klar".[31] So ist es dann wohl. Weitere Klarstellung scheint entbehrlich, auch wenn sie sicherlich nicht schädlich wäre.[32] Man weitergehend freilich darüber nachdenken, die Regelung zu streichen – und das wäre richtig. Denn mit der – ohnehin geltenden - Zweckbindung nach Art. 5 Abs. 1 lit. b) DSGVO hat das nach dem einen wie dem anderen Verständnis jedenfalls nichts zu tun. Danach dürfen Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Das ist gut und richtig so – einer der wesentlichen Grundsätze des Datenschutzes.[33] Durch die neue Vorschrift aber werden die Zwecke eben nicht durch den Verarbeiter vorgegeben, sondern durch den Gesetzgeber. Eine solche besondere Zweckbindung wäre nicht ganz ohne Vorbilder. Aber die früher z.B. in §§ 14 Abs. 4, 31 BDSG aF normierte besondere Zweckbindung bei Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, findet in der DSGVO keine Entsprechung und ist daher entfallen. In der Tat: Daten können auch zu anderen legitimen Zwecken durch die Kreditauskunfteien gespeichert werden.[34]. Solche „doppeltrelevanten" Daten müssen auch für mehrere legitime Zwecke verarbeitet werden können. Die Kreditauskunftei müsste sich sonst zwischen den Zwecken entscheiden und wird diese Entscheidung ggf. nicht am Verbraucherschutz orientieren, sondern an dem Geschäftsfeld, das profitabler ist - auch wenn die meisten Zwecke der Verarbeitung durch die Zwecksetzung des Absatz 1 also abgedeckt sein dürften (insb. etwa Geldwäscheprävention oder Betrugsbekämpfung durch Abs. 1 Nr. 1). Die weitergehende Forderung des Deutschen Anwaltsvereins, die Beschränkung also ganz zu streichen, hat also viel für sich.[35] Ebenso wichtig scheint der Hinweis der PKV in ihrer Stellungnahme[36]

[30] BT-Drucks. 20/10859, S. 33.
[31] BT-Drucks. 20/10859, S. 39.
[32] Gleichsinnig die Stellungnahme der Deutschen Kreditwirtschaft, S. 3.
[33] Ausführlich Paal/*Pauly/Frenzel*, 3. Aufl. 2021, DS-GVO Art. 5 Rn. 23 mwN.
[34] S. etwa die aktuellen Hinweise nach Art. 14 DSGVO nahezu gleichlautend mehrerer Kreditauskunfteien: „Die Verarbeitung der Daten erfolgt darüber hinaus zur Betrugsprävention, Geldwäscheprävention, Seriösitätsprüfung, Identitäts- und Altersprüfung, Anschriftenermittlung, Kundenbetreuung, Direktmarketing oder Risikosteuerung sowie Tarifierung oder Konditionierung. Neben den vorgenannten Zwecken verarbeitet die CRIF Bürgel GmbH personenbezogene Daten auch zu internen Zwecken (z.B. Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten, allgemeine Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten, Gewährleistung der IT-Sicherheit und des IT-Betriebs)".
[35] S. die Stellungnahme DSV, S. 4.
[36] Stellungnahme PKV, S. 5.

PKV, dass deren Unternehmen nicht einzuhalten, die mit eigenen Daten Wahrscheinlichkeitswerte errechnen, dies grds. immer mit Daten, die bereits vorher zu einem anderen Zweck verarbeitet wurden und auch nachfolgend noch zu anderen Zwecken dienen können. Das hat mit dem Geschäft der Auskunfteien, das man ja regeln will, nichts zu tun. Ich gehe davon aus, dass diese Scoreerstellung durch Art. 22 Abs. 2 lit. a) DS-GVO legitimiert ist, und dass man daran nicht rütteln will und – weil europarechtlich vorgegeben auch nicht rütteln kann. Der Ausschuss mag dies in seiner Stellungnahme festhalten – oder auch darauf verzichten, wenn er ohnehin so denkt und eine Klarstellung nicht für erforderlich hält.

3. Worauf bewusst – und zurecht! - verzichtet wurde

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. Die DSK stört das.[37] Das liegt auf einer Linie mit anderen Stellungnahmen des DSK, in der sie auch in ganz anderen Bereichen solche Zertifizierungen fordert, ohne dass dies der Gesetzgeber aufgegriffen hat. Auch hier sollte er davon Abstand nehmen, den Vorschlag aufzugreifen und dieser Forderung eben nicht nachkommen. Denn bereits nach aktuellem Recht und nach dem vorliegenden Wortlaut des § 37a Abs. 2 Nr. 3 lit. a BDSG-E ist ein Scoring ja nur erlaubt, wenn es wissenschaftlich anerkannten mathematisch-statistischen Verfahren folgt. Die Kreditauskunftei trägt hierfür die Beweis- und Darlegungslast. Wie sie der nachkommt, ist dann ihre Sache – Hauptsache, dass sie ihm nachkommt. Einfach mal drauflos zu machen, das kann sie ohnehin nicht, schwebt doch über all ihrem (möglichweise dann rechtswidrigem) Handeln das Damoklesschwert der Schadensersatzverpflichtung unabhängig vom Verschulden.[38] Das ist sicherlich verhaltenssteuernd genug. Eine Verengung auf eine Prä-Zertifizierung ist da fehlgehend. Hier würde Verwaltungsaufwand geschaffen werden, den die Politik gerade zurecht abbauen will.[39] Zudem wäre dies zuweilen durchaus kontraproduktiv im Sinne des Verbraucherschutzes: Schnelle Anpassungen des Scorings, wenn man Defizite des Verbraucherschutzes als Auskunftei erkannt hat, wären nicht möglich, müsste man doch stets den Umweg über eine Zertifizierung gehen. Wie systemfremd das wäre, das zeigt zudem auch der neue AI-Act: Hier ist eine obligatorische

[37] aaO, S. 9. Gleichsinnig vzbv: „Faires und transparentes Bonitätsscoring gesetzlich verankern - Stellungnahme des Verbraucherzentrale Bundesverbandes e.V. (vzbv) zum Regierungsentwurf zur Änderung des Bundesdatenschutzges etzes (BDSG) - 28. März 2024“,

[38] Ausführlich dazu *Thüsing/Zhou*, ZD 2024, S. 3 ff. sowie EuGH v. 11.4.2024 – Rd. 741/21, NJW 2024, 1561 (m. Anm. *Brams*).

[39] S. die Auseinandersetzung zwischen den Abgeordneten *Mahmut Özdemir* (SPD) und *Henrichmann* (CDU), Plenarprotokoll 20/168, S. 21634 f.

Konformitätsbewertung nach Artt. 16, 43 vorgesehen – aber eben nur für Anbieter von KI-Systemen mit hohem Risiko. Das ist der richtige Maßstab. Wenn das Scoring darunter fällt, dann bedarf es einer solchen Regelung nicht – wenn nicht, dann wäre er systematisch verfehlt.

Wenig überzeugend vor eben diesem Hintergrund von Beweislast und Haftungsrisiko ist die Forderung der DSK, zukünftig ausdrücklich in das Gesetz aufzunehmen, dass der Gesetzgeber Verfahren zur Sicherstellung richtiger und aktueller Daten für das Scoring implementieren sollte.[40] Diese Empfehlung hat keinen Eingang in § 37a BDSG-E gefunden. Die DSK verweist daher auf eine vorangegangene Stellungnahme vom 11. Mai 2023. In dieser Stellungnahme von 2023 forderte das Gremium bereits: „Im Rahmen technisch-organisatorischer Maßnahmen ist zu gewährleisten, dass die Daten korrekt erhoben werden und die Richtigkeit und Aktualität der Daten gewährleistet ist. Hierzu sollen Prozesse etabliert werden, die sowohl eine angemessene Erstprüfung als auch ein regelmäßiges Monitoring des Datenbestandes sicherstellen."[41]. Das tun die Auskunfteien bereits jetzt aus eigenem Interesse, und wenn sie es nicht tun sollten und es mit der Compliance nicht so genau nehmen, dann führt das bereits jetzt zu rechtswidriger Datenverarbeitung, die mit Sanktionen belegt ist. Eine weitergehende Compliance-Regel wäre hier systemwidrig, weil sie keine materiellen Anforderungen formuliert, sondern einen Prozess, der zu dem Ziel materieller Rechtsmäßigkeit führen soll. Der liegt aber in der Complianceverantwortung der handelnden Akteure, die e als die Sachnäheren im Einzelfall regelmäßig besser wissen als der Gesetzgeber, was dafür erforderlich ist und was nicht.

4. Ein Punkt, der wohl doch schon hinreichend klar ist: Erstellung und Verwendung von Wahrscheinlichkeitswerten über die Zahlungsfähig- und Zahlungswilligkeit

Der neu eingefügte Absatz 3 nimmt ebenfalls Bezug auf Art. 22 Ab. 1 DSGVO und regelt für den besonderen Fall der Erstellung und Verwendung von Wahrscheinlichkeitswerten über die Zahlungsfähig- und Zahlungswilligkeit von natürlichen Personen die zusätzlich zu Absatz 1 geltenden Bedingungen, unter denen Ausnahmen von dem Recht bestehen, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidungen unterworfen zu sein. Die sonstigen Regelungen entsprechen den Vorgaben der bisherigen Fassung des § 31 Abs. 2 S. 1 BDSG. Die ehemals in § 31 Abs. 2 S. 2 BDSG enthaltene Klarstellung, wonach die Zulässigkeit der Verarbeitung, einschließlich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht unberührt bleiben sollte, wurde

[40] aaO, s. 8.
[41] Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023 Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren, S. 6.

nicht übernommen. Diese Bestimmung hatte lediglich klarstellenden Charakter – dort, wo eine Klarstellung gar nicht erforderlich war.

5. Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person

Der neu einzufügende Absatz 6 setzt die Mindestvorgaben des Art. 22 Abs. 3 DSGVO zur Schaffung angemessener Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person um. Anlässlich Art. 22 Abs. 2 Buchstabe a) und c) DSGVO erklärt Art. 22 Abs. 3 DSGVO, dass zu diesen Maßnahmen mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens der verantwortlichen Stelle, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört. Dieser Mindeststandard wird auch für die Regelungen im neuen § 37a Abs. 1 und Abs. 2 übernommen. Wichtig ist zum Verständnis: Damit ist ein Recht auf Eingreifen durch den Entscheider, also den Kunden der Auskunftei geschaffen, nicht dessen, der maßgeblich auf diese Entscheidung durch den Score einwirkt. Hier würde ein solches Recht zum einen wenig bringen: Wie wollte man einen Algorithmus davon überzeugen, dass er irrt? Es geht um die Kreditwürdigkeit als Grundlage der Entscheidung für oder gegen den Kredit, nicht um die Richtigkeit des Scores.

6. Schutz von Geschäftsgeheimnissen

Der vorgesehene Absatz 5 nimmt die Anwendung des § 34 Abs. 1 S. 2 BDSG im Anwendungsbereich des neuen § 37a BDSG aus. Verantwortliche Stellen, die ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen treffen, unterliegen den besonderen Auskunftspflichten des Art. 15 Abs. 1 lit. h) DSGVO, wonach aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person bereitgestellt werden müssen. Der ebenfalls neu eingefügte § 34 Abs. 1 S. 2 BDSG enthält Regelungen zur Berücksichtigung schützenswerter Betriebs- und Geschäftsgeheimnisse bei der Prüfung von Auskunftsansprüchen. Ob das europarechtskonform ist, darüber mögen andere streiten. Wenn es die DS-GVO eins zu eins wiedergibt, dann ist es überflüssig – wenn es davon abweicht, dann ist es unwirksam. Die Gesetzesbegründung erläutert: Mit Blick auf nationale Rechtsprechung zur Abwägung zwischen dem Schutz von Betriebs- und Geschäftsgeheimnissen und der Auskunft über die abstrakte Methode der Berechnung der Wahrscheinlichkeitswerte könnte mit der Anwendung des § 34 Abs. 1 S. 2 BDSG im Anwendungsbereich des § 37a BDSG eine nationale Vorfestlegung einhergehen, die mit europarechtlichen Vorgaben nicht vereinbar sein könnte. Insbesondere im Hinblick auf erwartete Rechtsprechung des EuGH zur Auslegung des Art. 15 Abs. 1 lit. h) DSGVO wird die

Anwendung des § 34 Abs. 1 S. 2 BDSG im Anwendungsbereich des neuen § 37a BDSG daher ausgenommen. Eine inhaltliche Aussage über die Gewichtung schützenswerter Betriebs- und Geschäftsgeheimnisse im Kontext der Art. 15 Abs. 1 lit. h) und 22 Abs. 1 DSGVO wird damit nicht getroffen. Damit bleibt es beim Europarecht: Erwägungsgrund 63 S. 5 DSGVO stellt klar, dass das Auskunftsrecht nach Art. 15 DSGVO Geschäftsgeheimnisse nicht beeinträchtigen sollte, diese also gem. Art. 15 Abs. 4 DSGVO einem Auskunftsverlangen entgegengehalten werden können.[42] Das Interesse des Verantwortlichen am Schutz des Geschäftsgeheimnisses ist mit dem Auskunftsinteresse des Betroffenen in Einklang zu bringen.[43] Diese Erkenntnis ist nicht neu. Der EuGH streifte das Spannungsfeld von Geheimhaltungs- und Auskunftsinteresse bei der Erstellung von Scorewerten zwar,[44] verzichtete aber gleichwohl darauf, sich hier klar zu positionieren.[45]

7. Transparenzpflichten für verantwortliche Stellen

Absatz 4 sieht umfassende Transparenzpflichten für verantwortliche Stellen vor, die im Rahmen von ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidungen Wahrscheinlichkeitswerte nach Absatz 2 oder Absatz 3 erstellen und verwenden. Wichtig ist: Verwender des Scores ist der Onlinehandel oder die Bank, nicht die Auskunftei.

8. Fragen, die weiterhin offenblieben

Wichtige Fragen würde damit der Gesetzgeber klar beantworten – anderes bleibt offen. So bleibt unklar, welche Auswirkungen der neue § 37a BDSG auf nicht vollständig auf automatisierten Verarbeitungen beruhende Entscheidungen hat. Dort, wo etwa die Errechnung eines Wahrscheinlichkeitswertes nicht auf einer vollständig automatisierten Verarbeitung beruht, greift das Verbot nach Art. 22 DSGVO nicht, ebenso wenig die Öffnungsklausel gem. Art. 22 Abs. 2 lit. b DSGVO. Da nach dem Gesagten § 37a BDSG keine datenschutzrechtliche Erlaubnisnorm darstellt, ist die Rechtsgrundlage für die Verarbeitung in allgemeinem Datenschutzrecht zu suchen; auch und insbesondere für nicht auf vollständig automatisierter Verarbeitung beruhende Entscheidungen. Messlatte für die Rechtmäßigkeit der Verarbeitung ist also weiterhin Art. 6 Abs. 1 DSGVO. Auch insoweit kann die neue gesetzliche Regelung aber jedenfalls ein Fingerzeig darauf sein, welche personenbezogenen Daten für die Errechnung zulässigerweise verarbeitet werden dürfen und welche nicht. § 37a BDSG – das scheint naheliegend – kann also in verwandten Sachverhalten mittelbar dadurch Wirkung entfalten, dass er in offene Abwägungsklauseln wie

[42] S. hierzu ausf. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, 2023, S. 439 ff.
[43] *Thüsing/Thüsing/Pötters*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 18 Rn. 37.
[44] EuGH, Urt. v. 7.12.2023 – C-634/21, BB 2022, 270 Rn. 16, 56.
[45] Hierauf hinweisend auch Klein, BB 2024, 266, 268.

Art. 6 Abs. 1 lit. b) und f) DSGVO „hineingelesen" wird, freilich mangels Öffnungsklausel ohne eine letztverbindliche Aussage über die Rechtmäßigkeit der Verarbeitung zu treffen.

9. Bedeutung über das Scoring hinaus

Für das Scoring wird es also künftig klare Linien geben. Vielleicht ebenso wichtig an dem Urteil sind aber nicht nur die Auswirkungen auf die Kreditauskunfteien und die Kreditvergabe, sondern ihre über den Einzelfall hinausgehenden Folgen. Denn der Bereich der vollständig automatisierten Entscheidung, vor dem die DSGVO den Betroffenen schützen will, wird erheblich ausgeweitet – mit solch weitreichenden Konsequenzen, dass man die Sinnhaftigkeit durchaus hinterfragen kann.[46] Denn der EuGH verlagert den Zeitpunkt der Entscheidung nicht unerheblich nach vorne: Die automatisierte Entscheidung über einen Kreditantrag treffe nicht (allein) das Kreditinstitut auf Grundlage des Score-Wertes, sondern bereits die Kreditauskunftei durch die Berechnung des Score-Wertes, wenn das Kreditinstitut den Score-Wert seiner Entscheidung „maßgeblich zugrunde legt". Grundsätzlich bedeutet „ausschließlich automatisiert" aber „ohne jegliches menschliches Eingreifen".[47] Wenn es reicht, dass eine automatisierte Datenverarbeitung nun bereits dann ausschließlich automatisiert ergeht, wenn sie einen nicht unwesentlichen Einfluss auf die spätere menschliche Entscheidung hat (was anders könnte „maßgeblich zugrundelegen" heißen?[48]), dann vervielfältigen sich die Fallgestaltungen. Bereits Entscheidungsvorbereitungen sind jetzt am Maßstab der Entscheidung zu messen.[49] Die Auswirkungen sind weitreichend: Erstens bedürfte jede automatisierte Datenverarbeitung, auf die Entscheidungen maßgeblich gestützt werden, der besonderen gesetzlichen Legitimation bzw. Einwilligung, und zweitens bedürfte auch jede menschliche Entscheidung, die maßgeblich auf einer automatisierten Datenverarbeitung beruht, einer solchen gesetzlichen Legitimation bzw. Einwilligung Um es plastisch zu machen: Lehnt ein Vermieter einen Mieter ab, weil er ihn gegoogelt hat, dann stützt er sich auf eine ausschließlich automatisierte Datenverarbeitung; gleicht eine Bank Kontodaten eines Kunden mit den sog. Terrorlisten automatisiert ab und friert nach einem Treffer die Guthaben vorläufig bis zur weiteren Klärung ein, dann wäre dies, trotz menschlicher Entscheidung, von den besonderen Regeln

[46] S. auch die Kritik *Taegers*, BKR 2024, 41: „Während es im Tatbestand des Art. 22 DSGVO heißt, dass eine betroffene Person nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen sein darf, soll die Anwendung des Verbots aus Art. 22 DSGVO schon auf das externe Scoring nun von dem im Tatbestand nicht vorkommenden Begriff ‚maßgeblich' abhängen, der die Verwendung des Scorewertes durch den Kreditgeber im Verhältnis zur Wirtschaftsauskunftei also einem Dritten beschreibt. Es ist nicht nachvollziehbar, dass nach der „Theorie vom Zusammenwirken" die Rechtmäßigkeit der externen Wahrscheinlichkeitswertberechnung vom künftigen, nicht vorhersehbaren Verhalten des Empfängers eines Scores abhängen soll."

[47] Erwägungsgrund 71 S. 1 DSGVO.

[48] Zu den Deutungen durch den Generalanwalt s. *Thüsing/Peisker/Musiol*, RDV 2022, 189, 194. S. auch Heinen, NZA 2024, 33, 36.

[49] Entgegen der bisher h.M., s. *Heinen*, NZA 2024, 33: „Die herrschende Meinung lehnt eine Anwendung des Art. 22 I DS-GVO auf die automatisierte Entscheidungsvorbereitung ab".

vollständig automatisierter Verarbeitung erfasst, weil eben der Abgleich einen wesentlichen Einfluss hat. Jedes ärztliche Rezept, das maßgeblich auf Datenverarbeitungen z.B. in großen Kohortenstudien beruht, die mittels künstlicher Intelligenz ausgewertet werden, wäre ebenso eine automatisierte Entscheidung, wie die zugrundeliegende Datenverarbeitung. Selbst der Umweg des Taxifahrers, der nach Navi fährt, wäre eine automatisierte Entscheidung, die nach der DSGVO unzulässig wäre, sofern sie dem Betroffenen gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt.

All das könnte künftig eine sehr viel weitgehender Dimension erhalten. Zurecht erfolgte ein Hinweis des Hamburger Datenschutzbeauftragten noch am Tag der Entscheidung: „Urteil von wegweisender Bedeutung auch für KI-basierte Entscheidungen".[50] In der Tat: Dass das Ergebnis einer KI am Ende den Entscheidungsprozess maßgeblich beeinflusst, wird viel häufiger sein, als dass sie ihn ausschließlich bestimmt. Dann aber bedarf es auch hier jeweils ausdrücklicher gesetzlicher Ermächtigung. Wie dies angesichts der Vielgestalt möglicher KI-Anwendungen gelingen kann, ist offen. Dies wird eine weitere große Herausforderung künftiger Rechtsentwicklung sein.

IV. Hinweise zu Vorschlägen, die es nicht in den Entwurf geschafft haben, insb. zur Nutzung von Gesundheitsdaten durch die Unternehmen der PKV.

Schließlich ist der Blick kurz auf Vorschläge zu anderen Vorschriften des BDSG zu richten, die es nicht in den Entwurf geschafft haben. Dazu gehört etwa die Streichung des § 38 BDSG (Datenschutzbeauftragte nichtöffentlicher Stellen), die im Laufe des bisherigen Gesetzgebungsverfahrens intensiv diskutiert und mittlerweile aufgegeben wurde. Damit geht eine Stärkung der Stellung des Datenschutzbeauftragten einher. Darüber hinaus haben etwa auch Vorschläge zur Änderung des § 41 Abs. 1 S. 1 BDSG im Hinblick auf die Haftung juristischer Personen ihren Weg nicht in den Entwurf gefunden. Zu Recht, denn angesichts der unklaren Auswirkungen der EuGH-Vorgaben auf die Praxis[51] und der noch laufenden Verfahren, sollte noch gewartet werden. Die Bundesregierung ist sich aber bewusst, dass sich zukünftig gesetzgeberischer Handlungsbedarf ergeben könnte.[52]

Ein großer und wichtiger Bereich, der auf eine (umfassende) Regelung wartet, ist der Beschäftigtendatenschutz – s. auch die Stellungnahme der Deutschen Kreditwirtschaft und der PKV. Nach der Entscheidung des EuGH in der Rs. C-34/21 sind die dem Verfahren zu Grunde

[50] S. die Pressemitteilung vom selben Tag, Auswirkungen des Schufa-Urteils auf KI-Anwendungen, abrufbar https://datenschutz-hamburg.de/news/auswirkungen-des-schufa-urteil-auf-ki-anwendungen.
[51] EuGH, Urt. v. 5.12.2023 – C-807/21.
[52] BT-Drs. 20/10859, S. 40; s. auch *Wybitul/Zhou*, ZD 2024, 301.

liegenden hessischen Landesdatenschutzvorschriften nicht mehr aufrecht zu erhalten, weil sie die DSGVO inhaltsgleich wiederholen und damit keine spezifischeren Vorschriften i.S.d. Art. 88 DSGVO darstellen.[53] Das gilt auch für den nahezu identischen § 26 Abs. 1 S. 1 BDSG, der für die Verarbeitung personenbezogener Beschäftigtendaten nicht mehr herangezogen werden kann.[54] Ein unbefriedigender Zustand, der angegangen werden sollte. Die Bundesregierung hat bereits in ihrer Nationalen Datenstrategie aus 2023 ein eigenständiges Beschäftigtendatenschutzgesetz angekündigt,[55] dessen Regierungsentwurf aber bislang noch auf sich warten lässt.

Noch wichtiger vielleicht ist der auch von der PKV[56] in ihrer Stellungnahme angesprochene Regelungsdefizit im Hinblick auf die Nutzung von Gesundheitsdaten durch die Unternehmen der privaten Krankenversicherung: Angebote der PKV im Bereich des Gesundheitsmanagements zur Gewährleistung einer hochwertigen medizinischen Versorgung im Sinne der Versicherten erfordern eine korrespondierende Daten Verarbeitungsbefugnis der Versicherer. Hierfür kann auch die Analysen von Rechnungsdaten erforderlich sein für die Unterbreitung individueller Angebote des Gesundheitsmanagements, auch ohne die vorherige Einholung einer entsprechenden ausdrücklichen Einwilligung der Privatversicherten. Gleichbehandlung mit der GKV ist sinnvoll: Nach § 284 Abs. 1 Nr. 14, Abs. 3 S. 1 SGB V ist den gesetzlichen Krankenkassen die Erhebung und Speicherung von Daten zur Gewinnung von Versicherten für die Vorbereitung und Durchführung von Gesundheitsmanagementprogrammen ausdrücklich gestattet. Der entsprechende Vorschlag des PKV-Verbands zur klarstellenden Neufassung des § 22 BDSG ist sinnvoll und sollte umgesetzt werden.[57]

V. Eine kurze Summa

Der Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes ist – gemessen am Umfang – ein „kleines", aber wichtiges Update für das BDSG, mit dem einige Detailkorrekturen vorgenommen und EuGH-Rechtsprechung umgesetzt werden. Betrachtet man die beiden Kernanliegen des Entwurfs etwas näher, so muss man im Hinblick auf die Institutionalisierung der DSK aber konstatieren, dass der derzeit geplante § 16a BDSG-E zu keiner wirklichen Verbesserung des *status quo* führt. In Sachen Kredit-Scoring durch Wirtschaftsauskunfteien hat der Gesetzgeber mit § 37a BDSG-E eine umfassende Regelung

[53] EuGH, Urt. v. 30.3.2023 – C-34/21.
[54] S. etwa *Thüsing/Peisker*, NZA 2023, 213; *Zhou/Wybitul*, ArbRB 2023, 240. Ausführlich auch BAG v. 9.5.2023 - 1 ABR 14/22.
[55] Die Bundesregierung, Fortschritt durch Datennutzung – Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.pdf?__blob=publicationFile&v=3.
[56] Stellungnahme PKV, S. 6.
[57] Stellungnahme PKV, S. 7.

geschafft, die ihren Zweck erfüllen wird: Verbraucherschutz, Persönlichkeitsschutz und wirtschaftliche Handlungsfähigkeit in einen angemessenen Ausgleich zu bringen.

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 F

GESELLSCHAFT FÜR FREIHEITSRECHTE

20. Juni 2024

Stellungnahme

zum Gesetzentwurf der Bundesregierung „Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ (BT-Drs. 20/10859)

für die öffentliche Anhörung im Ausschuss für Inneres und Heimat des Deutschen Bundestags am 24. Juni 2024

von Dr. Simone Ruf,
Gesellschaft für Freiheitsrechte e.V.

A. Zusammenfassung

Hinsichtlich der im Gesetzentwurf der Bundesregierung vorgesehenen Reformen des Bundesdatenschutzgesetzes (im Folgenden „BDSG“) empfehlen wir, insbesondere die Erweiterung der Ausnahmen zu den datenschutzrechtlichen Auskunftsansprüchen in § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E zu streichen. Dies würde Betroffenenrechte und den Rechtsschutz gegen rechtswidrige Datenverarbeitungen erheblich schwächen (B).

Zwar begrüßen wir die Aufnahme von § 16a BDSG-E. Die Institutionalisierung der Datenschutzkonferenz (im Folgenden „DSK“) könnte aber grundsätzlich noch weiter gehen und auch eine Geschäftsstelle sowie eine verbindliche Beschlussfassung vorsehen (C).

Da der Einsatz biometrischer Fernidentifikationssysteme auch in Deutschland in der polizeilichen Praxis trotz fehlender Rechtsgrundlagen auf dem Vormarsch ist, empfehlen wir, die Gelegenheit der Reform des BDSG zu nutzen, den Gesetzentwurf durch ein **Verbot** von Datenverarbeitungen mittels **biometrischer Fernidentifikationssysteme im öffentlichen Raum** zu erweitern (D).

Der Einsatz derartiger Systeme ist mit enormen Risiken und Gefahren für Grund- und Menschenrechte verbunden und kann angesichts der nach wie vor hohen Fehleranfälligkeit und Diskriminierungseffekte dieser Systeme nicht zu einer effektiven Polizeiarbeit beitragen. Angesichts des Missbrauchspotenzials muss ein Einsatz durch Private erst recht ausgeschlossen sein.

Das Unionsrecht lässt den nationalen Gesetzgebern Spielraum für ein solches Verbot und auch das Grundgesetz ermöglicht es, Verbote im Rahmen der verfassungsrechtlichen

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Kompetenzordnung im BDSG vorzusehen. Die Verbote können für öffentliche Stellen der Länder zwar nur eingeschränkt Geltung beanspruchen, jedoch erweitert § 500 StPO den Anwendungsbereich des BDSG für die Tätigkeit der Landespolizei im repressiven Bereich.

Wir empfehlen ein möglichst umfassendes Verbot, welches Echtzeit- als auch retrograde Abgleiche umfasst. Diese pauschale, auf der KI-Verordnung basierende Unterscheidung ist aus grundrechtlicher Perspektive nur schwer nachvollziehbar und jedenfalls nicht das ausschlaggebende Kriterium für die Beurteilung der Eingriffsintensität. Vielmehr birgt auch der retrograde Abgleich das Risiko nachhaltiger Grundrechtsbeeinträchtigungen und spezifischer Gefahren.

Wir empfehlen, auch die Weiterverarbeitung von Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen aufgrund anderer Gesetze erhoben wurden, zu verbieten. Dadurch können potenzielle Lücken geschlossen werden, die sich gegebenenfalls künftig daraus ergeben könnten, dass auf Landesebene Rechtsgrundlagen für den Einsatz biometrischer Fernidentifizierungssysteme im öffentlichen Raum geschaffen werden. Ein **Formulierungsvorschlag** ist der Stellungnahme beigefügt.

B. Beschränkung des Auskunftsanspruchs durch § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E

Durch einen neuen Satz 2 soll sowohl in § 34 Abs. 1 Satz 2 BDSG als auch in § 83 Abs. 1 Satz 2 SGB X eine neue Ausnahme für Auskunftsansprüche eingeführt werden. Demnach soll das Recht auf Auskunft auch insoweit nicht bestehen, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt.

Diese Neuerung stellt eine **Verschlechterung für die Betroffenenrechte** dar. Es ist zu befürchten, dass damit ein Ausnahmetatbestand geschaffen wird, der von Verantwortlichen zum einen übermäßig in Anspruch genommen wird und zum anderen für Betroffene, die ihre Interessen darlegen müssen, mit erheblichem Aufwand verbunden ist. Da Auskunftsansprüche oft der erste Schritt sind, um Rechtsschutz gegen unzulässige Datenverarbeitungen zu ergreifen, werden damit mittelbar die Rechtsschutzmöglichkeiten geschmälert.

Der Normtext insinuiert außerdem, dass bei Vorliegen der Voraussetzungen die Ausnahme absolut gelten soll, also auch keine teilweise Beschränkung der Auskunft möglich sein soll. Dem steht insbesondere ErwGr. 63 der Verordnung (EU) 2016/679 (im Folgenden „DSGVO“) entgegen,

demgemäß Ausnahmen nicht dazu führen dürfen, dass der betroffenen Person jegliche Auskunft verweigert wird. Außerdem trägt bereits Art. 15 Abs. 4 DSGVO dem Schutz von Geschäfts- und Betriebsgeheimnissen Rechnung, sodass sich die Farge stellt, inwiefern die Neuregelung überhaupt erforderlich ist.

C. Institutionalisierung der Datenschutzkonferenz

§ 16a BDSG-E ist im Grundsatz zu begrüßen, da er einen Schritt in Richtung Institutionalisierung der DSK darstellt, die auch im Koalitionsvertrag enthalten ist.[1] Dort ist auch vorgesehen, rechtlich, wo möglich, verbindliche Beschlüsse zu ermöglichen.[2] Allerdings bleibt § 16a BDSG-E dahinter zurück und verankert lediglich den status-quo der DSK im BDSG. Sie gibt derzeit bereits Auslegungshilfen, Leitlinien oder Empfehlungen zu Voraussetzungen und Rechtsfolgen einschließlich allgemeiner Einschätzungen zur Vereinbarkeit von konkretisierten Datenverarbeitungen mit dem Datenschutzrecht heraus, die aber nicht verbindlich sind.

Um Einheitlichkeit und Rechtssicherheit bei der Auslegung datenschutzrechtlicher Normen künftig wirksam zu ermöglichen, könnte eine Befugnis aufgenommen werden, die es der DSK erlaubt, **verbindlich Beschlüsse** zu fassen. Die Verbindlichkeit könnte auch beschränkt werden auf das Innenverhältnis und ggf. den nicht-öffentlichen Aufsichtsbereich. Die Einrichtung einer **Geschäftsstelle** könnte darüber hinaus dazu beitragen, die Arbeit der DSK durch einen administrativen Unterbau effizienter zu gestalten. Mit Blick auf das Verfassungsrecht stellt sich dabei vor allem die Frage, ob es sich um eine zulässige Form der sogenannten Mischverwaltung[3] handelt. Es gibt überzeugende rechtliche Gründe, dass bei einer derartigen Institutionalisierung weder Unions- noch Verfassungsrecht verletzt wird, da die Mischverwaltung dadurch gerechtfertigt werde könne, dass mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein besonderer Sachgrund vorliege und die Datenschutzkonferenz zudem im Rahmen einer eng umgrenzten Sachmaterie tätig sei.[4] Dennoch sind damit einige verfassungsrechtliche Unsicherheiten verbunden, die, auch wenn eine Stärkung der Kooperation

[1] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://cms.gruene.de/uploads/assets/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf, S. 17.
[2] Ebd.
[3] Dazu z.B. *Ibler*, in: Dürig/Herzog/Scholz, 103. EL Januar 2024, GG Art. 87 Rn. 195 f.; *F. Kirchhof*, in: Dürig/Herzog/Scholz/, 103. EL Januar 2024, GG Art. 83 Rn. 117 ff.
[4] *Richter/Spiecker*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, Januar 2022, insb. S. 25 ff.

in Form gemeinsamer und verbindlicher Entscheidungen begrüßenswert ist, eingepreist werden müssen. Nichtsdestotrotz dürften die damit verbundenen Vorteile dafür sprechen, diese Unsicherheiten in Kauf zu nehmen.

D. Aufnahme eines Verbots biometrischer Fernidentifikation im öffentlichen Raum in das BDSG

Biometrische Fernidentifikation stellt eine besondere Gefahr für Grund- und Menschenrechte dar (I). Die Reformbestrebungen des BDSG sollten deshalb genutzt werden, um ein Verbot biometrischer Fernidentifikation im öffentlichen Raum im BDSG zu verankern (II). Das Verbot sollte dabei möglichst weitreichend gefasst werden (III).

I. Biometrische Fernidentifikation als Gefahr für die Grundrechte

Biometrische Fernidentifikation im öffentlichen Raum birgt erhebliche Risiken und Gefahren für die Verwirklichung und den Schutz von Grund- und Menschenrechten.

Dass biometrische Daten besonders schutzwürdig sind, ergibt sich aus der besonderen Nähe biometrischer Daten zur Individualität und Identifizierbarkeit einer Person. Normativ ist diese grundsätzliche Wertung zum Bespiel in Art. 9 Abs. 1 DSGVO und Art. 10 Richtlinie (EU) 2016/680 (im Folgenden „JI-RL") sowie in § 48 BDSG verankert und wurde auch vom Bundesverfassungsgericht besonders hervorgehoben.[5]

Der Einsatz derartiger Technologie im öffentlichen Raum birgt das Risiko ausufernder Massenüberwachung. Personen können immer und überall eindeutig identifiziert werden. Dadurch können umfassende **Bewegungs- und Persönlichkeitsprofile** erstellt werden. Denn der Kontext des Aufenthaltsortes ermöglicht auch Rückschlüsse auf höchstpersönliche Daten, wie beispielsweise auf politische Einstellungen, die sexuelle Orientierung oder auch den Gesundheitszustand einer Person. Anonymität im öffentlichen Raum droht sowohl gegenüber staatlichen Stellen als auch gegenüber Privaten verloren zu gehen.

Diese Risiken haben erhebliche Auswirkungen auf das Verhalten von Menschen im öffentlichen Raum. Der Einsatz biometrischer Fernidentifikation ist mit enormen Abschreckungseffekten verbunden. Menschen können hierdurch von der Ausübung ihrer Grundrechte, insbesondere der

[5] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 87.

Meinungs- und Versammlungsfreiheit abgeschreckt werden (sog. **chilling effects**[6]), wenn sie befürchten, dabei jederzeit identifiziert werden zu können, auch wenn sie sich gesetzestreu verhalten.[7]

Hinzukommt, dass diese Instrumente der biometrischen Fernidentifikation höchst **fehleranfällig** sind.[8] In Bezug auf Gesichtserkennungssysteme kann festgestellt werden, dass nicht weiße Menschen, aber auch non-binäre und transgender Personen besonders häufig falsch identifiziert werden und in der Folge illegitimen, grundrechtsbeschränkenden Maßnahmen ausgesetzt sind. Das haben inzwischen verschiedene Studien gezeigt.[9] Die Nutzung fehleranfälliger Systeme greift nicht nur erheblich in Grundrechte unbescholtener Menschen ein, sondern dürfte somit auch nicht den Ansprüchen an die Effektivität polizeilicher Arbeit gerecht werden. So führte fehlende Effektivität auch in Sachsen dazu, dass die 2019 geschaffene Rechtsgrundlage, die den Einsatz biometrischer Fernidentifikationssystemen im öffentlichen Raum legitimieren sollte, bereits nach ihrer ersten gesetzlich vorgesehenen Evaluation nicht verlängert wurde.[10]

Auch **strukturelle Diskriminierung** – insbesondere struktureller Rassismus – wird durch den Einsatz solcher Systeme verstärkt. Vor allem dann, wenn Referenzdatenbanken aus polizeilichen Datenbanken bestehen, setzen sich die darin angelegten Diskriminierungen fort. Das Risiko von weiteren polizeilichen Maßnahmen betroffen zu sein, ist somit für marginalisierte Gruppen deutlich höher.

Da biometrische Daten anders als beispielsweise Kreditkartennummern oder Passwörter nicht geändert werden können, aber oft als Authentifizierungsinstrument genutzt werden, kann es zu

---

[6] *Assion*, Überwachung und Chilling Effects, in: Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz, 2014, S. 31 ff.; vgl. auch BVerfG, Beschluss v. 17.02.2009, 1 BvR 2492/08, Rn. 131.

[7] Dazu ausführlich z.B. International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, S. 14 f., abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2.

[8] *Hälterlein*, Biometrische Gesichtserkennung – technologischer Solutionismus für mehr „Sicherheit", 8. April 2024, abrufbar unter https://www.cilip.de/2024/04/08/biometrische-gesichtserkennung-technologischer-solutionismus-fuer-mehr-sicherheit/; zur Trefferquote beim Pilotprojekt „Südkreuz": *Chaos Computer Club*, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, 13. Oktober 2018, abrufbar unter https://www.ccc.de/en/updates/2018/debakel-am-suedkreuz.

[9] Z.B. *Buolamwini/Gebru*, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in: Proceedings of Machine Learning Research, Vol. 81, 2018, S. 77-91; International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, S. 15 ff. m.w.N., abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2.

[10] Pressemitteilung des Sächsischen Staatsministerium des Innern v. 22. August 2023, abrufbar unter https://www.medienservice.sachsen.de/medien/news/1068787.

erheblichen Konsequenzen führen, wenn unberechtigte Zugriffe auf biometrische Datenbanken stattfinden. Dieses Risiko besteht sowohl für die private als auch die staatliche Nutzung. Die Verwendung von biometrischen Fernidentifikationssystemen würde tendenziell dazu führen, dass biometrische Datenbanken entstehen oder vergrößert werden. Mit dem Einsatz gehen somit erhebliche Risiken der **Datensicherheit** einher.

Nicht zuletzt aufgrund der enormen **Streubreite** biometrischer Fernidentifikation handelt es sich um schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Betroffen sind alle Personen, deren biometrische Daten abgeglichen werden. Das Bundesverfassungsgericht hat klargestellt, dass auch Nicht-Treffer Eingriffe in die Grundrechte der Personen, deren Daten abgeglichen werden, darstellen.[11] Dadurch, dass die Maßnahme heimlich stattfindet, verschärft sich der Eingriff, da Rechtsschutzmöglichkeiten für Betroffene dann regelmäßig nur sehr eingeschränkt möglich sind.[12]

II. Umsetzung eines Verbots im BDSG

Bereits in der Anhörung im Digitalausschuss zum Thema „Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz" am 15. Mai 2024 wurde die Möglichkeit, ein Verbot in das BDSG aufzunehmen thematisiert.[13]

Die Verankerung eines Verbots biometrischer Fernidentifikation im öffentlichen Raum in das BDSG ist angesichts der aktuellen Rechtslage und Praxis erforderlich, um den Koalitionsvertrag umzusetzen (1). Sowohl das Unionsrecht (2) als auch die nationale verfassungsrechtliche Kompetenzordnung (3) ermöglichen die Umsetzung eines Verbots im BDSG. Auch der Anwendungsbereich und die Auswirkungen eines Verbots im BDSG sprechen dafür, ein Verbot dort zu verankern (4).

1. Notwendigkeit gesetzgeberischer Klarstellung und Umsetzung des Koalitionsvertrags

Durch die **KI-Verordnung** (im Folgenden „KI-VO") selbst wird gem. Art. 5 Abs. 1 lit. h KI-VO nur ein kleiner Teil der biometrischen Fernidentifizierung im öffentlichen Raum verboten. Dieser betrifft die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich

[11] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51.
[12] BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07, Rn. 79.
[13] *Roth-Isigkeit*, Stellungnahme im Rahmen der öffentlichen mündlichen Anhörung am 15. Mai 2024 des Digitalausschusses des Bundestags zum Thema Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über künstliche Intelligenz, 15. Mai 2023, S. 27 f., abrufbar unter https://www.bundestag.de/resource/blob/1002542/9399017597afda26d626a23617a30bbb/Roth-Isigkeit.pdf.

zugänglichen Räumen zu Zwecken der Strafverfolgung und gilt auch nicht absolut, sondern sieht eine Reihe von Ausnahmen vor. Das Verbot betrifft damit „nur" die Strafverfolgung, wobei darunter nach Art. 3 Abs. 46 KI-VO auch die Abwehr von Gefahren für die öffentliche Sicherheit gehört.

Derzeit existieren für nationale **Polizei- und Sicherheitsbehörden** im Bereich der Strafverfolgung und Gefahrenabwehr keine spezifischen Rechtsgrundlagen, die den Einsatz biometrischer Fernidentifikation erlauben[14], sodass die Verwendung derzeit rechtswidrig wäre. Die KI-Verordnung stellt zwar Anforderungen an diese Systeme und potenzielle Befugnisnormen, beinhaltet selbst aber keine Rechtsgrundlagen, die staatliche Eingriffe durch biometrische Fernidentifikationssysteme legitimieren. Nichtsdestotrotz hat sich jüngst durch die mediale Berichterstattung[15] sowie kleine Anfragen in verschiedenen Landesparlamenten[16] gezeigt, dass solche Systeme bereits im Einsatz sind. Der Bundesgesetzgeber sollte deshalb unbedingt durch ein Verbot klarstellen, dass der Einsatz dieser Systeme nicht erlaubt ist.

Mit Blick auf das Verbot des Image-Scrapings in Art. 5 Abs. 1 lit. e KI-VO sind die Möglichkeiten **Privater** beim Einsatz von Systemen biometrischer Gesichtserkennung zwar teilweise schon beschränkt. Demnach ist es nicht erlaubt, ungezielt Gesichtsbilder aus dem Internet oder aus Videoüberwachungsaufnahmen auszulesen. Damit dürfte zwar die Nutzung von Systemen wie PimEyes oder Clearview schon nach der KI-VO eindeutig unzulässig sein. Ein umfassender, lückenloser Ausschluss biometrischer Fernidentifikation durch Private ist dadurch aber nicht sichergestellt. Denn Fernidentifikation kann nicht nur über den Abgleich von Gesichtsbildern, sondern auch mittels anderer physischer, physiologischer und verhaltensbezogener menschlicher Merkmale erfolgen, wie Augenbewegungen, Körperform, Stimme, Prosodie, Gang, Haltung, Herzfrequenz, Blutdruck, Geruch oder charakteristischer Tastenanschlag (vgl. ErwGr. 15

[14] Die Eingriffe werden z.B. auf §§ 163f, 100h StPO i.V.m. § 98a StPO gestützt, also einer Kombination aus Ermittlungsvorschriften, die weder für sich noch in Kombination Rechtsgrundlagen für den Einsatz biometrischer Fernidentifikationssysteme darstellen können, da sie vor dem Hintergrund des verfassungsrechtlichen Bestimmtheitsgrundsatzes weder den Einsatz dieser Systeme spezifisch adressieren noch die verfassungsrechtlichen Voraussetzungen an derart erhebliche Eingriffe in die informationelle Selbstbestimmung erfüllen. Auch § 98c StPO sowie § 48 BDSD erlauben nur geringfügige Eingriffe und können für die biometrische Fernidentifizierung deshalb nicht herangezogen werden.

[15] Z.B. *Monroy*, Polizei observiert mit Gesichtserkennung, netzpolitik.org v. 3 Mai 2024, abrufbar unter https://netzpolitik.org/2024/ueberwachungstechnik-polizei-observiert-mit-gesichtserkennung/; *Krempl*, Gesichtserkennung: Datenschutzaufsicht Niedersachsen prüft heimliche Observation, heise online v. 15 Juni 2024, abrufbar unter https://www.heise.de/news/Gesichtserkennung-Datenschutzaufsicht-Niedersachsen-prueft-heimliche-Observation-9764663.html?wt_mc=nl.red.ho.ho-nl-daily.2024-06-17.ansprache.ansprache.

[16] Z.B. Berlin: Drs. 19/18874, Drs. 19/18461; Sachsen: Drs. 7/16310, Drs. 7/16308.

KI-VO). Abgesehen davon bleibt auch das gezielte Auslesen von Gesichtsbildern weiterhin möglich und kann Grundlage für die Erstellung von Referenzdatenbanken sein.

Im Anwendungsbereich der **DSGVO** ist die Verarbeitung biometrischer Daten unter bestimmten Voraussetzungen möglich, sodass auch hier Rechtsunsicherheiten und etwaige Lücken durch ein eindeutiges Verbot, das Private als auch öffentliche Stellen betrifft, geschlossen werden sollten. Art. 9 Abs. 1 DSGVO untersagt zwar grundsätzlich die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person. Es bestehen aber nach Art. 9 Abs. 2 DSGVO Ausnahmen von diesem Verbot, die auch Spielräume für die Konkretisierung durch die Mitgliedstaaten eröffnen, die teilweise durch Fachgesetzte, aber auch durch § 22 BDSG ausgefüllt werden.[17]

Auch wenn zweifelhaft ist, ob es überhaupt Einzelfälle gibt, bei denen Private biometrische Fernidentifikation nach den Vorschriften der DSGVO einsetzen dürften, ist es angesichts der Ausnahmemöglichkeiten zu Art. 9 DSGVO erforderlich, etwaige Lücken zu schließen und auch den Einsatz durch nichtöffentliche Stellen zu verbieten.

Darüber hinaus hat sich die Bundesregierung im **Koalitionsvertrag** klar gegen den Einsatz von biometrischer Erfassung zu Überwachungszwecken ausgesprochen. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet sei zu gewährleisten.[18] Ein entsprechendes Verbot im BDSG zu verankern, würde dieses Versprechen bekräftigen.

2. Unionsrechtlicher Rahmen

Ein Verbot ist nach **Art. 9 Abs. 4 DSGVO** unbedenklich, der es den Mitgliedstaaten erlaubt, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Auch die **JI-Richtlinie** gibt hinsichtlich der Verarbeitung biometrischer Daten nach Art. 10 JI-RL nur Mindeststandards vor (vgl. Art. 1 Abs. 3 JI-RL) und stünde einem Verbot nicht entgegen.

Ebenso erlaubt die **KI-VO** nationale Verbotsregelungen einzuführen: Für die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen können die Mitgliedstaaten nach Art. 5

[17] Vgl. *Albers/Veit*, in: BeckOK DatenschutzR, 48. Ed. 1.5.2024, BDSG § 22 Rn. 15.
[18] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://cms.gruene.de/uploads/assets/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf, S. 86.

Abs. 5 Satz 5 KI-VO im Einklang mit dem Unionsrecht restriktivere Rechtsvorschriften für den Einsatz biometrischer Fernidentifizierungssysteme erlassen. Damit wäre auch ein vollständiges Verbot möglich. Gem. Art. 26 Abs. 10 UAbs. 7 KI-VO können die Mitgliedstaaten im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung erlassen, sodass auch für die retrograde Fernidentifikation eine nationale Verbotsvorschrift möglich ist. Da die KI-VO an vielen Stellen Bezug auf das unionsrechtliche Datenschutzrecht nimmt und dieses grundsätzlich unberührt lässt (Art. 2 Ab.s 7 KI-VO), bietet es sich an, diesen Ansatz auch in der nationalen Umsetzung aufzugreifen und die Verbote im BDSG zu verorten.

3. Gesetzgebungskompetenzen

Ein Verbot biometrischer Fernidentifizierung ist für die dem Bundesgesetzgeber innerhalb der ihm durch das Grundgesetz kompetenzrechtlich zugewiesenen Regelungsmaterien möglich.

Da sich das Datenschutzrecht als eine **Querschnittsmaterie** darstellt, ergibt sich die Gesetzgebungskompetenz des Bundes als Annex aus verschiedenen Sachkompetenzen der Art. 73 und 74 GG.[19] Die Kompetenz für den Bund zur Regelung des Datenschutzrechts ergibt sich also aus seiner jeweiligen Zuständigkeit für bestimmte Sachbereiche, in deren Rahmen Daten verarbeitet werden, also beispielsweise für das Strafrecht aus Art. 74 Abs. 1 Nr. 1, 72 GG oder den Zoll- und Grenzschutz aus Art. 73 Abs. 1 Nr. 5 GG. Die datenschutzrechtliche Regelungskompetenz des Bundesgesetzgebers für nichtöffentliche Stellen kann als Annexkompetenz auf Art. 74 Abs. 1 Nr. 1, 11 und 12 GG gestützt werden.[20] Für die Gefahrenabwehr der Länder ist der Bund hingegen nicht kompetent, sodass es den Landesgesetzgebern obliegt, entsprechende Verbotsnormen vorzusehen.

4. Anwendungsbereich und Wirkung des BDSG

Auch mit Blick auf den Anwendungsbereich und potenzielle Auswirkungen im Zusammenspiel mit anderen Gesetzen erscheint die Verankerung eines Verbots biometrischer Fernidentifikation im BDSG sinnvoll.

Für **nichtöffentliche Stellen** ergibt sich der Anwendungsbereich recht unproblematisch aus § 1 Abs. 1 Satz 2 BDSG. Gem. § 1 Abs. 1 Satz 1 Nr. 1 BDSG gelten die Regelungen des BDSG für **öffentliche**

[19] *Sydow*, in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl. 2022, Einleitung Rn. 92.
[20] Vgl. *Sydow*, in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl. 2022, Einleitung Rn. 93; *Gusy/Eichenhofer*, in: BeckOK DatenschutzR, 48. Ed. 1.11.2021, BDSG § 1 Rn. 76; BT-Drs. 18/11325, S. 71.

Stellen des Bundes. Für **öffentliche Stellen der Länder** gilt das BDSG nur **subsidiär** (§ 1 Abs. 1 Satz 1 Nr. 2 BDSG): Existiert landesspezifisches Datenschutzrecht, hat dieses Vorrang. Das BDSG gilt aber dann („soweit"), wenn die Vorschriften des Landesdatenschutzrechts einen Sachverhalt nicht oder nicht abschließend regeln und die weiteren Voraussetzungen des § 1 Abs. 1 S. 1 Nr. 2 vorlegen.[21]

Zwar ist das BDSG subsidiär zu spezielleren **Fachgesetzen** (§ 1 Abs. 2 Satz 1 BDSG). Wenn die Fachgesetze einen Sachverhalt, für den das BDSG gilt, aber nicht oder nicht abschließend regeln, finden hingegen die Vorschriften des BDSG Anwendung (vgl. § 1 Abs. 2 Satz 2 BDSG). Das BDSG gilt also subsidiär als Auffanggesetz mit dem Ziel, im bereichsspezifischen Recht Datenschutzlücken zu füllen und datenschutzrechtsfreie Räume zu vermeiden.[22]

Eine Verankerung im BDSG bietet sich deshalb an, weil es vorliegend um ein **klarstellendes, die Fachgesetze übergreifendes** und damit kein bereichsspezifisches Verbot geht. Denkbar sind davon unabhängig auch ergänzende bereichsspezifische Verbote in den Fachgesetzen. Die Subsidiaritätsklausel ist unbedenklich, solange in den Fachgesetzen keine Befugnisse oder Regelungen existieren, die die biometrische Fernidentifikation im Sinne einer Tatbestandskongruenz[23] adressieren.

Besonders hervorzuheben ist § 500 StPO, der für das Strafprozessrecht den **Anwendungsbereich für die Länder nochmals erweitert**, indem er anordnet, dass Teil 3 des BDSG entsprechend anzuwenden ist, soweit öffentliche Stellen der Länder im Anwendungsbereich der StPO personenbezogene Daten verarbeiten (Abs. 1) und soweit in der StPO nicht etwas anderes bestimmt ist. Daraus folgt, dass StPO und BDSG miteinander verschränkt sind und für die Polizei im repressiven Bereich das BDSG gilt.[24] Die §§ 45 ff. BDSG bilden den „allgemeinen Teil", welcher durch spezifische Rechtsvorschriften in der StPO für das Strafverfahren ergänzt wird.[25]

III. Reichweite des Verbots

Es sollte ein umfassendes Verbot im BDSG verankert werden, um Grund- und Menschenrechte effektiv zu schützen. Das Verbot soll sich folglich an öffentliche Stellen und Private richten (1), die retrograde als auch die Echtzeit-Fernidentifizierung erfassen (2) sowie die Erhebung und die

[21] *Klar*, in: Kühling/Buchner, 4. Aufl. 2024, BDSG § 1 Rn. 9.
[22] *Gusy/Eichenhofer*, in: BeckOK DatenschutzR, 48. Ed. 1.11.2021, BDSG § 1 Rn. 81.
[23] *Gola/Reif*, in: Gola/Heckmann, 3. Aufl. 2022, BDSG § 1 Rn. 10.
[24] *Singelnstein*, NStZ 2020, 639 (639).
[25] *Braun*, in: Gola/Heckmann, 3. Aufl. 2022, BDSG § 45 Rn. 4.

Weiterverarbeitung betreffen (3). Dies ließe sich konkret in bereits bestehende Normen des BDSG integrieren (4).

1. Öffentliche Stellen und Private als Adressat*innen

Ein Verbot sollte in jedem Fall für öffentliche Stellen im Sinne des § 2 BDSG gelten, und zwar sowohl im Anwendungsbereich der DSGVO als auch der JI-RL. Darüber hinaus sollte aber auch für Private der Einsatz biometrischer Fernidentifikationssysteme verboten werden. Somit sollte der Gesetzgeber ein Verbot sowohl in **Teil 2 als auch in Teil 3 des BDSG** verankern.

2. Retrograd und Echtzeit

Das Verbot sollte sowohl die biometrische Echtzeit-Fernidentifizierung als auch die retrograde biometrische Fernidentifizierung erfassen.

Zwar stellt EWG 32 der KI-VO darauf ab, dass mit der biometrischen Echtzeit-Fernidentifikation einige spezifische Risiken einhergehen, die sich aus der Unmittelbarkeit der Auswirkungen und den begrenzten Möglichkeiten weiterer Kontrollen oder Korrekturen ergeben. Dass bei einem Live-Abgleich der Aufenthaltsort einer Person bestimmt und auf die Person damit unmittelbar zugegriffen werden kann, mag ein spezifisches Echtzeit-Risiko zu sein. Allerdings birgt auch der **retrograde Abgleich spezifische Risiken**, sodass die retrograde Fernidentifikation nicht per se weniger eingriffsintensiv ist. Während Echtzeit Fernidentifikation punktuell eingriffsintensiv ist, ermöglichen es retrograde Abgleiche, über einen langen Zeitraum hinweg besonders verdichtete Bewegungs- und Persönlichkeitsprofile zu erstellen. Er schafft Anreize für lange Speicherfristen und Einschüchterungseffekte vertiefen sich, wenn Videomaterial auf unabsehbare Zeit in der Zukunft auswertbar ist. Hinzu kommt, dass auch ein retrograder Abgleich, anders als der Erwägungsgrund suggeriert, technisch zunächst keine Kontrollen und Korrekturen voraussetzt. Dabei handelt es sich vielmehr um Fragen der konkreten Ausgestaltung des Verfahrens in etwaigen gesetzlichen Ermächtigungsgrundlagen. Darüber hinaus betreffen die oben (B.I) dargestellten Risiken und Gefahren gerade jede Form der biometrischen Fernidentifikation und sind nicht prinzipiell reduziert, wenn der Abgleich später erfolgt. Denn das Risiko einer ausufernden Massenüberwachung, der Erstellung umfassender Bewegungs- und Persönlichkeitsprofile, einhergehende Einschüchterungseffekte, das Diskriminierungspotenzial und die Streubreite betreffen die Verwendung biometrischer Fernidentifikationssysteme insgesamt.

Maßgeblich für die Beurteilung des konkreten Eingriffsgewichts einer Maßnahme sind nach verfassungsgerichtlicher Rechtsprechung vielmehr andere Faktoren. Dazu gehören Art, Umfang

und denkbare Verwendung der Daten, die Gefahr ihres Missbrauchs, die Anzahl der betroffenen Grundrechtsträger*innen, die Intensität der Beeinträchtigungen und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben, ob eine Maßnahme heimlich stattfindet und wie die Rechtsschutzmöglichkeiten ausgestaltet sind.[26] Auch die Fehler- und Diskriminierungsanfälligkeit spielt dafür eine Rolle.[27]

3. Erhebung und Weiterverarbeitung

Neben einem Erhebungsverbot durch biometrische Fernidentifizierungssysteme sollten auch Weiterverarbeitungsverbote in das BDSG aufgenommen werden.

Da ein Erhebungsverbot im BDSG außerhalb des Anwendungsbereichs keine Wirkung entfaltet, ist es nicht ausgeschlossen, dass auf Landesebene zum Beispiel Rechtsgrundlagen in den jeweiligen Polizeigesetzen geschaffen werden. Diese könnten die dadurch erhobenen Daten an Bundesbehörden übermitteln bzw. selbst in Ermittlungsverfahren, also repressiv, nutzen wollen. § 161 Abs. 3 Satz 1 StPO schränkt lediglich die Verwertung derart erhobener Daten zu Beweiszwecken ein, steht aber einer Verwendung als Spurenansatz oder als Anlass eines Anfangsverdachts nicht entgegen.[28] Ein spezielles Weiterverarbeitungsverbot im BDSG für Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen aufgrund anderer Gesetze erhoben wurden, könnte eine Verwendung abseits der Verwertung zu Beweiszwecken verhindern, auch wenn sich die spezielle Vorschrift dann im „allgemeineren" Gesetz, nämlich im BDSG befinden würde.

4. Formulierungsvorschlag

Es wird vorgeschlagen, Erhebungs- und Weiterverarbeitungsverbote in die Normen des BDSG zu integrieren, die die Verarbeitung biometrischer Daten betreffen. Es sollte sichergestellt sein, dass die Begrifflichkeiten denen in der DSGVO, JI-RL und KI-VO entsprechen und einheitlich verwendet werden. Gegebenenfalls reicht auch ein Hinweis auf die Definitionen der verwendeten Begriffe in der Gesetzesbegründung aus. Jedenfalls sollte in der Gesetzesbegründung explizit darauf verwiesen werden, dass die Verbote zur Weiterverwendung auch im Rahmen in

[26] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 76 m.w.N.
[27] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 90.
[28] Vgl. *Kölbel/Ibold*, in: MüKoStPO, 2. Aufl. 2024, StPO § 161 Rn. 45; BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 29. Juni 2005, 2 BvR 866/05, Rn. 4.

repressiven Ermittlungsverfahren gelten und insofern neben § 161 Abs. 3 StPO treten, indem sie auch die Verwendung als Spurenansatz verbieten.

In **§ 22 BDSG** könnte folgender neuer Absatz 3 eingefügt werden:

„(3) Die Verarbeitung personenbezogener Daten durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) ist unzulässig."

In **§ 23 BDSG** könnte folgender neuer Satz 2 in Abs. 2 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."

In **§ 24 BDSG** könnte folgender neuer Satz 2 in Abs. 2 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."

In **§ 48 BDSG** könnte folgender neuer Absatz 3 eingefügt werden:

„(3) Die Verarbeitung personenbezogener Daten durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) ist unzulässig."

In **§ 49 BDSG** könnte folgender neuer Satz 3 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 G

Hochschule der Akademie der Polizei Hamburg, Carl-Cohn-Straße 39, 22297 Hamburg

An den
Ausschuss für Inneres und Heimat
im Deutschen Bundestag
Platz der Republik 1
11011 Berlin

Prof. Eike Richter
Professur für Öffentliches Recht, insbesondere Recht der Digitalisierung und IT-Sicherheitsrecht
Hochschule der Akademie der Polizei Hamburg
Carl-Cohn-Straße 39, 22297 Hamburg
Tel.: +49(0)40-4286-24400
eike.richter@poladium.de

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Drucksache 20/10859)

Sehr geehrter Herr stellvertretender Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

ich danke für die Gelegenheit zur Stellungnahme zum genannten Gesetzentwurf.

Ich konzentriere mich in meiner schriftlichen Stellungnahme auf zwei Themenbereiche des vorgelegten Gesetzentwurfs. Zunächst wird auf die Institutionalisierung der Datenschutzkonferenz eingegangen (dazu A). Im Anschluss nehme ich zur Erwägung Stellung, eine Regelung zur biometrischen Gesichtserkennung einzufügen (dazu B).

Um in der vorliegenden Stellungnahme Vorschriften des vorliegenden Gesetzentwurfs von geltenden Vorschriften unterscheiden zu können, sind erstere mit einem „-E“ in der Gesetzesbezeichnung ergänzt (z.B. § 16a BDSG-E). Seitenzahlen ohne Quellenangaben beziehen sich auf den Gesetzentwurf der Bundesregierung (Drucksache 20/10859).

Für einen schnellen Überblick verweise ich auf die nachstehende Übersicht sowie auf die grau hinterlegten Zusammenfassungen. Im Rahmen der Anhörung gehe ich gerne auf einzelne Punkte und weitere Themen des Gesetzentwurfs ein.

Die Ergebnisse zu den beiden genannten Themen lassen sich vorab wie folgt **zusammenfassen**:

> *1. Eine Ergänzung von § 16a BDSG-E um eine Befugnis der **Datenschutzkonferenz** zur verbindlichen Beschlussfassung über Auslegungsmaximen und andere Angelegenheiten des Datenschutzes sowie zur Öffentlichkeitsarbeit und zur Einrichtung einer gemeinsamen Geschäftsstelle wahrt bei entsprechender gesetzlicher Ausgestaltung die europa- und verfassungsrechtlichen Grenzen.*
>
> *2. Das Europa- und Verfassungsrecht steht einem bundesgesetzlichen **Verbot der biometrischen Gesichtserkennung** durch staatliche und private Akteure nicht grundsätzlich entgegen, gebietet ein solches Verbot aber auch nicht. Zur Wahrung der europa- und verfassungsrechtlichen Grenzen kommt insbesondere die Aufnahme einer allgemeinen Vorschrift in das BDSG in Betracht, nach der die biometrische Gesichtserkennung im öffentlichen Raum oder zur Überwachung und die Verarbeitung diesbezüglicher Daten verboten sind.*

Auf S. 27 und 53 finden sich zu beiden Themen Vorschläge für entsprechende Regelungen bzw. Ergänzungen im vorliegenden BDSG-E.

Überblick

A. Institutionalisierung der Datenschutzkonferenz

Im Koalitionsvertrag 2021-2025 (S. 17) haben sich die regierungstragenden Parteien zur Aufgabe gemacht:

> *„Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen."*

Der vorgelegte Gesetzentwurf sieht in § 16a BDSG-E folgende Regelung vor:

> *„§ 16a Datenschutzkonferenz*
>
> *Die Aufsichtsbehörden des Bundes und der Länder im Sinne des § 18 Absatz 1 Satz 1 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Die Datenschutzkonferenz gibt sich eine Geschäftsordnung."*

Der vorgelegte Regelungsentwurf beschränkt sich auf eine schlichte Benennung der Datenschutzkonferenz (DSK) und die Vorgabe, sich eine Geschäftsordnung zu geben. Er sieht von einer weitergehenden Institutionalisierung, insbesondere einer Befugnis der DSK zur verbindlichen Beschlussfassung über Auslegungsmaximen und anderen Angelegenheiten des Datenschutzes ab, um auch auf diese Weise die Durchsetzbarkeit und Kohärenz des Datenschutzrechts zu fördern. Entsprechendes gilt für die Verankerung einer Kompetenz zur gemeinsamen Öffentlichkeitsarbeit. Es stellt sich somit die Frage, welche rechtliche Möglichkeiten und Grenzen für den Bundesgesetzgeber für eine im Vergleich zu § 16a BDSG-E weitergehende Institutionalisierung der DSK – insbesondere im BDSG – bestehen.

Um diese Frage zu klären, sollen zunächst die Grenzen festgestellt werden, die der Bundesgesetzgeber zu beachten hat, wenn er eine weitergehende Kooperation, insbesondere eine Kompetenz zur Fassung verbindlicher Beschlüsse regeln will (dazu I). Soweit sich danach für den Bundesgesetzgeber ein rechtlich zulässiger, aber mit § 16a BDSG-E noch nicht ausgeschöpfter Gestaltungsspielraum ergibt, stellt sich in einem zweiten Schritt die Frage nach einer zweckmäßigen und im Vergleich zu § 16a BDSG-E erweiterten Ausgestaltung der Kooperation (dazu II). In einem letzten Schritt wird erörtert, wie die

in Betracht kommende Kooperationsausgestaltung rechtlich ausgestaltet werden kann, insbesondere durch eine entsprechende Regelung im BDSG (dazu III).

Die nachfolgenden Ausführungen beruhen im Wesentlichen auf einem entsprechenden Rechtsgutachten im Auftrag einer Arbeitsgemeinschaft der Datenschutzkonferenz, an dem der Unterzeichnete mitgewirkt hat und auf das im Übrigen verwiesen wird.[1]

I. Rechtliche Grenzen für den Bundesgesetzgeber zur Regelung einer Kooperation

Eine im Vergleich zum § 16a BDSG-E weitergehende Regelung zur Kooperation der DSK, die insbesondere gemeinsame und für die Mitglieder DSK verbindliche Entscheidungen über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten, eine gemeinsame Öffentlichkeitsarbeit und eine gemeinsame Geschäftsstelle vorsieht, wahrt die europarechtlichen (dazu 1) und die grundgesetzlichen Grenzen (dazu 2).

1. Wahrung der europarechtlichen Grenzen

Das europäische Primär- und Sekundärrecht zieht einer Stärkung der Kooperation der Datenschutzaufsichtsbehörden oder einer darüberhinausgehenden Institutionalisierung der DSK **keine grundsätzlichen**, sondern allenfalls **spezifische Grenzen**.

a. Grenzen der Unabhängigkeit der Datenaufsichtsbehörden

Dies gilt insbesondere für die nach Art. 51 Abs. 1, 52 DSGVO zu garantierende **(völlige) Unabhängigkeit** der Aufsichtsbehörden.[2] Die Mitgliedstaaten sind grundsätzlich frei in ihrer Wahl, ihre Aufsichtsbehörden zu organisieren. Möglich ist auch – wie in Deutschland – eine föderale Organisation, sofern gewährleistet ist, dass eine bestimmte Stelle alle

1 Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, vorgelegt von Eike Richter, Indra Spiecker gen. Döhmann unter Mitarbeit von Ref. iur. Mona Winau, Januar 2022, abrufbar unter www.bfdi.bund.de.

2 Zur Geltung nicht nur für den öffentlichen, sondern auch für den privaten Verarbeitungssektor vgl. EuGH, Urt. v. 9.3.2010, C-518/07, Kommission/Deutschland, ECLI:EU:C:2010:125, Rn. 30. Vgl. auch BVerfGE 65, 1 (46).

anderen Stellen im Europäischen Datenschutzausschuss (EDSA) vertritt und die Regeln des Kohärenzverfahrens aus Art. 63 DSGVO Beachtung finden (Art. 51 Abs. 3 DSGVO).[3] Dabei richtet sich die Unabhängigkeit der Aufsichtsbehörden nach dem Telos der Vorschriften auf die institutionelle Unabhängigkeit der Aufsichtsbehörden **von solchen Akteuren, die die Aufsichtsbehörden zu kontrollieren haben,** also etwa von der Regierung und der Verwaltung.[4] Eine solche Kontrollbeziehung besteht aber gerade nicht unter den Datenaufsichtsbehörden der Länder und des Bundes untereinander.

Soweit man daher die Unabhängigkeit überhaupt als Maßstab für das Verhältnis zwischen den Datenaufsichtsbehörden ansehen kann,[5] würde sie nicht eingeschränkt, wenn die hier in Rede stehende Erweiterung der Kooperationsregelung darauf beschränkt, die Kompetenz zu verbindlichen Beschlüssen nicht auf konkrete Kontrolleinzelfälle, sondern nur auf von solchen Einzelfällen **abstrahierte Angelegenheiten**, etwa die Auslegung von Rechtsvorschriften, zu beziehen. Die Unabhängigkeit jeder Aufsichtsbehörde, die Kontrollaufgabe in jedem ihr zugewiesenen Einzelfall durchzuführen, bliebe also von vornherein unberührt. Sie würde allenfalls auf einer abstrakten Ebene durch die Kooperation mitgeprägt, was sich jedoch nicht oder allenfalls, als eine geringe, dann aber zu rechtfertigende Einschränkung der Unabhängigkeit verstehen lässt.[6] Dies wird vor allem dann deutlich, wenn für die **Verbindlichkeit** der Beschlüsse Einstimmigkeit vorausgesetzt würde. Denn dann ist die Bindung an einen Beschluss der DSK Ausdruck einer Entscheidung, die jede Datenaufsichtsbehörde für sich und aus sich heraus treffen kann, und damit Ausdruck der eigenen Unabhängigkeit. Doch selbst wenn man ein geringeres Beschlussquorum, etwa die absolute Mehrheit ausreichen ließe, ginge damit allenfalls eine geringe Einschränkung der Unabhängigkeit einher, nämlich soweit eine Datenaufsichtsbehörde an einen Beschluss gebunden wird, obwohl sie sich nicht der Mehrheitsauffassung anschließen konnte. Denn auch dann ist der Beschluss in einem unabhängigen

3 Martini/Botta, DÖV 2022, 605, 607.

4 Vgl. EuGH, Urt. v.09.03.2010 - Rs. C-518/07 (Kommission/Deutschland), ECLI:EU:C:2010:125; EuGH, Urt. v. 16.10.2012 - C-614/10 (Kommission/Österreich), ECLI:EU:C:2012:631; EuGH, Urt. v. 8.4.2014 - C-288/12 (Kommission/Ungarn), ECLI:EU:C:2014:237.

5 Ablehnend etwa Diermann, Datenschutzaufsicht über die Tätigkeit der Finanzverwaltung, 2022, S. 90 und Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 999.

6 Generell zur Einschränkbarkeit der Unabhängigkeit etwa Grittmann, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 52 DSGVO Rn. 12; Kienle/Wenzel, ZD 2019, 107 (111); Martini/Botta, DÖV 2022, S. 605 (608).

Diskurs zustande gekommen, an dem jede Datenaufsichtsbehörde gleichberechtigt mitwirken konnte, und der – wie ausgeführt – ohnehin von vornherein gegenständlich keine konkreten Angelegenheiten einer einzelnen Datenaufsichtsbehörde betrifft. Demgegenüber steht der Mehrwert, im Interesse der Rechtssicherheit die Abgestimmtheit der Datenaufsichtsbehörden und die Vorhersehbarkeit ihrer Bewertungen und Vorgehensweisen zu stärken. Die Unabhängigkeit der einzelnen Datenaufsichtsbehörde, steht einer Pflicht, sich in der abstrakten Rechtsaufassung abstimmen zu müssen und dieser Auffassung zu folgen, nicht entgegen.[7] Freilich gilt dies nur – insoweit zieht die Unabhängigkeit eine spezifische Grenze –, wenn die so gewährleistete Unabhängigkeit der einzelnen Datenaufsichtsbehörde nicht sogleich wieder dadurch ausgehöhlt wird, dass die eingegangene und so intern strukturierte **Kooperation als solche** nicht in ihrer Unabhängigkeit geschützt ist.[8]

Dass so die europarechtlichen Grenzen und Vorstellungen zum Schutz aufsichtsbehördlicher Unabhängigkeit gewahrt werden, zeigt ein **Vergleich mit der Ausgestaltung des Europäischen Datenschutzausschusses** (EDSA) in Hinblick auf das Verhältnis der mitgliedstaatlichen Aufsichtsbehörden zueinander. In der letztlich auf Art. 65 DSGVO gründenden Verbindlichkeit der Entscheidungen des EDSA wird keine Verletzung der Unabhängigkeit der Aufsichtsbehörden gesehen, weil die EDSA selbst mit Unabhängigkeit ausgestattet sei und die Kohärenzentscheidung dazu führe, dass die Behörde zwar in ihrer Entscheidung eingeschränkt sei, gleichwohl aber immer noch in der Zuständigkeit unbeschränkt agiere.[9] Im Vergleich dazu dürfte die hier in Rede stehende Kooperation innerhalb der DSK sogar dahinter zurückbleiben. Denn sie würde sich auf die Vorgabe von Auslegungen und Interpretationen beschränken, aber die Ausgestaltung des Verfahrens, die eigentliche Einzelentscheidung und die Ausfüllung von Beurteilungs- und Ermessensspielräumen im Einzelfall unverändert den einzelnen Aufsichtsbehörden überlassen.

7 So auch Martini/Botta, DÖV 2022, S. 605 (608).

8 So auch Martini/Botta, DÖV 2022, S. 605 (608).

9 Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Art. 64 DSGVO Rn. 2.

b. Grenzen der Grundsätze der Effektivität und Effizienz

Auch die Grundsätze der Effektivität und Effizienz dürften einer weitergehenden Kooperation nicht entgegenstehen. Nach ihnen darf das Verfahren und Vorgehen bei der Ausübung von Befugnissen durch die Aufsichtsbehörden nicht in einer Weise ausgestaltet sein, die eine wirksame **Wahrnehmung der Befugnisse beeinträchtigt**, ineffizient oder gar unmöglich macht.[10] Dafür bestehen keine Anhaltspunkte. Durch ihre Mitwirkung in der DSK dürfte die Effektivität und Effizienz der Arbeit der einzelnen Aufsichtsbehörden schon gegenwärtig nicht beschränkt sein. Eine weitergehende Kooperation könnte das Potenzial haben, die Effektivität und Effizienz der Datenschutzaufsicht zu steigern, etwa indem datenschutzrechtliche Normen für alle Behörden konkretisiert und so der Zweck des einheitlichen Vollzugs im Bundesgebiet gefördert wird.

c. Grenzen des Äquivalenzgrundsatzes

Entsprechendes gilt für den Grundsatz der Äquivalenz. Danach dürfen nationale Verfahren für den **Vollzug von Unionsrecht nicht ungünstiger ausgestaltet** sein als das Verfahren bei entsprechenden Sachverhalten, die nur innerstaatliches Recht betreffen (Äquivalenz).[11] Der Grundsatz wäre betroffen, wenn eine Stärkung der Kooperation der Datenschutzaufsichtsbehörden die Gefahr bürge, dass die Datenschutzaufsichtsbehörden im Rahmen der Ausübung ihrer Befugnisse dem Unionsrecht eine geringere Bedeutung zuweisen würden als dem nationalen Recht. Dafür bestehen keine Anhaltspunkte. Im Gegenteil: Die Beschlussfassung der DSK bezieht sich schon heute auf das **gesamte Datenschutzrecht**, etwa allgemein auf die Abstimmung von Positionen zu datenschutzrechtlichen Auslegungsfragen,[12] und zwar auf das mitgliedstaatliche und unionale Recht gleichermaßen.

10 Vgl. Selmayr, in: Ehmann/ders. (Hrsg.), DSGVO (Kommentar), 3. Aufl. 2024, Art. 58 Rn. 5. Näher zu den Grundsätzen Kibler, Datenschutzaufsicht im europäischen Verbund, § 2 (S. 128 ff). Vgl. auch EG 129 S. 4 in Anschluss an Art. 58 Abs. 4 DSGVO.

11 Ludwigs, NVwZ 2018, S. 1417 (1418).

12 S. dazu die Geschäftsordnung der DSK (GO DSK), Stand 27.2.2024, abrufbar unter www.datenschutzkonferenz-online.de, dort Ziffer III GO DSK.

d. Grenzen der verwaltungsorganisatorischen Gliederung der mitgliedstaatlichen Datenaufsicht

Auch die europarechtlichen Vorgaben zur Verwaltungsorganisation (insbes. Art. 51-59 DSGVO) ziehen einer weitergehenden Kooperation keine grundsätzlichen Grenzen. Vielmehr sehen sie die Möglichkeit der Einrichtung mehrerer Datenschutzaufsichtsbehörden ausdrücklich vor (s. Art. 51 Abs. 3 DSGVO), zeigen sich dabei aber **kooperativen aufsichtsbehördlichen Vorgehensweisen gegenüber aufgeschlossen** (vgl. Art. 60, 63 ff. DSGVO) oder können sogar im Interesse datenschutzrechtlicher Effektivität, Effizienz und Kohärenz als Ermutigung zur verstärkten Kooperation verstanden werden.[13]

e. Zusammenfassung

Das Europarecht schließt eine Regelung zur Stärkung der Zusammenarbeit der Datenaufsichtsbehörden von Bund und Ländern nicht aus. Um das Ziel einer verbesserten Kohärenz des Datenschutzrechts zu erreichen, aber auch um die europarechtlich geforderte Effizienz und Effektivität des Datenschutzrechts zu fördern, kann eine solche Regelung auch über den vorgelegten § 16a BDSG-E hinausgehen und etwa gemeinsame, verbindliche Beschlüsse vorsehen. Zur Wahrung der europarechtlich zu garantierenden Unabhängigkeit darf sich die Beschlusskompetenz nicht auf Einzelfälle beziehen, sondern muss sich auf abstrakte Angelegenheiten des Datenschutzes, etwa die Auslegung von Datenschutzvorschriften beschränken. Dabei muss gewährleistet werden, dass die DSK als solche bei ihrer Kooperationstätigkeit unabhängig ist.

2. Wahrung der grundgesetzlichen Grenzen

Eine weitergehende Kooperationsregelung wahrt auch die grundgesetzlichen Grenzen. Insbesondere was die grundgesetzliche Vollzugskompetenzordnung und die ihr entnommenen sog. Verbote der Mischverwaltung (dazu a) und der Mischfinanzierung (dazu b) betrifft, greift eine erweiterte Kooperation der DSK zwar in die Vollzugskompetenzordnung und die Kompetenzordnung zur Staatsfinanzierung ein, ist aber insoweit verfassungsrechtlich gerechtfertigt bzw. rechtfertigbar.

13 Zur Kritik am Vollzugsdefizit der früher geltenden Datenschutzrichtlinie vgl. Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 186.

a. Keine Verletzung der Vollzugskompetenzordnung (sog. Verbot der Mischverwaltung)

aa. Begriff und Normativität

Vorliegend könnte vor allem das sog. Verbot der Mischverwaltung der beabsichtigen Stärkung der Kooperation eine Grenze ziehen. Dieses Verbot, das als solches dem Grundgesetz nicht explizit zu entnehmen ist, steht für den in den Art. 20 Abs. 1, 30, 70 ff., 83 ff., 92 ff. u. 109 ff. GG zum Ausdruck kommenden **Grundsatz eigenverantwortlicher Aufgabenwahrnehmung:** Bund und Länder haben die ihnen im Grundgesetz zugewiesenen Kompetenzen grundsätzlich selbständig und eigenverantwortlich wahrzunehmen. Insbesondere müssen die Gesetzesvollzugs- und Verwaltungszuständigkeiten von demjenigen Verband (Bund oder Land) wahrgenommen werden, dem diese Kompetenzen zugeordnet sind. Die Zuständigkeiten müssen also in diesem Sinne grundsätzlich getrennt sein. Sie konkretisieren die Staatsstrukturprinzipien des Bundesstaats-, Rechtsstaats- und Demokratieprinzips.[14] Für diese Wahrung der **Kompetenzordnung** hat sich die Bezeichnung des „Verbots der Mischverwaltung“ etabliert.[15]

Vorliegend kommt das Verbot der Mischverwaltung in den Blick, weil jeder Form der Kooperation zwischen den Datenaufsichtsbehörden inhärent ist (bzw. diese aus Gründen der Effizienz, der Gleichförmigkeit u.a. sogar darauf abzielt), dass die kooperierenden Aufsichtsbehörden jeweils an der Ausübung von Verwaltungskompetenzen mitwirken oder jedenfalls auf deren Ausübung einwirken, die nicht (nur) ihnen, sondern (auch) anderen Aufsichtsbehörden eines anderen Verbandes sachlich und örtlich zugewiesen sind. Dies führt dazu, dass der Vollzug des Datenschutzrechts insoweit nicht mehr nach Rechtsträgern getrennt, sondern „vermischt“ erfolgt.

Zugleich wird deutlich, dass es sich bei dem Verbot der Mischverwaltung zunächst nur um eine **deskriptive Sammelbezeichnung** für den grundsätzlich zwingenden Charakter der grundgesetzlichen Kompetenzzuweisungen für den Rechtsvollzug handelt, aus dem als solchem keine konturenscharfe Rechtsfolgerungen gezogen werden können,[16] schon

14 *Schulz*, DÖV 2017, S. 1028 (1029).
15 Vgl. *Gröpl*, in: Dürig/Herzog/Scholz (Hrsg.), GG (Kommentar), 103. EL 2024, Art. 91c Rn. 5 m.w.N.
16 Vgl. *Gröpl*, in: Dürig/Herzog/Scholz (Hrsg.), GG (Kommentar), 103. EL 2024, Art. 91c Rn. 5 m.w.N.

gar nicht ein absolutes Verbot.[17] Vielmehr begründet er in seiner Pauschalität und Plakativität die Gefahr, den rechtlichen Maßstab insoweit zu verkürzen, als es auch ein Zusammenwirken von Bund und Ländern geben kann, welches in diese allein maßgeblichen Kompetenzzuweisungen nicht eingreift. Ferner verkürzt er, dass selbst bei Vorliegen einer grundgesetzlichen Kompetenzzuweisung auch verfassungsrechtlich Ausnahmen möglich sind – unter den vom Bundesverfassungsgericht entwickelten strikten Beschränkungen. Die Bezeichnung „Verbot der Mischverwaltung“ steht somit nicht für mehr, als dass das Grundgesetz die Verwaltungstypen und -zuständigkeiten insbesondere in den **Art. 30, 83 ff. GG** grundsätzlich erschöpfend regelt und dass allein diese konkreten Regelungen den verfassungsrechtlichen Maßstab für die Verwaltungsorganisation und damit auch für den Grad der Kooperation bilden. Dies entspricht auch dem Ansatz des Bundesverfassungsgerichts in seinen für das sog. Verbot der Mischverwaltung maßgeblichen Entscheidungen.[18]

Nach Art. 30 GG erstreckt sich die Vollzugskompetenz der Länder auf die jeweils eigenen Landesgesetze. Darüber hinaus bestimmt Art. 83 Abs. 1 GG, dass die Länder grundsätzlich auch die Bundesgesetze als eigene Angelegenheit ausführen. Weil das Grundgesetz davon ausgeht, dass die Länder klar voneinander abgegrenzte und keine überlappenden Hoheitsgebiete haben und deswegen nicht in Kompetenzkonflikte kommen, liegt die Funktion der Art. 83 ff. GG vor allem darin, Bund und Länder voneinander organisatorisch zu scheiden und die Länder vor einem Eindringen des Bundes in ihren Verwaltungsbereich zu schützen.[19] In diesem Sinne geht es zur Auslotung der grundgesetzlichen Grenzen für die hier in Rede stehende Kooperation nicht um die Prüfung eines begrifflich unklaren und grundgesetzlich wenig angebundenen Verbots der Mischverwaltung, sondern

17 Vgl. BVerfGE 119, 331 (367).

18 Vgl. BVerfGE 63, 1 („Schornsteiger-Entscheidung“); 119, 331 („SGB II-Entscheidung“); 137, 108 (142 ff.); 139, 194 (226).

19 BVerfGE 137, 108, 147 Rn. 90 sowie 119, 331 (358, 364 und 366); 126, 77, 98. Vgl. auch *F. Kirchhof*, in: Dürig/Herzog/Scholz (Hrsg.), GG-Kommentar, 103. EL 2024, Art. 83, Rn. 111. Die weitgehende Zuweisung der Vollzugskompetenzen an die Länder ist auch vor dem Hintergrund der starken Kompetenzen des Bundes für die Gesetzgebung zu sehen.

darum, ob eine solche Kooperation konkrete Komptenzenzuweisungen des Grundgesetzes verletzen würde.[20] Was die Trennung der Verwaltungskompetenzen von Bund und Ländern betrifft, bringt das Bundesverfassungsgericht dies so zum Ausdruck, dass

> *„eine verwaltungsorganisatorische Erscheinungsform [...] nicht deshalb verfassungswidrig [ist], weil sie als Mischverwaltung einzuordnen ist, sondern nur, wenn ihr zwingende Kompetenz- oder Organisationsnormen oder sonstige Vorschriften des Verfassungsrechts entgegenstehen.“*[21]

Dies wäre bei einer hier in Rede stehenden, weitergehenden Kooperation der Datenaufsichtsbehörden nicht der Fall, wie die nachfolgende Erörterung zeigt.

bb. Eingriff in den Gewährleistungsbereich der Vollzugskompetenzordnung: liegt eine „Mischverwaltung“ vor?

Wem, unter welchen Voraussetzungen und in welchen Hinsichten die Aufgabe des Vollzugs der Gesetze zugeordnet ist, bestimmen vor allem die **Art. 83 ff. GG**. Sie bilden ein differenziertes und feingliedriges Geflecht von Kompetenznormen unterschiedlicher Reichweiten, die zudem erst mit Blick auf die konkret zu vollziehende Sachmaterie – hier das Datenschutzrecht – **greifbare Kompetenzzuordnungen** erkennen lassen, nämlich welchem Verband – Bund oder Ländern – welche Vorschriften des Datenschutzrechts zum Vollzug zugeordnet sind und welche Tätigkeiten mit welchen Anforderungen von einer solchen Vollzugsaufgabe umfasst sind. Erst vor dem Hintergrund einer solchen (in diesem Fall: datenschutzrechts-)spezifischen Bestimmung der Vollzugskompetenzverteilung zwischen Bund und Ländern – und nicht etwa an einem pauschalen Begriff der „Mischverwaltung“ – lässt sich feststellen, ob und welche Formen der Kooperation zwischen Bund und Ländern in die grundgesetzliche Vollzugskompetenzordnung eingreifen.

(1) Bei der Bestimmung der spezifischen Vollzugskompetenzverteilung ist zu beachten, dass sich das zu vollziehende Datenschutzrecht auf **drei Normebenen** – Union, Bund, Land – verteilt. Zudem beantwortet das Grundgesetz nicht ausdrücklich, wer – Bund oder Länder – für den **Vollzug von Unionsrecht** zuständig ist, was sich wegen der zentralen

20 Vgl. Trute, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 83 Rn. 28; Hermes; in: Dreier (Hrsg.), GG (Kommentar), 3. Aufl. 2018, Art. 83 Rn. 47 ff; vgl. auch Broß/Mayer; in: von Münch/Kunig, Grundgesetz-Kommentar, 7. Aufl. 2021, Art. 83 Rn. 15 ff; BVerfGE 63, 1 (38); 108, 169 (182).

21 BVerfGE 63, 1 (38).

Bedeutung der DSGVO gerade für die Bestimmung der Kompetenzordnung im Datenschutzrecht besonders komplizierend auswirkt. Um die Lücke zu schließen, wird sich für die Zuordnung der Kompetenz zum Vollzug der DSGVO verbreitet an der grundgesetzlichen Verteilung der Gesetzgebungskompetenzen für das Datenschutzrecht orientiert. Eine Vorschrift der DSGVO wird demnach etwa dem Bund zum Vollzug zugeordnet, wenn sie – wäre sie eine deutsche Rechtsvorschrift – in die Gesetzgebungskompetenz des Bundes fallen *würde*. Allerdings führt dies im Bereich des Datenschutzrechts nur mit einer gewissen Einschränkung zu einer eindeutigen Zuordnung von Vollzugskompetenzen für das europäische Datenschutzrecht, denn das Grundgesetz sieht keine spezifische und ausdrückliche Gesetzgebungskompetenz für das Datenschutzrecht vor. Diese wird als Annex jener Gesetzgebungsmaterie im Sinne der Art. 73 f. GG entnommen, in deren Sachzusammenhang die Datenverarbeitung jeweils stattfindet.

(2) Auf dieser – komplexen – Grundlage lässt sich die Vollzugskompetenzverteilung im Bereich des Datenschutzrechts wie folgt skizzieren:

- Für die verwaltungsmäßige Ausführung der **Landesdatenschutzgesetze** und der landesspezialgesetzlichen Regelungen sind ausschließlich die Länder zuständig (Art. 30 GG).
- Das Gleiche gilt für den Vollzug **unionsrechtlicher Datenschutzregelungen**, die – wären sie mitgliedstaatliche Regelungen – in die Gesetzgebungskompetenz der Länder fielen.
- Der Vollzug **bundesrechtlicher sowie unionsrechtlicher Datenschutzregelungen**, die – wären sie mitgliedstaatliche Regelungen – in die Gesetzgebungskompetenz des Bundes fielen, fällt
    - **grundsätzlich** in die Vollzugskompetenz der **Länder**, d.h. von ihnen einzurichtende Behörden haben diese Regelungen auf Grundlage landesrechtlicher Verfahren auszuführen (Art. 83, 84 Abs. 1 S. 1 GG). Trifft der Bund aufgrund seiner Ausnahmekompetenzen aus Art. 84 Abs. 1 S. 2 oder S. 5 GG Regelungen zur Behördeneinrichtung und/oder zum Verwaltungsverfahren in den Ländern, haben die Länder die unionsrechtlichen Datenschutzregelungen nach diesen bundesrechtlichen Bestimmungen auszuführen, soweit sie

nicht aufgrund ihrer Abweichungskompetenz (Art. 84 Abs. 1 S. 2 Hs. 2 GG) anderes geregelt haben.

- **ausnahmsweise** in die Vollzugkompetenz des **Bundes**, wenn und soweit hierfür durch einfaches Bundesgesetz eine Bundesoberbehörde eingerichtet wurde (Art. 87 Abs. 3 S. 1 GG). Dies trifft etwa auf die Regelungen im BDSG zur Errichtung des BfDI und zu dessen Aufsicht über die öffentlichen Stellen des Bundes und über bestimmte Telekommunikationsdienstleistungsunternehmen zu.

In Hinblick auf die **Reichweite** der so zugeordneten Vollzugskompetenzen ist zu beachten: Auch wenn die Vollzugskompetenzvorschriften des GG nicht durchgängig von „Vollzug“ sprechen, sondern auch andere Begriffe zur Rechtsfolgenkonkretisierung verwenden (Einrichtung bzw. Errichtung der Behörden etc.), umfassen die so zugeordneten Vollzugskompetenzen regelmäßig die Festlegung aller Elemente und Aspekte, die zur **verwaltungsmäßigen Ausführung** der jeweiligen Gesetze notwendig sind, also insbesondere

- die **Verwaltungsorganisation**: die Ein- und Errichtung der Behörden, deren Ausgestaltung, innere Organisation und Ausstattung mit Personal und Sachmitteln, die Festlegung ihres Aufgabenkreises einschließlich der Übertragung von Aufgaben und Befugnissen sowie
- das **(innere und äußere) Verwaltungsverfahren**: die Art und Weise sowie die Form des Verwaltungshandelns, die behördliche Willensbildung und Entscheidung, deren Zustandekommen und Durchsetzung sowie verwaltungsinterne Mitwirkungs- und Kontrollvorgänge.

Soweit danach einem Verband (Bund oder Land) die Aufgabe des Vollzugs von gesetzlichen Datenschutzregelungen zugewiesen ist, hat er sie **mit eigenem Personal, eigenen Sachmitteln und eigener Organisation** wahrzunehmen.

(3) Auf Grundlage dieser datenschutzrechtsspezifischen Bestimmung der Vollzugskompetenzverteilung zwischen Bund und Ländern sprechen die überwiegenden Gründe dafür, dass eine im Vergleich zum vorgelegten § 16a BDSG-E weitergehende Kooperationsregelung in die verfassungsrechtliche Kompetenzordnung im Sinne der Art. 83 ff. GG

eingreift und daher in diesem Sinne als **Mischverwaltung** anzusehen ist. Denn die angedachten Erweiterungen führen dazu, dass die Datenschutzaufsichtsbehörden von Bund und Ländern in den ihnen jeweils nicht zugeordneten Vollzugsbereichen des Datenschutzrechts in einer Art und Weise mitwirken, die nach der Rechtsprechung des BVerfG als **verwaltungsmäßige Ausführung** anzusehen ist oder die die **eigenverantwortliche Wahrnehmung** durch die jeweils zuständige Datenschutzaufsichtsbehörde tangiert:[22]

- **Verbindliche Beschlüsse gemeinsamer Auslegungsmaximen** und Stellungnahmen zu Angelegenheiten des Datenschutzes durch die DSK betreffen die verwaltungsmäßige Ausführung im Sinne des Art. 83 GG. Zwar sind sie nicht Teil eines konkreten Verwaltungsverfahrens, sondern werden gleichsam „vor die Klammer“ gezogen und dienen deren abstrakter Vorbereitung. Aufgrund der Verbindlichkeit führen sie allerdings zu einer Einschränkung des Auslegungs- und ggf. Anwendungsspielraums in konkreten Verfahren und wirken so abstrakt in die verwaltungsmäßige Ausführung der jeweils zuständigen Aufsichtsbehörde ein.
- Auch eine **gemeinsame Öffentlichkeitsarbeit** von Bund und Ländern durch die DSK im Sinne einer Information der Öffentlichkeit über deren Tätigkeiten und der Veröffentlichung der von ihr beschlossenen Auslegungsmaximen und Stellungnahmen stellt eine gemeinsame Gesetzesausführung dar, die gemäß den grundgesetzlichen Kompetenzzuweisungen von Bund und Ländern jeweils eigenverantwortlich wahrzunehmen ist (vgl. auch Art. 57 Abs. 1 lit. b DSGVO). Öffentlichkeitsarbeit wirkt nach außen und ist damit Teil der verwaltungsmäßigen Ausführung der Gesetze, auch wenn sie keine rechtliche Regelungswirkung gegenüber dem Bürger entfaltet.
- Schließlich greifen auch die **Einrichtung und der Betrieb einer Geschäftsstelle** zur administrativen und inhaltlichen Begleitung der DSK in den Gewährleistungsgehalt der Kompetenzordnung aus Art. 83 ff. GG ein. Denn die Geschäftsstelle dient gerade und insbesondere der kooperativen Wahrnehmung von Aufgaben wie

22 Zur „verwaltungsmäßigen Ausführung“ s. BVerfGE 63, 1 Rn. 143 ff.; 119, 331 Rn. 154. Kriterien für eine Beurteilung, ab welchem Grad einer Kompetenzvermischung der Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung nicht mehr gewahrt ist, lassen sich der Rechtsprechung hingegen nicht entnehmen.

der Bestimmung von Auslegungsmaximen und der Öffentlichkeitsarbeit, die ihrerseits – wie ausgeführt – die verwaltungsmäßige Ausführung betreffen.

cc. Rechtfertigung: handelt es sich um eine „verbotene“ Mischverwaltung?

Soweit man die genannten Weiterungen einer Kooperation als Eingriffe in die verfassungsrechtliche Kompetenzordnung für den Vollzug des Datenschutzrechts ansieht, folgt hieraus nicht automatisch die verfassungsrechtliche Unzulässigkeit. Wie bereits ausgeführt, ist das sog. Verbot der Mischverwaltung auch nach der Rechtsprechung des BVerfG nicht absolut zu verstehen, sondern zeigt sich **abwägungsoffen**. Es ist daher zu prüfen, inwieweit die jeweiligen Eingriffe in die Vollzugskompetenzordnung **ausnahmsweise gerechtfertigt** werden können.

Nach der Rechtsprechung des **BVerfG** ist eine Mischverwaltung nur dann mit den Vorgaben der Art. 83 ff. GG nicht vereinbar, wenn sie dem aus Rechtsstaats- und Demokratieprinzip folgenden Gebot der Rechts- und Verantwortungsklarheit nicht genügt oder die Grenzen der eigenverantwortlichen Aufgabenwahrnehmung durch eine nicht nur geringfügige Inanspruchnahme des nicht zuständigen Verwaltungsträgers überschreitet, die auch nicht aus einem besonderem Sachgrund gerechtfertigt werden kann und sich auf eine eng umgrenzte Verwaltungsmaterie beschränkt.[23] An diesem Maßstab lassen sich nicht nur die vorgelegte Regelung des § 16a BDSG-E, sondern auch die hier in Rede stehenden Erweiterungen der Kooperation rechtfertigen:

(1) So können die Kooperationserweiterungen, also das gemeinsame Fassen verbindlicher Beschlüsse, eine gemeinsame Öffentlichkeitsarbeit und die Einrichtung einer gemeinsamen Geschäftsstelle auf einen besonderen Sachgrund gestützt werden und betreffen auch nur eine eng umgrenzte Verwaltungsmaterie, so dass die **Grenzen eigenverantwortlicher Aufgabenwahrnehmung** gewahrt werden.

23 BVerfGE 119, 331 (367). Vgl. zur parallelen Anwendung der Kriterien der Verantwortungsklarheit und eigenverantwortlichen Aufgabenwahrnehmung auch Trute, v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 6. Aufl. 2010, Art. 83 Rn. 19; Berger, Die Ordnung der Aufgaben im Staat, 2016, S. 61; eine Abschwächung der kompetenziellen Grenzen nimmt Burgi für Verwaltungstätigkeiten an, bei denen mangels klassischer Vollzugswirkung Rechtsstaats- und Demokratieprinzip nicht beeinträchtigt werden, in: Butzer/Kaltenborn/Meyer (Hrsg.), FS Schnapp, 2008, 18 (22 ff).

So besteht mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein **besonderer Sachgrund**. Dies gilt insbesondere für die Datenverarbeitung privater Stellen, da für sie bundesweit grundsätzlich dieselben Vorschriften gelten, was im Interesse eines einheitlichen Vollzugs des Datenschutzrechts eine Abstimmung zwischen den Datenschutzbeauftragten erforderlich macht.[24] Dies wird durch die unionsrechtlich vorgesehene Teilnahme am europäischen Kohärenzverfahren und die damit einhergehende Notwendigkeit der Entwicklung gemeinsamer Positionen unterstrichen. Denn damit eine Abstimmung auch schon vor dem konkreten Einzelfall, der aus dem EDSA an die Aufsichtsbehörden herangetragen wird, grundsätzlich möglich wird, bedarf es weitergehender Kooperationsmechanismen. Dem würde insbesondere die Herstellung von Verbindlichkeit in der Auslegung von Rechtsfragen des Datenschutzes entsprechen. Dass für eine stärkere Kohärenz der Auslegung des Datenschutzrechts auch ein dringender praktischer Bedarf besteht, hat sich wiederholt gezeigt. Eine Harmonisierung oder Vereinheitlichung der datenschutzrechtlichen Auslegung erfolgt zwar auch auf unionsrechtlicher Ebene, insbesondere auch durch entsprechende Entscheidungen des EuGH. Eine gerichtliche Rechtsharmonisierung ist allerdings ein Effekt der nachträglichen Kontrollfunktion anhand von Einzelfällen. Er nimmt den Verwaltungen von Bund und Ländern nicht ihre orignäre Aufgabe der Ausführung der Gesetze und die damit verbundene Eigenständigkeit und Verantwortung. Die Ausführung der Gesetze umfasst aber vor allem und insbesondere deren Auslegung.

Die DSK wird zudem im Rahmen einer **eng umgrenzten Verwaltungsmaterie** tätig. Zwar hat das Datenschutzrecht einen Querschnittscharakter und betrifft dementsprechend viele Bereiche. Rechtsgegenständlich ist aber präzise umgrenzt, nämlich auf die Verarbeitung personenbezogener Daten bezogen. Zudem würden sich die Entscheidungen der DSK nicht auf Einzelfallentscheidungen erstrecken, sondern sich auf allgemeine Grundsätze und Auslegungen, die diesbezügliche Öffentlichkeitsarbeit und eine Geschäftsstelle beschränken. Entscheidungen und Maßnahmen im Einzelfall bleiben Sache der Aufsichtsbehörden, was die Verantwortlichkeiten zwischen der DSK und einzelner

24 Martini/Botta, DÖV 2022, S. 605 (610).

Aufsichtsbehörde klar abgrenzt. Insbesondere kämen der DSK keine Aufsichtsbefugnisse zu.[25]

(2) Eine Kooperationserweiterung wahrt auch das **Gebot der Rechts- und Verantwortungsklarheit**.[26] Die Datenschutzbeauftragten werden vom Parlament gewählt und erhalten so ein hohes Maß demokratischer Legitimation. Durch die Bindung an Beschlüsse über die Auslegung des Datenschutzrecht oder andere Entscheidungen, die sie nicht allein, sondern von der DSK getroffen werden, wird die demokratische Legitimationskette zum Wahlvolk ihres jeweiligen Bundeslandes geschwächt. Dies zumal dann, wenn sie an Mehrheitsentscheidungen gebunden werden, die sie selbst befürwortet.

Der insoweit gelockerte Zurechnungszusammenhang lässt sich aber durch die – rechtlich abzusichernde – **Unabhängigkeit** der DSK rechtfertigen.[27] Insbesondere wenn alle Datenschutzbeauftragten stimmberechtigt sind, garantiert ihre Unabhängigkeit einen von der Einflussnahme anderer Staatsorgane freien Entscheidungsprozess, als dessen Teil sie selbst Grundrechtsschutz gewährleisten (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), statt allein grundrechtsgebunden zu sein.[28] Insoweit kann die Mitwirkung an der kollektiven Willensbildung der DSK den Verlust an souveräner Entscheidungsmacht des einzelnen Datenschutzbeauftragten bis zu einem gewissen Grad kompensieren.[29] Um dem Grundsatz der Verantwortungsklarheit zu entsprechen, sollten die Entscheidungen der DSK gegenüber datenverarbeitenden Stellen und betroffenen Personen aber nicht unmittelbar gelten. Vielmehr sollten die Landesdatenschutzbeauftragten gemeinsame Entscheidungen jeweils als die ihrige umsetzen, auch mit Blick auf die örtliche Zuständigkeit (vgl. § 3 VwVfG).[30]

25 Martini/Botta, DÖV 2022, S. 605 (610).

26 Zu Folgenden auch Martini/Botta, DÖV 2022, S. 605 (610).

27 Vgl. hinsichtlich der Landesmedienanstalten BVerwG, Urt. v. 15.7.2020, 6 C 6.19, Rn. 38. Hierzu und zum Folgenden auch Martini/Botta, DÖV 2022, S. 605 (610 f.) m.w.N.

28 Anders stellte sich dies beim Glücksspielkollegium dar, das im grundrechtssensiblen Hoheitsbereich tätig war, vgl. Degenhart, Rechtsfragen des ländereinheitlichen Verfahrens nach dem Entwurf eines ersten Staatsvertrags zur Änderung des Staatsvertrags zum Glücksspielwesen, 2011, S. 26.

29 Vgl. BayVerfGH, Entsch. v. 25.9.2015, Vf. 9-VII/13, Vf. 4/VII/14, Vf. 10/VII/14, Rn. 157.

30 So auch Martini/Botta, DÖV 2022, S. 605 (610 f.).

dd. Zwischenergebnis

Am Maßstab der bundesverfassungsgerichtlichen Rechtsprechung sprechen die überwiegenden Gründe dafür, dass eine über § 16a BDSG-E hinausgehende Stärkung der Kooperation insbesondere in Form gemeinsamer und verbindlicher Entscheidungen über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten, gemeinsamer Öffentlichkeitsarbeit und einer gemeinsamen Geschäftsstelle in die verfassungsrechtliche Kompetenzordnung für den Vollzug des Datenschutzrechts eingreift. Allerdings lässt sich dieser Eingriff verfassungsrechtlich rechtfertigen und damit als verfassungsrechtlich zulässige „Mischverwaltung" qualifizieren. So besteht mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein besonderer Sachgrund. Die DSK wird zudem im Rahmen einer eng umgrenzten Verwaltungsmaterie tätig. Denn ihre Entscheidungen erstrecken sich nicht auf konkrete Einzelfälle, sondern beschränken sich auf allgemeine Grundsätze und Auslegungen in einem gegenständlich präzise umgrenzten Rechtsgebiet. Entscheidungen und Maßnahmen im Einzelfall bleiben Sache der Aufsichtsbehörden, was die Verantwortlichkeiten zwischen DSK und einzelner Aufsichtsbehörde klar abgrenzt. Dasselbe gilt für eine gemeinsame Öffentlichkeitsarbeit und eine die DSK unterstützende Geschäftsstelle, wenn und weil sie sich auf denselben Verwaltungsgegenstand beziehen.

b. Keine Verletzung der Kompetenzordnung zur Staatsfinanzierung (sog. Verbots der Mischfinanzierung)

Soweit die Aufsichtsbehörden in ihrer Zusammenarbeit über die DSK wie dargestellt gestärkt würden, erzeugt dies **Kosten**, die finanziert werden müssen. Insbesondere die Einrichtung und der Betrieb einer gemeinsamen Geschäftsstelle mit personalem Unterbau zur inhaltlichen und administrativen Begleitung der DSK ziehen Kosten nach sich. Damit stellt sich die Frage nach den verfassungsrechtlichen Grenzen und Vorgaben, wie die **Finanzierungslasten** verteilt sein dürfen, wenn Bund und Länder zusammenwirken. Diese Grenzen müssten gewahrt werden.

Die **bundesstaatliche Finanzverfassung** ist grundsätzlich zweigliedrig aufgebaut und unterscheidet die Ebene des Bundes und die der Länder (vgl. Art. 104a ff. GG). Aufgrund dieser grundgesetzlichen Vorstrukturierungen hängen die rechtlichen Grenzen für die Lasten- und Einnahmenverteilung innerhalb einer Kooperation in erster Linie von der Partnerkonstellation ab. Dabei normieren die Bestimmungen der Art. 104a ff. GG vor al-

lem Gebote und Zuweisungen, um die Staatsfinanzierung zu regeln. Sie bestimmen regelmäßig keine expliziten Verbote. Dementsprechend findet sich auch **kein ausdrückliches Verbot einer Mischfinanzierung**.[31] Im Sinne von nicht zu überschreitenden verfassungsrechtlichen Grenzen verboten sind dementsprechend solche Lastenverteilungen, die sich – im Umkehrschluss – nicht durch die Gebote und Zuweisungen der Art. 104a ff. GG rechtfertigen lassen.

Aus dem Gebot der getrennten Lasttragung folgt für Verwaltungsausgaben gem. Art. 104a Abs. 5 S. 1 Hs. 1 GG absolut (sog. **Trennungsgebot für Verwaltungsausgaben**) und für Zweckausgaben aus Art. 104a Abs. 1 GG grundsätzlich (sog. **allgemeines Trennungsgebot**), dass derjenige Verwaltungsträger, dem die Ausführung einer Aufgabe verfassungsrechtlich zugewiesen ist, auch die daraus resultierenden Kosten zu tragen hat. Dieser Lastenverteilungsgrundsatz verbietet, dass ein unzuständiger Verwaltungsträger solche Kosten trägt, die aus der Wahrnehmung einer Aufgabe resultieren, die eindeutig einem anderen Verwaltungsträger zugeordnet ist. Dieses Verbot setzt allerdings voraus, dass es sich überhaupt um nach unterscheidbaren Aufgaben trennbare Kosten handelt. Dementsprechend regelt Art. 104a GG solche Konstellation wie die vorliegende, in denen eine Aufgabe kooperativ wahrgenommen wird und die daraus resultierenden Kosten nicht zuordenbar sind, nicht unmittelbar. In diesen Fällen wird vertreten, die Rechtsfolge des Art. 104a dahingehend zu relativieren, dass eine **Aufteilung der Lastentragung entlang der grundsätzlich getrennten Vollzugskompetenzen zu treffen ist**.[32]

Bei der hier in Rede stehenden Erweiterung der DSK um eine Kompetenz zu gemeinsamen, verbindlichen Beschlüssen über die Rechtsauslegung, eine gemeinsame Öffentlichkeitsarbeit und eine gemeinsame Geschäftsstelle, sind die damit einhergehenden Verwaltungs- und Zweckausgaben für die Tätigkeiten in der DSK eine **Folge einer gemeinsamen Verwaltungstätigkeit** von Bund und Ländern. Sie lassen sich – wie oben ausgeführt – nicht mehr der Vollzugskompetenz des Bundes oder der Länder zuordnen.

31 Vgl. BVerfGE 81, 312 (314).

32 Sieckmann, in: Sachs (Hrsg.), GG (Kommentar), 9. Aufl. 2021, Art. 104a Rn. 18a; Dulde/Porsch, NVwZ 2011, 833 (834); Heun, in; Dreier (Hrsg.), GG (Kommentar), 3. Aufl. 2018, Art. 104a GG Rn. 21, 35; BVerwGE 81, 312 (314); a.A. Meyer, DVBl 2011, 449.

Die kooperative Erweiterung der DSK lässt sich somit nicht mehr ohne Weiteres auf das grundgesetzliche Gebot der getrennten Lastentrennung stützen und würde im Sinne einer „Mischfinanzierung“ die verfassungsrechtlichen Grenzen überschreiten, wenn für ihre Finanzierung keine angemessene Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wird. Dies ist insbesondere der Fall, wenn allein der Bund oder allein die Länder die DSK finanzieren sollten. Es ist daher eine **entsprechende gesetzliche Regelung zu treffen**, z.B. durch Übernahme des sog. **„Königsteiner Schlüssels“.** Die verfassungsrechtliche Kompetenzordnung zur Staatsfinanzierung ist dann gewahrt.

Die mit einer im Vergleich zu § 16a BDSG-E weitergehenden Kooperation einhergehenden Kosten wahren die finanzverfassungsrechtlichen Grenzen, wenn für deren Finanzierung eine angemessene, gesetzliche Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wird, z.B. durch Übernahme des sog. „Königsteiner Schlüssels“.

3. Zusammenfassung zu den rechtlichen Grenzen und Spielräumen für den Bundesgesetzgeber zur Regelung einer Kooperation

Soweit erwogen wird, die DSK über den vorgelegten § 16a BDSG-E hinaus in ihrer Kooperation zu stärken, indem sie insbesondere Kompetenzen bzw. Befugnisse erhält, über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten verbindlich zu entscheiden, Öffentlichkeitsarbeit und eine Geschäftsstelle zu betreiben, wahrt dies grundsätzlich die europa- und verfassungsrechtlichen Grenzen.

Insbesondere was die grundgesetzliche Vollzugskompetenzordnung und Finanzverfassung und die ihr entnommenen sog. Verbote der Mischverwaltung und -finanzierung betrifft, greift die genannte weitergehende Kooperationsstärkung zwar in den verfassungsrechtlichen Gewährleistungsgehalte ein, ist aber insoweit verfassungsrechtlich gerechtfertigt bzw. rechtfertigbar, wenn folgende Grenzen und Spielräume eingehalten und durch eine entsprechende gesetzliche Regelung gewährleistet werden:

1. Die Beschlusskompetenz darf sich nicht auf Einzelfälle beziehen, sondern muss sich auf abstrakte Angelegenheiten des Datenschutzes, etwa die Auslegung von Datenschutzvorschriften beschränken.

2. Es muss gewährleistet werden, dass die DSK als solche bei ihrer Kooperationstätigkeit unabhängig ist.

3. Es muss eine Kostenregelung zur angemessenen Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wurden, z.B. in Form des sog. „Königsteiner Schlüssels“.

II. Erwägungen zur zweckmäßigen Ausgestaltung einer erweiterten Kooperation

Die vorstehenden Ausführungen haben die Grenzen bestimmt, die bei einer kooperativen Erweiterung der DSK zu beachten sind. Damit werden zugleich die Spielräume deutlich, die der Einschätzungsprärogative des Gesetzgebers zur konkreten Ausgestaltung der Kooperation verbleiben. Sie betreffen die Verbindlichkeit der Beschlüsse sowie Quoren, unten denen sie zustande kommen (dazu 1), zudem die verfahrensbezogene Ausgestaltung der gemeinsamen Öffentlichkeitsarbeit (dazu 2) sowie die Verortung der gemeinsamen Geschäftsstelle (dazu 3). Bei seinen Zweckmäßigkeitserwägungen sollte sich der Gesetzgeber von der Erkenntnis leiten lassen, dass die bisherige Zusammenarbeit in der DSK trotz der Bemühungen aller Beteiligten immer wieder zu stark divergierenden und sich für Private, Unternehmen und staatliche Akteure misslich auswirkenden Auslegungen der datenschutzrechtlichen Bestimmungen geführt hat, was sich insbesondere für einen effektiven und gleichmäßigen Grundrechtsschutz als Kernaufgabe der Aufsichtsbehörden häufig nicht als förderlich erwiesen hat.[33]

1. Verbindlichkeit, Gegenstände und Quoren der Beschlüsse

Mit der Stärkung der DSK verbindet sich das Ziel, die einheitliche inhaltliche Positionierung zwischen den deutschen Aufsichtsbehörden voranzutreiben, damit insgesamt eine höhere Effizienz zu erreichen und vorhandene Ressourcen besser zu nutzen. Dabei richtet die DSK schon heute ihren Fokus vor allem auf allgemeine Fragestellungen im Zusammenhang mit dem Datenschutzrecht (Auslegungshilfen, Leitlinien oder Empfehlungen zu einzelnen Datenschutzvorschriften) und stimmt hierüber mit einfacher bzw. bei

33 So auch Martini/Botta, DÖV 2022, 605, 606 m.w.N., insbesondere mit Hinweis auf die Privatwirtschaft, für die fehlende Einigkeit und Rechtssicherheit bei der Auslegung ein Dorn im Auge sei.

sog. Entschließungen mit Zweidrittel-Mehrheit ab.[34] Die Entscheidungen entfalten allerdings keine Bindungswirkung, weder gegenüber anderen privaten und staatlichen Akteuren noch zwischen den Datenschutzaufsichtsbehörden.

Inwieweit die hier in Rede stehende und grundsätzlich zulässige (s. vorstehend I) Erweiterung der Beschlusskompetenz dazu beisteuert, die beabsichtigte Kohärenz des Datenschutzrechts zu stärken, hängt maßgeblich von der Ausgestaltung der Verbindlichkeit der Beschlüsse und von den Quoren ab, die sie voraussetzen. So hätte eine Verbindlichkeit im Außenverhältnis eine weitreichende Wirkung, würde aber weitergehende Rechtsfragen, insbesondere der Rechtssubjektivität aufwerfen.[35] Dem Kohärenzziel wäre im Vergleich dazu auch bereits mit einer **Verbindlichkeit im Innenverhältnis** gedient, die dadurch sichergestellt würde, dass eine Verbindlichkeit im Außenverhältnis explizit durch Gesetz auszuschließen wäre. Selbst ein formal nur innenverbindlicher Beschluss dürfte das Kohärenzziel auch insoweit „nach außen“ fördern, als bei (außenstehenden) Akteuren **die Erwartungshaltung** erzeugt wird kann, dass sich die jeweilige Aufsichtsbehörde auch in ihren Entscheidungen nach außen an die innenverbindlichen Beschlüsse der DSK hält. Vor allem für überregional tätige Unternehmen hätte eine solche Verbindlichkeit den Vorteil höherer Rechtssicherheit. Zugleich würde sie misslichen Praktiken, wie die unternehmerische Einflussnahme auf die behördliche Zuständigkeit durch Wahl und Wechsel der Hauptniederlassung (sog. „Behörden-Hopping“, vgl. auch § 40 Abs. 2 Satz 1 BDSG i.V.m. Art. 4 Nr. 16 DSGVO) entgegenwirken.

Auch über die Festlegung notwendiger **Beschlussquoren** können die Auswirkungen von Verbindlichkeit gestaltet werden. So dürfte das Erfordernis der Einstimmigkeit und die damit einhergehende hohe Anforderung an die Kompromissfindung häufig dazu führen, dass die Beschlüsse inhaltlich eine hohe Abstraktion und Relativierung erfahren, was – auch wenn sie verbindlich sind – auf diese Weise ihre inhaltliche Steuerungskraft regelmäßig absenkt. Dies spricht für eine Beschlussfassung mit der **Mehrheit der Mitglieder**.

34 Siehe Ziffer IV.3 GO DSK.

35 Als institutionelle Beispiele auf nationaler Ebene sind die gemeinsamen Organe der Landesmedienanstalten (§§ 104 ff. Medienstaatsvertrag) bzw. das ehemalige Glücksspielkollegium der Länder (§ 9a Glücksspielstaatsvertrag a.F.) und auf Unionsebene der Europäische Datenschutzausschuss (EDSA) zu nennen, dazu auch Martini/Botta, DÖV 2022, 605, 607.

Schließlich ist es zwar nicht rechtlich geboten, aber zur Begrenzung der Beschlusskompetenz der DSK zu erwägen, diese auf **konkret benannte Gegenstände** zu beschränken. Es könnte ein abschließender Katalog von Gegenständen formuliert werden, auf die sich bindende Beschlüsse beziehen dürfen, z.B. auf Zuständigkeitskonflikte zwischen den Behörden oder auf grundlegende Rechtsfragen, die mehrere Landesdatenschutzbeauftragte in ihrer Amtsausübung betreffen.[36]

2. Gemeinsame Öffentlichkeitsarbeit

Mit der gemeinsamen Öffentlichkeitsarbeit soll insbesondere erreicht werden, dass die Auslegungsmaximen und Stellungnahmen der DSK auch nach außen gegenüber Verantwortlichen, Auftragsverarbeitern und Betroffenen effektiv kommuniziert werden können, um auch in der Praxis eine einheitliche Anwendung des Datenschutzrechts zu fördern. Damit wird ein allgemeiner, der Öffentlichkeit zugänglicher Wissensfundus über die Auslegung relevanter datenschutzrechtlicher Normen geschaffen. Gerade der viel kritisierten Rechtsunsicherheit, die bei den Adressaten des Datenschutzrechts durch unterschiedliche Auslegungshinweise, Empfehlungen und Praktiken der Aufsichtsbehörden entsteht, kann dadurch entgegengewirkt werden. Dabei kann das **Verfahren der Öffentlichkeitsarbeit** innerhalb der DSK unterschiedlich ausgestaltet werden. So ist zu empfehlen, auch Öffentlichkeitsverlautbarungen grundsätzlich dem Beschlussverfahren zu unterwerfen, um Missverständnisse zu vermeiden und klare Verantwortlichkeit für die Öffentlichkeitsarbeit zu begründen.[37]

3. Einrichtung einer gemeinsamen Geschäftsstelle

Die Einrichtung einer gemeinsamen Geschäftsstelle soll dazu beitragen, Effektivität und Effizienz der Kooperation zu stärken, etwa indem Verfahrensabläufe zu strukturiert und die jeweiligen wechselnden Vorsitze unter Wahrung von Kontinuität und Professionalität

36 Siehe Martini/Botta, DÖV 2022, S. 605 (608 f.).

37 So schon jetzt, allerdings nur auf der Ebene des Geschäftsordnungsrechts vorsehend Ziffer III GO DSK.

begleitet werden. Daher ist eine **passende Verortung und Organisation** der Geschäftsstelle zu empfehlen, die die Kooperation fördern und die Wissensdistribution aus den und in die Aufsichtsbehörden gleichmäßig absichern.

4. Zusammenfassung

Die unter Ziffer I.3 dargestellten europa- und verfassungsrechtlichen Grenzen eröffnen einen Gestaltungsspielraum für die konkrete Ausgestaltung der Kooperation, der unter Zweckmäßigkeitserwägungen ausgefüllt werden kann. Dabei ist Folgendes zu empfehlen:

1. Die Außenwirkung von Beschlüssen der DSK sollte im Gesetz explizit ausgeschlossen werden.

2. Es sollte im Gesetz festgelegt werden, dass Beschlüsse mit der Mehrheit der Mitglieder der DSK zustandekommen.

3. Die gesetzliche Grundlage für eine verbindliche Beschlussfassung kann einen abschließenden Katalog von Tatbeständen formulieren, in denen ein bindender Beschluss ergehen kann (z.B. Zuständigkeitskonflikte, übergreifende Bedeutung einer Rechtsfrage).

4. Es sollte gesetzlich vorgegeben werden, dass Öffentlichkeitsverlautbarungen grundsätzlich dem Beschlussverfahren unterliegen.

5. Im Gesetz sollte ein Rahmen für eine passende Verortung und Organisation der Geschäftsstelle festgelegt werden.

III. Rechtliche Umsetzung durch bundesgesetzliche Regelung im BDSG

Unter Wahrung der dargelegten europa- und verfassungsrechtlichen Grenzen (dazu vorstehend I) sowie unter Einbeziehung der Ausgestaltungsempfehlungen (dazu vorstehend II) könnte die Kooperation über den vorgelegten § 16a BDSG hinaus beispielsweise wie folgt normiert werden:

„(1) Die Aufsichtsbehörden des Bundes und der Länder im Sinne des § 18 Absatz 1 Satz 1 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).

(2) Die Datenschutzkonferenz hat die Aufgabe

1. auf eine einheitliche Anwendung des Datenschutzrechts hinzuwirken,

2. zu Angelegenheiten des Datenschutzes Stellung zu nehmen und

3. die Öffentlichkeit hierüber zu informieren.

Aufgaben, Zuständigkeiten und Befugnisse der Aufsichtsbehörden nach Bundes- oder Landesrecht bleiben unberührt. Art. 52 Abs. 1 bis 3 der Richtlinie (EU) 2016/679 gelten für die Tätigkeit der Datenschutzkonferenz und für die Mitwirkung an ihr entsprechend.

(3) In Ihrem Aufgabenbereich entscheidet die Datenschutzkonferenz durch Beschluss der Mehrheit seiner Mitglieder. Beschlüsse binden die Mitglieder untereinander, entfalten im Übrigen keine Bindungswirkung, dienen nicht dem Schutz Dritter und begründen keine einklagbaren Rechte. Die Datenschutzkonferenz gibt sich eine Geschäftsordnung.

(4) Der Vorsitz der Datenschutzkonferenz informiert die Öffentlichkeit über die Tätigkeit und Beschlüsse der Datenschutzkonferenz nach Maßgabe ihrer Beschlüsse.

(5) Zur organisatorischen Unterstützung der Datenschutzkonferenz wird bei der oder dem Bundesbeauftragten eine Geschäftsstelle eingerichtet, die ebenso wie die Öffentlichkeitsarbeit hälftig vom Bund und von den Ländern nach dem Königsteiner Schlüssel zu finanzieren ist.“

Zu prüfen ist, ob diese Norm auch als **bundesgesetzliche Regelung im BDSG** erlassen werden darf.

1. Gesetz als notwendige und hinreichende Regelungsebene

Die dargelegte erweiterte Kooperation hätte ein verfassungsrechtliches Gewicht, das die **Wesentlichkeitsgrenze** überschreitet. Sie ist somit dem parlamentarischen **Gesetz** vorbehalten und kann damit nicht etwa als Verwaltungsvereinbarung normiert werden.[38] Dies gilt mit Blick auf die Relativierung des finanzverfassungsrechtlichen Trennungsgebots insbesondere auch für die Finanzierung der Kooperation, insbesondere einer einzurichtenden Geschäftsstelle. Allein durch untergesetzliche Abmachung der Beteiligten kann die verfassungsrechtliche Finanzordnung hingegen nicht modifiziert werden.[39]

Hingegen bedarf es **keiner** (zusätzlichen) Anpassung oder **Ergänzung der Verfassung**. Vielmehr beruht das Grundgesetz darauf, dass die verfassungsgemäß konstituierten und für bestimmte Bereiche vorgesehenen staatlichen Organe – wie die Verwaltung von Bund

38 Siehe dazu etwa Maurer/Waldhoff, Allgemeines Verwaltungsrecht, 21. Aufl. 2024, § 6 Rn. 3 ff.

39 Vgl. Siekmann, in: Sachs (Hrsg.), Grundgesetz (Kommentar), 9. Auflage 2021, vor § 104a, Rn. 27.

und Länder – in diesen Bereichen prinzipiell handeln dürfen, soweit sie die jeweils einschlägigen Grenzen des Verfassungsrechts beachten.[40] Das wäre vorliegend in dem Moment der Fall, in dem die Kooperation auf eine Rechtsgrundlage gestellt würde, die dem Wesentlichkeitsgrundsatz Rechnung trägt. Ein darüberhinausgehender, allgemeiner Vorbehalt der Verfassung für Staatstätigkeiten in dem Sinne, dass die staatlichen Organe ohne hinreichend explizite Ermächtigung im GG selbst nicht tätig werden dürfen, besteht nicht.[41] Eine verfassungsrechtliche Grundlage, die eine Kooperation zwischen den Aufsichtsbehörden in der beschriebenen Form einer DSK ausdrücklich zulässt, dürfte erst dann (und ggf. zusätzlich) notwendig werden, wenn man in der beabsichtigten Kooperation nicht nur einen Eingriff in die grundgesetzliche Kompetenzordnung sähe, sondern diesen Eingriff auch und entgegen der obigen Darlegungen nicht für verfassungsrechtlich gerechtfertigt und – auf Grundlage einer unveränderten Verfassung – auch nicht rechtfertigbar hielte.[42] Selbstverständlich würde eine entsprechende Verfassungsergänzung – etwa im Bereich der Art. 91a ff. GG – jedenfalls dazu beitragen, stets verbleibende Rechtsunsicherheiten zu minimieren.[43] Notwendig ist eine Verfassungsänderung nach der hier vorliegenden Bewertung jedoch nicht.

2. Gesetzgebungskompetenz des Bundes

Für die Umsetzung der Regelung als Vorschrift im BDSG müsste dem Bund die dafür notwendige Gesetzgebungskompetenz zustehen. Dabei ist insbesondere zwischen den Regelungen zu verbindlichen Beschlüssen über Auslegungsmaximen, zur Öffentlichkeitsarbeit und zur Einrichtung einer gemeinsamen Geschäftsstelle zu differenzieren.

40 Grzeszick, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 20 Rn. 58 m.w.N.

41 Grzeszick, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 20 Rn. 58.

42 Vgl. BVerfGE 98, 218 (246).

43 Dies gilt nicht nur in Hinblick auf die Vollzugskompetenzordnung nach Art. 30, 83 ff, sondern auch die Staatsfinanzierungsvorgaben der Art. 104a ff. GG. So wird auch Art. 91c Abs. 1 GG in Hinblick auf die Einrichtung des IT-Planungsrats nicht als zwingend notwendig erachtet, vgl. Siekmann, in: Sachs (Hrsg.), GG (Kommentar), 9. Aufl. 2021, Art. 91c GG Rn. 6 m.w.N. Anders wohl Kment, in: Jarass/Pieroth (Hrsg.), GG (Kommentar), 16. Aufl. 2020, Art. 91c GG Rn. 1. Dazu auch Gröpl, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 91 Rn. 18 ff. u. Rn. 27. Zu den Grenzen solcher verfassungsrechtlichen Kooperationsnormen Sommermann, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 20 Rn. 49.

a. Annexkompetenz zu Art. 23 Abs. 1 S. 2 GG

Gute Gründe sprechen dafür, speziell für die Zusammenarbeit der Aufsichtsbehörden in datenschutzrechtlichen Konkretisierungsfragen eine Gesetzgebungskompetenz wegen der unionsrechtlich vorgegebenen Notwendigkeit der Zusammenarbeit und Abstimmung zwischen den einzelnen Datenschutzaufsichtsbehörden für ein einheitliches Auftreten im unionsweiten Kohärenzverfahren als **Annexkompetenz** zu Art. 23 Abs. 1 S. 2 GG abzuleiten. Nach Art. 23 Abs. 1 S. 2 GG kann der Bund zur Verwirklichung eines vereinten Europas durch Gesetz mit Zustimmung des Bundesrats Hoheitsrechte übertragen.

Bereits die aktuelle Fassung des **§ 18 BDSG** wurde vom Bundesgesetzgeber auf eine solche Annexkompetenz und auf die Kompetenz für auswärtige Angelegenheiten gestützt.[44] Aus der Befugnis des Bundes, Hoheitsrechte auf die Union zu übertragen, folge dessen Befugnis, die Mitwirkung in einer unionsrechtlichen Institution (nämlich des EDSA) zu regeln, die auf der Übertragung von Hoheitsrechten beruhe. Der EDSA übe gerade keine mitgliedstaatliche, sondern eine unionale Verwaltungstätigkeit aus. Der mitgliedstaatliche Vertreter der Aufsichtsbehörden im EDSA habe eine doppelte Funktion als Repräsentant des Mitgliedstaats und als Teil einer unionsrechtlichen Institution. Betroffen sei mit der Vertretung daher die europäische Integration, die Sache des Bundes sei. Dies gelte auch dann, wenn innerstaatlich Länderkompetenzen betroffen seien. Den innerstaatlichen Kompetenzen der Länder sei durch das Zustimmungserfordernis des Bundesrats als institutionelles Element und das Mitwirkungsrecht der Länder an der Beschlussfassung über einen einheitlichen Standpunkt im europäischen Kohärenzverfahren als inhaltliches Element einer „kompetenzschonenden Kooperation“ Rechnung getragen.[45]

Auf die hier in Rede stehende Erweiterung der DSK lässt sich diese Begründung einer Annexkompetenz aus Art. 23 Abs. 1 S. 2 GG i.V.m. der Bundeskompetenz für auswärtige Angelegenheiten teilweise **übertragen**: Denn die DSK soll deshalb mit der Befugnis zur zur inhaltlichen Konkretisierung des Datenschutzrechts mit verbindlicher Wirkung für die Datenschutzaufsichtsbehörden ausgestattet werden, weil die Regulierung des Daten-

44 Zum Folgenden BT-Drs. 18/11325, S. 71.
45 BT-Drs. 18/11325 S. 71 f.

schutzrechts weitgehend auf die Union übertragen wurde, dessen **kohärente Anwendung zu gewährleisten** ist. In einem föderal strukturieren Staat betrifft dies unvermeidlich die *mitgliedstaatlichen* Verwaltungskompetenzen, also die Kompetenzverteilung zwischen Bund und Länder zur Ausführung des Datenschutzrechts in den Art. 30, 83 ff. GG.

Es ließe sich allerdings einwenden, dass es sich bei einer inhaltlichen Beschlussbefassung zur Vorbereitung der Ausführung des Unionsrechts, die letztverantwortlich von den mitgliedstaatlichen Aufsichtsbehörden selbst ausgeübt wird, weder um eine Mitwirkung in einer unionsrechtlichen Institution, die aufgrund vom Bund übertragener Hoheitsrechte geschaffen wurde, noch um eine Vertretung des Bundes in auswärtigen Angelegenheiten handelt. Vielmehr scheint die inhaltliche Konkretisierung unvermeidbare Voraussetzung für den Vollzug des Unionsrechts durch die Mitgliedstaaten zu sein, für dessen Organisation und Verfahren aber die nationale Rechtsordnung, also die grundgesetzliche Kompetenzordnung, gelten würde. Daraus ließe sich wiederum schließen, dass sich für die Erweiterung der DSK eine Annexkompetenz des Bundes nur insoweit aus Art. 23 Abs. 1 S. 2 GG ergibt, als durch die DSK die einheitliche Beschlussfassung für das Kohärenzverfahren und die Vertretung der Bundesrepublik im EDSA gewährleistet wird. Da dies aber gerade nicht vorgesehen ist, sondern die Regelung des § 18 BDSG beibehalten werden soll, bliebe für die hier in Rede stehenden Regelung einer erweiterten DSK keine Kompetenz mehr übrig, die sich aus Art. 23 Abs. 1 S. 2 GG ableiten ließe.

Eine solche Argumentation würde allerdings ausblenden, dass die Beschlüsse der DSK sich auf inhaltliche Fragen der Gesetzeskonkretisierung beziehen, die **sowohl bei der Abgabe eines gemeinsamen Standpunkts im unionsweiten Kohärenzverfahren als auch bei der Ausübung der nationalen Verwaltungskompetenzen relevant werden können**. Eine inhaltliche Differenzierung beider Zweckrichtungen ist zwar theoretisch denkbar, praktisch aber kaum möglich. Dies zeigt sich, wenn man annimmt, die DSK würde zukünftig auch die Positionierung im EDSA entgegen der jetzigen Regelung des § 18 BDSG leisten. Eine Differenzierung könnte dann lediglich nach der Bindungswirkung erfolgen. Gemeinsame Standpunkte im EU-Kohärenzverfahren wären in diesem Fall als bindend für die einzelnen Aufsichtsbehörden bei ihrem Auftreten gegenüber anderen mitgliedstaatlichen Behörden oder Unionseinrichtungen anzusehen, nicht jedoch für ihre Verwaltungstätigkeiten auf nationaler Ebene. Eine solche formale Trennung würde zu der

absurden Situation führen, dass eine solche DSK für ihren gemeinsamen Standpunkt im Kohärenzverfahren eine inhaltliche Konkretisierung der DSGVO-Normen beschließt, die einzelnen Aufsichtsbehörden aber außerhalb des Kohärenzverfahrens eine davon abweichende Auslegung derselben Normen vertreten und anwenden könnten, soweit keine verbindliche Beschlussfassung des EDSA in dieser Sache vorliegt. Dies liefe dem Ziel des VII. Kapitels der DSGVO eklatant zuwider, eine einheitliche Anwendung des Unionsrechts im gesamten Unionsgebiet herzustellen. Die **einheitliche Anwendung des Datenschutzrechts** innerhalb eines Mitgliedstaats muss dagegen als eine Voraussetzung für eine kohärente Anwendung innerhalb der Union angesehen werden. In diesem Sinne kann die kohärente Anwendung des Datenschutzrechts **verständigerweise nicht geregelt** werden, **ohne zugleich die föderale Kooperation der Datenaufsichtsbehörden** in dem dafür notwendigen Maß mit zu regeln.[46]

Der europäische Integrationsprozess im Bereich des Datenschutzrechts – konkretisiert durch die harmonisierten Bestimmungen der DSGVO[47] – setzt voraus, dass die Bestimmungen im Rahmen der nationalen Staatsstrukturen auch möglichst **einheitlich in den Mitgliedstaaten angewendet und vollzogen** werden.[48] Diese unionsweite Kohärenz setzt wiederum die interne Abstimmung und die einheitliche Rechtsanwendung innerhalb eines Mitgliedstaats voraus[49] und lässt sich auf nationaler Ebene am effektivsten durch verbindliche Entscheidungen wenigstens in allgemeinen Auslegungsfragen durch Kooperation mit einem Mindesteingriff in föderale Prinzipien verwirklichen.

Mit anderen Worten: Wenn dem Bund die Kompetenz zusteht, Hoheitsrechte im Bereich des Datenschutzrechts auf die Union zu übertragen und aus der Ausübung dieser unionalen Regelungskompetenz für die Mitgliedstaaten verbindliche (Ziel-)Vorgaben der Ko-

46 Vgl. zu den insoweit erhöhten, hier aber gut zu begründenden Voraussetzungen für eine Bundeskompetenz aus Art. 23 Abs. 1 S. 2 GG BVerfGE 106, 62 (115). Kritisch Martini/Botta, DÖV 2022, S. 605 (609, mit Fn. 52).

47 Vgl. EG 2 u. 3 DSGVO.

48 Vgl. zum Harmonisierungsbedarf als Anlass zur Reform des europäischen Datenschutzrechts, Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 186.

49 Vgl. EG 135 S.1 i.V.m. EG 119 DSGVO.

operation und Kohärenz (Art. 51 Abs. 3, 60 ff. DSGVO) zur Gewährleistung eines gleichwertigen Grundrechtsniveaus in den Mitgliedstaaten und des freien Verkehrs personenbezogener Daten in der Union folgen (EG 123 S. 1 DSGVO), folgt daraus auch die **Kompetenz**, die dazu **notwendigen innerstaatlichen Verfahren** der Kooperation und Abstimmung **zu regeln**. Dies entspricht auch dem vorrangigen Ziel der DSGVO, das unter Geltung der DSRL deutlich hervorgetretene Vollzugsdefizit zu beheben,[50] indem vor allem die **verfahrens- und vollzugsrechtlichen Bestimmungen** angepasst und erweitert werden, während die inhaltlichen Vorgaben nur geringe Änderungen erfahren haben.[51] Das gesamte VII. Kapitel der DSGVO mit den Regelungen zur Zusammenarbeit der mitgliedstaatlichen Aufsichtsbehörden bis hin zum Kohärenzverfahren, das Verbindlichkeit herstellt, trägt diesem Anliegen Rechnung.

Eine gesetzliche Aufgaben- und Befugniszuweisung an die DSK, verbindliche Beschlüsse über Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes zu fassen, kann also umfänglich auf eine Bundeskompetenz als Annex zu Art. 23 Abs. 1 S. 2 GG gestützt werden, und zwar auch, soweit sie sich nicht nur auf die **Auslegung der DSGVO**, sondern **auch** des **Datenschutzrechts des Bundes und der Länder** erstreckt. Denn Art. 23 Abs. 1 S. 2 GG erfasst die Hoheitsrechte der Bundesrepublik ungeachtet ihrer jeweiligen föderalen Verankerung und damit insbesondere auch – wie dies Art. 23 Abs. 6 GG erkennbar voraussetzt – die öffentliche Gewalt im Kompetenzbereich der Länder.[52] Diese kompetenzielle Reichweite ist mit Blick auf die zentrale Aufgabe, die eine in ihrer Kooperation erweiterte DSK erfüllen soll, nämlich einheitliche Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes herauszugeben, auch sachlich geboten. Bereits die Abgrenzung von rein unionsrechtlichem Datenschutzrecht und solchem des Bundes und der Länder wäre zwar formal anhand der jeweiligen Rechtakte vorstellbar, mit Bezug auf die Sachregelung aber im Einzelnen schwierig und typischerweise nicht trennscharf möglich.

50 Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 209.

51 Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 212 ff.

52 Jarass, in: ders./Pieroth (Hrsg.), GG (Kommentar), 18. Aufl. 2024, Art. 23 Rn. 22.

Die DSGVO setzt einen harmonisierten Rechtsrahmen für das Datenschutzrecht, der zahlreiche Öffnungsklauseln vorsieht und jedenfalls in diesen Bereichen erst durch ergänzende Vorschriften des nationalen Rechts vervollständigt wird. Ergibt sich die Rechtslage in einem konkreten Anwendungsbereich erst aus dem **Zusammenspiel von unionsrechtlichen und nationalen Rechtsvorschriften**, stellt sich regelmäßig die Frage, ob es sich um Datenschutzrecht der Union oder des Bundes bzw. der Länder handelt. So normiert beispielsweise § 4 BDSG für die Videoüberwachung im öffentlichen Raum eine besondere Rechtsgrundlage. Ob diese Regelung im Anwendungsbereich des Unionsrechts nur die Videoüberwachung durch öffentliche Stellen erfasst, muss anhand einer unionsrechtskonformen Auslegung danach beantwortet werden, inwieweit sie auf eine Öffnungsklausel der DSGVO gestützt werden kann.[53] Eine Aussage über den Anwendungsbereich der bundesgesetzlichen Regelung setzt folglich eine Auslegung der entsprechenden Öffnungsklauseln des Unionsrechts voraus. Die Frage, welche datenschutzrechtlichen Anforderungen an eine nach § 4 BDSG zulässige Videoüberwachung zu stellen wären, müsste ebenfalls anhand der Vorgaben der DSGVO einerseits und den einschlägigen ergänzenden Vorschriften des BDSG und des jeweiligen Landesrechts andererseits beantwortet werden. Das Beispiel veranschaulicht, dass bei einer anwendungsbezogenen Konkretisierung des Datenschutzrechts, wie sie von den Aufsichtsbehörden bereitgestellt und durch die Abstimmung in der DSK vorbereitet werden soll, regelmäßig Normen des Unionsrechts verzahnt mit solchen des Bundes- oder Landesrechts anwendbar sein werden. Die Zuordnung von Auslegungsfragen als solche des Unionsrechts oder des Bundes- oder Landesrechts ist in diesen Fällen nicht eindeutig durchführbar.

Folgerte man daraus eine Beschränkung von DSK-Beschlüssen unter dem BDSG auf Stellungnahmen zu Angelegenheiten des Datenschutzrechts, die sich allein auf die unionsrechtlichen Rahmenvorgaben und damit nur einen Teil der einschlägigen Rechtsvorgaben bezögen, stellten solche Beschlüsse kaum taugliche Konkretisierungen für die Praxis bereit. Sie verfehlten damit einen zentralen Zweck der Aufgaben der DSK und der Ziele der DSGVO, die Rechtssicherheit für Verantwortliche, Auftragsverarbeiter und letztlich auch Betroffene zu verbessern. Es ist daher geboten, die innerstaatliche Abstimmung

53 Vgl. hierzu Frenzel, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG (Kommentar), 3. Aufl. 2021, § 4 Rn. 5.

auch auf das Bundes- und Landesdatenschutzrecht zu erstrecken, um eine einheitliche Anwendung des Datenschutzrechts im Bundesgebiet zu fördern und damit dem allgegenwärtigen Vollzugsdefizit entgegenzuwirken. Den Kompetenzen der Länder würde ebenso wie bei der gegenwärtigen Regelung durch die Zustimmungspflicht des Bundesrats für ein entsprechendes Bundesgesetz institutionell und inhaltlich durch die gleichwertige Mitwirkung der Länder und des Bundes an den Beschlüssen der DSK Rechnung getragen.

b. Hilfsweise: Verwaltungskompetenzen aus Art. 83 ff. GG oder Gesetzgebungszuständigkeiten aus Art. 70 ff. GG

Hilfsweise lassen sich Regelungskompetenzen des Bundes entweder aus den Ingerenzrechten des Art. 84 Abs. 1 GG (dazu a) oder aus dem Sachzusammenhang zu den konkurrierenden Gesetzgebungszuständigkeiten des Art. 74 Abs. 1 GG (dazu b) ableiten – allerdings im Vergleich zur Kompetenz aus Art. 23 Abs. 1 S. 2 GG jeweils **nur mit Einschränkungen**.

aa. Ingerenzrechte des Bundes aus Art. 84 Abs. 1 S. 2 Hs. 2 u. S. 5 GG

Zur Normierung der gemeinsamen verbindlichen Beschlussfassung über Auslegungsmaximen und Stellungnahmen ergibt sich das Gesetzgebungsrecht aus Art. 84 Abs. 1 S. 2 Hs. 1 GG. Die Bundeskompetenz erstreckt sich allerdings nur auf die Ausführung von Bundesrecht durch die Länder. **Als Gegenstand der Beschlussfassung** könnte daher nur Unionsrecht und Bundesrecht, **nicht Landesrecht** festgelegt werden. Zu beachten sind außerdem das Abweichungsrecht der Länder aus Art. 84 Abs. 1 S. 2 Hs. 2 GG und die Rück-Abweichungskompetenz des Bundes aus Art. 84 Abs. 1 S. 5 GG. Ein Verfahren der Öffentlichkeitsarbeit innerhalb der DSK ebenfalls auf Art. 84 Abs. 1 S. 2 Hs. 1 GG unter Beachtung der Abweichungskompetenzen aus Art. 84 Abs. 1 S. 2 Hs. 2 u. S. 5 GG gestützt werden. Aufgrund der Bundeskompetenz aus Art. 84 Abs. 1 S. 2 Hs. 1 GG kann eine gemeinsame **Geschäftsstelle nur als Einrichtung der Landesverwaltung** geschaffen werden. Für die Einrichtung einer Geschäftsstelle in Anbindung an den BfDI besteht keine Kompetenz des Bundes aus Art. 84 Abs. 1 GG.

bb. Gesetzgebungszuständigkeiten des Bundes kraft Sachzusammenhang zu Art. 74 Abs. 1 GG

Soweit man Art. 23 Abs. 1 S. 2 GG nicht für eine tragfähige Kompetenzgrundlage des Bundes ansieht und auch die Ingerenzrechte des Bundes aus Art. 84 Abs. 1 GG nicht für maßgeblich hält,[54] lässt sich eine Regelungskompetenz – allerdings ebenfalls nur mit Einschränkungen – aus den Gesetzgebungszuständigkeiten des Bundes nach Art. 70 ff. GG ableiten, wenn man die gesetzliche, verwaltungsbezogene Ausgestaltung der DSK gleichsam als (materielles) Datenschutzrecht begreift.

Zwar weist das Grundgesetz dem Bund die Gesetzgebungsbefugnis für das Datenschutzrecht nicht ausdrücklich zu. Allerdings lassen sich viele dem Bund etwa in den Art. 73 f. GG zugewiesene Sachmaterien häufig nicht sinnvoll regeln, ohne zugleich das Datenschutzrecht mitzuregeln. Für den Bereich der **privaten Datenverarbeitung** wird die Kompetenz des Bundes auf den **Sachzusammenhang zum bürgerlichen Recht, Recht der Wirtschaft und der Arbeit** gestützt, die ihm gem. Art. 74 Abs. 1 Nr. 1, Nr. 11 und Nr. 12 GG in konkurrierenden Gesetzgebungszuständigkeit zugewiesen sind. Hierauf ließe auch die weiterentwickelte DSK stützen, soweit sie mit ihren erweiterten Befugnissen im Bereich der privaten Datenverarbeitung tätig wird.[55]

Hingegen lässt sich eine Tätigkeit der DSK im den öffentlichen Datenverarbeitungsbereich nicht mehr auf die Gesetzgebungszuständigkeiten der Art. 70 ff. GG stützen.[56] Eine gesetzliche Normierung im BDSG müsste daher den **öffentlichen Datenverarbeitungsbereich von Zuständigkeit der DSK ausnehmen**. Am Maßstab der Art. 70 ff. GG stellt sich die Regelung der Datenverarbeitung durch staatliche Stellen als originäre Kompetenz der Länder dar. Der Bund kann grundsätzlich nur für seine eigenen öffentlichen Stellen Vorgaben erlassen, für öffentliche Stellen der Länder hingegen lediglich insoweit, als sie Bundesgesetze ausführen. Die entsprechende Lücke wäre durch einen Staatsvertrag zu schließen.

---

54 So wohl Martini/Botta, DÖV 2022, S. 605 (608 f.). Zum grundlegenden, verfassungsrechtlich ungeklärten Verhältnis zwischen den Verwaltungskompetenzen der Art. 83 ff. GG und den Gesetzgebungskompetenzen der Art. 70 ff. GG s. Trute, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 83 Rn. 13.

55 Dazu Martini/Botta, DÖV 2022, S. 605 (608 f.) m.w.N. Siehe auch § 40 BDSG.

56 Zum Folgenden Martini/Botta, DÖV 2022, S. 605 (609) m.w.N.

3. Zusammenfassung

Die Erweiterung der DSK mit den Aufgaben und Befugnissen einer (intern) verbindlichen gemeinsamen Beschlussfassung über Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes, einer gemeinsamen Öffentlichkeitsarbeit und zur Einrichtung einer Geschäftsstelle ist verfassungsrechtlich so gewichtig, dass sie auf der ***Ebene des Gesetzes*** *normiert werden müsste.*

Für eine Regelung im BDSG könnte sich der Bund auf eine ***Annexkompetenz zu Art. 23 Abs. 1 S. 2 GG*** *mit Blick auf die Notwendigkeit eines innerstaatlichen Abstimmungsverfahrens der Datenschutzaufsichtsbehörden stützen, um die unionsrechtlich vorgegebenen Ziele der einheitlichen Anwendung des Datenschutzrechts und eines effektiven Vollzugs bestmöglich zu fördern.*

Hilfsweise *ergibt sich eine Regelungskompetenz des Bundes aus den Ingerenzrechten des* ***Art. 84 Abs. 1 GG*** *oder aus den Gesetzgebungszuständigkeiten des Bundes kraft Sachzusammenhangs zu Art. 74 Abs. 1 GG. Die Bundeskompetenz erstreckt sich dann allerdings nur auf die Ausführung von Bundesrecht durch die Länder, so dass als Gegenstand der Beschlussfassung nur Unionsrecht und Bundesrecht,* ***nicht Landesrecht*** *bzw. der öffentliche Datenverarbeitungssektor festgelegt werden dürfte. Zudem bestünde für* ***die Einrichtung einer Geschäftsstelle keine Kompetenz*** *des Bundes.*

B. Einführung einer Regelung zur biometrischen Gesichtserkennung

Im Koalitionsvertrag 2021-2025 (S. 18 u. 109) haben sich die regierungstragenden Parteien zur Aufgabe gemacht:

> *„Biometrische Erkennung im öffentlichen Raum […] sind europarechtlich auszuschließen. […]. […] und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität […] im öffentlichen Raum […] ist zu gewährleisten.“*

In der Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz – KI-VO) wurde die Verwendung biometrischer Identifizierungssysteme reguliert, ohne ihren Einsatz vollständig oder jedenfalls im öffentlichen Raum auszuschließen. Es stellt sich daher die Frage, ob und inwieweit ein Verbot biometrischer Gesichtserkennung durch staatliche und private Akteure im öffentlichen Raum bundesgesetzlich – etwa im BDSG

– unter Wahrung der verfassungsrechtlichen und europarechtlichen Grenzen normiert werden kann.

Dazu soll zunächst kursorisch auf den Stand der technischen Entwicklung biometrischer Gesichtserkennung sowie auf die Zwecke, Möglichkeiten und Risiken ihres Einsatzes durch private und staatliche Akteure eingegangen werden (dazu I). Im Anschluss sind anhand einer gedachten Verbotsnorm (dazu II) die europarechtlichen (dazu III) und die verfassungsrechtlichen Grenzen (dazu IV) für ein bundesgesetzliches Verbot der biometrischen Gesichtserkennung zu bestimmen, um abschließend aus verfassungsrechtlicher Perspektive auf Bedarf und Gebotenheit einer solchen Regelung (dazu V) einzugehen. Die Ergebnisse werden abschließend zusammengefasst und mit einem beispielhaften Regelungsvorschlag *für das BDSG* ergänzt (dazu VI).

I. Biometrische Gesichtserkennung – Stand der technischen Entwicklung und Zwecke, Möglichkeiten und Risiken ihres Einsatzes

Bei der biometrischen Gesichtserkennung handelt es sich um eine automatisierte Verarbeitung von digitalen Bildern, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung oder Kategorisierung durchzuführen.[57] Im hiesigen Kontext wird im Wesentlichen die biometrische Gesichtserkennung als die Form von Technologie betrachtet, die ein **menschliches Gesicht aus einem digitalen Bild erkennt** und extrahieren kann, um es dann vor allem mit Datenbanken oder –beständen zuvor identifizierter Gesichter **abzugleichen**.[58] Dies kann sowohl in Echtzeit als auch retrograd erfolgen. Der Echtzeit-Abgleich charakterisiert sich dadurch, dass die Erfassung biometrischer Daten ohne eine erhebliche Verzögerung erfolgt. Dies umfasst die sofortige Identifizierung sowie die Identifizierung mit zeitlich begrenzten kurzen Verzögerungen. Alle weiteren Einsatzformen biometrischer Gesichtserkennung werden der Ex-post-Fernidentifizierung zugewiesen. So werden also entweder unverzüglich oder im Nachhinein durch mathematische Berechnungen einer Erkennungssoftware Vergleiche von

57 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, 2012, S. 2, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf [11.06.2024].

58 Hahn, Die Regulierung biometrischer Fernidentifizierung in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission, ZfDR 2023, S. 142.

zuvor gespeicherten Gesichtsbildern mit videografierten Gesichtsbildern angestellt. Die die Gesichtsbilder verarbeitende Software unterscheidet dabei nach charakteristischen Eigenschaften der Gesichter, bildet diese in einem sog. Template ab und macht sie dadurch mathematisch vergleichbar. Hierbei werden die einen Menschen identifizierenden Merkmale des Gesichtsbereichs, wie seine Augenhöhlen, Wangenknochen, Ohren, Nase, Mund oder Kinn durch die Software lokalisiert und anschließend mittels algebraischer Verfahren in Merkmalsdaten codiert. Die dabei generierten Templates werden anschließend mittels mathematischer Algorithmen kombiniert. Abschließend wird durch die Software eine Berechnung zum Grad der Ähnlichkeit der untersuchten Gesichtsbilder angestellt. Abhängig von der konkreten Gestaltung der Erkennungssoftware, des verwendeten Verfahrens zur Mustererkennung und seiner Toleranzgrenzen wird ein Resultat ausgegeben, welches eine Einstufung vornimmt, inwiefern die überprüften Gesichtsbilder in ihren Identifikationsmerkmalen übereinstimmen oder nicht übereinstimmen.[59]

Bei der biometrischen Gesichtserkennung handelt es sich um eine **vergleichsweise junge Technologie**. Unter anderem wird der Einsatz von Gesichtserkennungssoftware in Deutschland seit 2002 durch das Bundesamt für Sicherheit in der Informationstechnik untersucht. So wurden beispielsweise Verfahren der Gesichtserkennung im praktischen Einsatz in Bezug auf den Einsatz von Personaldokumenten betrachtet.[60] Ferner werden weltweit Gesichtserkennungssysteme durch Akteure der Wirtschaft und staatlicher Institutionen erprobt und in Betrieb genommen. Auf staatlicher Seite ist etwa das Pilotprojekt „Sicherheitsbahnhof Berlin Südkreuz“ der Deutsche Bahn AG in Kooperation mit der Bundespolizei und dem Bundesministerium des Innern und für Heimat zu nennen, aber auch Projekte wie EasyPASS, das (teil-)automatisierte Grenzkontrollen an deutschen Flughäfen ermöglicht[61] oder das Gesichtserkennungssystem des Bundeskriminalamtes (GES),

59 Bundesamt für Sicherheit in der Informationstechnik, Biometrische Verfahren, Gesichtserkennung, abrufbar unter www.bsi.bund.de [11.06.2024].

60 Bundesamt für Sicherheit in der Informationstechnik, Projektreihe BioP, abrufbar unter www.bsi.bund.de [11.06.2024].

61 EasyPASS-Registered Traveller, www.easypass.de [11.06.2024].

welches seit 2008 im Einsatz ist.[62] Auch auf Seiten **privater Akteure** werden Einsatzmöglichkeiten biometrischer Gesichtserkennung erprobt oder betrieben. Amazon.com, Inc. bietet mit seinem Produkt „Amazon Rekognition“ eine Gesichtserkennungssoftware an, die für die Gesichtsanalyse oder die Suche nach Gesichtern zur Verifizierung und zur Identifizierung von Personen verwendet wird.[63] Ebenso forschte der Konzern Meta an dem open source Modell „DeepFace“, einer Erkennungssoftware, die Gesichter in Digitalen Bildern erkennen und feststellen soll, ob die verglichenen Gesichter identisch sind oder nicht. Dabei soll die Software eine Genauigkeit von 97,35 Prozent erreichen.[64] Nicht zuletzt nutzen bereits eine Vielzahl an Bürgerinnen und Bürger Deutschlands bewusst oder unbewusst biometrische Gesichtserkennungssoftware über ihre elektronischen Endgeräte wie den Privaten- oder Arbeitscomputer sowie das Smartphone. Hierbei werden die verschiedenen Erkennungssoftware-Produkte wie „FaceID“ der Apple Inc. oder „Windows Hello“ der Microsoft Corporation dafür verwendet, um mittels des Gesichts der nutzenden Person das Endgerät zu entsperren oder die Sicherheitstechnologie der Zwei-Faktorauthentifizierung bei digitalen Einkäufen oder dem Online-Banking zu nutzen.[65] Nicht zuletzt erreichte die biometrische Gesichtserkennung mediale Aufmerksamkeit, als private Personen mittels der frei verfügbaren Gesichtserkennungssoftware „PimEyes“ den Aufenthaltsort einer zur Fahndung ausgeschriebene RAF-Terroristin erfolgreich ermittelten und dadurch die Strafverfolgungsbehörden in die Lage versetzten, die gesuchte Person festzunehmen.[66]

Staatliche Akteure nutzen die biometrische Gesichtserkennung, um die **öffentliche Sicherheit** zu erhöhen, da die Technologie es ermöglicht, Personen in Echtzeit zu identifizieren oder zu überwachen. An öffentlichen Orten wie Bahnhöfen, Flughäfen oder Stadien könnte die Gesichtserkennung folglich dazu beitragen, potenzielle Gefahren frühzei-

62 Bundeskriminalamt, Gesichtserkennungssystem (GES), https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html, [11.06.2024].

63 Amazon.com, Inc., Amazon Rekognition, https://aws.amazon.com/de/rekognition/, [11.06.2024]

64 Facebook AI Research, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, 2014, abrufbar unter research.facebook.com [12.06.2024].

65 Apple Inc., About Face ID Advanced technology, support.apple.com/en-us/102381 [12.06.2024]

66 Verfassungsblog.de, PimEyes User auf den Spuren der RAF, verfassungsblog.de/pimeyes-user-auf-raf-spuren [12.06.2024].

tig zu erkennen und gegebenenfalls zu verhindern. Ebenso könnte Gesichtserkennungstechnologie z.B. die Verfahren an Grenzübergängen beschleunigen, indem Reisende automatisch identifiziert werden und manuelle Kontrollen verringert werden. Des Weiteren könnte die Gesichtserkennung die Strafverfolgung **unterstützen**, da Verdächtige schneller identifiziert oder aufgespürt werden würden. **Unternehmen** hingegen nutzen Gesichtserkennungssoftware zur **Sicherung ihrer Einrichtungen**, indem die Software bei der Zugangskontrolle zu sensiblen Bereichen verwendet wird. Vorstellbar ist ebenso, dass der Einsatz von Gesichtserkennungssoftware es Unternehmen ermöglicht **Geschäftsprozesse zu optimieren**, indem Kunden analysiert werden, um personalisierte Angebote zu erstellen und das Einkaufserlebnis zu verbessern. Ferner wird durch die Verwendung von Gesichtserkennung potentiell Kundenzufriedenheit generiert, da sichere, schnelle und unkomplizierte Lösungen zur Identifikation bei Transaktionen geschaffen werden können. Bei weiterer Forschung im Bereich biometrischer Gesichtserkennung sind so weitere Potentiale für zukünftige Anwendungen zu erwarten, wovon sowohl staatliche als auch private Akteure profitieren würden.

Der Verwendung biometrischer Gesichtserkennung werden aber auch **Gefahren und Risiken** für Bürgerinnen und Bürger zugeschrieben. Gesichter in Echtzeit oder ex-post zu erkennen und über Kameras zu verfolgen, könnte eine weitere **Ausleuchtung der Privatsphäre** bedeuten, da die so überwachten Personen ohne ihr Wissen oder Zustimmung überwacht und deren sensiblen personenbezogenen Daten in Form von Gesichtsmerkmalen gespeichert und verarbeitet werden.[67] Weiterhin wird darauf hingewiesen, dass Gesichtserkennungssysteme aufgrund einer unzureichenden Basis an Trainingsdaten zu **diskriminierenden Ergebnissen** führen könnten. Das National Institute of Standards and Technology (NIST) fand in seiner Studie „Face Recognition Vendor Test (FRVT)" heraus, dass die Fehlerquoten je nach ethnischer Herkunft und Geschlecht stark variieren. Eine Vielzahl an überprüften Systemen zeigten höhere **Fehlerquoten** bei der Identifikation von Personen mit dunkler Hautfarbe im Vergleich zu Personen mit helleren Hauttönen.[68]

67 IEEE Transactions on Information Forensics and Security, Privacy–Enhancing Face Biometrics: A Comprehensive Survey, 2021

68 NIST Interagency/Internal Report (NISTIR) – 8280, 2019, www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects [13.06.2024].

II. Fortgang der Prüfung anhand einer gedachten Verbotsnorm

Mit ihrem Koalitionsvertrag haben sich die regierungstragenden Parteien zur Aufgabe gemacht, die biometrische Gesichtserkennung im öffentlichen Raum sowie zu Überwachungszwecken auszuschließen. Hieran ansetzend könnte eine **denkbare Verbotsnorm** könnte lauten:

> *„Biometrische Gesichtserkennung im öffentlichen Raum sowie zur Überwachung ist verboten."*

Um die für den Bundesgesetzgeber bestehenden europa- und verfassungsrechtlichen Grenzen hervortreten zu lassen, wird im Folgenden geprüft, ob und unter welchen Voraussetzungen und Modifikationen eine solche gedachte, die Zielsetzung des Koalitionsvertrags ausschöpfende Verbotsnorm mit den europa- (dazu III) und verfassungsrechtlichen (dazu IV) Vorgaben vereinbar wäre.

Dabei ist auf folgende **begriffliche Differenzierung** hinzuweisen, die sich im Fortgang als strukturbildenden und auch rechtssystematisch als zentral erweist. So setzt die vorstehende Verbotsnorm an der biometrischen Gesichtserkennung im Sinne einer *Tätigkeit* an. Im Vergleich dazu knüpft die KI-VO im Sinne einer Technikregulierung vorrangig an Systemen, also an *Mitteln oder Instrumenten* an, erweitert ihren Bezugspunkt aber auch auf den Umgang bzw. die Tätigkeit mit diesen Mitteln (vgl. Art. 1 lit. a KI-VO: „Inverkehrbringen, Inbetriebnahme und Verwendung von Systemen"). Das Datenschutzrecht wiederum knüpft in erster Linie an Daten, in diesem Sinne also an die *Ergebnisse* oder den *Gegenstand* einer Tätigkeit an, bezieht dabei aber regulativ ebenfalls die Tätigkeit mit ein (vgl. Art. 1 Abs. 1 DSGVO: „Verarbeitung personenbezogener Daten").

III. Europarechtliche Grenzen zur Regulierung durch den Mitgliedstaat

Zu prüfen ist zunächst, ob eine bundesgesetzliche Verbotsregelung europarechtliche Grenzen verletzen würde. Solche Grenzen können sich zum einen in Hinblick auf die Regelungskompetenz der Mitgliedstaaten ergeben (dazu 1), zum anderen in Hinblick auf die Verletzung europarechtlicher Grundfreiheiten und Grundrechte (dazu 2).

1. Regulierungskompetenz der Mitgliedstaaten

Die Regelung einer Verbotsnorm durch den Bundesgesetzgeber scheitert nicht daran, dass den Mitgliedstaaten europarechtlich keine Kompetenz (mehr) zur Regelung der biometrischen Gesichtserkennung zustünde. Die Regelungskompetenz der Bundesrepublik Deutschland als Mitgliedstaat gründet sich im Ausgangspunkt auf deren **staatliche Souveränität**, wird allerdings in dem Maße eingeschränkt, in dem sie gem. Art. 23 Abs. 1 S. 2 u. 3 GG Hoheitsrechte auf die EU überträgt. In der Folge laufen die deutschen Regulierungskompetenzen leer, soweit die **EU von den ihr übertragenen Kompetenzen durch Regelungen Gebrauch gemacht hat**, die (wie etwa EU-Verordnungen nach Art. 288 Abs. 2 AEUV) in den Mitgliedstaaten unmittelbar gelten.[69] Jedenfalls gehen die europarechtlichen den mitgliedstaatlichen Regelungen in der Anwendung vor, soweit letztere über die Grenzen hinausgehen, die die europarechtlichen Regeln den Mitgliedstaaten ziehen.[70]

Soweit ersichtlich, hat die EU keine spezifischen Regelungen zur biometrischen Gesichts*erkennung*, mit der **DSGVO** und der Richtlinie (EU) 2016/680 – sog. **JI-RL** – sehr wohl aber Regelungen zur Verarbeitung *biometrischer Daten* erlassen. Zudem hat sie jüngst auf Grundlage von Art. 114 und Art. 16 Abs. 2 AEUV die **KI-VO** erlassen und dort konkrete Vorschriften zum Umgang mit Systemen Künstlicher Intelligenz (KI-Systeme) statuiert, die auch *KI-Systeme* zur Erstellung von Datenbanken zur Gesichtserkennung sowie *KI-Systeme* zur biometrischen Fernidentifizierung erfassen, soweit diese insbesondere in öffentlich zugänglichen Räumen und in Echtzeit für Zwecke der Strafverfolgung eingesetzt werden sollen (vgl. insbes. Art. 5 Abs. 1 lit. e u. h, Abs. 2 bis 7 KI-VO). Indem sie so von den ihr zustehenden Kompetenzen wirksam[71] Gebrauch gemacht hat, hat sie

69 Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 70 Rn. 10; Jarass/Pieroth, Art. 70 Rn. 11.

70 Zur Unterscheidung von Anwendungs- und Geltungsvorrang des EU-Recht s. Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 23 Rn. 47.

71 Es werden allerdings Bedenken angemeldet, dass die EU die ihr übertragenen Kompetenzen beim Erlass der KI-VO überschritten habe. Gemäß Artikel 114 AEUV steht der EU die Kompetenz zu, Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorzusehen. Zudem begründet Artikel 16 Abs. 2 AEUV die Kompetenz der EU, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten zu erlassen, die in den Anwendungsbereich des Unionsrechts fallen. Für die sich vorliegend stellende Frage der verbleibenden Regulierungskompetenz wirken sich die Bedenken allerdings nicht aus, solange sie nicht zur Rechtsunwirksamkeit der KI-VO führen.

notwendig in einem gewissen Maße auch die biometrische Gesichtserkennung geregelt und die Mitgliedstaaten in ihrer diesbezüglichen Regulierungskompetenz spiegelbildlich eingeschränkt. Die insoweit zentralen Grenzziehungen für die verbleibende mitgliedstaatliche Regulierungskompetenz folgen vor allem aus Art. 5 KI-VO (dazu a und b) und Art. 6 ff. KI-VO (dazu c) sowie aus den Vorschriften der DSGVO und der JI-RL (dazu d). Sie belassen den Mitgliedstaaten eine Kompetenz für die (weitere) regulative Ausgestaltung der biometrischen Gesichtserkennung, die – wie nachfolgend ausgeführt wird – auch die Möglichkeit eines weitgehenden Verbotes tragen würde.

a. Grenzen des Art. 5 Abs. 1 lit. d KI-VO

Art. 5 KI-VO nimmt den Mitgliedstaaten nicht die Kompetenz, den Einsatz biometrischer Gesichtserkennung unter Beachtung seiner Festlegungen weiter zu regulieren. Art. 5 KI-VO verbietet bestimmte Praktiken im Bereich der Künstlichen Intelligenz und ist als Verbotsnorm mit Ausnahmen ausgestaltet, die den Spielraum des nationalen Gesetzgebers zwar beschränkt, aber nicht ausschließt. Insbesondere ein an den nationalen Gesetzgeber gerichtetes Gebot für den Einsatz bestimmter KI-Systeme – oder umgekehrt ein Verbot, solche Systeme zu verbieten – kann Art. 5 KI-VO nicht entnommen werden.

Ähnlich wie die JI-RL verfolgt auch die KI-VO einen risikobasierten Ansatz. Auf der höchsten Risikostufe stehen hierbei die in **Art. 5 Abs. 1** lit. a bis d KI-VO beschriebenen **Praktiken**, die wegen der mit ihnen einhergehenden unvertretbaren Risikos **grundsätzlich verboten** sind. Zu diesen gehört gem. **lit. d** auch die Verwendung biometrischer Fernidentifizierungssysteme, sofern diese in Echtzeit in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken erfolgt. Allerdings sieht lit. d unter i bis iii Ausnahmen von diesem Verbot vor. Soweit das so konturierte Verbot reicht, ist die Regulierungskompetenz der BRD als Mitgliedstaat und damit auch des Bundes entsprechend ausgeschlossen.

aa. Biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen

Der Begriff der **Strafverfolgung** in Art. 5 Abs. 1 lit. d KI-VO ist weit zu verstehen und umfasst nicht nur die repressivpolizeiliche Tätigkeit, sondern **auch die Gefahrenabwehr** im Sinne des deutschen Polizeirechts. Dies zeigt nicht nur die Begriffsbestimmung in Art.

3 Abs. 46 KI-VO, sondern auch Art. 5 Abs. 1 lit. d. iii KI-VO, der als Zulässigkeitsvoraussetzung die Abwendung einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags und damit eine klassische präventivpolizeiliche Tätigkeit normiert. Dem entspricht die systematische Nähe der KI-VO zur JI-RL, der ebenfalls und unstrittig ein weiter Strafverfolgungsbegriff zu Grunde liegt.

Den Begriff der **Fernidentifizierung in Echtzeit** i.S.v. Art. 5 Abs. 1 lit. d KI-VO regelt Art. 3 Nr. 37 KI-VO. Ein biometrisches Echtzeit-Fernidentifizierungssystem ist hiernach ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, wobei dies zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung umfasst, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen.

Unter einem **öffentlich zugänglichen Raum** i.S.v. Art. 5 Abs. 1 lit. d KI-VO ist schließlich gemäß Art. 3 Nr. 39 KI-VO ein der Öffentlichkeit zugänglicher physischen Ort zu verstehen, unabhängig davon, ob für ihn bestimmte Zugangsbedingungen gelten.

bb. Ausnahmen vom grundsätzlichen Verbot

Die in Art. 5 Abs. 1 lit. d i bis iii KI-VO normierten Fälle sind als Ausnahmen vom grundsätzlichen Verbot des Art. 5 Abs. 1 lit. d KI-VO zu lesen und beziehen sich auf Fälle, in denen das **öffentliche Interesse an einer effizienten Strafverfolgung bzw. Gefahrenabwehr** das Interesse der von einer Maßnahme gem. Art 5 Abs. 1 lit. d KI-VO möglicherweise betroffenen Personen am Schutz ihrer Rechte **überwiegt**.

Aus diesen Ausnahmen vom grundsätzlichen Verbot des Art. 5 Abs. 1 lit. d KI-VO lässt sich jedoch **kein** an die Mitgliedstaaten gerichtetes **Gebot** ableiten, Systeme der biometrischen Gesichtserkennung in den von den Ausnahmen umfassten Fällen auch **einzusetzen**. Der mit Art. 5 Abs. 1 KI-VO in engem Zusammenhang zu lesende Abs. 4 zeigt verdeutlicht, dass die KI-VO den Mitgliedstaaten lediglich die Möglichkeit gewährt, eine vollständige oder teilweise Genehmigung der Verwendung biometrischer Echtzeit-Identifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Art. 5 Abs. 1 lit. d, Abs. 2 und Abs. 3 KI-VO aufgeführten Grenzen und unter den dort genannten Bedingungen vorzusehen.

d. Grenzen des Art. 5 Abs. 1 lit. e KI-VO

Entsprechend wird die Regulierungskompetenz der Mitgliedstaaten durch Art. 5 Abs. 1 lit e KI-VO eingeschränkt, aber nicht ausgeschlossen. Danach sind die Möglichkeiten **Privater** beim Einsatz von Systemen biometrischer Gesichtserkennung europarechtlich beschränkt worden. Unzulässig ist es, **ungezielt** Gesichtsbilder aus dem Internet oder aus Videoüberwachungsaufnahmen auszulesen (sog. Image-Scraping). Europarechtlich ungeregelt blieb dagegen beispielsweise die Fernidentifikation mittels anderer physischer, physiologischer und verhaltensbezogener menschlicher Merkmale erfolgen, wie etwa die Augenbewegungen (vgl. ErwGr. 15), ebenso das **gezielte** Auslesen von Gesichtsbildern.

c. Grenzen des Art. 6 ff. KI-VO

Auch Art. 6 ff. KI-VO verschließt den Mitgliedstaaten nicht die Kompetenz, den Einsatz biometrischer Gesichtserkennung in dem vorgegebenen Rahmen zu regulieren, insbesondere auch weitgehend zu verbieten. Die Vorschriften enthalten vor allem **Anforderungen für KI-Systeme**. Ein an den nationalen Gesetzgeber gerichtetes Gebot, derartige Systeme zuzulassen, ist auch hier nicht enthalten.

Art. 6 ff. KI-VO regeln die sog. **Hochrisiko-KI-Systeme**, die sich im Vergleich zu den verbotenen Praktiken des Art. 5 KI-VO als weniger eingriffsintensiv darstellen und sich somit auf der zweiten Stufe der Risikopyramide befinden. Für sie gelten vor allem die in **Art. 8 bis 51 KI-VO statuierten Anforderungen und Regularien**. Dementsprechend wird die Regelungskompetenz der Mitgliedstaaten begrenzt, soweit diese europarechtlichen Vorschriften reichen. Dies hängt maßgeblich davon ab, was unter einem Hochrisiko-KI-System zu verstehen ist und ob und inwieweit Systeme der biometrischen Gesichtserkennung darunter zu fassen sind.

Die KI-VO enthält allerdings **keine Definition** des Hochrisiko-Systems, sondern arbeitet mit Konkretisierungen in Form von Listen. Gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a KI-VO gelten auch Systeme als Hochrisiko-Systeme, die im Bereich der biometrischen Identifizierung und Kategorisierung natürlicher Personen verwendet werden. Hierunter sind Systeme zu verstehen, die bestimmungsgemäß für die **biometrische Echtzeit-Fernidentifizierung und nachträgliche biometrische Fernidentifizierung** natürlicher

Personen verwendet werden sollen. Daraus folgt, dass biometrische Fernidentifizierungssysteme, die die Verbotsnorm des Art. 5 Abs. 1 lit. d KI-VO nicht erfüllen, als Hochrisiko-KI-Systeme zu qualifizieren sind und etwa den Anforderungen der Art. 8 ff. KI-VO unterliegen (z.B. im Hinblick auf die Einrichtung eines Risikomanagementsystems, die Daten-Governance oder Dokumentations- und Transparenzpflichten).

d. Grenzen der DSGVO bzw. der JI-RL

Die mitgliedsstaatliche Kompetenz zur Regulierung biometrischer Gesichtserkennung wird darüber hinaus auch nicht durch andere europarechtliche Vorschriften eingeschränkt, insbesondere nicht durch Vorschriften der DSGVO und der JI-RL. So regeln insbesondere Art. 9 DSGVO und die entsprechende Parallelnorm des Art. 10 JI-RL grundsätzliche **Verbote zur Verarbeitung biometrischer Daten** sowie spezifische Verbotsausnahmen. Da bei Systemen der biometrischen Gesichtserkennung biometrische Daten verarbeitet werden, sind diese Vorschriften in ihrem jeweiligen Anwendungsbereich von sich aus zu berücksichtigen. Eine Einschränkung der Kompetenz der Mitgliedstaaten zur Regelung der biometrischen Gesichtserkennung folgt daraus nicht. Dies wird durch **Art. 9 Abs. 4 DSGVO** und **Art. 1 Abs. 3 JI-RL** bestätigt.

2. Verletzung von europäischen Grundfreiheiten und -rechten

Eine bundesgesetzliche Vorschrift zum Verbot biometrischer Gesichtserkennung verletzt keine europarechtlichen Grundfreiheiten oder Grundrechte der Grundrechte-Charta (GrCH). Solange das Verbot insbesondere inländische wie ausländische Produkte gleichermaßen betreffen würde, dürfte es insbesondere nicht die **Warenverkehrsfreiheit** (Art. 28 bis 37 AEUV) verletzen. Mitgliedstaatliche Einschränkungen oder Regelungen der Marktfreiheit sind zulässig, wenn sie – wie vorliegend das angedachte Verbot – alle Marktteilnehmer, die ihre Tätigkeit in Deutschland ausüben, gleichermaßen betreffen sowie wenn die Verkaufsmodalitäten die inländischen Produkte sowie Produkte aus anderen EU-Ländern (ehemals EG-Ländern) rechtlich wie tatsächlich in gleicher Weise betreffen.[72]

72 Siehe hierzu EuGH, Urt. v. 24. November 1993, Rs. C-267/91 u. C-268/91 – Keck und Mithouard.

IV. Verfassungsrechtliche Grenzen zur Regulierung durch Bundesgesetz

Zu prüfen ist, inwieweit eine bundesgesetzliche Verbotsregelung verfassungsrechtliche Grenzen verletzen würde. Zu wahren sind insbesondere die Grenzen der Gesetzgebungskompetenzen (dazu 1) und die Grundrechte (dazu 2). Zudem könnte eingebracht werden, dass ein weitgehendes Verbot im Widerspruch zur Aufgabe des Staates steht, die Sicherheit zu gewährleisten (dazu 3).

1. Grenzen der Gesetzgebungskompetenzen

Die Verankerung des angedachten Verbots des Einsatzes biometrischer Gesichtserkennung im BDSG als Bundesgesetz setzt voraus, dass innerhalb der bundesstaatlichen Ordnung dem Bundesgesetzgeber die dafür notwendige Gesetzgebungskompetenz zusteht. Dies richtet sich nicht nach den Art. 30, 70 ff. GG, die auch für die gesetzliche Ausfüllung von Regelungsspielräumen gelten, die dem Mitgliedstaat zur Ausfüllung in Folge der Übertragung von Hoheitsrechten auf die EU verbleiben (s. vorstehend III.1).[73] Danach steht dem Bund für das hier in Rede stehende Verbot der biometrischen Gesichtserkennung eine Gesetzgebungskompetenz nur zu, **soweit sich das Verbot auf die** in den Art. 73 Abs. 1 Nr. 1 bis 14 GG und Art. 74 Abs. 1 Nr. 1 bis 33 GG genannten **Materien stützen lässt**. Soweit das Verbot die Verarbeitung biometrischer Daten erfasst, kann sich der Bund auf seine Annexkompetenzen zu den verschiedenen Sachmaterien stützen, wie dies für den Datenschutz allgemein anerkannt ist, also für die Verarbeitung im privaten Bereich vor allem auf Art. 74 Abs. 1 Nr. 1, 11 und 12 GG und für die Verarbeitung in einem Teil des öffentlichen Bereichs etwa auf die Art. 73 Abs. 1 Nr. 5 GG und Art. 74 Abs. 1 Nr. 1, 72 GG. Im Übrigen fällt den Ländern die Gesetzgebung zu (Art. 70 GG). Dies gilt insbesondere für die allgemeine und polizeiliche Gefahrenabwehr. Entsprechendes dürfte gelten, soweit das hier in Rede stehende Verbot nicht nur die Verarbeitung biometrischer Daten, also die Tätigkeit der und die Ergebnisse von Gesichtserkennung, sondern auch die dabei eingesetzten Mittel, insbesondere KI-gestützte Informationstechnik, miterfasst.

73 Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 70 Rn. 10.

2. Grundrechtliche Grenzen

Ein Verbot würde keine Grundrechte verletzen. Auf Grund des technischen Potenzials der biometrischen Gesichtserkennung und der prinzipiell vielfältigen Einsatzmöglichkeiten in unterschiedlichen Lebensbereichen dürfe ein Verbot in einzelne Grundrechte, jedenfalls aber in die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG **eingreifen**. Von den besonderen Grundrechten gilt dies insbesondere für die Unternehmerfreiheit nach Art. 12 GG, weil ein weitgehendes Verbot biometrischer Gesichtserkennung das Wirtschaften mit entsprechenden Techniken und Dienstleistungen stark, wenn nicht weitgehend vollständig einschränken dürfte. Gemäß der vom BVerfG zu Art. 12 GG verwendeten sog. Drei-Stufen-Theorie dürfte ein generelles Verbot des Inverkehrbringens, der Inbetriebnahme bzw. der Verwendung von biometrischen KI-Systemen auf der dritten und höchsten Intensitätsstufe der Eingriffe (objektive Zulassungsschranke) einzuordnen sein. Auch soweit Unternehmen erwägen, beispielsweise die Kontrolle der Leistungserbringung ihrer Beschäftigten auch mittels biometrischer Gesichtserkennung zu organisieren, würde deren Verbot die unternehmerische Freiheit insoweit einschränken.

Soweit demnach einem Verbot biometrischer Gesichtserkennung ein grundrechtliches Eingriffsgewicht zufällt, ist es allerdings gleich durch **mehrere gewichtige Schutzgüter gerechtfertigt**, selbst wenn man speziell in Bezug auf Art. 12 GG entsprechend der sog. Drei-Stufen-Theorie vorliegend Beschränkungen ausschließlich zur Abwendung einer nachweislichen oder höchstwahrscheinlichen Gefahr für ein überragend wichtiges Gemeinschaftsgut verlangen würde.

aa. Mit der biometrischen Gesichtserkennung verbinden sich besondere Gefährdungen der grundrechtlich durch Art. 2 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG geschützten **informationellen Selbstbestimmung**. Der Grund hierfür liegt in der besonderen Bedeutung höchstpersönlicher Merkmale wie das Gesicht[74] und anderer biometrischer Daten für Individualität, Privatheit und Intimität und damit letztlich für den innersten Kern menschlicher Persönlichkeitsentfaltung (vgl. auch Art. 9 Abs. 1 DSGVO und Art. 10 JI-RL).[75] Soweit zu ihrer Erzeugung und Verarbeitung zudem wirkmächtige Technologien wie etwa

74 Vgl. BVerfG v. 18.12.2018 – 1 BvR 142/15, Rn. 53.
75 Vgl. BVerfG v. 16.2.2023 – 1 BvR 1547/19, 1BvR 2634/20, Rn. 87.

KI-basierte Software eingesetzt werden, verstärken sich die Grundrechtsgefährdungen und drohen sich zu Bewegungs- und Persönlichkeitsprofilen auszuweiten, die der Preisgabe und Verwendung der persönlichsten Daten die Selbstbestimmung nehmen und zu einer verdichteten Überwachung, jedenfalls aber doch zu einem stetigen Gefühl des **Überwachtwerdens** führen können. Hinzu kommt, dass mit der zwangsläufigen Ausweitung biometrischer Datenbestände die Gefahr des **Missbrauchs** durch privat und staatliche Akteure wachsen dürfte. Schließlich entfalten Instrumente der biometrischen Gesichtserkennung regelmäßig eine hohe **Streubreite**, betreffen also viele Menschen, und zwar auch dann, wenn sie hierfür keinen spezifischen Anlass bilden.[76]

bb. Über die Gefährdung der informationellen Selbstbestimmung hinaus können sich biometrische Identifizierungsinstrumente erheblich auf das Verhalten von Menschen auswirken und sie von der Wahrnehmung und Ausübung grundrechtlicher Freiheiten abhalten, etwa ihre Religion auszuüben (Art. 4 Abs. 2 GG), ihre Meinung zu äußern (Art. 5 Abs. 1 S. 1 GG), sich künstlerisch oder wissenschaftlich zu betätigen (Art. 5 Abs. 3 S. 1 GG), an Versammlungen teilzunehmen (Art. 8 Abs. 1 GG) oder an Vereinigungen mitzuwirken (Art. 9 Abs. 1 GG). Solche **einschüchterungsbedingten Grundrechtsgefährdungen** beeinträchtigen nicht nur die individuellen Entfaltungschancen des Einzelnen, sondern auch das **Gemeinwohl**, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.[77]

cc. Mit den Möglichkeiten biometrischer Gesichtserkennung verbinden sich zudem besondere Gefahren der **Diskriminierung**, also von Ungleichbehandlungen wegen des Geschlechtes, der Abstammung, der Rasse, der Sprache, der Heimat und Herkunft, des Glaubens, der religiösen oder politischen Anschauungen von Menschen, wie dies durch Art. 3 Abs. 3 GG gerade absolut auszuschließen ist. So wurde bereits darauf hingewiesen, dass Gesichtserkennungssysteme aufgrund einer unzureichenden Basis an Trainingsdaten zu diskriminierenden Ergebnissen führen könnten (s. vorstehend I.).

76 Vgl. hierzu BVerfG v. 18.12.2018 – 1 BvR 142/15, Rn. 51.
77 Vgl. bereits BVerfG v. 15.12.1983 – 1 BvR 209/83, Rn. 146.

dd. Die grundrechtliche Gefährdungslage vertieft sich weiter, wenn man einbezieht, dass die biometrische Gesichtserkennung auch entscheidungsassistierend fungieren kann, etwa indem sie Risikoprofile oder Prognosen erstellt, die auch - soweit sie diskriminierend sind – **Anlass und Grund für weitergehende Handlungen und Maßnahmen** sein können (s. hierzu auch § 54 BDSG).

3. Grenzen der staatlichen Aufgabe zur Gewährleistung der inneren Sicherheit

Soweit der Staat, insbesondere die Sicherheitsbehörden, die Möglichkeiten der biometrischen Gesichtserkennung einsetzen oder einzusetzen erwägen, könnte gegen ein weitgehendes Verbot biometrischer Gesichtserkennung vorgebracht werden, dass es im Widerspruch zur Aufgabe des Staates steht, die Sicherheit zu gewährleisten.

Die Gewährleistung der inneren Sicherheit, also vor allem von Gefahrenabwehr und Strafverfolgung wird verbreitet als notwendige **Staatsaufgabe** angesehen.[78] Auch wenn sie im Grundgesetz nicht explizit und speziell geregelt, kommt sie in verschiedenen staatsorganisationsrechtlichen Regelungen zum Ausdruck (etwa Art. 35 Abs. 2 S. 1, 73 Abs. 1 Nr. 10 lit. b, 87 Abs. 1 S. 2 u. 91 GG). Zur **verfassungsrechtlichen Begründung** tragen aber vor allem die Grundrechte bei, soweit ihnen – z.B. Art. 2 Abs. 2 S. 1 u. 2 GG – nicht nur ein subjektives Recht des Einzelnen auf Abwehr staatlicher Eingriffe, sondern auch eine (objektivrechtliche) Pflicht des Staates zum Schutz des Einzelnen vor Beeinträchtigung entnommen wird. Verletzt der Staat seine Schutzpflicht, so verletzt er grundsätzlich auch das betroffene subjektive Grundrecht.[79] Dem Staat obliegt es nicht nur, Eingriffe Dritter in grundrechtlich geschützte Positionen – etwa mithilfe des Strafrechts – gesetzlich zu verbieten, sondern auch, die gesetzlichen Eingriffsverbote – typischerweise mithilfe des Gefahrenabwehrrechts – effektiv durchzusetzen.

Bei der **Wahl der Mittel**, die dem Staat und insbesondere auch den Exekutivorganen wie der Polizei zur Gewährleistung der inneren Sicherheit zur Verfügung gestellt werden, fällt dem Gesetzgeber allerdings ein sehr **weitreichender Gestaltungsspielraum** zu, der nur in seinen äußersten Grenzen verfassungsrechtlich angeleitet ist. Diese Grenze findet sich

78 Vgl. etwa Schoch/Kießling, in: Schoch/Eifert, Besonderes Verwaltungsrecht, 2. Aufl. 2023, Kap. 1 Rn. 66 ff.

79 Vgl. etwa BVerfGE 77, 170 (214).

insbesondere dort, wo sich ganz bestimmte Mittel als erforderlich zum Schutz des Schutzguts erweisen oder wo die Verfassung bestimmte Mittel des Schutzes vorschreibt (etwa gerichtlicher Rechtsschutz gegen Eingriffe Dritter als Gebot des Rechtsstaatsprinzips). Der Gesetzgeber überschreitet seine Grenzen, wenn er völlig untätig bleibt, eindeutig zu wenig zum Schutz unternimmt oder Vorkehrungen zum Schutz der Grundrechte trifft, die gänzlich ungeeignet oder völlig unzulänglich sind.[80] Selbst wenn man die biometrische Gesichtserkennung – trotz der dargelegten, derzeitigen Fehleranfälligkeit (s. oben I) – grundsätzlich als geeignet ansieht, zur Erfüllung staatlicher Aufgaben, insbesondere zur Gewährleistung der inneren Sicherheit beizutragen, würde die verfassungsrechtlichen Grenzen in Anbetracht der zahlreichen alternativen Mittel nicht überschritten, wenn der Gesetzgeber ein weitgehendes Verbot biometrischer Gesichtserkennung normieren würde.

V. Bedarf und verfassungsrechtliche Gebotenheit eines gesetzlichen Verbots

In den aufgezeigten Grenzen obliegt es der **Einschätzung des Gesetzgebers**, ob eine Regelung eines gesetzlichen Verbots zweckmäßig ist. Dies ist eine Frage des rechtspolitischen Bedarfs, nicht der verfassungsrechtlichen Gebotenheit. Insbesondere aus den Grundrechten folgt keine zwingende Notwendigkeit, biometrische Gesichtserkennung einfachgesetzlich zu verbieten. Allerdings ist zu berücksichtigen, dass das BVerfG in einer Reihe von Entscheidungen die erhebliche grundrechtliche Eingriffstiefe und die **Menschenwürde- (Art. 1 Abs. 1 GG) und Diskriminierungsrelevanz (Art. 3 Abs. 3 GG)** der automatisierten Verarbeitung persönlicher und insbesondere auch biometrischer Daten sowie des Einsatzes digitaler Instrumente hervorgehoben hat, die etwa darin deutlich werden, dass sie etwa mit dem Schutz besonders gewichtiger Rechtsgüter vor zumindest hinreichend konkretisierten Gefahren gerechtfertigt werden müssen.[81]

Bei genauer Betrachtung muss allerdings festgestellt werden, dass jedenfalls den staatlichen Stellen schon nach der jetzigen Rechtslage die biometrische Gesichtserkennung in dem Sinne verboten ist, als sie durch den Gesetzgeber nicht erlaubt wurde. Nach dem

80 Vgl. BVerfGE 46, 160 (164 f.); 77, 170 (214 f.).

81 Vgl. nur beispielhaft BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02, NJW 2006, 1939, Rn. 117 f.; BVerfGE 156, 11 (Rn. 39 f, 73); BVerfG v. 16.2.2023 – 1 BvR 1547/19, 1BvR 2634/20.

aus dem Gesetzmäßigkeitsprinzip (Art. 20 Abs. 3 GG) und den Grundrechten abgeleiteten **Vorbehalt des Gesetzes** sind grundrechtswesentliche Tätigkeiten nicht zulässig, solange und soweit sie nicht durch Gesetz (positiv) zugelassen wurden. Dies hat allerdings die Praxis nicht davon abgehalten, biometrische Gesichtserkennung durchführen (s. oben I), obwohl sie sich dafür allenfalls auf gesetzliche Befugnisse berufen kann (vgl. etwa §§ 98c, 100h i.V.m. 98a, 163f StPO sowie § 48 BDSG), die kaum hinreichend sind, um die dargelegte Eingriffsintensität biometrischer Gesichtserkennung zu rechtfertigen. Insoweit könnte die Einführung eines ausdrücklichen Verbots dazu beitragen oder sogar angezeigt sein, um die Bindung an Recht und Gesetz nach Art. 20 Abs. 3 GG – im Sinne des **Vorrangs des Gesetzes** – und deren zentrale Bedeutung für die rechtsstaatliche Demokratie zu verdeutlichen.

VI. Ergebnis und Vorschlag einer Regelung für das BDSG

Das Europa- und Verfassungsrecht steht einem bundesgesetzlichen Verbot der biometrischen Gesichtserkennung durch staatliche und private Akteure nicht grundsätzlich entgegen, gebietet ein solches Verbot aber auch nicht. Es obliegt der Einschätzung des Gesetzgebers, der dabei den Vorrang der bereits europarechtlich geregelten Aspekte zu beachten hat (insbes. Art. 5 lit. d u. e, Art. 6 ff. KI-VO).

Ein bundesgesetzliches Verbot darf die biometrische Gesichtserkennung gegenständlich nur soweit erfassen, wie die Gesetzgebungskompetenzen des Bundes reichen. Vom Verbot auszunehmen ist somit insbesondere die allgemeine und polizeiliche Gefahrenabwehr.

Für die Aufnahme des Verbots **in das BDSG** spricht dessen fachgesetzübergreifender und querschnittsartiger Anwendungsbereich, der der beabsichtigten Reichweite des Verbots, insbesondere der grundsätzlichen Erstreckung sowohl auf private als auch staatliche Akteure, sowie den dargelegten Grenzen Rechnung tragen würde (vgl. insbes. § 1 Abs. 1, 4 bis 8 BDSG). Zudem blieben Ausnahmen vom Verbot kraft originärer Gesetzgebungskompetenz der Länder nicht nur durch Landesgesetz (vgl. auch § 1 Abs. 1 S. 1 Nr. 2 BDSG), sondern auch durch Bundesgesetz (vgl. § 1 Abs. 2 BDSG) möglich.

Das Verbot sollte dabei gegenständlich (auch) an der biometrischen Gesichtserkennung anknüpfen, um sowohl die Verarbeitung biometrischer Daten als auch die dafür einge-

setzten Mittel (etwa Echtzeit- und Retrograd-KI-Systeme) zu erfassen (s. oben II). In Hinblick auf seine Grundsätzlichkeit, aber auch zur textsparsamen Umsetzung bietet sich eine Einfügung als allgemeine Vorschrift („vor die Klammer“) an, etwa als neuer **§ 4a BDSG-E**:

> *„Biometrische Gesichtserkennung im öffentlichen Raum oder zur Überwachung und die Verarbeitung diesbezüglicher Daten sind verboten.“*

Soweit das Verbot auch auf die Strafverfolgungstätigkeit der Länder erstreckt werden soll, erscheint wegen des Verweisungsbefehls in § 500 StPO (nur) auf Teil 3 des BDSG zudem eine klarstellende Ergänzung in den §§ 45 ff. BDSG als zweckmäßig, etwa durch die Ergänzung in Form eines neuen **§ 48 Abs. 3 BDSG-E**:

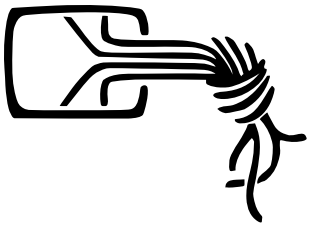
> *„Soweit öffentliche Stellen der Länder im Anwendungsbereich der Strafprozessordnung in der jeweils geltenden Fassung personenbezogene Daten verarbeiten, ist § 4a entsprechend anzuwenden.“*

Prof. Eike Richter

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 H



Private Daten schützen.

Stellungnahme zum Gesetzentwurf der Bundesregierung
zur Änderung des Bundesdatenschutzgesetzes (Drucksache 20/10859)

24. Juni 2024

Matthias Marx
Linus Neumann

Inhalt

Einleitung

Der Chaos Computer Club setzt sich für ein Verbot biometrischer Fernidentifikationssysteme ein. Gleichermaßen sollen Bußgelder und Zwangsmittel gegen öffentliche Stellen ermöglicht, und das Recht auf Auskunft stärker geschützt werden.

1. Verbot biometrischer Fernidentifikationssysteme

Der Chaos Computer Club fordert ein unmissverständliches Verbot von Gesichtserkennung im öffentlichen Raum.

Die Regierungskoalition hat sich darauf geeinigt, dass *„[b]iometrische Erkennung im öffentlichen Raum"* auszuschließen ist und der *„Einsatz von biometrischer Erfassung zu Überwachungszwecken"* abgelehnt wird.

In der jüngsten Vergangenheit kam es immer wieder zum Einsatz biometrischer Fernidentifikationssysteme durch Polizeibehörden, welche die fehlende Rechtsgrundlage einfach ignorieren. Die Gelegenheit der BDSG-Novelle sollte daher genutzt werden, diese Gesichtserkennung im öffentlichen Raum unmissverständlich zu verbieten.

- Erst kürzlich wurde bekannt, dass die sächsische Polizei verfassungswidrige Echtzeit-Gesichtserkennung ohne Kenntnis der Datenschutzbehörde im öffentlichen Raum eingesetzt hat. [1] Heimlich wurde mit der gleichen Technik auch in Nordrhein-Westfalen, Brandenburg, Baden-Württemberg, Berlin und Niedersachsen überwacht.

- Ebenfalls ohne vorherige Kenntnis der Datenschutzbehörde und auch ohne Rechtsgrundlage stellte das Bundeskriminalamt (BKA) Gesichtsbilder von ca. drei Millionen Personen aus der zentralen INPOL-Datenbank dem Fraunhofer Institut für Graphische Datenverarbeitung zur Verfügung, um eine Marktrecherche von Gesichtserkennungssystemen durchzuführen. [2,3]

- Zum Hamburger G20-Gipfel nutzte die Polizei eine Gesichtserkennungssoftware. Wieder gab es keine Rechtsgrundlage für die Erfassung und Verarbeitung der biometrischen Daten von mehr als 100.000 Personen. Sogar auf die Errichtungsanordnung nach § 490 StPO wurde verzichtet. Die Löschanordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) wurde obendrein ignoriert.[4]

  Der Rechtsweg konnte also keine Rechtssicherheit sicherstellen. Das Gerichtsverfahren zwischen Innenbehörde und HmbBfDI zog sich so lange hin, bis die Ermittlungsverfahren der Polizei abgeschlossen waren und die Polizei die illegale Gesichterdatenbank nicht mehr benötigte und löschte. Damit wurde das Verfahren eingestellt.[5]

[1] https://netzpolitik.org/?p=459282
[2] https://www.tagesschau.de/investigativ/br-recherche/gesichtserkennung-bka-software-test-100.html
[3] https://fragdenstaat.de/a/203968
[4] https://netzpolitik.org/?p=236484
[5] https://datenschutz-hamburg.de/news/gerichtsverfahren-zu-videmo-360-eingestellt

- Bei den Versuchen zur Gesichtserkennung am Berliner Bahnhof Südkreuz waren die Ergebnisse im Abschlussbericht nicht überzeugend und sogar absichtlich geschönt worden.[6]

Biometrische Überwachung greift fundamental in Grundrechte wie das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit ein. Menschen, die sich überwacht fühlen, verhalten sich vermeintlich konform. Die Meinungsfreiheit wird insbesondere auch durch Verletzung des Rechts auf anonyme Teilnahme an Versammlungen gefährdet. Die Polizei kann mit Hilfe ihrer wachsenden Gesichter-Datenbanken immer mehr Menschen jederzeit, ungefragt und auch im Nachhinein identifizieren – und tut dies auch insbesondere bei Demonstrationen.

Erschwerend kommt hinzu, dass die biometrischen Datenbanken nicht wirksam und nicht dauerhaft gegen illegitime Zugriffe und Interessen gesichert werden können.[7] Bei einem Verlust, anders als bei einem verlorengegangenen Passwort, können wir unsere biometrischen Daten auch nicht einfach verändern.

Deshalb gilt es nun, die im *AI Act* der Europäischen Union explizit vorgesehene Möglichkeit der nationalen Verschärfung europäischer Regeln sowohl für Echtzeit- als auch für nachträgliche biometrische Fernidentifizierung zu nutzen und das Verbot biometrischer Überwachung im BDSG zu verankern.

In Bezug auf mögliche Ausnahmetatbestände ist zu beachten, dass auch bei einer Einschränkung des Einsatzes von Gesichtserkennung auf schwere Straftaten eine dauerhafte Überwachung des öffentlichen Raums die Folge wäre. Es liegt in der Natur der Technik, dass auch dann alle Personen biometrisch erfasst werden müssen, wenn nur eine einzige Person gesucht wird. Insbesondere an hochfrequentierten Orten wie Flughäfen oder Bahnhöfen mit z.T. mehreren Hunderttausend Passieren pro Tag ließe sich immer argumentieren, dass ein schwerer Straftäter erwartet wird. Dauerhafte biometrische Überwachung aller Passagiere wäre die Folge.

Für einen konkreten Formulierungsvorschlag verweisen wir auf die Stellungnahme der Gesellschaft für Freiheitsrechte.

[6] https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz
[7] https://www.ccc.de/de/updates/2022/afghanistan-biometrie

2. Bußgelder und Zwangsmittel gegen öffentliche Stellen

Der Chaos Computer Club fordert, dass auch gegen Behörden und andere öffentliche Stellen bei Datenschutzverstößen Bußgelder verhängt und Zwangsmittel angeordnet werden können. Entsprechend soll § 43 Abs. 3 BDSG gestrichen werden.

Öffentliche Stellen können ihre Datenschutzbeauftragten hinhalten und ignorieren, selbst bei schwerwiegenden Datenschutzverstößen, fragwürdigen Biometrie-Experimenten an der Bevölkerung oder sonstigen Anfragen und Anordnungen. Diese Missachtung führt dazu, dass Datenschutz- und IT-Sicherheitsprobleme nicht angemessenen angegangen und behoben werden.

So ist es nicht überraschend, dass zunehmend auch öffentliche Stellen ins Visier von „Double Extortion"-Angriffen geraten.[8] Dabei wird nach der Verschlüsselung von Daten und Systemen auch mit der Veröffentlichung sensibler Daten gedroht, um ein Lösegeld zu fordern. Bürger*innen sind hiervon in mehrfacher Hinsicht betroffen: Erstens können sie angebotene Dienstleistungen nicht nutzen. Zweitens geraten ihre Daten zunächst „nur" in die Hände von Kriminellen und sind später teilweise offen zugänglich im Internet.

Im Rahmen der Weitergabe von INPOL-Gesichtsdaten zeigte sich das BKA wenig beeindruckt vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Der BfDI wurde nicht in die Vorbereitung oder Durchführung der Marktrecherche eingebunden. Wichtige Fragen des BfDI wurden, wenn überhaupt, nur widerwillig und erst nach Abschluss der Recherche vom BKA beantwortet. So teilte das BKA bspw. die Ergebnisse der Recherche erst nach fünf Nachfragen des BfDI:[9]

1. 19.04.2021: „Für eine Mitteilung der Ergebnisse der durchgeführten Studie(n) bzw. des in Aussicht gestellten Berichts wäre ich Ihnen dankbar."
2. 25.05.2021: „für eine Sachstandsmitteilung wäre ich dankbar."
3. 21.06.2021: „gibt es vielleicht schon einen neuen Sachstand?"
4. 06.08.2021: „bislang liegt mir keine Rückmeldung des BKA vor. Bitte übersenden Sie die Stellungnahme/Bericht bis zum 11. August 2021. Andernfalls bitte ich um Mitteilung der Hinderungsgründe."
5. 16.08.2021: „ich wäre Ihnen dankbar, wenn Sie sich dieser Angelegenheit annehmen würden. Die Zulieferungsfrist hat das BKA kommentarlos verstreichen lassen. Ebenso blieb eine Sachstandsanfrage bei DS im Monat Juni ohne Antwort."

Erst am 16.08.2021 übermittelte das BKA den Fraunhofer-Bericht mit Datum vom 20.12.2019 an den BfDI.

[8] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
[9] https://fragdenstaat.de/a/261260#nachricht-903742

Die Einführung von Bußgeldern und Zwangsmitteln gegen öffentliche Stellen wären wirksame Mittel, um Datenschutzverstößen und schwerwiegenden Konsequenzen für die Bürgerinnen vorzubeugen.

> *"Die Bußgelder sind bisher viel zu niedrig"*, sagte GdP-Bundesvize Mertens 2019 über Verkehrssünder. *"Wir sind europaweit der Discounter. Die Bußgelder müssen erhöht werden, damit sie spürbar werden, weh tun und erzieherisch wirken."*[10]

Es ist bedauerlich, dass auch Datenschutzverletzungen als Kavaliersdelikte behandelt werden – ungeachtet der Konsequenzen für Individuum und Gesellschaft.

[10] https://www.zeit.de/news/2019-08/16/viel-kritik-an-busspur-plaenen-aber-lob-fuer-andere-ideen

3. Das Recht auf Auskunft schützen

Der Chaos Computer Club wendet sich gegen die Schwächung der Auskunftsrechte durch § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E.

Das Recht auf Auskunft dient dem Schutz der informationellen Selbstbestimmung. Betroffene Personen haben ein Recht darauf zu erfahren, welche Daten über sie gesammelt, gespeichert und verarbeitet werden. Die Einschränkung dieses Rechts zugunsten von Geschäftsgeheimnissen stellt eine unverhältnismäßige Einschränkung der Grundrechte betroffener Personen dar, und lädt zu großzügigem Missbrauch ein.

Die vorgeschlagene Regelung könnte zu leicht von Unternehmen oder öffentlichen Stellen missbraucht werden, um Transparenzanforderungen zu umgehen: Allzu leicht lassen sich Sachverhalte konstruieren, in denen auch personenbezogene Daten als Betriebs- oder Geschäftsgeheimnis deklariert werden, um sich der gesetzlichen Verpflichtung zur Auskunft entziehen und damit eine wirksame Kontrolle verhindern.

- Auskunftsersuchen zeigen, dass die amerikanische Gesichter-Suchmaschine Clearview AI auch Personen in der EU erfasst und überwacht. In der Folge verhängten Datenschutzbehörden in Italien, Griechenland, Frankreich und Großbritannien hohe Bußgelder gegen Clearview AI, da das Unternehmen rechtswidrig biometrische Daten von Millionen Europäerinnen verarbeite.[11]

- Auch Auskunftsersuchen ermöglichten nachzuvollziehen, wie Facebook-/Cambridge-Analytica-Daten genutzt wurden, um durch politische Werbung Einfluss auf Wahlkämpfe zu nehmen.[12]

- Durch ein Auskunftsersuchen wurde öffentlich, dass Amazon für jeden Klick bis zu fünfzig zusätzliche Informationen speichert. Aus diesen Daten kann Amazon bspw. Aufenthaltsorte, Familienbesuche, Schlafverhalten oder die bevorzugte Zeitung ableiten.[13]

- Tracking in der Forschung bedroht neben der informationellen Selbstbestimmung der Forschenden auch die Wissenschaftsfreiheit.[14] Mittels Auskunftsersuchen kann untersucht werden, welche Daten Wissenschaftsverlage über ihre Nutzerinnen erheben und an welche Akteure sie diese Daten verkaufen.

Als wichtige Mittel der Transparenz und der Aufdeckung von Verstößen sollten Auskunftsrechte nicht geschwächt werden.

---

[11] https://www.spiegel.de/netzwelt/netzpolitik/frankreich-verdonnert-clearview-ai-zu-20-millionen-euro-geldstrafe-a-f2947fd1-b219-4b35-be3f-6a403fb08a5f
[12] https://www.heise.de/-4042938
[13] https://www.spiegel.de/netzwelt/web/amazon-experiment-was-der-konzern-mit-jedem-klick-erfaehrt-a-1205079.html
[14] https://www.dfg.de/de/aktuelles/neuigkeiten-themen/info-wissenschaft/2021/info-wissenschaft-21-43

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)420

Stellungnahme

zum Gesetzentwurf der Bundesregierung für ein „Erstes Gesetz zur Änderung des Bundesdaten-schutzgesetzes“ (BT-Drs. 20/10859)

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:
Silvia Frömbgen
Telefon: +49 30 20225-5372
Telefax: +49 30 20225-5345
E-Mail: silvia.froembgen@dsgv.de

Berlin, 17. April 2024

Federführer:
Deutscher Sparkassen- und Giroverband e. V.
Charlottenstraße 47 | 10117 Berlin
Telefon: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

A. Allgemeine Bewertung

Mit dem vorliegenden Gesetzesentwurf wird den Ergebnissen aus der Evaluierung des Bundesdatenschutzgesetzes (BDSG) zumindest teilweise Rechnung getragen und eine Verbesserung des Datenschutzrechts angestrebt. Die Deutsche Kreditwirtschaft (DK) begrüßt, dass mit der Gesetzesnovelle die nach der EU-Datenschutzgrundverordnung (DSGVO) weiterhin möglichen Gestaltungsmöglichkeiten im nationalen Recht genutzt werden. Auch wird eine Verbesserung der Kohärenz des Datenschutzes sehr unterstützt, um bürokratische Hürden abzubauen, die Rahmenbedingungen für die Digitalisierung zu verbessern und Rechtssicherheit zu gewährleisten.

Des Weiteren ist positiv zu vermerken, dass das Urteil des Europäischen Gerichtshofs vom 7. Dezember 2023 (C-634/21 „SCHUFA Holding (Scoring)“) mit einen neuen § 37a BDSG zum Anlass genommen wird, Rechtssicherheit für die Erstellung von Scorewerten durch Auskunfteien und die Verwendung dieser Werte durch Kreditinstitute zu gewährleisten.

Allerdings halten wir die Streichung der bewährten Regelung zur Videoüberwachung für den nicht-öffentlichen Bereich (§ 4 BDSG) für die Praxis der Unternehmen nach wie vor nicht für hilfreich. Auch bietet aus unserer Sicht das Gesetzesvorhaben die Chance, die Kohärenz in der Datenschutzaufsicht noch weiter als vorgesehen zu verbessern.

B. Im Einzelnen

Im Einzelnen haben wir folgende Anmerkungen:

1. § 37a BDSG-E: Schaffung von Rechtssicherheit für das Scoring von Auskunfteien wird begrüßt

Wir begrüßen den Vorschlag der Bundesregierung, das Urteil des Europäischen Gerichtshofs vom 7. Dezember 2023 (C-634/21 „SCHUFA Holding (Scoring)“) zum Anlass zu nehmen, Rechtssicherheit für die Erstellung von Scorewerten durch Auskunfteien und die Verwendung dieser Werte durch Kreditinstitute zu gewährleisten. Hierbei wird zutreffend die Gestaltungsmöglichkeit des nationalen Gesetzgebers in Art. 22 Abs. 2 b DSGVO genutzt, um das für die kreditgebende Wirtschaft wichtige Auskunftei-Scoring abzusichern und diesbezügliche Rahmenbedingungen für die hierbei verwendbaren Daten und die Transparenz gegenüber Betroffen zu schaffen. Gleichwohl besteht Verbesserungsbedarf wie folgt:

- **Anwendungsbereich des § 37a BDSG**
  Gemäß der genannten EuGH-Rechtsprechung sollte der § 37a BDSG-E nur das Scoring von Auskunfteien erfassen und dafür nach Art. 22 Abs. 2 b DSGVO eine gesonderte Grundlage schaffen. Für ein z.B. im Rahmen der Kreditwürdigkeitsprüfung nach § 18a KWG erfolgendes bankinternes Scoring besteht kein Regelungsbedarf, weder aufgrund der EuGH-Rechtsprechung noch aufgrund der DSGVO. Vielmehr ist das bankinterne Scoring EU-weit einheitlich bereits mit Art. 6 Abs. 1 b DSGVO i. V. m. Art. 22 Abs. 2 a DSGVO legitimiert. EU-rechtlich kann das bankinterne Scoring auch nicht in Bezug auf die hierfür nutzbaren Datenarten weiter eingeschränkt werden. Dies würde dem Vollharmonisierungsansatz widersprechen, denn dann würden in Deutschland strengere Regelungen für das bankinterne Scoring gelten als in

anderen EU-Mitgliedstaaten. Auch ein Konflikt mit bankaufsichtsrechtlichen Rahmen-bedingungen in § 10 Abs. 2 KWG würde auftreten. Denn § 10 Abs. 2 KWG konkretisiert Art und Umfang des bankinternen Scorings, damit Kreditinstitute eine möglichst treffsichere Bonitätsanalyse ihrer Kunden vornehmen und damit „Adressausfallrisiken" vermindern können. Etwaige Einschränkungen wären risikoerhöhend für Kreditinstitute. **Daher schlagen wir zur Klarstellung des Anwendungsbereichs der Vorschrift vor, bereits in der Überschrift zum Ausdruck zu bringen, dass § 37a BDSG-E nur für das Scoring von Auskunfteien Anwendung findet.**

- **Datenverwendungsverbote**
  Nach § 37a Abs. 2 Nr. 1 c) BDSG-E sollen „Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten" nicht zum Zwecke des Scoring genutzt werden dürfen. Wie oben bereits betont, sollte der § 37a BDSG insgesamt auf das Scoring von Auskunfteien begrenzt werden. Denn für das bankinterne Scoring sind insbesondere der Zahlungskontensaldo, auf dem Zahlungskonto in Anspruch genommene Überziehungskredite, die Zahl von auf dem Zahlungskonto mangels Deckung nicht eingelösten Lastschriften und etwaige Pfändungen in das Zahlungskonto wichtige Risikoerkennungsmerkmale für die Bonitätsbewertung eines Kunden. Das erkennt auch die bankaufsichtrechtliche Vorschrift des § 10 Abs. 2 KWG an, wonach von Kreditinstituten im Rahmen der Bewertung von Ausfallrisiken u.a. das „Zahlungsverhalten und (die) Vertragstreue der betroffenen Person" und „Zwangsvollstreckungsmaßnahmen" einzubeziehen sind.

- **Zweckbindung**
  Aus Sicht von Auskunfteien und Auskunfteinutzern (z.B. Kreditinstitute) ist die in § 37a Abs. 2 Nr. 3b BDSG-E vorgesehene Zweckbindung problematisch, da sie sich auf die Datengrundlage und nicht auf das Scoring-Ergebnis bezieht. Damit besteht die Gefahr, dass eine Auskunftei keine Bonitätsauskunft (ohne Scoring) mehr geben dürfte, obwohl dies – allgemein anerkannt - der eigentliche Zweck von Kreditauskunfteien ist. Vermutlich liegt ein redaktionelles Versehen vor, denn der Bundesregierung geht es wohl eher darum, dass der Scorewert der Auskunftei nicht für andere als die beschriebenen Zwecke verwendet werden darf. In der Stellungnahme des Bundesrates vom 22. März 2024 wird dieser Aspekt auch angesprochen (vgl. BR-Drs. 72/24 Ziff. 5).

- **Remonstrationsrecht des Betroffenen**
  Des Weiteren sollte der Anwendungsbereich von § 37a Abs. 6 BDSG-E auf solche Entscheidungen begrenzt werden, die sich im Sinne des EuGH-Urteils vom
  7. Dezember 2023 „maßgeblich" auf den Scorewert einer Auskunftei stützen. Im Übrigen ist der Betroffene durch das allgemeine Remonstrationsrecht bei negativen vollautomatisierten Entscheidungen nach Art. 22 Abs. 3 DSGVO geschützt.

- **Umsetzungsfrist**
  Auch wenn sich die Vorschrift richtigerweise nur auf Auskunfteien erstrecken sollte (s.o.), sind gleichwohl verfahrenstechnische Umsetzungsmaßnahmen bei Auskunfteien und mittelbar bei den Nutzern von Auskunfteien (z.B. Kreditinstitute) zu bedenken, die ihre Zeit brauchen**. Es sollte daher eine Umsetzungsfrist von mindestens 6 Monaten vorgesehen werden.**

2. Durchsetzung und Kohärenz des Datenschutzes: Weiterer Verbesserungsbedarf

Der Regierungsentwurf schlägt vor, in Umsetzung der Vorgaben des Koalitionsvertrags der Bundesregierung in § 16a, § 18, § 40a und § 27 Absatz 5 und § 40a Vorschriften „zur besseren Durchsetzung und Kohärenz" zu treffen. Dieser Ansatz ist zu unterstützen, allerdings sind die Verbesserungen für die Wirtschaft nicht ausreichend. Mit § 40a BDSG wird zwar eine als solche zu begrüßende Regelung für die federführende Aufsichtsbehörde im Falle der gemeinsamen Verantwortung etabliert. Klarstellend sollte für den Erhalt der Verwaltungsvereinfachung auch aufgenommen werden, dass die Zuständigkeitsregel ebenfalls für den Fall der a) späteren Aufnahme eines weiteren Unternehmens mit größerem Umsatz, b) das Ausscheiden der die Zuständigkeit begründenden Vertragspartei und c) für den Fall einer gemischt in Auftragsverarbeitung und gemeinsamer Verantwortung geführten Datenverarbeitung gilt. Soweit bei gemischten Verträgen sowohl gemeinsame- als auch Auftragsdatenverarbeitung wegen unterschiedlicher Datenverarbeitungszwecke vorkommen, drohen ohne eine entsprechende Festlegung konkurrierende Zuständigkeiten. Derzeit sieht der Entwurf nur für den Fall veränderter Größenverhältnisse zwischen den Vertragsparteien eine unveränderte Zuständigkeit vor.
Allerdings spielt die gemeinsame Verantwortung nach Art. 26 DSGVO in der Kreditwirtschaft bislang nur eine untergeordnete Rolle**. Aus Sicht der Kreditwirtschaft besteht aber allgemein ein Bedürfnis, dass die Datenschutzbehörden in ihrer Aufsichtspraxis mit einer Stimme sprechen.** Die BDSG-Novelle könnte hierfür eine gute Chance bieten.

Die teilweise unterschiedliche Verwaltungspraxis in verschiedenen Bundesländern stellt Wirtschaft und betroffene Personen weiterhin vor erhebliche Probleme. Die bundesländerspezifische Praxis von 16 Aufsichtsbehörden und deren Entwicklungen im Blick zu behalten, ist ein wesentlicher Kosten- und Risikofaktor. Dies stellt sowohl bundesländerübergreifend als auch regional tätige Kreditinstitute vor große Herausforderungen und steht dem Grundprinzip der DSGVO entgegen, wonach die Aufsichtsbehörden zusammenarbeiten müssen, um eine einheitliche Anwendung und Durchsetzung der DSGVO zu gewährleisten (vgl. Artikel 57 Absatz 1 g DSGVO, Erwägungsgründe (7), (8), (119) Satz 1 DSGVO). Während zur Beförderung des EU-Binnenmarkts nach Kapitel VII der DSGVO für EU-grenzüberschreitende Sachverhalte eine Einheitlichkeit der Vorgaben der Datenschutzaufsicht das Ziel ist, erlaubt die der Zusammenarbeit dienende Satzung der Datenschutzkonferenz der Datenschutzaufsichtsbehörden (DSK) eine unterschiedliche Verwaltungspraxis, indem selbst bei einheitlichen Beschlüssen der DSK eine unterschiedliche Rechtsanwendung möglich bleibt. Im Vergleich zu anderen EU-Mitgliedsstaaten, die nur eine einzige nationale Aufsichtsbehörde haben, ist diese heterogene Situation ein Standortnachteil für Wirtschaftsunternehmen in Deutschland.

Die Zuständigkeit für Datenschutz auf Länderebene muss für eine Verbesserung der Lage nicht grundsätzlich geändert werden. **Es dürfte unseres Erachtens genügen, die Verfahrensprinzipien aus Kapitel VII der DSGVO auf die DSK zu übertragen und dort, wo vergleichbare Sachverhalte bei mehr als einer Aufsichtsbehörde vorliegen, eine Pflicht zum Einvernehmen zu schaffen.** Zwar muss gemäß Erwägungsgrund (138) der DSGVO eine einheitliche Rechtsanwendung als

Zulässigkeitsvoraussetzung nur zwischen den betroffenen Aufsichtsbehörden stattfinden. Soweit jedoch ein Sachverhalt mit bundesweiter Relevanz vorliegt, sollte eine zersplitterte Rechtsanwendung je nach Aufsichtsbehörde vermieden werden.

Für einen Bürokratieabbau sollte der one-stop-shop Mechanismus des Artikel 56 DSGVO auch bei Sachverhalten in Deutschland gelten. Wie bei EU-grenzüberschreitender Datenverarbeitung sollte eine federführende Aufsichtsbehörde als Ansprechpartner für Betroffene und Verantwortliche dienen. **Eine verbindliche Abstimmung einheitlicher Rechtsanwendung sollte unter den Aufsichtsbehörden stattfinden.** Die Kohärenzabstimmung unter den Datenschutzbehörden innerhalb Deutschlands sollte der Abstimmungsnotwendigkeit zwischen den EU-Mitgliedsstaaten entsprechen.

3. § 4 BDSG - Videoüberwachung öffentlich zugänglicher Räume: Regelung auch für nicht-öffentlichen Bereich fortführen

§ 4 BDSG zur Videoüberwachung öffentlich zugänglicher Räume ist für Banken und Sparkassen von erheblicher Bedeutung. Denn die Aufzeichnung von Bilddaten dient dem Schutz von Kunden und Mitarbeitern, der Wahrnehmung des Hausrechts und dem Zweck der Beweissicherung von Straftaten (beispielsweise an Geldautomaten, an Selbstbedienungsterminals und in den öffentlich zugänglichen Geschäftsräumen).

Der Gesetzentwurf begründet die in Art. 1 Ziffer 3 c) vorgesehene Beschränkung des § 4 BDSG zur Videoüberwachung öffentlich zugänglicher Räume auf den öffentlichen Bereich mit dem BVerwG-Urteil vom 27. März 2019 (Az. 6 C 2.18). Diese Einschränkung halten wir nicht für zwingend erforderlich, zumal der § 4 BDSG eine wichtige Hilfestellung für die Praxis der Videoüberwachung im nicht-öffentlichen Bereich bietet. Zudem würde der Wegfall der auf das Wesentliche fokussierten Hinweispflicht in § 4 Absatz 2 BDSG erheblichen Anpassungsbedarf für die Videoüberwachungshinweisschilder zur Folge haben. Daraus resultieren erhebliche Kosten, die in der Wirtschaft vermutlich im zweistelligen Millionenbereich liegen dürften und in der Gesetzesfolgenabschätzung bislang fehlen. **Wir plädieren daher für die Beibehaltung der Vorschrift, um zusätzlichen – bürokratischen - Aufwand für die Wirtschaft zu vermeiden.**

Sollte gleichwohl an dem Ansatz des Gesetzentwurfs festgehalten werden, ist die Aussage in der Gesetzesbegründung wichtig, dass sich in der Praxis der Videoüberwachung im nicht-öffentlichen Bereich gegenüber der bisherigen Rechtslage wenig ändern würde, da auch nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO die Rechtmäßigkeit der Videoüberwachung im nicht-öffentlichen Bereich weiterhin unter Beachtung der bisherigen Voraussetzungen fortbesteht.

4. Weiterer Verbesserungsbedarf: Erhaltung des § 26 BDSG als kollektivrechtliches Gestaltungsmittel

Mit EuGH-Urteil vom 30. März 2023 – C-34/21 wurde § 26 BDSG zum Beschäftigtendatenschutz als unzureichend konkret für die Anforderungen des Artikels 88 Absatz 1 DSGVO angesehen. Kollektivarbeitsrechtliche Regelungen anstelle vieler Einzelregelungen stellen gerade im datenschutzrechtlich sensiblen Beschäftigtendatenschutz eine der Stärken des Wirtschaftslebens in Deutschland dar.

Erwägungsgrund (43) DSGVO hemmt umfassende Regelungen zwischen Arbeitgeber und Arbeitnehmer wegen des Ungleichgewichts der Vertragsparteien. Wegen des auf lange Zeit angelegten Beschäftigungsverhältnisses können die wesentlichen Regeln für die Verarbeitung von Beschäftigtendaten nicht bei Abschluss des Arbeitsvertrages ausgehandelt werden. Dagegen besteht bei den Parteien von Betriebs- und Tarifverträgen dieses Ungleichgewicht nicht und ermöglicht ausgewogene Regelungen im Interesse von Beschäftigten und Arbeitgebern.

Auch im Hinblick auf ein von der Bundesregierung geplantes Beschäftigtendatenschutzgesetz **sollte § 26 BDSG zumindest vorläufig in der Weise angepasst werden, dass kollektivrechtliche Regelungen grundsätzlich weiter Anwendung im Datenschutzrecht finden. Andernfalls könnte unter Umständen erheblicher Anpassungsaufwand für Wirtschaftsunternehmen entstehen.**

5. § 34 Absatz 1 neuer Satz - Auskunftsrecht der betroffenen Person: Berücksichtigung der Rechte Dritter wird unterstützt

Im Gesetzentwurf ist in Artikel 1 Ziffer 10 a) bb) vorgesehen, unter Nutzung des Artikel 23 Absatz 1 Buchstabe i DSGVO eine ausdrückliche Ausnahme vom Auskunftsrecht für den Fall zu schaffen, dass das Interesse an der Geheimhaltung der Betriebs- und Geschäftsgeheimnisse das Interesse der betroffenen Person an der Information überwiegt. Im Lichte der Rechtsprechung des EuGH ist diese Einschränkung des Auskunftsrechts konsequent und eine wichtige Hilfestellung für die Praxis bei der Bearbeitung von Auskunftsersuchen.

***

Deutscher Bundestag

Ausschussdrucksache
20(4)426

Stellungnahme

zum

Gesetzentwurf der Bundesregierung
Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

- Anders als in zahlreichen anderen EU-Ländern enthält das Bundesdatenschutzgesetz (BDSG) bislang keine eindeutige gesetzliche Erlaubnisgrundlage für die **Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Versicherungsverträgen**. Die Versicherungswirtschaft stützt sich allgemein auf Art. 9 Abs. 2 lit. f der Datenschutzgrundverordnung (DSGVO), doch gibt es dazu bei den deutschen (Landes-)Datenschutzbehörden unterschiedliche Auffassungen. Die vorliegende Überarbeitung des BDSG bietet eine Gelegenheit, für Versicherte und Versicherer eine belastbare Rechtsgrundlage zu schaffen.
- Der PKV als integralem Bestandteil des deutschen Gesundheitssystems sollten die gleichen datenschutzrechtlichen Befugnisse für die Verarbeitung von Gesundheitsdaten wie für die GKV eingeräumt werden. Um der PKV analog zur GKV das **Angebot und die Durchführung von Gesundheits- und Präventionsprogrammen** für alle Privatversicherten rechtssicher zu ermöglichen, sollten die Erlaubnisnormen in § 22 BDSG entsprechend (klarstellend) ergänzt werden.
- Im Hinblick auf **betriebliche Kranken- und Pflegeversicherungsangebote** der PKV besteht das (praktische) Erfordernis, für die Begründung derartiger Versicherungsverhältnisse die Verarbeitung von Beschäftigtendaten ausdrücklich zuzulassen; dies sollte in § 26 BDSG klargestellt werden.
- Bei der Neuregelung des **Scorings** muss sichergestellt werden, dass den PKV-Unternehmen die rechtssichere Erstellung und Nutzung von Wahrscheinlichkeitswerten unter Verwendung von Gesundheitsdaten in den durch Art. 22 Abs. 4 DSGVO vorgegebenen Grenzen möglich bleibt.

Postfach 511040
50946 Köln

Gustav-Heinemann-Ufer 74c
50968 Köln

Telefon
(0221) 99 87 – 0

Telefax
(0221) 99 87 – 39 50

E-Mail
verband@pkv.de

Internet
www.pkv.de

I. Allgemeine Anmerkungen

Die PKV begrüßt und unterstützt das Ziel der Bundesregierung, notwendige Anpassungen im Bundesdatenschutzgesetz (BDSG) vorzunehmen und hierbei die Erfahrungen und Erfordernisse im nationalen Recht nach Inkrafttreten der Datenschutzgrundverordnung (DSGVO) zu berücksichtigen.

Klarstellungsbedarf sehen wir bei der Streichung § 37a BDSG-RegE. Es muss sichergestellt werden, dass den Unternehmen der Privaten Kranken- und Pflegeversicherung die rechtssichere Erstellung und Nutzung von Wahrscheinlichkeitswerten unter Verwendung von Gesundheitsdaten in den durch Art. 22 Abs. 4 DSGVO vorgegebenen Grenzen möglich bleibt. Aufgrund der Auslegungsbedürftigkeit der vorgesehenen Regelungen zur Nutzung u. a. von (vorhandenen) Gesundheitsdaten für unternehmenseigene Scorings werden Rechtsunsicherheiten und zudem über die Vorgaben der DSGVO hinausreichende Restriktionen geschaffen, die nachteilige Folgen u. a. für bestehende technische Prozesse in den Versicherungsunternehmen haben.

Der vorliegende Gesetzesentwurf zeigt aus Sicht der PKV dringenden weiteren Ergänzungsbedarf, da für die PKV u. a. sinnvolle gesetzliche Klarstellungen hinsichtlich des Umfangs bestehender Datenverarbeitungsbefugnisse fehlen und für die PKV insoweit (weiterhin) datenschutzrechtliche Rechtsrisiken bestehen. Zur Förderung einer einheitlichen Normauslegung durch die (Landes-)Datenschutzaufsichtsbehörden ist es erforderlich, dass der Gesetzgeber Klarstellungen für Datenverarbeitungen der PKV-Unternehmen insbesondere bei Gesundheits- und Präventionsprogrammen sowie der betrieblichen Kranken- und Pflegeversicherung vornimmt. Es muss sichergestellt werden, dass abweichende Auslegungen einzelner Datenschutzaufsichtsbehörden zu Datenverarbeitungsbefugnissen und damit einhergehende Rechtsrisiken für die Versicherer nicht dazu führen, dass den PKV-Versicherten – im Gegensatz zu den Versicherten der Gesetzlichen Krankenversicherung (GKV) – der Zugang zu wichtigen Bestandteilen eines modernen (digitalen) Gesundheits- und Versorgungsmanagements (Managed Care) erschwert, wenn nicht gar unmöglich gemacht wird. Dies läuft dem gesetzgeberischen Ziel der Transformation der PKV vom reinen Kostenerstatter zum Gesundheitsmanager zuwider, behindert den gerechten Systemwettbewerb zwischen GKV und PKV und führt letztlich zu einer versorgungsrelevanten Benachteiligung der Privatversicherten.

Mit Blick auf die aktuelle Weiterentwicklung der Digitalgesetzgebung für das deutsche Gesundheitswesen ist zudem sicherzustellen, dass für die PKV vergleichbare Datenverarbeitungsbefugnisse wie in der GKV bestehen bzw. geschaffen werden, damit alle Bürgerinnen und Bürger unabhängig vom Versicherungsstatus unter Wahrung höchster datenschutzrechtlicher Standards gleichberechtigt und verwaltungsbarrierefrei von den neuen digitalen Gesundheitsangeboten und -möglichkeiten profitieren können.

Letztlich begrüßen wir insbesondere die im Regierungsentwurf vorgesehene klarstellende Ergänzung des § 34 Abs. 1 BDSG, welche den datenschutzrechtlichen Auskunftsanspruch der betroffenen Person bei entgegenstehenden überwiegenden Betriebs- und Geschäftsgeheimnissen sachgerecht einschränken soll.

II. Zu ausgewählten Regelungen des Gesetzentwurfs

Zu Art. 1 Nr. 12 (§ 34 Abs. 1 S. 2 BDSG-RegE – Beschränkung des Auskunftsrechts bei überwiegenden Betriebs- oder Geschäftsgeheimnissen)

Vorgeschlagene Regelung
Unter § 34 Abs. 1 BDSG soll auf der Grundlage der Öffnungsklausel in Art. 23 Abs. 1 lit. i DSGVO ein neuer Satz 2 angefügt werden, der eine ausdrückliche Ausnahme vom Auskunftsrecht vorsieht, wenn das Interesse des Verantwortlichen an der Geheimhaltung von Betriebs- und Geschäftsgeheimnissen das Interesse der betroffenen Person an der Information überwiegt.

Bewertung
Wir begrüßen die im Regierungsentwurf in § 34 Abs. 1 BDSG vorgesehene – klarstellende – Ergänzung, dass das Auskunftsrecht nach Art. 15 DSGVO auch insoweit nicht besteht, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt. Dieses Verständnis lässt sich bereits aus § 29 Abs. 1 Satz 2 BDSG herleiten. Die vorgesehene Klarstellung in § 34 BDSG trägt zur Rechtssicherheit bei.

Diese Klarstellung erscheint sogar geboten. Entgegen der Annahme des Bundesrats besteht bei einer ausdrücklichen Berücksichtigung des Schutzes von Betriebs- und Geschäftsgeheimnissen im BDSG nicht die Gefahr, dass die erwähnten Kranken- und Pflegeversicherer als Verantwortliche künftig datenschutzrechtliche Auskunftsansprüche rechtsmissbräuchlich zurückweisen würden, um strukturelle Beweislastprobleme zum Nachteil von betroffenen Personen / Verbrauchern in Rechtsstreitigkeiten auszunutzen.

Insbesondere geht es in den zuletzt gehäuft aufgekommen Verfahren zur Frage der Zulässigkeit von Beitragsanpassungen in der PKV, die für diese Begründung Anlass gegeben haben mögen, nicht darum, den Betroffenen einen datenschutzrechtlichen Auskunftsanspruch unter Berufung auf Betriebs- und Geschäftsgeheimnisse vorzuenthalten. Vielmehr sind in der Praxis zunehmend Auskunftsverlangen (regelmäßig von selbst ernannten „Verbraucheranwälten“) mit datenschutzfremdem Hintergrund zu beobachten, um in den betreffenden Gerichtsverfahren (Stufen-)Klagen bei klägerseitig zu vertretenden Darlegungs- und Beweislastproblemen schlüssig zu machen. Regelmäßig wird dabei die erneute Zurverfügungstellung von Unterlagen (z. B. Beitragserhöhungsschreiben) angestrebt und insoweit der datenschutzrechtliche Auskunftsanspruch rechtsmissbräuchlich instrumentalisiert. Ein solcher (erneuter) Abschriftenanspruch, der sich nicht nach dem Datenschutzrecht, sondern nach den maßgeblichen zivil- bzw. versicherungsvertragsrechtlichen Normen richtet, existiert indes grundsätzlich nicht. Zuletzt hat der Bundesgerichtshof mit Urteil vom 27. September 2023 (Az.: IV ZR 177/22) ausdrücklich entschieden, dass dem Versicherungsnehmer ein Anspruch auf Abschriften zu zurückliegenden Prämienanpassungen allenfalls dann aus Treu und Glauben (§ 242 BGB) zusteht, wenn unter Berücksichtigung der jeweiligen Umstände des Einzelfalls in entschuldbarer Weise eine Unkenntnis über Bestehen und Umfang des Rechts aus dem Versicherungsvertrag besteht. Einen Anspruch auf Abschriften der Begründungsschreiben zu

den Prämienanpassungen samt Anlagen aus Art. 15 Abs. 1 und 3 DSGVO hat der BGH hingegen klar verneint. Insofern zeigt sich, dass gerade der seitens der Bundesratsausschüsse gesehene Zusammenhang zwischen dem datenschutzrechtlichen Auskunftsrecht und strukturellen Beweislastproblemen im Bereich der Privaten Kranken- und Pflegeversicherung regelmäßig nicht durchgreift.

Soweit es nicht die vorgenannten Konstellationen, sondern die datenschutzrechtlich anerkannte Einschränkung des Auskunftsanspruchs in Fällen der berechtigten Berufung des Verantwortlichen auf Betriebs- und Geschäftsgeheimnisse im engeren Sinne betrifft, würde die im Gesetzentwurf vorgesehene Regelung hingegen zu einer wünschenswerten Klarstellung auch für die Verbraucher führen.

Zu Art. 1 Nr. 14 (§ 37a BDSG-RegE – Erstellung und Verwendung von Scoring-Werten)

Vorgeschlagene Regelung
§ 37a BDSG-RegE soll den bisherigen § 31 BDSG in eine neue Ausnahmeregelung vom Verbot des Art. 22 Abs. 1 DSGVO überführen und um weitere Bestimmungen zur angemessenen Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person gemäß Art. 22 Abs. 2 lit. b DSGVO ergänzen. Absatz 1 der vorgeschlagenen Regelung soll unter Bezugnahme auf Art. 22 Abs. 1 und 2 lit. b DSGVO regeln, unter welchen Bedingungen Ausnahmen von dem Recht bestehen, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Die Ausnahme des § 37a Abs. 1 Nr. 1 BDSG-RegE betrifft die Erstellung und Verwendung von Wahrscheinlichkeitswerten über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses. Die (gegenüber dem bisherigen § 31 BDSG ergänzten) Bedingungen, unter denen die Ausnahme greift, sollen in § 37a Abs. 2 BDSG-RegE geregelt werden. Nicht erlaubt sein soll nach der Neuregelung u. a. die Nutzung von Gesundheitsdaten für die Erstellung von Wahrscheinlichkeitswerten (§ 37a Abs. 2 Nr. 1 lit. a BDSG-RegE) und die genutzten personenbezogenen Daten sollen für keine anderen Zwecke verarbeitet werden dürfen (§ 37a Abs. 2 Nr. 3 lit. b BDSG-RegE).

Bewertung
Die in § 37a Abs. 1 BDSG-RegE vorgesehene neue Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO kann für Versicherungsunternehmen zum einen als Verwender von Scorewerten relevant sein, die sie von Auskunfteien erhalten. § 37a Abs. 1 Nr. 1 BDSG-RegE kann aber auch einschlägig sein, wenn ein Versicherungsunternehmen selbst mit bereits vorliegenden Daten Wahrscheinlichkeitswerte errechnet.

Private Kranken- und Pflegeversicherer benötigen Score-(Wahrscheinlichkeits-)Werte nicht nur in Gestalt klassischer Wirtschaftsauskünfte zur Bonitätsprüfung. Wahrscheinlichkeitswerte werden in vielen Bereichen entlang der gesamten Kundenbeziehung benötigt, bspw. prozesstechnisch für die Gestaltung effizienter Sachbearbeitungsprozesse im Massenverfahren Leistungsbearbeitung (z. B. Prüfung und Abrechnung von Rechnungstellungen der Leistungserbringer), für das Angebot und die Durchführung von Gesundheitsmanagementprogrammen und künftig auch verstärkt im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz.

Das in § 37a Abs. 2 Nr. 1 BDSG-RegE vorgesehene Verbot der Ermittlung von Score-Werten u. a. auf der Basis von Gesundheitsdaten geht über die Vorgabe von Art. 22 Abs. 4 DSGVO hinaus und konterkariert die vom Gesetzgeber beabsichtigte Ausnahmeregelung in § 37a Abs. 1 Nr. 1 BDSG-RegE durch die Schaffung nicht gerechtfertigter Restriktionen zum Nachteil der Unternehmen der privaten Kranken- und Pflegeversicherung. Zudem ist die vorgesehene Neuregelung bereits dahingehend auslegungsbedürftig, was konkret unter einem „bestimmten zukünftigen Verhalten der Person" zum Zweck der Entscheidung über die „Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person" zu verstehen ist (bspw. sind Erkrankungen häufig auch auf Lebens- bzw. Verhaltensweisen zurückzuführen). Dies schafft unnötig neue Rechtsunsicherheiten für die Private Kranken- und Pflegeversicherung, die sich u. a. auf wesentliche automatisierte Bestandsprozesse der Versicherer auswirken können.

Zudem ist die in § 37a Abs. 2 Nr. 3 lit. b BDSG-RegE vorgesehene Restriktion, dass die genutzten personenbezogenen Daten für keine anderen Zwecke verarbeitet werden dürfen, für PKV-Unternehmen nicht einzuhalten, die mit eigenen Daten Wahrscheinlichkeitswerte errechnen. Wenn ein Versicherungsunternehmen einen eigenen Wahrscheinlichkeitswert errechnet, geschieht dies grds. immer mit Daten, die bereits vorher zu einem anderen Zweck verarbeitet wurden und auch nachfolgend noch zu anderen Zwecken dienen können. Da sich eine Zweckbindung bereits aus Art. 6 Abs. 4 DSGVO ergibt, ist die vorgesehene Regelung nicht erforderlich.

Es ist deshalb gesetzlich sicherzustellen, dass den Unternehmen der Privaten Kranken- und Pflegeversicherung die rechtssichere Erstellung und Nutzung von Wahrscheinlichkeitswerten unter Verwendung von Gesundheitsdaten in den durch Art. 22 Abs. 4 DSGVO vorgegebenen Grenzen möglich bleibt.

III. Weiterer Regelungsbedarf

§ 22 BDSG – Klarstellung der Berechtigung der PKV, (Gesundheits-)Daten der Versicherten für das Angebot und die Durchführung von Gesundheitsmanagementprogrammen zu verarbeiten

Aktuelle Gesetzeslage

Sowohl im internationalen Kontext als auch auf nationaler Ebene, zuletzt im Koalitionsvertrag der aktuellen Bundesregierung, wird die Sinnhaftigkeit und der Nutzen von Gesundheitsförderungs- und Präventionsmaßnahmen als wichtige Bausteine für ein gesundes Leben betont und der Ausbau entsprechender Angebote allgemein angeregt bzw. empfohlen.

Der Gesetzgeber hat der PKV bereits in dem Gesetz zur Reform des Versicherungsvertragsrechts das Leitbild zugrunde gelegt, dass diese nicht mehr auf die reine Kostenerstattung fokussiert ist, sondern als moderner Gesundheitsmanager neue Formen und Methoden zur wirksamen Kostensteuerung bei gleichzeitigem Erhalt bzw. Steigerung der medizinischen Behandlungsqualität anwendet. Als Beispiel nennt die Gesetzesbegründung u. a. ausdrücklich das „Disease Management", das auch Gesundheitsmanagement- und Vorsorgeangebote umfasst (vgl. u. a. BT-Drs. 16/3945, S. 55).

Angebote der PKV im Bereich des Gesundheitsmanagements zur Gewährleistung einer hochwertigen medizinischen Versorgung im Sinne der Versicherten erfordern eine korrespondierende Datenverarbeitungsbefugnis der Versicherer. Maßstab und Grenzen bestimmen insoweit die allgemeinen Grundsätze des Art. 9 Abs. 2 lit. h DSGVO i. V. m. § 22 Abs. 1 Nr. 1 lit. b BDSG.

Allerdings können die Unternehmen der privaten Krankenversicherung u. a. aufgrund der Auslegungsbedürftigkeit des § 22 BDSG nicht hinreichend sicher davon ausgehen, dass einzelne (Landes-)Datenschutzaufsichtsbehörden nicht zu (unzutreffenden) abweichenden Auslegungsergebnissen gelangen und z. B. Analysen von Rechnungsdaten für die Unterbreitung individueller Angebote des Gesundheitsmanagements ohne die vorherige Einholung einer entsprechenden ausdrücklichen Einwilligung der Privatversicherten als unzulässig erachten. Diese für die PKV unbefriedigende Situation wird dadurch verschärft, dass der Gesetzgeber entsprechende Datenverarbeitungsbefugnisse der GKV für Gesundheitsmanagementprogramme ausdrücklich festgelegt hat. Nach § 284 Abs. 1 Nr. 14, Abs. 3 S. 1 SGB V ist den gesetzlichen Krankenkassen die Erhebung und Speicherung von Daten zur Gewinnung von Versicherten für die Vorbereitung und Durchführung von Gesundheitsmanagementprogrammen ausdrücklich gestattet. Den gesetzlichen Krankenkassen wird damit u. a. die Möglichkeit eingeräumt, versichertenbezogene Daten zur Identifizierung chronisch Erkrankter auszuwerten (z. B. aus Abrechnungsunterlagen), u. a. um diese in strukturierte Behandlungsprogramme einbinden bzw. entsprechende Gesundheitsförderungsvorschläge unterbreiten zu können.

Der Fokus des Gesetzgebers, klar normierte Datenverarbeitungsbefugnisse zu schaffen, zeigt sich aktuell auch in dem jüngst verabschiedeten Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG). Danach wird den gesetzlichen Kranken- und Pflegekassen unter § 25b SGB V (neu) ausdrücklich die Befugnis eingeräumt, datengestützte Auswertungen zum individuellen Gesundheitsschutz ihrer Versicherten vorzunehmen und insoweit ihre Versicherten individuell anzusprechen. Hierzu werden die gesetzlichen Kranken- und Pflegekassen befugt, die bei ihnen vorliegenden personenbezogenen Daten der Versicherten ohne deren Einwilligung automatisiert zu verarbeiten, soweit dies zur Erkennung von potenziell schwerwiegenden gesundheitlichen Risiken der Versicherten erforderlich und geeignet ist. Die Versicherten können dieser Datenverarbeitung widersprechen.

Auch den Privaten Kranken- und Pflegeversicherern liegen vielfältige versichertenindividuelle Daten vor, in denen umfangreiche Informationen über medizinisch und pflegerisch relevante Sachverhalte enthalten sind. Diese Daten können und sollten ebenfalls zur Erkennung und Vermeidung von potenziell schwerwiegenden gesundheitlichen Risiken genutzt werden. Es ist nicht ersichtlich, weshalb Privatversicherte nicht im gleichen Umfang Zugang zum individuellen Gesundheitsschutz und -management wie GKV-Versicherten haben sollten.

Daher ist sicherzustellen, dass für die PKV ausreichend klare Datenverarbeitungsbefugnisse für Gesundheitsdaten im Rahmen von Gesundheitsmanagementangeboten wie für die GKV bestehen. Faktischen Restriktionen infolge von Rechtsunsicherheiten durch unterschiedliche Auslegungen der für die PKV maßgeblichen datenschutzrechtlichen Erlaubnisnormen im deutschen Recht sollte durch gesetzliche Klarstellungen begegnet werden. Um die Durchführung individueller Gesundheitsförderungs- und Präventionsprogramme für alle Privatversicherten rechtssicher zu ermöglichen, sollte

§ 22 BDSG als datenschutzrechtliche Erlaubnisnorm unter Abs. 1 Nr. 1 lit. b wie folgt klarstellend ergänzt werden:

> ***§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten***
> *(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig*
> *1. durch öffentliche und nichtöffentliche Stellen, wenn sie*
> *(…)*
> *b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, für die Erkennung von Gesundheitsrisiken sowie darauf aufbauend das Angebot und die Durchführung von Gesundheitsmanagementprogrammen durch Unternehmen der privaten Krankenversicherung oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, (…)*

§ 26 BDSG – Klarstellung, dass die Verarbeitung von Beschäftigtendaten für die Begründung und Verwaltung von betrieblichen Kranken- und Pflegeversicherungsversicherungsverhältnissen zu Gunsten der Beschäftigten zulässig ist

<u>Aktuelle Gesetzeslage</u>
Betriebliche Kranken- und Pflegeversicherungsversicherungsprodukte stellen eine sinnvolle Ergänzung des bestehenden Gesundheitsschutzes dar und erfreuen sich sowohl bei Arbeitgebern als auch bei den Beschäftigten sehr großer Beliebtheit.

Bei den Landesdatenschutzaufsichtsbehörden bestehen jedoch – vergleichbar der vorstehend geschilderten Situation bei Gesundheitsmanagementprogrammen – teilweise unterschiedliche Rechtsauffassungen dahingehend, ob im Rahmen von betrieblichen Kranken- und Pflegeversicherungsangeboten Beschäftigtendaten für die Begründung und Verwaltung von Versicherungsverhältnissen genutzt bzw. verarbeitet werden dürfen. Zur Umsetzung des dbzgl. (Gruppen-)Vertrages zwischen dem Arbeitgeber, der seine Mitarbeiter entsprechend informiert, und dem Versicherer müssen dabei üblicherweise Beschäftigtendaten (insb. Name und Adressdaten) an das Versicherungsunternehmen weitergegeben werden, um dem Versicherer insbesondere die Identifizierung der versicherten Personen ermöglichen und deren Berechtigung zur Inanspruchnahme von betreffenden Versicherungsleistungen ermitteln zu können.

§ 26 BDSG sollte dahingehend klargestellt werden, dass die Verarbeitung von Beschäftigtendaten für die Begründung und Verwaltung von betrieblichen Kranken- und Pflegeversicherungsverhältnissen zu Gunsten der Beschäftigten zulässig ist.

Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

DEUTSCHER STEUERBERATER-VERBAND e.V.

WIRTSCHAFTSPRÜFERKAMMER
Körperschaft des öffentlichen Rechts

BUNDESRECHTSANWALTSKAMMER

Deutscher Bundestag
Herrn Prof. Dr. Lars Castellucci
stellv. Vorsitzender des
Ausschusses für Inneres und Heimatschutz
Platz der Republik 1
11011 Berlin

E-Mail: innenausschuss@bundestag.de

Unser Zeichen: Li/Ft
Tel.: +49 30 240087-81
Fax: +49 30 240087-77
E-Mail: praesident@bstbk.de

8. Mai 2024

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Drs. 20/10859 - 168. Sitzung des Deutschen Bundestages

Sehr geehrter Herr Prof. Dr. Castellucci,
sehr geehrte Ausschussmitglieder,

im Vorfeld der anstehenden ersten Beratung des o. g. Gesetzes im Bundestag am 15. Mai 2024 fordern wir eine weitere sachgerechte Beschränkung der Betroffenenrechte.

Wir begrüßen grundsätzlich, dass der vorliegende Regierungsentwurf von der in der DSGVO enthaltenen nationalen Öffnungsklausel Gebrauch macht und eine interessengerechte Einschränkung des Auskunftsanspruchs in § 34 BDSG vorsieht.

Wir halten eine weitere interessengerechte Beschränkung der Betroffenenrechte nach Art. 15 und Art. 20 DSGVO zugunsten des nationalen Berufsrechts der von uns vertretenen Berufsträger (Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, vereidigte Buchprüfer) für erforderlich. Andernfalls droht das gesetzlich geregelte berufsrechtliche Zurückbehaltungsrecht (§ 66 Abs. 3 StBerG, § 50 Abs. 3 BRAO bzw. § 51b Abs. 3 WPO) ins Leere zu laufen. Aktuell besteht sowohl in der Rechtsprechung als auch in der Berufspraxis diesbezüglich eine große Rechtsunsicherheit.

Entsprechende Lösungsvorschläge und weitere Erläuterungen finden Sie in der anliegenden gemeinsamen Stellungnahme.

Mit freundlichen Grüßen

[redacted]	[redacted]	[redacted]	[redacted]
Prof. Dr. Hartmut Schwab Präsident BStBK	Torsten Lüth Präsident DStV e.V.	Andreas Dörschell Präsident WPK	Dr. Ulrich Wessels Präsident BRAK

Anlage

Bundessteuerberaterkammer
K.d.ö.R.
Behrenstraße 42, 10117 Berlin
Telefon: 030 240087-0
Telefax: 030 240087-99

Deutscher Steuerberaterverband e.V.
Haus der Verbände
Littenstraße 10, 10179 Berlin
Telefon: 030 27876-2
Telefax: 030 27876-799

Wirtschaftsprüferkammer
K.d.ö.R.
Rauchstraße 26, 10787 Berlin
Telefon: 030 726161-0
Telefax: 030 726161-212

Bundesrechtsanwaltskammer
K.d.ö.R.
Littenstraße 9, 10179 Berlin
Telefon: 030 284939-0
Telefax: 030 284939-11

Anlage

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Bundestag Drucksache 20/10859

1. Beschränkung des Auskunftsanspruchs (Art. 15 DSGVO) zugunsten des zivilrechtlichen Zurückbehaltungsrechts

Art. 23 Abs. 1 der DSGVO regelt eine nationale Öffnungsklausel und erlaubt dem nationalen Gesetzgeber eine Einschränkung der Betroffenenrechte der DSGVO, nicht nur zum Schutz der Rechte und Freiheiten anderer Personen, sondern nach Buchstabe j auch zur Durchsetzung zivilrechtlicher Ansprüche.

§ 34 Abs. 1 BDSG enthält bereits heute entsprechende Regelungen zur Beschränkung des Auskunftsanspruchs nach Art. 15 DSGVO. Auch in weiteren Vorschriften des BDSG hat der Gesetzgeber von den Öffnungsklauseln Gebrauch gemacht, z. B. in §§ 29, 32, 33 BDSG.

Mit der Ergänzung des § 34 Abs. 1 BDSG (vgl. Art. 1 Ziff. 12 des Entwurfs eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes [BDSG-ÄndG]) hinsichtlich der Einschränkung des Auskunftsrechts des Betroffenen zum Schutze von Betriebs- oder Geschäftsgeheimnissen ist bereits eine wichtige Anpassung der Beschränkungen des Auskunftsanspruchs nach Art. 15 DSGVO geplant.

Wir halten es darüber hinausfür dringend erforderlich, dass das Auskunftsrecht nach Art. 15 DSGVO über § 34 BDSG eine weitere Einschränkung erfährt. Vergleichbar den in § 33 Abs. 1 Ziff. 2 Buchst. a) BDSG geregelten Einschränkungen der Informationspflichten nach Art. 14 DSGVO sollte auch das Auskunftsrecht des Art. 15 DSGVO über § 34 BDSG zur Durchsetzung zivilrechtlicher Ansprüche eingeschränkt werden.

Ohne eine solche Regelung besteht regelmäßig die Gefahr, dass Gerichte – wie bereits ergangene Entscheidungen zeigen – auch dem missbräuchlichen Auskunftsanspruch gem.

Bundessteuerberaterkammer
K.d.ö.R.
Behrenstraße 42, 10117 Berlin
Telefon: 030 240087-0
Telefax: 030 240087-99

Deutscher Steuerberaterverband e.V.
Haus der Verbände
Littenstraße 10, 10179 Berlin
Telefon: 030 27876-2
Telefax: 030 27876-799

Wirtschaftsprüferkammer
K.d.ö.R.
Rauchstraße 26, 10787 Berlin
Telefon: 030 726161-0
Telefax: 030 726161-212

Bundesrechtsanwaltskammer
K.d.ö.R.
Littenstraße 9, 10179 Berlin
Telefon: 030 284939-0
Telefax: 030 284939-11

Art. 15 DSGVO stattgeben, was zur faktischen Aushöhlung des zivilrechtlichen Zurückbehaltungsrechts führt.

Das Zurückbehaltungsrecht des Steuerberaters gem. § 66 Abs. 3 StBerG, des Rechtsanwalts gem. § 50 Abs. 3 BRAO bzw. des Wirtschaftsprüfers/vereidigten Buchprüfers gem. § 51b Abs. 3 WPO wird in der Rechtsprechung auf § 273 bzw. § 320 BGB gestützt und stellt damit einen zivilrechtlichen Anspruch dar (vgl. OLG Düsseldorf, Urteil vom 11. September 2018, Az. 23 U 155/17).

Nach § 66 Abs. 2 StBerG, § 50 Abs. 2 BRAO bzw. § 51b WPO hat der Mandant grundsätzlich einen Anspruch auf Herausgabe der Handakte. In § 66 Abs. 3 StBerG, § 50 Abs. 3 BRAO bzw. § 51b Abs. 3 WPO ist für den Fall, dass offene Vergütungsansprüche des Berufsträgers existieren, ein Zurückbehaltungsrecht normiert. Dieses ist insbesondere im Falle der Mandatsbeendigung von praktischer Bedeutung und soll Berufsträger insbesondere für solche Fälle absichern, in denen sie ihre Mandantschaft in Krisenlagen beraten bzw. vertreten.

Demgegenüber regelt Art. 15 Abs. 1 DSGVO einen datenschutzrechtlichen Anspruch des Betroffenen über sämtliche von ihm gespeicherten persönlichen Daten. Nach Art. 15 Abs. 3 DSGVO hat der Betroffene in der Regel sogar einen Anspruch auf die Herausgabe einer vollständigen (Daten-)Kopie. Im Zeitalter der Digitalisierung ist diese (Daten-)Kopie faktisch deckungsgleich mit der Handakte. Art. 15 Abs. 4 DSGVO beschränkt den Anspruch auf Herausgabe einer (Daten-)Kopie lediglich für den Fall, dass hierdurch die Rechte und Freiheiten anderer (dritter) Personen beeinträchtigt werden.

Somit besteht zwar grundsätzlich die Möglichkeit, die (Original-)Handakte wegen zivilrechtlicher Ansprüche zurückzubehalten, über das Auskunftsrecht nach Art. 15 DSGVO müsste dann aber ggf. eine Kopie der Handakte herausgegeben werden, sodass das zivilrechtliche Zurückbehaltungsrecht ins Leere läuft.

Das Verhältnis zwischen datenschutzrechtlichem Auskunftsanspruch und zivilrechtlichem Zurückbehaltungsrecht wird in der Instanz-Rechtsprechung und Literatur unterschiedlich beantwortet. Eine klare gesetzliche Regelung existiert bisher ebenso wenig wie höchstrichterliche Rechtsprechung.

Es ist zur Schaffung von Rechtssicherheit bei der Gesetzesanwendung und -auslegung und zur Verhinderung des Aushebelns des zivilrechtlichen Zurückbehaltungsrechts, insbesondere der geschützten Berufsträger (u. a. Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, vereidigte Buchprüfer), auf der Grundlage der bestehenden nationalen Öffnungsklausel eine entsprechende Beschränkung des Auskunftsrechts nach Art. 15 DSGVO vorzunehmen und in § 34 BDSG zu ergänzen.

Vergleichbar den in § 33 Abs. 1 Nr. 2 Buchst. a) BDSG geregelten Einschränkungen der Informationspflichten nach Art. 14 DSGVO sollte auch das Auskunftsrecht des Art. 15 DSGVO über § 34 BDSG zur Durchsetzung zivilrechtlicher Ansprüche eingeschränkt werden.

Dies könnte beispielhaft wie folgt umgesetzt werden:

> *§ 34 Abs. 1 Nr. 3-neu BDSG-E*
>
> *(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn*
>
> *(…)*
>
> ***3. dies die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt,***
>
> *(…)*

Da die vorstehende Regelung eine einzelfallbezogene Interessenabwägung vorsieht, wäre mit einer solchen Regelung sowohl der Schutz der Betroffenenrechte in erforderlichem Maß als auch das zivilrechtliche Zurückbehaltungsrecht gesichert.

2. Weitere Beschränkung des Auskunftsanspruchs (Art. 15 DSGVO) zugunsten der berufsrechtlichen Verschwiegenheitspflicht

Auch zugunsten der Verschwiegenheitsverpflichtung der Berufsträger (u. a. Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, vereidigte Buchprüfer) ist eine Beschränkung des Auskunftsanspruchs nach Art. 15 DSGVO erforderlich.

Dies betrifft insbesondere die Fallkonstellationen, in denen ein getrenntlebender Ehegatte Auskunfts- bzw. Herausgabeansprüche nach Art. 15 DSGVO aus der Zeit der gemeinsamen steuerlichen Veranlagung geltend macht, sowie entsprechende Begehren von KG-Gesellschaftern, bei denen die KG steuerlich oder rechtlich beraten wird.

Nach Erwägungsgrund 63 DSGVO soll das Auskunftsrecht aus Art. 15 DSGVO dem Betroffenen dazu dienen, sich der Verarbeitung der personenbezogenen Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Die Auskünfte dienen auch zur Wahrnehmung weiterer Rechte nach Art. 16, 17 und 18 DSGVO. Wenn jedoch keine der in Erwägungsgrund 63 DSGVO genannten Interessen verfolgt werden, sondern die Daten offensichtlich allein zur Verfolgung unterhaltsrechtlicher Ansprüche in Familiensachen dienen, muss auch ein Steuerberater, Rechtsanwalt oder Wirtschaftsprüfer bzw. vereidigter Buchprüfer den Umfang des Auskunftsanspruchs nach Art. 15 DSGVO einschränken können.

Auch hierzu gibt es keine gefestigte Rechtsprechung. Teilweise wird vertreten, dass ein steuerlicher Vertreter von der Verschwiegenheitspflicht für die Veranlagungsjahre der gemeinsamen Beauftragung auch nach der Trennung der Ehegatten bzw. der KG-Gesellschafter entbunden ist. Andererseits darf der Auskunftsanspruch aber auch nur so weit gehen, dass die Rechte Dritter nicht beeinträchtigt werden. Das kann im Ergebnis zu der Tendenz führen, dass in der Instanzenrechtsprechung die Entbindung von der Verschwiegenheitspflicht bei der Geltendmachung des Auskunftsanspruchs nach Art. 15 DSGVO regelmäßig angenommen wird, bei der Herausgabe der Unterlagen nach § 66 StBerG, § 50 BRAO bzw. § 51b WPO hingegen verneint wird. Daher ist auch insoweit eine ausdrückliche Regelung in § 34 BDSG erforderlich – ggf. unter Verwendung der Kriterien in Erwägungsgrund 63 zur DSGVO.

3. Beschränkung des Rechts auf Datenübertragbarkeit (Art. 20 DSGVO) zugunsten des zivilrechtlichen Zurückbehaltungsrechts

Des Weiteren besteht für die Berufsträger (u. a. Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, vereidigte Buchprüfer) in der Praxis auch regelmäßig ein Problem hinsichtlich der Anwendbarkeit des Art. 20 DSGVO (Anspruch auf Datenübertragung) und dessen Verhältnis zum Zurückbehaltungsrecht (§ 66 Abs. 3 StBerG für Steuerberater, § 50 Abs. 3 BRAO für Rechtsanwälte und § 51b Abs. 3 WPO für Wirtschaftsprüfer und vereidigte Buchprüfer).

So fordern Mandanten regelmäßig ihren Steuerberater, Rechtsanwalt oder Wirtschaftsprüfer/vereidigten Buchprüfer nach Mandatsbeendigung zur vollständigen Übertragung ihrer Mandatsdaten auf und berufen sich hierzu auf Art. 20 DSGVO.

Nach unserer Auffassung ergibt sich aus Art. 20 DSGVO regelmäßig keine rechtliche Grundlage für die Datenübertragung aller verlangten Mandatsdaten.

So hat gem. Art. 20 DSGVO die betroffene Person das Recht auf Datenübertragbarkeit solcher personenbezogenen Daten, die die betroffene Person dem Verantwortlichen bereitgestellt hat. Hierzu zählen hingegen solche Daten nicht, die der Verantwortliche, ggf. auch unter Verwendung erfasster oder direkt eingegebener Daten, erzeugt oder verarbeitet hat. Zu den Arbeitsergebnissen zählen insbesondere Steuererklärungen, Jahresabschlüsse, Buchführung, Lohnbuchführung.

Diese vertraglich geschuldeten Arbeitsergebnisse sind auch nicht „erlangt“ i. S. d. §§ 675 Abs. 1, 667 2. Alt. BGB, sondern Gegenstand des vertraglichen Erfüllungsanspruchs. An diesen Daten steht dem Steuerberater, Rechtsanwalt oder Wirtschaftsprüfer/vereidigten Buchprüfer wegen des synallagmatischen Zusammenhangs mit dem Honoraranspruch ein Zurückbehaltungsrecht gem. § 273 BGB zu.

Abgesehen davon, dass Arbeitsergebnisse schon vom Wortlaut des Art. 20 DSGVO nicht erfasst sind, wird der Anspruch nach Art. 20 Abs. 1 DSGVO durch Art. 20 Abs. 4 DSGVO beschränkt, nach welchem das Recht auf Datenübertragbarkeit keineswegs Rechte und Freiheiten anderer Personen beinträchtigen darf. Hierzu zählt zusätzlich zu den Geschäftsgeheimnissen und dem Recht auf geistiges Eigentum auch das Zurückbehaltungsrecht des

Steuerberaters, Rechtsanwalts oder Wirtschaftsprüfers/vereidigten Buchprüfers gegenüber seinem Mandanten nach §§ 675, 273 Abs. 1 BGB.

Seitens der Datenschutzbehörden wird demgegenüber teilweise dem Recht auf Datenübertragbarkeit nach Art. 20 DSGVO der Vorrang gegeben, da es sich hierbei um Unionsrecht handelt und der deutsche Gesetzgeber von der in Art. 23 DSGVO vorgesehenen nationalen Öffnungsklausel in Bezug auf Art. 20 DSGVO bisher keinen Gebrauch gemacht hat.

§ 29 Abs. 1 BDSG sieht für Berufsgeheimnisträger nur Ausnahmereglungen zu den Auskunfts- und Informationspflichten (Art. 13 ff. DSGVO) vor.

Aus unserer Sicht ist daher zur Schaffung der Rechtssicherheit und zur Absicherung der bestehenden nationalen berufsrechtlichen Regelungen der Berufsgeheimnisträger und des Zurückbehaltungsrechts eine Klarstellung im BDSG erforderlich.

Innenausschuss Postfachaccount PA4

Von:	Lasmar, Anne (DAV) <lasmar@anwaltverein.de> im Auftrag von Narewski, Nicole (DAV) <Narewski@anwaltverein.de>
Gesendet:	Montag, 22. April 2024 17:24
An:	Lasmar, Anne (DAV)
Betreff:	DAV-Stellungnahme Nr. 24/2024 zur Neuregelung des Scoring im Gesetzesentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes
Anlagen:	DAV SN_24-2024.pdf

DeutscherAnwaltVerein

DAV-Stellungnahme Nr. 24/2024 zum Gesetzesentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes; § 37a BDSG-E

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen die Stellungnahme Nr. 24/2024 des Deutschen Anwaltvereins (DAV) durch den Ausschuss Informationsrecht zum Entwurf einer neuen Regelung über auf einer automatisierten Verarbeitung personenbezogener Daten beruhenden Entscheidungen gegenüber Betroffenen (Ersetzung des bisherigen § 31 durch § 37a BDSG) im Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes, Stand 31.01.2024, und zu der Stellungnahme des Bundesrats vom 22.03.2024.

Der DAV begrüßt, dass die Bundesregierung rasch auf die Entscheidung des EuGH zur Verwendung von Scoring-Werten der SCHUFA bei der Kreditvergabe (Urt. v. 7.12.2023 – C-634/21) reagieren möchte. Er stimmt an vielen Punkten mit den Regelungsansätzen überein, hat jedoch verschiedentlich konkrete Formulierungsvorschläge zur Klarstellung einzelner Aspekte. Beispielsweise regt er die Aufnahme eines festen Fristbeginns bei der Speicherpflicht der Wahrscheinlichkeitswerte an.

Die in § 37a Abs. 3 Nr.2 BDSG-E vorgesehene Regelung, nach der personenbezogene Daten, die für das Scoring verwendet werden, nicht für andere Zwecke verarbeitet werden dürfen, sollte vollständig gestrichen werden, da dies von der DSGVO so nicht für die Regelung innerhalb der Mitgliedsländer vorgesehen ist. Darüber hinaus sieht der DAV Normkonflikte mit der DSGVO bei der neu vorgesehenen Mitteilungspflicht, da das Verhältnis zu den Art.13-15 DSGVO und der weitergehende mögliche Regelungsinhalt unklar bleiben.

An seiner Forderung, erweiterte Befugnisse der DSK in einem Staatsvertrag zu regeln, hält der DAV fest.

Für weitere Details verweise ich Sie auf die im Anhang beigefügte Stellungnahme.

Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Mit freundlichen Grüßen

Nicole Narewski
Geschäftsführerin

_____

Deutscher Anwaltverein
Nicole Narewski
Berufsrecht / Datenschutz / Elektronischer Rechtsverkehr /
IT-Recht / Kanzleimanagement /
Mediation / Medizinrecht / Zivilverfahrensrecht
Littenstraße 11, 10179 Berlin
Tel. +49 30 726152-128
narewski@anwaltverein.de
www.anwaltverein.de

LinkedIn | X | Bluesky | Facebook | YouTube

Jetzt anmelden zum Deutschen Anwaltstag 2024!

Virtuell: 03. – 05. Juni
In Bielefeld: 05. – 07. Juni

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Entwurf einer neuen Regelung über auf einer automatisierten Verarbeitung personenbezogener Daten beruhenden Entscheidungen gegenüber Betroffenen (Ersetzung des bisherigen § 31 durch § 37a BDSG) im Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes, Stand 31.01.2024, und zu der Stellungnahme des Bundesrats vom 22.03.2024.

Stellungnahme Nr.: 24/2024 Berlin, im April 2024

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof. Niko Härting, Berlin (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn (Berichterstatter)
- Rechtsanwältin Dr. Kristina Schreiber, Köln (Berichterstatterin)
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

I. Vorbemerkung

Der DAV begrüßt grundsätzlich die geplante Neuregelung der Bestimmungen zum Scoring im Bundesdatenschutzgesetz (BDSG), sieht allerdings an einigen Stellen Nachbesserungsbedarf. Die Erwägungen des Bundesrats in seiner Stellungnahme vom 22.03.2024 hält der DAV teilweise für nicht zutreffend.

1. Für nicht weitgehend genug hält der DAV die im BDSG geplanten Regelungen für die Datenschutzkonferenz (DSK). An seiner Forderung, erweiterte Befugnisse der DSK in einem Staatsvertrag zu regeln (siehe https://anwaltverein.de/de/newsroom/pm-30-23-dav-fordert-staatsvertrag-fuer-den-datenschutz), hält der DAV fest. Nur durch einen Staatsvertrag kann ein schlagkräftigeres Handeln der DSK und eine bessere Abstimmung der Datenschutzbehörden des Bundes und der Länder erreicht werden.

2. Die Bundesregierung möchte rasch auf die Entscheidung des EuGH zur Verwendung von Scoring-Werten der SCHUFA bei der Kreditvergabe (Urt. v. 7.12.2023 – C-634/21) reagieren. Dies erscheint vorausschauend und sinnvoll. Der bisherige § 31 BDSG soll durch einen neuen § 37a BDSG ersetzt werden. Die Norm soll den Konflikt zwischen der Kreditwirtschaft und Verbrauchern ausgleichen im Interesse einer transparenten und nachvollziehbaren Entscheidung über die Kreditvergabe unter Berücksichtigung europarechtlich durch die Richtlinie 2008/48/EG v. 23.4.2008 vorgegebenen Prüfverpflichtungen der Kreditwirtschaft. Entsprechendes gilt für Unternehmen

aus anderen Branchen wie Telekommunikationsanbietern, die vor Vertragsabschlüssen die Kreditwürdigkeit ihrer Kunden prüfen wollen.

3. Dass für die Berechnung der Wahrscheinlichkeitswerte nach der neuen Regelung besondere Kategorien personenbezogener Daten nicht verwendet werden dürfen (**§ 37a Abs. 2 Nr. 1 Buchst. a BDSG-E**) ist nachvollziehbar und zur Wahrung der Voraussetzungen des Art. 22 Abs. 2 Buchst. b DSGVO ebenso notwendig wie der Ausschluss der Berechnung von Wahrscheinlichkeitswerten für Minderjährige (**§ 37a Abs. 2 Nr. 2 BDSG-E**). Der Ausschluss von Daten, die durch Art. 9 DSGVO besonders geschützt sind, ergibt sich zwar weitgehend schon aus Erwägungsgrund 71 zur DSGVO. Es erscheint jedoch vertretbar, die Regelung des Art. 22 Abs. 4 DSGVO, der die Verwendung der besonderen Kategorien personenbezogener Daten zur automatisierten Entscheidungsfindung ohnehin schon weitgehend ausschließt, bei den hier speziell geregelten Fällen zu verschärfen.

4. Nicht neu ist die Voraussetzung, dass der Scorewert mit einem wissenschaftlich anerkannten mathematisch-statistischen Verfahren berechnet werden muss (**§ 37a Abs. 2 Nr. 3 Buchst. a BDSG-E**, bislang § 31 Abs. 1 Nr. 2 BDSG). Diese Voraussetzung ist auch eine zentrale Vorschrift zur Wahrung des europarechtlich vorgegebenen Rechtsrahmens (Erwägungsgrund 71 zur DSGVO). Forderungen aus dem politischen Raum, dass das Verfahren – anders als bislang – durch einen neutralen, nicht von der jeweiligen Auskunftei beauftragten Gutachter (bzw. eine Gutachterin) geprüft werden soll, sind diskutabel, dürften allerdings für die zuständigen Datenschutzbehörden mit erheblichem Mehraufwand verbunden sein, da nur sie als ein geeigneter Auftraggeber für solche Gutachten in Betracht kommen.

5. Skeptisch zu beurteilen ist die vom Bundesrat vorgeschlagene Einrichtung unabhängiger Prüfstellen für die Scorewerte. Eine solche Einrichtung müsste notwendigerweise von den Datenschutzbehörden begleitet und überwacht werden und dürfte deren begrenzte Kapazitäten überfordern.

II. Bezugnahme auf Art. 22 Abs. 2 Nr. 2 DSGVO

Zu begrüßen ist, dass die neu vorgeschlagene Norm in § 37a Abs. 1 BDSG-E durch ihren Wortlaut deutlich macht, dass es um eine weitere, über die in Art. 22 DSGVO unmittelbar vorgesehenen Ausnahmen hinausgehende Erlaubnis für eine automatisierte Entscheidung geht. Damit wird auch klar, dass der Gesetzgeber von der in Art. 22 Abs. 2 Buchst. b DSGVO eingeräumten Befugnis Gebrauch macht, solche Regelungen zu treffen. § 31 BDSG in der bisherigen Fassung war insoweit unklar. Der klare Bezug auf Art. 22 Abs. 2 Nr. 2 DSGVO in § 37a BDSG-E ist zu begrüßen.

III. Systemwidrige Regelung zur Datennutzung

Durch die Bezugnahme steht auch fest, dass § 37a BDSG-E nur die Verwendung aus vorhandenen Daten errechneter Wahrscheinlichkeitswerte für eine automatisierte Entscheidung regelt. Er ist – ebenso wie Art. 22 DSGVO – keine Rechtsgrundlage dafür, dass die für die Berechnung der Wahrscheinlichkeitswerte benötigten personenbezogenen Daten erhoben, gespeichert und genutzt werden dürfen. Ob dies der Fall ist, richtet sich nach Art. 6 DSGVO, insbesondere nach Art. 6 Abs. 1 S. 1 Buchst. f und Abs. 4 DSGVO. Die DSGVO sieht insoweit auch keine Möglichkeit zu einer einzelstaatlichen Regelung vor (Radtke, MMR 2024, 156 f.).

Die in § 37a Abs. 3 Nr.2 BDSG-E vorgesehene Regelung, nach der personenbezogene Daten, die für das Scoring verwendet werden, nicht für andere Zwecke verarbeitet werden dürfen, erscheint vor diesem Hintergrund systemwidrig. Dies gilt erst recht für die vom Bundesrat vorgeschlagenen Ergänzungen der Norm. Denn Art. 22 Abs. 2 Nr. 2 DSGVO lässt zwar Regelungen zu zur Befugnis automatisierter Entscheidungen, eröffnet den Mitgliedsstaaten jedoch keine weitergehenden Befugnisse, Erlaubnisse oder Verbote der Verarbeitung von Einzeldaten zu erlassen, die in das Scoring einfließen. Um Konflikte mit der DSGVO zu vermeiden, bedarf es einer Streichung des § 37a Abs. 3 Nr. 2 BDSG-E.

IV. Unklare Formulierungen

An einigen Stellen gibt es Verbesserungsbedarf.

1. **§ 37a Abs. 1 Nr. 2 BDSG-E** ist unklar formuliert, da offenbleibt, worauf sich der Halbsatz „und unter Einbeziehung von Informationen über Forderungen“ bezieht. Gemeint dürfte sein, dass es ausschließlich um von Auskunfteien erstellte Wahrscheinlichkeitswerte geht, bei deren Berechnung die Auskunfteien Informationen über Forderungen verwenden.

   Um dies deutlicher zum Ausdruck zu bringen, ließe sich formulieren:

   „ihre Zahlungsfähig- und -willigkeit, wenn dies durch Auskunfteien unter Einbeziehung von Informationen über Forderungen geschieht."

2. Neu ist das vollständige Verbot der Verwendung des Namens der betroffenen Person und von Anschriftendaten bei der Ermittlung der Wahrscheinlichkeitswerte in **§ 37a Abs. 2 Nr. 1 lit. d BDSG-E**. Das von der Bundesregierung in der Begründungangesprochene Diskriminierungsrisiko bei der Verwendung von Anschriftendaten ist nachvollziehbar, jedenfalls erscheint eine solche Regelung als zusätzliche Sicherung der Rechte und Interessen der Betroffenen vertretbar.

   Zu erwägen ist indes eine ergänzende Regelung, um klarzustellen, worauf sich das Verbot bezieht und worauf nicht:

   „Name und Anschrift der betroffenen Person dürfen nach Erstellung eines Wahrscheinlichkeitswerts mit diesem zur weiteren Verwendung verbunden werden.“

3. Ähnliches gilt auch für das Verbot der Nutzung von Daten aus sozialen Netzwerken (**§ 37a Abs. 2 Nr. 1 lit. b BDSG-E**) und von Informationen über Zahlungseingänge und -ausgänge und von Bankkonten (**§ 37a Abs. 2 Nr. 1 lit. c BDSG-E**). Zu § 37a Abs. 2 Nr. 1 lit. c BDSG-E heißt es in der Entwurfsbegründung, dass gesetzliche Regelungen, die die Erhebung solcher Daten vor der Kreditvergabe oder dem Vertragsschluss vorschreiben, unberührt bleiben. Für eine rechtssichere Anwendung sollte dies auch in der Regelung selbst klargestellt werden.

   So könnte § 37a Abs. 2 BDSG-E durch einen zweiten Halbsatz in Nr. 1 ergänzt werden, der lautet:

„dies gilt nicht, wenn und soweit die Verwendung der in Buchstabe a) bis d) genannten Daten gesetzlich erlaubt oder vorgeschrieben ist;“.

Durch eine solche Ergänzung würde sich der isolierte Vorschlag zu § 37a Abs. 2 Nr. 1 lit. d BDSG-E (s.o. IV. 2.) erübrigen.

4. Die in § 37a Abs. 3 BDSG-E vorgesehenen Einschränkungen entsprechen den bislang geltenden Regelungen in § 31 Abs. 1 BDSG. Sie sollen sicherstellen, dass Negativmerkmale nur dann verwendet werden, wenn Zahlungsverzögerungen und -ausfälle gesichert vorliegen. Dies ist wie bisher bei den in § 37a Abs. 3 Nr. 1 bis 4 BDSG-E geregelten Fällen gegeben. Anders ist dies bei **§ 37a Abs. 3 Nr. 5 BDSG-E**: Hier reicht der für eine Kündigung ausreichende Zahlungsrückstand nach dem Wortlaut des Entwurfs auch dann aus, wenn der Schuldner ihn bestreitet. Die in Nr. 4 der Vorschrift vorgesehene Voraussetzung, dass ein Zahlungsrückstand nur berücksichtigt wird, wenn der Schuldner die Forderung nicht bestritten hat, fehlt in Nr. 5. Sie sollte ergänzt werden:

   “deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann, ohne dass der Schuldner das Vorliegen des Kündigungsgrundes bestreitet, und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist.“

5. Im Grundsatz zu begrüßen ist die Regelung, nach der der Betroffene das Recht hat, seinen eigenen Standpunkt darzulegen und eine Entscheidung einer natürlichen Person zu verlangen (§ 37a Abs. 6 BDSG-E). Diese stellt sicher, dass die Voraussetzungen des Art. 22 Abs. 2 Nr. 2 DSGVO gewährleistet sind. Allerdings sollte eine Präzisierung nach dem Vorbild bekannter Beschwerdeverfahren erfolgen, etwa aus § 111a EnWG, um eine rechtssichere Handhabung zu gewährleisten:

   „Verantwortliche sind verpflichtet, Beanstandungen und Beschwerden von betroffenen Personen hinsichtlich der jeweiligen auf Wahrscheinlichkeitswerten nach Absatz 1 beruhenden

Entscheidung innerhalb einer Frist von vier Wochen ab Zugang beim Verantwortlichen zu beantworten und die Entscheidung einer natürlichen Person herbeizuführen. Wird der Beschwerde durch den Verantwortlichen nicht abgeholfen, hat der Verantwortliche die Gründe in Textform darzulegen. Der betroffenen Person steht es frei, hiergegen Beschwerde nach Art. 77 DSGVO einzulegen oder vor den ordentlichen Gerichten vorzugehen."

V. Normkonflikte mit Art. 13 bis 15 DSGVO

1. Probleme weist die in **§ 37a Abs. 4 BDSG-E** vorgesehene umfassende Mitteilungspflicht des für die Berechnung der Wahrscheinlichkeitswerte Verantwortlichen auf. Er muss u.a. Auskunft über „die Gewichtung von Kategorien von Kriterien und der einzelnen zueinander" geben, die „den Wahrscheinlichkeitswert am stärksten beeinflussen". Dem Verantwortlichen steht auch nicht die für die Auskunftsplicht in **§ 34 BDSG-E** neu geplante Ausnahme zum Schutz seiner Geschäftsgeheimnisse zu, nach der eine Auskunft nicht zu erteilen ist, wenn das Geheimhaltungsinteresse überwiegt.

   Die Mitteilungspflicht geht weit über die bisher vom BGH (Urt. v. 28.1.2014 – VI ZR 156/13) geregelten Auskunftspflichten hinaus und erscheint im Interesse eines transparenten Verbraucherschutzes grundsätzlich vertretbar, führt jedoch zu möglichen Regelungskonflikten mit der DSGVO. Denn es ist unklar, in welchem Verhältnis die Mitteilungspflicht zu den nach Art. 13 Abs. 2 lit. f, 14 Abs. 2 Buchst. g und Art. 15 Abs. 1 lit. h DSGVO bestehenden Informations- und Auskunftspflichten bei automatisierter Entscheidungsfindung steht. Inhaltlich handelt es sich um eine Auskunftspflicht. Die Informationspflichten bleiben damit zwar unberührt. Ob aber die in § 37a Abs. 4 BDSG-E bestehende Mitteilungspflicht inhaltlich weiter geht als die – ja weiterhin bestehende – Auskunftspflicht nach Art. 15 Abs. 1 Buchst. h DSGVO, ist unklar und hängt von der Auslegung der beiden Normen ab. Auf solche Normkonflikte sollte verzichtet werden, selbst wenn sie – was angesichts der Konfliktsituation zweifelhaft ist - europarechtlich zulässig sein sollten.

2. Der DAV teilt die Bedenken des Bundesrats gegen **§ 34 Abs. 1 Satz 2 BDSG-E** und den dort vorgesehenen Ausschluss des Auskunftsrechts bei einem überwiegenden Schutz von Betriebs- und Geschäftsgeheimnissen nicht. Das vom Bundesrat angesprochene „strukturelle Beweislastproblem“ sollte nicht im BDSG unter datenschutzrechtlichen Gesichtspunkten, sondern im jeweiligen Sachzusammenhang – etwa im Versicherungsrecht – gelöst werden.

3. Wird keine eigenständige Auskunfts- bzw. Mitteilungspflicht in § 37a Abs. 4 BDSG-E vorgesehen, kann auch auf **§ 37a Abs. 5 BDSG-E** verzichtet werden. Interesse an der Wahrung von Geschäftsgeheimnissen müssen bei der automatisierten Entscheidungsfindung in ähnlicher Weise berücksichtigt werden wie sonst auch. In den für den Betroffenen sehr wichtiger Entscheidungen wie der der Kreditgewährung werden freilich die Interessen der Betroffenen an der Auskunft den Geheimnisschutz eher überwiegen als in anderen Fällen. Hier sollte auf die tradierten Regelungen zum Geheimnisschutz zurückgegriffen werden; es bedarf keiner Sonderregelungen.

VI. Speicherpflichten

Wichtig erscheint es, die Verantwortlichen im Interesse der betroffenen Verbraucher zu verpflichten, die erstellten Wahrscheinlichkeitswerte und ihre Empfänger für ein Jahr zu speichern. Nur so kann sichergestellt werden, dass die schon bestehende Auskunftspflicht über diese Wahrscheinlichkeitswerte auch tatsächlich realisiert werden kann. § 37a Abs. 4 S. 2 BDSG-E sollte daher in angepasster Form im Gesetz verbleiben, allerdings hinsichtlich des Fristbeginns für die Speicherung präzisiert werden:

> *„Verantwortliche haben die erstellten Wahrscheinlichkeitswerte und ihre Empfänger für ein Jahr ab Erstellung des jeweiligen Wahrscheinlichkeitswertes zu speichern.“*

Verteiler

Deutschland

Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesministerium für Wirtschaft und Klimaschutz

Ausschuss für Inneres und Heimat im Deutschen Bundestag
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitales im Deutschen Bundestag
Fraktionen im Deutschen Bundestag

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe e.V.
Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
Staatsanwälte e.V. (DRB)
Deutscher Notarverein
Deutscher Steuerberaterverband e.V. Berlin
Bundesverband der Deutschen Industrie e.V.
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
Deutscher EDV-Gerichtstag e.V.
GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
Bitkom e. V.
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)

ver.di - Vereinte Dienstleistungsgewerkschaft
Gewerkschaft der Polizei
Deutsche Polizeigewerkschaft im DBB (DPolG)

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung GmbH
Süddeutsche Zeitung GmbH
Redaktion NJW
JUVE Verlag für juristische Information GmbH
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
juris GmbH
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
DER SPIEGEL GmbH & Co. KG

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)446

BDIU
Bundesverband Deutscher Inkasso-Unternehmen

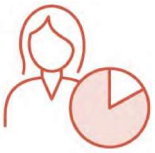
Stellungnahme
Entwurf der Bundesregierung eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

9. April 2024

Der Bundesverband Deutscher Inkasso-Unternehmen e.V.

Rund
450

Mitglieder vereint der Bundesverband Deutscher Inkasso-Unternehmen.



90 Prozent

Marktabdeckung durch BDIU-Mitglieds-unternehmen

33,4 Mio.

Forderungen werden von BDIU-Mitgliedern jährlich übergeben.

15 Tsd.

Menschen arbeiten in Mitgliedsunternehmen des BDIU.

5 Mrd. Euro

führen BDIU-Mitglieds-unternehmen jährlich zurück in den Wirtschaftskreislauf.

500 Tsd.

Auftraggeber wenden sich jährlich an BDIU-Mitglieds-unternehmen.

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

1. Zusammenfassung

Der Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) begrüßt den Entwurf der Bundesregierung eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestags-Drucksache 20/10859).

Allerdings enthält der Entwurf auch Mängel. Insofern schlägt der BDIU zu Artikel 1 Nr. 14 folgende Änderungen (**fett** bzw. ~~**fett**~~ hervorgehoben) im einzufügenden § 37a sowie weitere kleinere Änderungen vor (siehe zu letzteren nachfolgend unter 5.):

„Nach § 37 wird folgender § 37a eingefügt:

„§ 37a
Scoring

(1) […]
(2) Wahrscheinlichkeitswerte im Sinne des Absatzes 1 dürfen nur erstellt oder verwendet werden, wenn
1. für die Erstellung folgende Daten nicht genutzt werden
   a) […]
   […]
   d) **ausschließlich** Anschriftendaten
2. sie keine minderjährige Person betreffen und
3. die genutzten personenbezogenen Daten ~~**a)**~~ unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind ~~**und**~~
   ~~**b) für keine anderen Zwecke verarbeitet werden.**~~

[…]“

2. Gesamtvorhaben

Materiell geht es dem Entwurf vor allem um eine Änderung der Regelungen zum Scoring, d.h. dem bisherigen § 31 BDSG. Diese sollen in einen § 37a BDSG-RegE überführt und dort erheblich geändert werden. Hiermit soll einerseits der Verbraucherschutz verbessert und andererseits Vorgaben des EuGH, die sich aus dem sog. SCHUFA-Urteil vom 07.12.2023 ergeben (Rs. C-634/21), Rechnung getragen werden.

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

Art. 22 Abs. 1 DSGVO enthält ein grundsätzliches Verbot der für die digitalisierte Wirtschaft (z.B. Online-Handel) unabdingbaren automatisierten Entscheidungen. Art. 22 Abs. 2 DSGVO sieht enge Ausnahmen von diesem Verbot vor. Aus dem SCHUFA-Urteil des EuGH vom 07.12.2023 ergibt sich, dass diese Vorschriften in bestimmten Konstellationen auch für Auskunfteien gelten. Konkret geht es um Fälle, in denen ein Unternehmen (z.B. eine Bank) eine automatisierte Entscheidung trifft und hierbei ausschließlich auf den Score abstellt, den es hierfür von einer Auskunftei bezogen hat. Für eine solche Konstellation hat der EuGH im SCHUFA-Urteil entschieden, dass die Auskunftei als derjenige anzusehen ist, der die automatisierte Entscheidung trifft und dass folglich die Vorgaben des Art. 22 DSGVO direkt für die Auskunftei gelten.

Weil das Urteil Unschärfen aufweist, führt es zu erheblicher Rechtsunsicherheit für Auskunfteien und ihre Kundinnen und Kunden und damit alle Unternehmen in Deutschland, die im Rahmen der gesetzlichen Vorgaben Auskunftei-Scores nutzen.

In dem SCHUFA-Urteil hat der EuGH auch darauf hingewiesen, dass § 31 BDSG eine grundsätzlich zulässige Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO darstellt, wenn er unionsrechtskonform ist. Insofern soll § 37a BDSG-RegE bestehende Zweifel an der Unionsrechtskonformität des § 31 BDSG ausräumen und die Rechtsunsicherheit für Auskunfteien und Auskunftei-Kundinnen und -Kunden infolge des SCHUFA-Urteils beseitigen.

Wie viele andere Unternehmen sind auch Mitglieder des BDIU mitunter auf Scores von Auskunfteien angewiesen. Sie haben daher ein vitales Interesse daran, dass die Scores von den Auskunfteien rechtssicher bereitgestellt werden und möglichst unverfälscht sind.

Der BDIU befürwortet daher den Gesetzentwurf im Grundsatz. Er hält aber zwei Änderungen in § 37a Abs. 2 BDSG-RegE für erforderlich, da ansonsten eine bedeutende Verschlechterung von Scores die Folge wäre und die angestrebte Rechtssicherheit nicht erreicht wird.

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

3. Das generelle Verbot der mathematisch-statistischen Berücksichtigung von Anschriftendaten sollte gestrichen werden

1. Geltende Regelung

Gemäß § 31 Abs. 1 Nr. 2 i.V.m. Abs. 2 Satz 1 BDSG müssen Auskunfteien beim Berechnen von Scores wissenschaftlich anerkannte mathematisch-statistische Verfahren verwenden. Das gilt auch, soweit eine Auskunftei Anschriftendaten in die Berechnung einfließen lässt (vgl. § 31 Abs. 1 Nr. 3 BDSG). Außerdem darf gem. § 31 Abs. 1 Nr. 3 BDSG die Wahrscheinlichkeit nicht ausschließlich unter Nutzung von Anschriftendaten berechnet werden.

2. Änderung durch § 37a BDSG-RegE

Nach dem neuen § 37a BDSG-RegE soll die *mathematisch-statistische Berücksichtigung von Anschriftendaten aufgrund wissenschaftlich anerkannter Verfahren* verboten werden. Stattdessen dürfen Anschriftendaten überhaupt nicht mehr berücksichtigt werden. Das ergibt sich aus der Streichung des § 31 BDSG und dem stattdessen eingefügten § 37a BDSG-RegE, insbesondere dessen Abs. 2 Nr. 1 Buchtstabe d).

3. Vorschlag des BDIU

Der BDIU schlägt vor, die *mathematisch-statistische Berücksichtigung von Anschriftendaten im Rahmen wissenschaftlich anerkannter Verfahren* durch Auskunfteien *nicht* zu verbieten. Er schlägt insoweit folgende Änderung des § 37a Abs. 2 BDSG-RegE vor (Änderungen sind **fett** bzw. ~~**fett**~~ hervorgehoben):

> (2) Wahrscheinlichkeitswerte im Sinne des Absatzes 1 dürfen nur erstellt oder verwendet werden, wenn
>
> 1. für die Erstellung folgende Daten nicht genutzt werden:
>
> a) […]
> […]
>
> d) **ausschließlich** Anschriftendaten,
>
> 2. sie keine minderjährige Person betreffen und

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

3. die genutzten personenbezogenen Daten ~~a)~~ unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind".

4. Begründung

Die heutigen deutschen Vorschriften für Scoring durch Auskunfteien sind streng. Nach dem restriktiven SCHUFA-Urteil des EuGH besteht die Gefahr, dass Deutschland der Wirtschaft zusätzliche Beschränkungen auferlegt, die in diesem Punkt das Ziel des Verbraucherschutzes verfehlen und zugleich zu einer bedeutenden Verschlechterung von Auskunftei-Scores führen; das ist weder im Interesse der die Scores nutzenden Wirtschaft noch derjenigen Verbraucherinnen und Verbraucher und Unternehmerinnen und Unternehmer in Deutschland, deren Scores § 37a BDSG-RegE regelt.

§ 31 BDSG enthält die Vorgabe, dass „zur Berechnung des Wahrscheinlichkeitswerts genutzte Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahren nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind". Das gilt für *alle* in das Scoring einfließenden Daten. Dieser hohe Standard hat sich bewährt.

Dieser Standard gilt auch für Anschriftendaten soweit diese in die Score-Berechnung *mit* einfließen. Anschriften dürfen zudem nie allein einen Score bestimmen (§ 31 Abs. 1 Nr. 3 BDSG). Erlaubt ist also die Berücksichtigung von Anschriften nur als eine Information von mehreren und auch nur, soweit diese Berücksichtigung wissenschaftlich nachweisbar die mathematisch-statistisch Berechnung stützt. (Nur) das ist heute im Hinblick auf Anschriftendaten beim Scoring erlaubt.

§ 37a Abs. 2 Nr. 1 Buchstabe d) BDSG-RegE verbietet also gerade *diese wissenschaftlich* nachweisbare *Mit*-Berücksichtigung von Anschriftendaten. Das Verbot ist daher nicht zielführend. Es dient *nicht* dem Verbraucherschutz; es ist weder im Interesse von Verbraucherinnen und Verbrauchern, noch von Unternehmerinnen und Unternehmern (auf die sich Scores ebenfalls beziehen), wenn die Scores wissenschaftlich nachweisbar schlechter werden.

Die Gesetzesbegründung dieses mit § 37a Abs. 2 Nr. 1 Buchstabe d) BDSG-RegE neu eingeführten Verbots verweist allein auf ein „Diskriminierungsrisiko"; diesem habe die bisherige Regelung „nicht hinreichend Rechnung" getragen. Diese Aussage ist unzutreffend. Sie kann

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

sich gerade nicht auf wissenschaftliche Erkenntnisse oder entsprechende evidenzbasierte Untersuchungen stützen. Solche sind dem BDIU jedenfalls nicht bekannt.

Tatsächlich führt, umgekehrt, das Verbot der Verwendung von Anschriftendaten im Rahmen von wissenschaftlich anerkannten Verfahren zu einer Ungleichbehandlung, die es vorher nicht gab: Unternehmerinnen und Unternehmer oder Verbraucherinnen und Verbraucher, deren Bonitäts-Score besser ist, weil *auch* Anschriftendaten berücksichtigt werden, haben künftig einen im Vergleich schlechteren Score und erhalten im Einzelfall z.B. einen Kredit nicht, den sie sonst bekommen hätten. Sie werden gleich behandelt mit Unternehmen und Verbrauchern, die mathematisch-statistisch zu Recht den schlechteren Score haben. Diese Ungleichbehandlung ist sachlich nicht gerechtfertigt. Denn sie stellt gerade darauf ab, dass es auf den wissenschaftlichen Nachweis nicht ankommen darf. Auf eine Einführung des Verbots sollte daher verzichtet werden.

Der BDIU geht davon aus, dass es sich bei dem Verbot um einen handwerklichen Fehler handelt. Insgesamt wäre es eine bedenkliche Tendenz, qua Gesetz zu verbieten, unternehmerische Entscheidungen auf wissenschaftliche Erkenntnis zu stützen.

Hinzu kommt eine weitere Ungleichbehandlung. Anschriftendaten sind nicht annähernd vergleichbar sensibel wie die Kategorien personenbezogener Daten, deren Verwendung beim Scoring durch § 37a Abs. 2 Nr. 1 Buchstabe a) bis c) ansonsten verboten werden.

4. Das Verbot der unionsrechtlichen Ausnahmen für Zweckänderungen sollte gestrichen werden

1. Zweckänderungen gemäß DSGVO

Gemäß Art. 5 Abs. 1 Buchstabe b) DSGVO gilt für die Weiterverarbeitung personenbezogener Daten der Grundsatz der Zweckbindung. Gemäß Art. 6 Abs. 4 DSGVO dürfen Daten ausnahmsweise zu anderen Zwecken verarbeitet werden. Maßgeblich hierfür sind die strengen Kriterien des Art. 6 Abs. 4 Buchstabe a) bis e) DSGVO.

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

2. Änderung durch § 37a BDSG-RegE

Diese europaweit einheitliche Zweckbindung soll durch das BDSG weiter verschärft werden. § 37a Abs. 2 Nr. 3 Buchstabe b) BDSG-RegE schreibt vor, dass

> „die genutzten personenbezogenen Daten […] für keine anderen Zwecke verarbeitet werden“

dürfen. Eine ausnahmsweise Verarbeitung zu anderen Zwecken gemäß Art. 6 Abs. 4 DSGVO soll hiernach also ausscheiden.

3. Begründung

Der BDIU hält die Verschärfung der Zweckbindung für europarechtswidrig.

Denn Art. 6 Abs. 4 DSGVO sieht vor, dass Daten zu anderen Zwecken verarbeitet werden dürfen, wenn die strengen Kriterien des Art. 6 Abs. 4 Buchstabe a) bis e) DSGVO dies gestatten.

Art. 6 Abs. 4 a.A. i.V.m. Art. 23 Abs. 1 DSGVO enthält eine Öffnungsklausel. Er gestattet den Mitgliedstaaten, *weitere Ausnahmen* vom Zweckbindungsgrundsatz zu regeln. Die DSGVO enthält aber keine Vorschrift, wonach die Mitgliedstaaten die Ausnahmen in der DSGVO für zweckändernden Datenverarbeitung aufheben dürfen. Im Gegenteil: Von Art. 6 Abs. 4 Buchstabe a) bis e) DSGVO darf nicht abgewichen werden.

Das absolute Verbot jedweder Zweckänderung in § 37a Abs. 2 Nr. 3 Buchstabe b) BDSG-RegE verstößt nicht nur gegen die DSGVO. Sondern es würde Auskunfteien und ihre Kundinnen und Kunden – und damit viele Unternehmen in Deutschland – gegenüber Wirtschaftsakteuren im Ausland auch benachteiligen. Ebendies verbietet wiederum Art. 1 Abs. 3 DSGVO, wonach der „freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“ darf.

Es ist auch politisch nicht sinnvoll, die ohnehin sehr strengen Vorgaben der DSGVO für Deutschland noch weiter zu verschärfen. Auch gibt es keine Anhaltspunkte dafür, dass die unionsrechtlichen Regelungen insofern für Probleme gesorgt hätten. Wäre dies aber der Fall, läge es in der alleinigen Kompetenz des Unionsgesetzgebers, sie zu ändern.

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

Hinzu kommt, dass mit § 37a Abs. 2 Nr. 3 Buchstabe b) BDSG-RegE der Bundesgesetzgeber das eigene Ziel gefährdet, die Rechtsunsicherheit, die aufgrund des SCHUFA-Urteils des EuGH entstanden ist, zu beseitigen. Denn die Rechtsicherheit, die durch § 37a BDSG-RegE geschaffen werden soll, wird durch den unionsrechtswidrigen § 37a Abs. 2 Nr. 3 Buchstabe b) BDSG-RegE insgesamt infrage gestellt. Das Verbot birgt das Risiko, dass Gerichte § 37a BDSG insgesamt nicht anwenden werden. Daher sollte das Verbot der Zweckänderung gestrichen werden.

5. Weitere Änderungen zur Beseitigung handwerklicher Mängel

Der BDIU begrüßt, dass die Bundesregierung umgehend auf das SCHUFA-Urteil des EuGH vom 07.12.2023 reagiert und sehr zügig ihren Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes vorgelegt hat. In einigen Detailfragen enthält der Entwurf aber noch Mängel, die dem eiligen Verfahren bis hierher geschuldet sein dürften, die sich nun im parlamentarischen Verfahren aber beseitigen lassen. Hierzu verhalten sich die folgenden Vorschläge:

1. Konkret schlägt der BDIU vor, in § 37a Abs. 6 BDSG-RegE folgende Klarstellung einzufügen (**fett** hervorgehoben):

   „Gegenüber einen Verantwortlichen, **der einen Wahrscheinlichkeitswert nach Absatz 1 verwendet,** hat die betroffene Person hinsichtlich der jeweiligen auf Wahrscheinlichkeitswerten nach Absatz 1 beruhenden Entscheidung das Recht auf Anfechtung, Darlegung des eigenen Standpunkts und Entscheidung einer natürlichen Person."

2. Außerdem sollte in § 37a Abs. 2 Nr. 3 BDSG-RegE folgende Klarstellung eingefügt werden (**fett** hervorgehoben):

   „3. Die **für die Erstellung** genutzten personenbezogenen Daten"

Ansprechpartner:
Dennis Stratmann
Geschäftsführer
030 2060736-27
bdiu@inkasso.de

3. Schließlich regt der BDIU an,

   auf den neuen § 34 Abs. 1 Satz 2 BDSG-RegE zu verzichten.

   Intention diese Vorschrift ist, die Reichweite des Schutzes von Betriebs- und Geschäftsgeheimnissen im Rahmen von Beauskunftungen gemäß Art. 15 DSGVO klarzustellen und insofern die Abwägungsklausel des Art. 15 Abs. 4 DSGVO näher zu konturieren. Allein die Diskussion im bisherigen Gesetzgebungsverfahren (vgl. einerseits Stellungnahme des Bundesrates, Bundesrats-Drucksache 72/24 (Beschluss) vom 22.03.2024, S. 5, andererseits Gegenäußerung der Bundesregierung, Bundestags-Drucksache 20/10859, S. 42 f.) zeigt, dass die Klarstellung nicht gelingt. Es sollte daher auf sie verzichtet werden. Es reicht, es bei der allgemeinen Abwicklungsklausel des Art. 15 Abs. 4 BDSG zu belassen.

GDV Gesamtverband der Versicherer

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)448

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Regierungsentwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Inhalt

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Datenschutz/Grundsatzfragen

E-Mail
data-protection@gdv.de

Zusammenfassung

Die Streichung von § 31 BDSG und die Einfügung von § 37a BDSG-RegE sind wichtige Schritte, um nach dem Schufa-Urteil des EuGH wieder mehr Rechtssicherheit für die Erstellung und Verwendung von Wahrscheinlichkeitswerten zu schaffen. Allerdings sollten § 37a Abs. 2 Nr. 1 Buchst. c) und Nr. 3 Buchst. b) BDSG-RegE präziser gefasst werden, um keine ungewollten Auswirkungen zu haben (dazu Ziffer 1).

Die in § 37 BDSG geregelten Ausnahmen für vollautomatisierte Einzelentscheidungen sollten erweitert werden, um im Massengeschäft der Versicherer schnelle automatisierte Vertragsabschlüsse und Schadenregulierungen zu ermöglichen (dazu Ziffer 2).

Die Regelungen zur Zuständigkeit der Aufsichtsbehörden in § 27 Abs. 5 und § 40a BDSG-RegE sind ein guter Ansatz, um divergierende Entscheidungen unterschiedlicher Aufsichtsbehörden zu verhindern. § 40a BDSG-RegE sollte jedoch auf alle Datenverarbeitungen in Unternehmensgruppen ausgeweitet werden und mehr Flexibilität bei der Bestimmung der zuständigen Behörde gewähren (dazu Ziffer 3).

Weitere Anregungen enthält unsere Stellungnahme zum Referentenentwurf.

1. § 37a RegE BDSG

Mit der Streichung des § 31 BDSG und der Einfügung des neuen § 37a BDSG-RegE hat die Bundesregierung auf das Urteil des Europäischen Gerichtshofs vom 07.12.2023 in der Rechtssache C 634/21 (Schufa) reagiert. Dies ist nötig, um Rechtssicherheit für Auskunfteien und ihre Kunden zu schaffen.

Die in § 37a Abs. 1 BDSG-RegE vorgesehene neue Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO kann für Versicherungsunternehmen zum einen als Verwender von Scorewerten, die sie von Auskunfteien erhalten, relevant sein. § 37a Abs. 1 Nr. 1 BDSG-RegE kann aber auch einschlägig sein, wenn ein Versicherungsunternehmen selbst einen Wahrscheinlichkeitswert über ein zukünftiges Verhalten errechnet, um über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses zu entscheiden.

Allerdings sind einige Anforderungen des § 37a Abs. 2 und 5 BDSG-RegE für die Datenverarbeitung in den Versicherungsunternehmen zu eng und teilweise auch missverständlich.

1.1 Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten (§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE)

§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE legt fest, dass Wahrscheinlichkeitswerte im Sinne von § 37 Abs. 1 BDSG-RegE keine Informationen über Zahlungseingänge und -ausgänge auf und von Bankkonten enthalten dürfen. Ziel der Regelung ist es, zu vermeiden, dass „im großen Umfang Erkenntnisse über persönliche Aspekte der Lebensführung“ gewonnen und verwertet werden (RegE, Begründung zu Nummer 14).

Die Regelung ist jedoch so weit formuliert, dass sie Zahlungseingänge auf irgendeinem Bankkonto (und damit korrespondierende einzelne Zahlungsausgänge vom Konto eines Kunden) erfasst.

Beispiel

> Ein Versicherungsunternehmen bewertet, u. a. anhand der ihm selbst vorliegenden Daten über Beitragszahlungen, die Bereitschaft eines Kunden, seine Versicherungsverträge zu erfüllen. Dieser Wahrscheinlichkeitswert soll an die Stelle des Scorewertes einer Auskunftei treten oder diesen ergänzen. Er ist in aller Regel in der jeweiligen Konstellation treffsicherer als ein allgemeiner Wert einer Auskunftei.

Nicht zulässig wären im Beispielfall nach dem Wortlaut des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE die Einbeziehung von Zahlungseingängen auf dem Konto des Versicherungsunternehmens selbst, denen einzelne Zahlungsausgänge von dem Konto des Kunden entsprechen. Der Wortlaut der Norm geht weit über den Regelungszweck des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE hinaus. Denn hier kann das Versicherungsunternehmen keine umfassenden Erkenntnisse über persönliche Aspekte der Lebensführung des Kunden gewinnen, weil es nur punktuell die Zahlungsvorgänge betrachtet, die es selbst angehen.

Um sich nicht auf eine im Ergebnis unsichere teleologische Reduktion des § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE verlassen zu müssen, sollte der Wortlaut der Norm präziser gefasst werden.

Vorschlag der deutschen Versicherungswirtschaft

§ 37a Abs. 2 Nr. 1 Buchst. c) BDSG-RegE sollte wie folgt präzisiert werden:

> „Informationen über eine Vielzahl verschiedener Zahlungseingänge und -ausgänge auf und von Bankkonten der vom Scoring betroffenen Person, durch deren Zusammenspiel neue Erkenntnisse über persönliche Aspekte der Lebensführung der vom Scoring betroffenen Person gewonnen werden

können,“

1.2 Keine anderen Zwecke (§ 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE)

Nach § 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE dürfen die genutzten personenbezogenen Daten für keine anderen Zwecke verarbeitet werden.

Diese Anforderung ist für ein Versicherungsunternehmen, das mit eigenen Daten Wahrscheinlichkeitswerte errechnet, nicht einzuhalten. Wenn ein Versicherungsunternehmen einen eigenen Wahrscheinlichkeitswert errechnet, der den von einer Auskunftei errechneten Wert ersetzen oder ergänzen soll, geschieht dies immer mit Daten, die bereits vorher zu einem anderen Zweck verarbeitet wurden und auch nachfolgend noch zu anderen Zwecken dienen können.

Beispiel

> Das Unternehmen bewertet anhand der ihm vorliegenden Zahlungseingänge seines Kunden zu verschiedenen Verträgen dessen Bereitschaft, künftig Versicherungsverträge zu erfüllen. Die Information, dass der Kunde die Versicherungsprämie für einen bestimmten Vertrag nicht gezahlt hat, dient auch dem Zweck, den Kunden zu mahnen bzw. weitere Schritte zum Inkasso einzuleiten.

Da sich eine Zweckbindung ohnehin aus Art. 6 Abs. 4 DSGVO ergibt, ist die Regelung nicht nötig. Sie sollte gestrichen oder zumindest auf Auskunfteien beschränkt werden.

Vorschlag der deutschen Versicherungswirtschaft

§ 37a Abs. 2 Nr. 3 Buchst. b) BDSG-RegE sollte gestrichen oder zumindest wie folgt präzisiert werden:

> „in den Fällen des § 37a Abs. 1 Nr. 2 BDSG für keine anderen Zwecke verarbeitet werden.“

1.3 Keine unerlaubte Konkretisierung des Art. 6 DSGVO durch § 37a Abs. 2 BDSG-RegE

Es ist nicht auszuschließen, dass der Gesetzestext des § 37a Abs. 2 BDSG-RegE dahingehend interpretiert wird, dass die in § 37a Abs. 1 Nr. 1 und 2 genannten Wahrscheinlichkeitswerte immer die Anforderungen des § 37a Abs. 2 BDSG-RegE erfüllen müssen, unabhängig davon, ob von der Ausnahme nach § 37a Abs. 1 BDSG-RegE oder einer anderen Ausnahme des Art. 22 Abs. 2 DSGVO Gebrauch

gemacht wird. Eine solche Regelung wäre dann aber – wie der EuGH es für § 31 BDSG erwägt – nur eine Konkretisierung der allgemeinen Erlaubnisnorm des Art. 6 DSGVO. Sie wäre somit nach der Rechtsprechung des EuGH (Urteil vom 07.12.2023, a. a. O., Rn. 68 ff.) nicht wirksam.

Die Absicht des Gesetzgebers, in § 37a Abs. 2 BDSG-RegE lediglich die auf Art. 22 Abs. 2 lit. b) DSGVO gestützte und in § 37a Abs. 1 BDSG-RegE formulierte Ausnahme vom Verbot des Art. 22 Abs. 1 DSGVO zu konkretisieren, sollte nicht nur in der Gesetzesbegründung sondern auch im Gesetzestext deutlich werden.

1.4 Schutz von Geschäftsgeheimnissen (§ 37a Abs. 5 BDGS-RegE)

§ 37a Abs. 5 BDGS-RegE schließt die Anwendung des neu geschaffenen § 34 Abs. 1 Satz 2 BDSG-RegE im Anwendungsbereich des § 37a BDSG-RegE vollständig aus. Damit kann der Ersteller eines Wahrscheinlichkeitswertes einem Auskunftsersuchen nach § 37a Abs. 4 BDSG-RegE ein Geschäftsgeheimnis unter keinen Umständen entgegenhalten.

Es ist wichtig, dass die betroffene Person nachvollziehen kann, welche Kriterien bei der Ermittlung des Wahrscheinlichkeitswertes eine Rolle gespielt haben und letztlich für die Entscheidung maßgeblich waren. Andererseits müssen Unternehmen davor geschützt werden, dass § 37a Abs. 4 BDSG-RegE extensiv ausgelegt wird und Berechnungsformeln, die im Wettbewerb eine wichtige Rolle spielen, bekannt gemacht werden müssen. Diese gegenläufigen Interessen berücksichtigt § 34 Abs. 1 Satz 2 BDSG-RegE, indem er die Verweigerung der Auskunft nur zulässt, wenn das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt. Er sollte daher anwendbar bleiben.

Zudem ist der Wortlaut des § 37a Abs. 5 RegE sehr weit formuliert und wird erst durch die Begründung eingeschränkt. Dies kann zu Missverständnissen führen.

Vorschlag der deutschen Versicherungswirtschaft:

> § 37a Abs. 5 BDSG-RegE sollte gestrichen werden.

2. Vollautomatisierte Einzelentscheidungen zur Risiko- und Leistungsprüfung in der Versicherungswirtschaft (§ 37 BDSG)

Sinnvoll ist die Klarstellung in § 37a Abs. 1 BDSG-RegE, dass Artikel 22 Abs. 2 Buchst. a) und c) DSGVO von der neuen Regelung unberührt bleiben. Denn der europäische Gesetzgeber hat vollautomatisierte Einzelentscheidungen, die zum Abschluss eines Vertrages erforderlich sind bzw. die mit wirksamer Einwilligung

erfolgen, erlaubt. Diese Erlaubnis kann der deutsche Gesetzgeber nicht einschränken, sondern über die Öffnungsklausel des Artikel 22 Abs. 2 Buchst. b) lediglich weitere Erlaubnisgrundlagen schaffen.

Aktuell wird die Digitalisierung von Risiko- und Leistungsprüfungen in der Versicherungswirtschaft allerdings dadurch behindert, dass Artikel 22 Abs. 2 Buchst. a) und c) DSGVO von den Datenschutzbehörden sehr restriktiv ausgelegt werden. Sie enthalten zudem keine Lösung für die Prüfung und Regulierung von Ansprüchen, die nicht Vertragspartner, sondern dritte Personen (zum Beispiel Geschädigte in der Haftpflichtversicherung) geltend machen.

Das Versicherungsgeschäft ist ein Massengeschäft. Unsere Mitgliedsunternehmen verwalten mehr als 465 Mio. Versicherungsverträge. Sie regulieren Schäden und erbringen Leistungen in Höhe von jährlich mehr als 180 Mrd. Euro. Könnten die vollautomatisierte Risikoprüfung beim Vertragsschluss sowie die Leistungsprüfung und -abwicklung im Schadenfall vollautomatisiert erfolgen, würden Kunden und Geschädigte unkomplizierter und erheblich schneller als bei manueller Bearbeitung Versicherungsschutz bzw. die ihnen im Versicherungsfall zustehenden Leistungen erhalten.

Um der Digitalisierung in der Versicherungswirtschaft angemessen Rechnung zu tragen, wäre es hilfreich, § 37 BDSG so anzupassen, dass vollautomatisierte Entscheidungen zum Abschluss und zur Durchführung eines Versicherungsvertrages, einschließlich der Regulierung von Ansprüchen Dritter in der Haftpflichtversicherung grundsätzlich zulässig sind, wenn Transparenz über die Entscheidung und ein Recht auf menschliche Überprüfung bestehen.

Vorschlag der deutschen Versicherungswirtschaft

> § 37 BDSG sollte auch den Abschluss und die Durchführung von Versicherungsverträgen erfassen und nicht auf Entscheidung über die Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beschränkt sein.

Einzelheiten, Beispiele und ein konkreter Formulierungsvorschlag sind Ziffer 4.2.2. unserer Stellungnahme zu dem Referentenentwurf zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes zu entnehmen.

3. Zuständigkeit der Datenschutzaufsichtsbehörden

§ 40a und § 27 Abs. 5 BGSG-RegE, die es ermöglichen, die Zuständigkeit einer einzigen Landesdatenschutzaufsichtsbehörde für gemeinsame Vorhaben mehrerer Verantwortlicher zu begründen, sind ein guter Schritt in die richtige Richtung. Sie verhindern divergierende Entscheidungen unterschiedlicher Behörden in

gleichgelagerten Sachverhalten und dienen damit der im Koalitionsvertrag vorgesehenen besseren Durchsetzung und Kohärenz des Datenschutzes.

Allerdings sollte § 40a BDSG-RegE **über die gemeinsame Verantwortlichkeit hinaus für jede Datenverarbeitung in einer Unternehmensgruppe** gelten. Nicht jede Datenverarbeitung innerhalb eines Konzerns ist eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DSGVO. Es kommt nicht selten vor, dass ein Prozess abstrakt konzerneinheitlich gestaltet wird, die Verarbeitung personenbezogener Daten aber dann in alleiniger Verantwortung der jeweiligen Konzerngesellschaften ausgeführt wird. Auch in derartigen Fällen ist es problematisch, wenn durch den Sitz der jeweiligen Konzernunternehmen unterschiedliche Aufsichtsbehörden zuständig sind und ggf. unterschiedliche Ansichten zur Zulässigkeit der Verarbeitung vertreten. In Erwägungsgrund 48 erkennt die DSGVO ausdrücklich das berechtigte Interesse an Datenflüssen innerhalb von Unternehmensgruppen an. Daher sollte § 40a BDSG neben Fällen der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO generell auf die Datenverarbeitung innerhalb einer Unternehmensgruppe erweitert werden.

Außerdem erscheint es **zu starr**, zwingend die Zuständigkeit der Aufsichtsbehörde anzunehmen, in deren Zuständigkeitsbereich das Unternehmen fällt, das in dem der Antragstellung vorangegangenen Geschäftsjahr den größten weltweiten **Jahresumsatz** erzielt hat. So kann innerhalb eines Versicherungskonzerns ein operativ tätiges Tochterunternehmen den höchsten Umsatz haben, während die maßgebenden Entscheidungen für die Datenverarbeitung in der Konzernholding oder einer Servicegesellschaft getroffen werden. Art. 26 DSGVO lässt den gemeinsam Verantwortlichen einen weitgehenden Spielraum bei der Ausgestaltung ihrer Rechte und Pflichten, solange darüber Transparenz besteht. So können sie z. B. nach Art. 26 Abs. 1 Satz 2 DSGVO in transparenter Form festlegen, wer von ihnen welche Verpflichtung nach der DSGVO erfüllt. Daher spricht auch nichts dagegen, dass die Unternehmen festlegen, wer das „führende“ Unternehmen ist. Die Datenschutzbehörde, in deren Zuständigkeitsbereich dieses Unternehmen fällt, wäre dann zuständig.

Vorschlag der deutschen Versicherungswirtschaft

> § 40a BDSG-RefE sollte über die gemeinsame Verantwortlichkeit hinaus auf die Datenverarbeitung in einer Unternehmensgruppe erweitert werden.
>
> Die Zuständigkeit der Datenschutzbehörden sollte daran anknüpfen, welches Unternehmen die Verantwortlichen für den Verarbeitungsprozess vertraglich als führend festgelegt haben.

4. Weitere Vorschläge

In unserer Stellungnahme zu dem Referentenentwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes haben wir weitere Vorschläge unterbreitet, die mehr Rechtssicherheit schaffen und die Digitalisierung erleichtern würden. Dazu gehören nationale gesetzliche Erlaubnisgrundlagen für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft (Ziffer 4.3.) und für die Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen im Sinne von Art. 10 DSGVO (Ziffer 4.4.). Ferner fordern wir klare Rechtnormen für die Anonymisierung und Pseudonymisierung sowie für die Entwicklung und für Tests von IT-Anwendungen, Produkten und Systemen (Ziffer 4.5.). Schließlich regen wir Klarstellungen in den Regelungen zu den Betroffenenrechten an (Ziffer 4.6.).

Wegen Einzelheiten dieser Forderungen verweisen wir auf unsere Stellungnahme zu dem Referentenentwurf.

Berlin, den 28.02.2024

GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
Lobbyregister-Nr. R000774

zum Referentenentwurf
eines Ersten Gesetzes zur Änderung des
Bundesdatenschutzgesetzes vom 9. August 2023

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000
Lobbyregister-Nr. R000774

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Datenschutz/Grundsatzfragen

E-Mail
datenschutz@gdv.de

1. Inhalt

2. Zusammenfassung

Die Novellierung des BDSG sollte unbedingt genutzt werden, um der Datenstrategie der Bundesregierung in der Praxis zur Geltung zu verhelfen. Erste ausbaufähige Ansätze des Referentenentwurfs (BDSG-RefE) sind die Regelungen zur Zuständigkeit einer Datenschutzaufsichtsbehörde bei gemeinsam Verantwortlichen (§ 40a und § 27 Abs. 5 BDSG-RefE – dazu Punkt 4.1. dieser Stellungnahme) sowie die Einschränkung des Auskunftsrechts zum Schutz von Geschäftsgeheimnissen (§ 34 BDSG-RefE – Dazu Punkt 4.6.1).

Aus Sicht der Versicherungswirtschaft sind weitere Regelungen nötig, um Datennutzung und Digitalisierung voranzubringen:

§ 37 BDSG sollte **vollautomatisierte Entscheidungen** der Versicherer bei Vertragsabschlüssen und bei der Prüfung von Leistungsansprüchen erlauben, um im Massengeschäft Kunden und Geschädigte schnell und unkompliziert bedienen zu können. § 37 Abs. 1 Nr. 1 BDSG sollte nicht gestrichen werden (dazu Punkt 4.2).

- In das BDSG sollte nach dem Vorbild anderer EU-Staaten eine eindeutige gesetzliche Erlaubnisgrundlage für die Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Versicherungsverträgen aufgenommen werden (dazu Punkt 4.3.).

- In das BDSG sollte eine eindeutige Rechtsgrundlage i. S. v. Art. 10 DSGVO für die **Verarbeitung von Daten über Straftaten** und strafrechtliche Verurteilungen in der Versicherungswirtschaft eingefügt werden (dazu Punkt 4.4.).

- Es sollten – insbesondere für besondere Kategorien personenbezogener Daten – eindeutige Rechtsgrundlagen für die **Anonymisierung und Pseudonymisierung von Daten** sowie für die **Nutzung pseudonymisierter Daten zur Entwicklung und zum Test neuer Anwendungen und Systeme** geschaffen werden (dazu Punkt 4.5).

- Schließlich sollten **Unstimmigkeiten in den Ausnahmen zu den Betroffenenrechten beseitigt** werden (dazu Punkt 4.6.2. und 4.6.3)

3. Einleitung

In dem RefE-BDSG sollen die datenschutzrechtlich relevanten Vereinbarungen im Koalitionsvertrag und die Ergebnisse der Evaluierung des Bundesdatenschutzgesetzes im Jahr 2021 umgesetzt werden. Insofern sind die Regelungen in § 40a und § 27 Abs. 5 RefE und § 34 RefE ein Schritt in die richtige Richtung.

Die BDSG-Novellierung sollte jedoch darüber hinaus genutzt werden, um den richtigen Ansätzen in der Datenstrategie der Bundesregierung in der Praxis zur Geltung zu verhelfen. In dem dazu kürzlich veröffentlichten Papier „Fortschritt durch Datennutzung“ führt die Bundesregierung auf den Seiten 20 und 21 aus, dass sie den Datenschutz „einfacher, kohärenter und praktikabler“ machen will. Die Ziele, einen „ermöglichenden Datenschutz“ zu schaffen, indem „Spielräume und Öffnungsklauseln der DSGVO“ durch neue „gesetzliche Erlaubnistatbestände, Regelbeispiele und Klarstellungen …“ genutzt werden, unterstützen wir uneingeschränkt.

Wir regen dringend an, diese Ziele schon mit der BDSG-Novellierung in konkreten Regelungen umzusetzen, um den Anschluss an die Digitalisierung nicht zu verpassen.

4. Stellungnahme zu einzelnen Bestimmungen

Zu dem Referentenentwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 9. August 2023 **(RefE-BDSG)** nehmen wir nachfolgend im Einzelnen Stellung.

4.1. Zuständigkeit der Datenschutzaufsichtsbehörden

Die Regelungen in § 40a und § 27 Abs. 5 RefE, die die Zuständigkeit einer einzigen Landesdatenschutzaufsichtsbehörde für gemeinsame Vorhaben mehrerer Verantwortlicher begründen, sind ein guter Schritt in die richtige Richtung. Sie verhindern divergierende Entscheidungen unterschiedlicher Behörden in gleichgelagerten Sachverhalten und dienen damit der im Koalitionsvertrag vorgesehenen besseren Durchsetzung und Kohärenz des Datenschutzes.

4.1.1. Anknüpfungspunkt und Maßstab des § 40a BDSG

Es ist zu begrüßen, dass § 40a BDSG für den Fall der gemeinsamen Verantwortlichkeit im Sinne von Art. 26 DSGVO die Möglichkeit schafft, dass nur eine Datenschutzbehörde zuständig ist.

Allerdings sollte diese Möglichkeit **über die gemeinsame Verantwortlichkeit hinaus für jede Datenverarbeitung in einer Unternehmensgruppe** geschaffen werden. Nicht jede Datenverarbeitung innerhalb eines Konzerns ist eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DSGVO. Es kommt nicht selten vor, dass ein Prozess abstrakt konzerneinheitlich gestaltet wird, aber dann in alleiniger Verantwortung der jeweiligen Konzerngesellschaften ausgeführt wird, z. B. weil unterschiedliche IT-Systeme zu Grunde liegen. Auch in derartigen Fällen ist es problematisch, wenn durch den Sitz der jeweiligen Konzernunternehmen unterschiedliche Aufsichtsbehörden zuständig sind und ggf. unterschiedliche Ansichten zur Zulässigkeit der Verarbeitung vertreten. In Erwägungsgrund 48 erkennt die DSGVO ausdrücklich das berechtigte Interesse an Datenflüssen innerhalb von Unternehmensgruppen an. Daher sollte § 40a BDSG neben Fällen der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO generell auf die Datenverarbeitung innerhalb einer Unternehmensgruppe erweitert werden.

Schließlich erscheint es **zu starr**, zwingend die Zuständigkeit der Aufsichtsbehörde anzunehmen, in deren Zuständigkeitsbereich das Unternehmen fällt, das in dem der Antragstellung vorangegangenen Geschäftsjahr den größten **Jahresumsatz** erzielt hat. So kann innerhalb eines Versicherungskonzerns ein operativ tätiges Tochterunternehmen den höchsten Umsatz haben, während die maßgebenden Entscheidungen für die Datenverarbeitung in der Konzernholding oder einer Servicegesellschaft getroffen werden. Art. 26 DSGVO lässt den gemeinsam Verantwortlichen einen weitgehenden Spielraum bei der Ausgestaltung ihrer Rechte und Pflichten, solange darüber Transparenz besteht. So können sie z. B. nach Art. 26 Abs. 1 Satz 2 DSGVO in transparenter Form festlegen, wer von ihnen welche Verpflichtung nach der DSGVO erfüllt. Daher spricht auch nichts dagegen, dass die Unternehmen festlegen, wer das „führende“ Unternehmen ist. Die Datenschutzbehörde, in deren Zuständigkeitsbereich dieses Unternehmen fällt, wäre dann zuständig.

Die deutsche Versicherungswirtschaft schlägt daher vor

- **§ 40a BDSG-RefE über die gemeinsame Verantwortlichkeit hinaus auf die Datenverarbeitung in einer Unternehmensgruppe zu erweitern und**
- **die Zuständigkeit der Datenschutzbehörden daran anzuknüpfen, welches „führende“ Unternehmen die Verantwortlichen für den Verarbeitungsprozess vertraglich festgelegt haben.**

4.1.2. Zu enge Regelung in § 27 Abs. 5 BDSG

Es ist nicht nachvollziehbar, wieso sich die Erleichterung für gemeinsam Verantwortliche, die nicht oder nicht ausschließlich Unternehmen sind, auf den eng

begrenzten Fall des § 27 BDSG beziehen soll. Damit sind nur Vorhaben erfasst, bei denen besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeitet werden. Es sind aber zahlreiche weitere Zwecke denkbar, in denen eine enge Zusammenarbeit von öffentlichen und privaten Stellen die Zuständigkeit einer einzigen Landesdatenschutzbehörde sinnvoll erscheinen lässt. Zu denken ist etwa an Maßnahmen zur Vermeidung oder Behebung öffentlicher Notstände oder an Forschungsvorhaben, die nicht die Verarbeitung besonderer Kategorien personenbezogener Daten erfordern.

Die deutsche Versicherungswirtschaft schlägt daher vor

die Regelung allgemeiner zu fassen und in § 40a BDSG zu integrieren.

4.2. Vollautomatisierte Einzelentscheidungen in der Versicherungswirtschaft (§ 37 BDSG)

§ 37 BDSG hat im Massengeschäft der Versicherungswirtschaft eine erhebliche Bedeutung. Um Rechtssicherheit zu erhalten und den Anforderungen der Digitalisierung gerecht zu werden, sollte nicht § 37 Abs. 1 Nr. 1 BDSG gestrichen, sondern die Norm insgesamt überarbeitet werden.

4.2.1. Keine Streichung des § 37 Abs. 1 Nr. 1 BDSG

Nach den Vorschlägen zur Änderung des § 37 BDSG (Artikel 1, Ziffer 11 RefE-BDSG) soll § 37 Abs. 1 Nr. 1 BDSG gestrichen werden.

§ 37 Abs. 1 Nr. 1 BDSG erlaubt bisher ausdrücklich vollautomatisierte Entscheidungen von Versicherungsunternehmen im Einzelfall, mit denen dem Antrag von Kunden bzw. Geschädigten auf eine Versicherungsleistung entsprochen wird. Die Streichung wird damit begründet, dass eine Entscheidung, die einem Begehren der betroffenen Person vollumfänglich stattgibt, schon nicht unter das Verbot der automatisierten Entscheidung nach Artikel 22 Abs.1 DSGVO falle. Die Norm solle nur vor solchen Entscheidungen schützen, die mit einer beeinträchtigenden Wirkung für die betroffene Person verbunden sind (RefE-BDSG, Begründung zu Nr. 11).

Wir halten diese Rechtsauffassung des Ministeriums zwar für sehr gut vertretbar. Sie wird auch in der Literatur geteilt (z. B. Buchner in Kühling/Buchner, Art. 22 Rn. 25; Herbst in Auernhammer, Art. 22 Rn. 14). Eine starke Gegenmeinung geht jedoch immer noch davon aus, dass Art. 22 Abs. 1 DSGVO auch stattgebende Entscheidungen grundsätzlich verbietet (z. B. Helfrich in Sydow/Marsch, Art. 22 Rn. 48; Martini in Paal/Pauly, Art. 22 Rn. 26; Weichert in Däubler/Wedde/

Weichert/Sommer, Art. 22 Rn. 27), sodass hier keine Rechtssicherheit besteht.

Den vom Europäischen Datenschutzausschuss (EDSA) übernommenen Leitlinien WP 251 rev. 01 der Artikel-29-Gruppe (S. 23) und auch den Schlussanträgen des Generalanwalts in der vor dem EuGH anhängigen Rechtssache C 634/21 (Rn. 34) ist lediglich zu entnehmen, dass Art. 22 nur „schwerwiegende Auswirkungen“ erfassen soll. Dies lässt sich zwar dahingehend interpretieren, dass stattgebende Entscheidungen nicht von der Norm erfasst werden, jedoch ist auch dies nicht eindeutig. Gemeint sein könnte auch, dass jede Entscheidung erfasst ist, die potenziell schwerwiegende Beeinträchtigungen zur Folge haben kann. Auch die deutschen Datenschutzbehörden haben bisher nicht bestätigt, dass Art. 22 Abs. 1 DSGVO stattgebende Entscheidungen nicht erfasst.

Die Rechtslage bleibt daher unsicher, solange keine Entscheidung des EuGH vorliegt.

Um die Rechtssicherheit für die Versicherungswirtschaft bis zu einer Entscheidung des EuGH zu erhalten, schlagen wir daher vor,

§ 37 Abs. 1 Nr. 1 BDSG nicht zu streichen.

4.2.2. Anpassung der Ausnahmen in § 37 BDSG für automatisierte Einzelfallentscheidungen in der Versicherungswirtschaft

Um der Digitalisierung in der Versicherungswirtschaft angemessen Rechnung zu tragen, halten wir es darüber hinaus für geboten, § 37 BDSG so anzupassen, dass in diesem Bereich vollautomatisierte Entscheidungen grundsätzlich zulässig sind.

Das Versicherungsgeschäft ist ein Massengeschäft. Unsere Mitgliedsunternehmen verwalten mehr als 465 Mio. Versicherungsverträge. Sie regulieren Schäden und erbringen Leistungen in Höhe von jährlich mehr als 180 Mrd. Euro. Durch die vollautomatisierte Leistungsprüfung und -abwicklung erhalten Kunden und Geschädigte unkomplizierter und erheblich schneller als bei manueller Bearbeitung die ihnen zustehenden Leistungen. Im Zuge zunehmender Digitalisierung müssen Versicherer auch in der Lage sein, vollautomatisiert über Anträge auf Versicherungsschutz zu entscheiden. Nur so kann den Wünschen der Kunden, die eine schnelle Bearbeitung ihrer Anliegen erwarten, Rechnung getragen werden.

Beispiele:

- Ein Kunde möchte eine Unfallversicherung noch vor einem Sporturlaub am Wochenende elektronisch abschließen. Der Versicherer bietet hierfür einen Online-Abschluss mit einer Gesundheitsfrage an.
- Ein Unfallversicherer zahlt bei einem Krankenhausaufenthalt Krankentagegeld aus. Der Kunde beantragt Tagegeld für 11 Tage, legt aber eine Bescheinigung vor, aus der hervorgeht, dass er nur 10 Tage lang im Krankenhaus war. Die Bescheinigung wird automatisiert ausgelesen, der Bescheid wird automatisiert erstellt und verschickt und der Kunde erhält sofort Krankentagegeld für 10 Tage. Wegen des verbleibenden Tages kann er sich mit seinem Versicherer in Verbindung setzen, sofern er weiterhin der Ansicht ist, hierfür Ersatz beanspruchen zu können.

In dem zuerst genannten Beispiel wären nach § 37 BDSG in der aktuellen Fassung vollautomatisierte Entscheidungen nicht ausdrücklich erlaubt, weil § 37 BDSG das Antragsverfahren nicht abdeckt. Im zweiten Beispiel wäre keine vollautomatisierte Entscheidung möglich, weil dem Begehren nicht vollumfänglich stattgegeben wird und der in § 37 Abs. 1 Nr. 2 genannte Sonderfall (Krankenversicherung) nicht vorliegt.

Die in Art. 22 Abs. 2 DSGVO enthaltenen Ausnahmen helfen zurzeit in der Praxis nicht weiter, denn sie werden von den Datenschutzbehörden sehr eng ausgelegt. Die Behörden betrachten vollautomatisierte Entscheidungen als nicht „erforderlich“ für den Abschluss oder die Erfüllung des Versicherungsvertrages im Sinne von Art. 22 Abs. 2 lit. a) DSGVO, da der Vertrag auch manuell abgeschlossen und durchgeführt werden könne. Ist die betroffene Person nicht selbst der Vertragspartner des Versicherers (z. B. ein von der versicherten Person geschädigter Dritter in der Kfz-Haftpflichtversicherung), greift die Ausnahme nach Art. 22 Abs. 2 Buchst. a) DSGVO gar nicht. Daher ist für diese in der Praxis häufige Konstellation unbedingt eine Regelung nötig. Für diesen Fall erkennt auch bereits der **Evaluierungsbericht** des BMI zum BDSG auch dem Jahr 2021 den Regelungsbedarf (S. 52). Auch Einwilligungen gemäß Art. 22 Abs. 2 lit. c) DSGVO ermöglichen keine vollautomatisierte Entscheidung, denn die deutschen Datenschutzbehörden sehen diese nur dann als freiwillig an, wenn das Unternehmen von Anfang an eine menschliche Prüfung als frei wählbare Alternative anbietet. Die in Art. 22 Abs. 3 DSGVO ohnehin vorgesehene menschliche Prüfung auf Wunsch des Kunden nach der Entscheidung (also sozusagen auf zweiter Stufe) reicht den Behörden nicht aus.

Vorschlag der deutschen Versicherungswirtschaft:

Dem dargestellten Bedarf und dem von Artikel 1 Ziffer 11 des Referentenentwurfs verfolgten Zeil könnte rechtssicher mit einer Änderung des § 37 BDSG Rechnung getragen werden. Die dazu erforderlichen Öffnungen enthält die DSGVO in Art. 22 Abs. 2 lit. b) und Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. g) DSGVO.

Wir schlagen daher vor, **§ 37 BDSG Abs. 1 wie folgt zu ändern**:

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel 22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen **des Abschlusses eines Versicherungsvertrages oder** der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde oder

2. ~~**die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und**~~ der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens im Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

4.3. Eindeutige gesetzliche Erlaubnisnorm für die Verarbeitung von Gesundheitsdaten zu Versicherungszwecken (§ 22 BDSG)

In § 22 BDSG sollte eine eindeutige gesetzliche Erlaubnisgrundlage für die Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Versicherungsverträgen (einschließlich der Rückversicherung) aufgenommen werden. Zumindest sollte die Anwendbarkeit des Art. 9 Abs. 2 lit. f) DSGVO, der die Verarbeitung von Gesundheitsdaten zur Geltendmachung, Ausübung und Verteidigung rechtlicher Ansprüche erlaubt, auf die Durchführung von Versicherungsverträgen in der Gesetzesbegründung klargestellt werden.

In der Lebens-, Kranken- und Unfallversicherung (einschließlich der Rückversicherung) können Verträge nur abgeschlossen und durchgeführt werden, wenn Gesundheitsdaten verarbeitet werden. Gesundheitsdaten müssen aber auch in der Haftpflicht- und Rechtsschutzversicherung verarbeitet werden, wenn Ansprüche wegen Gesundheitsschäden geltend gemacht werden.

Nach Auffassung der deutschen Versicherungswirtschaft ist die zur Durchführung eines Versicherungsvertrages erforderliche Verarbeitung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. f) DSGVO erlaubt. Denn hier geht es um die Durchsetzung bzw. Abwehr von Ansprüchen. Die Rechtslage ist allerdings unsicher. Von den deutschen Datenschutzbehörden wird dies überwiegend abgelehnt.

Andere EU-Länder verfügen über spezielle nationale Erlaubnisnormen unterschiedlichen Umfangs zur Verarbeitung von Gesundheitsdaten zum Abschluss und/oder zur Durchführung eines Versicherungsvertrages. Ein Beispiel ist § 11a des österreichischen Versicherungsvertragsgesetzes. Andere Länder, z. B. Bulgarien, Niederlande, Polen, Slowakei und Spanien haben entsprechende spezielle Regelungen. Die Regelungen basieren z. T. auf Art. 9 Abs. 2 b), g) bzw. h) DSGVO oder sie werden auf Art. 9 Abs. 4 DSGVO gestützt. Teils werden sie auch als Konkretisierungen des Art. 9 Abs. 2 lit. f) DSGVO verstanden. Die Datenschutzbehörden einiger EU-Länder, z. B. Dänemark und Tschechien, wenden Art. 9 Abs. 2 lit. f) DSGVO direkt an.

Greift keine gesetzliche Erlaubnis, muss die Verarbeitung der Gesundheitsdaten auf eine Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DSGVO gestützt werden. **Die Verhandlung einer Muster-Einwilligung zwischen der deutschen Versicherungswirtschaft und der Datenschutzkonferenz dauert inzwischen schon mehr als vier Jahre an**. Inzwischen greifen einzelne Datenschutzbehörden die Einwilligung sogar als unfreiwillig an[1], sodass nicht einmal mehr auf diese Weise Rechtssicherheit erzielt werden kann.

Die unklare Rechtslage führt zu kritischen Nachfragen von Geschädigten und ihren Rechtsanwälten, die die Einholung einer Einwilligung als Versuch der Versicherungswirtschaft ansehen, die Schadenregulierung zu verzögern. Es kommt schließlich zu Schwierigkeiten im grenzüberschreitenden Datenverkehr mit Ländern, in denen Versicherer keine Einwilligung einholen müssen. Deren Rückversicherer mit Sitz in Deutschland erhalten keine Einwilligung über den ausländischen Erstversicherer. Sie haben aber auch keinen direkten Kontakt zu dem Kunden in dem anderen Land, um dessen Einwilligung einzuholen.

Eine eindeutige gesetzliche Erlaubnisgrundlage für die Datenverarbeitung zum

[1] 5. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen über das Ergebnis der Tätigkeit im Jahr 2022, Ziffer 16.8, S. 75.

Abschluss und zur Durchführung von Versicherungsverträgen würde für deutsche Erst- und Rückversicherer die dringend benötigte Rechtsklarheit schaffen. Sie würde den Datentransfer zur Abwicklung des Versicherungsgeschäfts auf europäischer Ebene erleichtern und diese Standortnachteile deutscher Erst- und Rückversicherer aufheben. Zudem würde die Regelung verhindern, dass bei einem Widerruf der Einwilligung Vertragsrecht und Datenschutzrecht auseinanderlaufen. Die Erbringung der vertraglich geschuldeten Leistungen würde nicht an einer ggf. fehlenden Einwilligung scheitern.

Vorschlag der deutschen Versicherungswirtschaft:

Wir schlagen vor, in § 22 Abs. 1 Nr. 1 BDSG eine **gesetzliche Erlaubnisgrundlage für die Datenverarbeitung zum Abschluss und zur Durchführung von Versicherungsverträgen einschließlich der Rückversicherung und der Regulierung von Drittansprüchen in der Haftpflichtversicherung** aufzunehmen. Vorbild könnte § 11a Abs. 1 des österreichischen Versicherungsvertragsgesetzes sein.

Hilfsweise würde aber auch schon eine **Klarstellung in der Begründung zu § 22 BDSG**, dass diese Verarbeitung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. f) DSGVO als Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erlaubt ist, für Rechtssicherheit sorgen.

Ferner verweisen wir auf die Forderungen in der Stellungnahme des PKV-Verbandes, die wir ebenfalls unterstützen.

4.4. Rechtssicherheit für die Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen (Art. 10 DSGVO)

Die Versicherungswirtschaft ist darauf angewiesen, Daten über Straftaten und strafrechtliche Verurteilungen zu verarbeiten. Das gilt insbesondere für die Erfüllung der Anforderungen an die **Überprüfung der Zuverlässigkeit von Personen in Leitungs- und Schlüsselfunktionen** sowie von Versicherungsvermittlern. Daten über Straftaten können darüber hinaus in **vielfältigen Konstellationen beim Abschluss und der Durchführung von Versicherungsverträgen** anfallen.

Beispiele:

- Versicherungsunternehmen sind zur Überprüfung der Zuverlässigkeit von Personen in Leitungs- und Schlüsselfunktionen nach Art. 273 Nr. 4 VO(EU) 2015/35 sowie von Versicherungsvermittlern nach Art. 10 Abs. 3 der Richtlinie (EU) 2016/97 verpflichtet. Dazu müssen sie Führungszeugnisse nach dem

Bundeszentralregistergesetz oder vergleichbare Unterlagen anfordern, aus denen sich ggf. strafrechtliche Verurteilungen ergeben. Wenn es später zu einer Straftat der Personen gekommen ist, müssen sie nachweisen können, dass sie eine entsprechende Prüfung vorgenommen haben.

- Bei der Strafrechtsschutzversicherung sind Straftaten, strafrechtliche Ermittlungen, Verfahren und Verurteilungen Leistungsauslöser für den Versicherungsschutz, aber auch für die Entscheidung über den Abschluss eines Versicherungsvertrages relevant.
- Hat ein Arbeitnehmer eine Rechtsschutzversicherung abgeschlossen und wird sein Arbeitsverhältnis wegen einer (vermeintlich oder tatsächlich begangenen) Straftat oder Verurteilung gekündigt, muss der Versicherer den Fall bearbeiten können.
- Geschädigte begründen Ansprüche damit, dass der Schädiger eine Straftat begangen hat, z. B. ein Verkehrsdelikt in der Kraftfahrt-Haftpflichtversicherung.
- In der Gebäudeversicherung wird geprüft, ob Brandstiftung vorliegt.

Außerdem müssen Unternehmen in der Lage sein, einen gegen sie gerichteten Betrug abzuwehren und erfahren dabei ggf. auch von einer strafrechtlichen Verurteilung. Die DSGVO bejaht ausdrücklich ein berechtigtes Interesse des für die Datenverarbeitung Verantwortlichen zur Betrugsabwehr (ErwGr. 47, Satz 6 DSGVO). Schließlich muss eine Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen auch möglich sein, um durch eine strafbare Handlung entstandene zivilrechtliche Ansprüche durchsetzen zu können.

In allen genannten Fällen ist die Datenverarbeitung nach Art. 6 DSGVO zulässig.

Gemäß Art. 10 DSGVO dürfen Daten über Straftaten und strafrechtliche Verurteilungen auf Grundlage von Art. 6 Abs. 1 DSGVO aber nur verarbeitet werden

- unter behördlicher Aufsicht oder
- wenn dies nach Unionsrecht oder dem Recht eines Mitgliedstaates, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorsieht, zulässig ist.

Die Versicherungswirtschaft ist der Ansicht, dass die Versicherungsaufsicht als eine „behördliche Aufsicht“ i. S. v. Art. 10 DSGVO verstanden werden sollte. In der Kommentarliteratur wird der Begriff jedoch häufig sehr eng verstanden[2].

Vorschlag der deutschen Versicherungswirtschaft:

[2] Z. B. Schwartmann/Jaspers/Thüsing/Kugelmann, Datenschutz-GVO/BDSG, 2. Aufl. 2020, Art. 10 Rn. 4; Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018 Art. 10 Rn. 7.

- **Im BDSG sollte geregelt werden, dass Art. 10 DSGVO der Verarbeitung von Daten über Straftaten und strafrechtliche Verurteilungen nicht entgegensteht, wenn diese zur Erfüllung aufsichtsrechtlicher Anforderungen, im laufenden Versicherungsgeschäft, zur Verhinderung von Betrug oder zur Durchsetzung rechtlicher Ansprüche erforderlich ist. Eine Öffnungsklausel für eine solche Regelung enthält Art. 10 Satz 1 DSGVO.**
- **Sofern davon ausgegangen wird, dass die Versicherungsaufsicht eine „behördliche Aufsicht" i. S. v. Art. 10 DSGVO ist, sollte das BDSG dies zumindest klarstellen.**

4.5. Rechtssicherheit für die Umsetzung der europäischen Digitalstrategie

4.5.1. Anonymisierung und Pseudonymisierung

Der europäische Gesetzgeber verpflichtet Unternehmen, im Rahmen von Vorgaben zum Datenteilen Daten zu anonymisieren, aggregieren oder pseudonymisieren, ohne hierfür eine eindeutige Rechtsgrundlage zu schaffen, z. B. Art. 18 Abs. 5 Data Act. Die deutschen Datenschutzbehörden einschließlich des BfDI vertreten überwiegend die Ansicht, dass die Anonymisierung eine Verarbeitung darstelle und daher einer Rechtsgrundlage bedarf[3], die z. B. der Data Act zumindest ausdrücklich nicht enthält. Selbst wenn man in derartigen Fällen Art. 6 Abs. 1 lit c) oder lit. f) DSGVO als Rechtsgrundlage betrachtet, gilt dies nicht für **besondere Kategorien personenbezogener Daten**. Entgegen dem Erwägungsgrund 50 der DSGVO verstehen die deutschen Datenschutzbehörden auch Art. 6 Abs. 4 DSGVO nur als Erlaubnis für die Zweckänderung, aber nicht als Rechtsgrundlage für die Datenverarbeitung.

Eine Rechtsgrundlage für Anonymisierungen und Pseudonymisierungen zur Erfüllung rechtlicher Verpflichtungen sollte daher in das BDSG aufgenommen werden, damit die Unternehmen, die Anfragen erfüllen müssen, keinem Bußgeld- oder Schadensersatzrisiko ausgesetzt sind. Die Rechtsgrundlage sollte auch Anonymisierungen und Pseudonymisierungen erfassen, die nötig sind, um die Kopien der Daten zu anderen legitimen Zwecken, z. B. zur Entwicklung neuer Anwendungen und Systeme und deren Tests, zu nutzen. Eine Öffnungsklausel für eine solche Regelung enthält für besondere Kategorien personenbezogener Daten Art. 9 Abs. 2 lit. g) DSGVO. Alternativ könnte eine entsprechende Klarstellung in die Gesetzesbegründung, z. B. bei § 24 BDSG, aufgenommen werden.

[3] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVP unter besonderer Berücksichtigung der TK-Branche, 29.06.2020, Pkt. 3., S. 6

Die deutsche Versicherungswirtschaft schlägt vor,

- **eine eindeutige Rechtsgrundlage für die Anonymisierung und Pseudonymisierung von Daten zu schaffen, die auch besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DSGVO erfasst.**
- **Sofern für die Anonymisierung nach Auffassung der Bundesregierung keine Rechtsgrundlage nötig sein, sollte dies klargestellt werden.**

4.5.2. Entwicklung und Tests von Systemen und Anwendungen

Es existiert bisher keine eindeutige Rechtslage für das Training und Tests von neuen IT-Anwendungen und Systemen mit besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten). Der Vorschlag der EU-Kommission zu einer Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO) sieht zwar in Art. 10 Abs. 5 eine Rechtsgrundlage vor. Diese beschränkt sich aber leider auf die Entwicklung von hochriskanter KI und gilt nur, soweit dies unbedingt für Zwecke der Verhinderung von Diskriminierungen erforderlich ist. Dieser Ansatz ist ein guter erster Schritt, der in keinem Fall wieder – wie im EU-Parlament gefordert – eingeschränkt werden sollte. Da es im Interesse der Allgemeinheit ist, dass KI- und andere IT-Systeme zu korrekten Ergebnissen kommen, sollten Tests mit pseudonymisierten Echtdaten, inklusive Gesundheitsdaten, zugelassen werden.

Die deutsche Versicherungswirtschaft schlägt vor,

eine eindeutige Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, insbesondere von besonderen Kategorien nach Art. 9 Abs. 1 DSGVO, für die Entwicklung und Tests von neuen IT-Anwendungen und Systemen zu schaffen.

4.6. Regelungen zu Betroffenenrechten

Dass der deutsche Gesetzgeber die Öffnungsklausel des Art. 23 DSGVO nutzt, ermöglicht eine sachgerechte und verhältnismäßige Anwendung der Regelungen der DSGVO zu den Betroffenenrechten. Die deutsche Versicherungswirtschaft begrüßt die neue ausdrückliche Ausnahme in § 34 Abs. 1 Satz 2 RefE-BDSG (neu) zum Schutz von Betriebs- und Geschäftsgeheimnissen sehr. Darüber hinaus möchten wir auf einige Unstimmigkeiten in den Ausnahmen zu den Betroffenenrechten hinweisen, die im Zuge der aktuellen Änderung des BDSG behoben

werden sollten.

4.6.1. Schutz von Betriebs- und Geschäftsgeheimnissen nach § 34 Abs. 1 Satz 2 RefE-BDSG

Die deutsche Versicherungswirtschaft begrüßt ausdrücklich die Ergänzung des Satzes 2 in § 34 Abs. 1 Satz 2 RefE-BDSG (Artikel 1, Ziffer 10, a), bb)). Damit wird klargestellt, dass das Recht auf Auskunft nach Art. 15 DSGVO auch insoweit nicht besteht, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt. Dieses Verständnis lässt sich zwar auch bereits aus § 29 Abs. 1 Satz 2 BDSG herleiten. Durch die Änderung des § 34 BDSG wird aber Rechtssicherheit hergestellt.

4.6.2. Verweis in § 34 Abs. 1 Nr. 1 BDSG auf § 33 Abs. 1 Nr. 2 lit. b) BDSG ergänzen

In § 34 Abs. 1 Nr. 1 BDSG befindet sich derzeit eine **Regelungslücke**. Die Vorschrift sieht zwar eine Ausnahme vom Auskunftsanspruch vor, wenn die betroffene Person nach § 33 Abs. 1 Nr. 2 lit. b) BDSG nicht informiert werden müsste. Es fehlt aber eine entsprechende Ausnahme für § 33 Abs. 1 Nr. 2 lit. a). Danach kann auf eine Information verzichtet werden, wenn diese die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder die Verhütung von Schäden durch Straftaten betrifft.

Die Übertragung der Ausnahme von der Informationspflicht auch auf die Auskunftspflicht erscheint sachgerecht und notwendig. So sollte es – z. B. wenn ein Betrug naheliegt – möglich sein, vorerst keine Auskünfte nach Art. 15 DSGVO zu erteilen. Das gilt insbesondere, wenn das Unternehmen noch die Erstattung einer Strafanzeige prüft oder wenn bereits polizeiliche Ermittlungen laufen.

Vorschlag der deutschen Versicherungswirtschaft:

> **Die Verweisung in § 34 Abs. 1 Nr. 1 BDSG sollte sich auch auf § 33 Abs. 1 Nr. 2 lit. a) BDSG erstrecken. Es sollte möglich sein, vorerst keine Auskünfte zu erteilen, wenn dies die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche oder die Verhütung von Schäden durch Straftaten beeinträchtigen würde.**

4.6.3. Übertragung der Ausnahme des § 32 Abs. 2 Satz 3 BDSG in § 33 Abs. 2 BDSG

Eine Unstimmigkeit besteht auch zwischen § 32 Abs. 2 Satz 3 und § 33 Abs. 2 BDSG.
Nach § 32 Abs. 1 Nr. 4 und 5 BDSG kann auf eine Information der Betroffenen nach Art. 13 DSGVO verzichtet werden, wenn diese die Verteidigung von Rechtsansprüchen oder die vertrauliche Übermittlung an eine öffentliche Stelle gefährden könnte. Für diese Fälle sieht § 32 Abs. 2 Satz 3 BDSG vor, dass auch die Pflichten zur Information der Öffentlichkeit und die Dokumentationspflicht nach § 32 Abs. 2 Satz 1 und 2 BDSG nicht gelten. Dies würde nämlich die Zwecke dieser Ausnahmen unterlaufen.

In § 33 Abs. 2 BDSG, der sich auf die vergleichbaren Ausnahmen von der Informationspflicht nach Art. 14 DSGVO in § 33 Abs. 1 Nr. 2 a) und b) BDSG bezieht, fehlt jedoch eine entsprechende Ausnahme. Es gibt keinen Grund, warum hier Pflichten zur Information der Öffentlichkeit und die Dokumentationspflicht bestehen sollten. Vielmehr ist die Interessenlage bei der Information nach Art. 13 und Art. 14 DSGVO gleich, sodass die Regelung des § 32 Abs. 2 Satz 3 BDSG in § 33 Abs. 2 BDSG übertragen werden sollte.

Vorschlag der Versicherungswirtschaft:

> **Die in § 32 Abs. 2 Satz 3 BDSG getroffene Regelung zum Verzicht auf Maßnahmen wie einer Information der Öffentlichkeit in besonderen Fällen, sollte in § 33 Abs. 2 BDSG übernommen werden.**

Berlin, den 6. September 2023

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)449

Gesellschaft für Datenschutz
und Datensicherheit e.V.

An die Mitglieder des Innenausschusses über das Sekretariat
des Innenausschusses

Innenausschuss@bundestag.de

Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes

- Beamtenrechtliche Stellung des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit -

GDD e.V.
Heinrich-Böll-Ring 10
53119 Bonn
T +49 228 969675-00
F +49 228 969675-25
info@gdd.de
www.gdd.de

Der Amtsantritt von Frau Prof. Dr. Specht-Riemenschneider als BfDI, verzögert sich offensichtlich aus beamtenrechtlichen Gründen. Die Regelungen zur Ernennung der oder des BfDI sind erkennbar nicht darauf angelegt, verbeamtete Experten und Expertinnen aus den Bundesländern für dieses Amt zu gewinnen. Da die Beauftragten für Datenschutz sich nach der DS-GVO durch eine entsprechend hohe Expertise im Datenschutz auszeichnen sollen, ist es sinnvoll den Kreis möglicher Bewerbenden auch für die Zukunft möglichst weit zu ziehen. Offensichtlich bestehende beamtenrechtliche Probleme für Beamte der Länder sollten beseitigt werden, um diese nicht dadurch von einer Übernahme dieses wichtigen Amtes abzuhalten, da ihr bisheriger Status durch die Wahl zur bzw. zum BfDI gefährdet sein kann.

Das beamtenrechtliche Problem liegt darin begründet, dass mit der Ernennung ein besonderes Amtsverhältnis zum Bund begründet wird, das nach § 22 Abs. 2 Beamtenstatusgesetz grundsätzlich zur Auflösung des bisherigen Beamtenverhältnisses zum Land führt. Durch den Verweis in § 12 Abs. 3 BDSG auf das Bundesministergesetz ist lediglich gewährleistet, dass die oder der BfDI vom Land zurückgenommen werden kann, nicht jedoch, dass dies auf Antrag gewährleistet ist und der ursprüngliche Status wiederhergestellt wird. Stattdessen ist der Ruhestand die Folge, wenn das Land die oder den ausscheidenden BfDI nicht wieder anstellen möchte. Dies ist schon deswegen nicht zweckmäßig, da die Tätigkeit als BfDI von vornherein auf maximal 10 Jahre angelegt ist. Wird zum BfDI gewählt, wer das Mindestalter gerade so erfüllt, stünde für diese Person mit 45 Jahren der Ruhestand in Aussicht und nicht das Fortwirken an alter Stelle. Das erscheint wenig motivierend für engagierte Bewerbende.

Zweckmäßiger erscheint daher, die BfDI-Regelungen künftig an den Regelungen des Abgeordnetengesetzes zu orientieren. Die §§ 5 ff. AbgG sehen ein Ruhen des bisherigen Status sowie Rückkehrrechte der Mandatsträger vor.

Die anstehende Überarbeitung des BDSG sollte daher genutzt werden, die bestehenden beamtenrechtlichen Probleme im Zusammenhang mit der BfDI-Ernennung direkt zu lösen. Entsprechende Anpassungen im § 12 BDSG würden hier eine schnelle Lösung bieten, die sowohl künftige Verzögerung beim Antritt von Landesbeamten – wie wir sie derzeit sehen - vermeiden, als auch dieses wichtige Amt noch einmal attraktiver für junge und hochqualifizierte Bewerbende machen würden.

Wir schlagen dafür folgende Ergänzung des § 12 Abs. 1 BDSG vor:
Die Rechte und Pflichten aus dem Dienstverhältnis einer oder eines Beamten mit Dienstbezügen ruhen mit dem Beginn des Amtsverhältnisses. Mit erfolgter Wahl gilt das Einvernehmen im Sinne des § 22 Abs. 2 S. 1 Beamtenstatusgesetz oder § 31 Abs. 1 S. 2 Nr. 2 Bundesbeamtengesetz zur Fortdauer eines bestehenden Beamtenverhältnisses zu einem anderen Dienstherrn als erteilt. Nach Beendigung des Amtsverhältnisses ist die Beamtin oder der Beamte auf ihren oder seinen Antrag, der binnen drei Monaten seit der Beendigung des Amtsverhältnisses zu stellen ist, spätestens drei Monate nach Antragstellung wieder in das frühere Dienstverhältnis zurückzuführen. Das ihr oder ihm zu übertragene Amt muss derselben oder einer gleichwertigen Laufbahn angehören wie das zuletzt bekleidete Amt und mit mindestens demselben Endgrundgehalt ausgestattet sein. Vom Tage der Antragstellung an erhält sie oder er die Dienstbezüge des zuletzt bekleideten Amtes. Für Hochschullehrer im Sinne des § 42 des Hochschulrahmengesetzes gilt das vorstehende mit der Maßgabe, dass sie in ihrem bisherigen Amt an der gleichen Hochschule und unter Beibehaltung der vor der Begründung des Amtsverhältnisses gewährten Leistungsbezüge wiederverwendet werden müssen.

Als größte Fachgesellschaft für Datenschutz und Datensicherheit würden wir es begrüßen, wenn die Mitglieder des Innenausschusses das Problem aufgreifen und mit der skizzierten oder einer gleichwertigen Anpassung des § 12 BDSG einer Lösung zuführen und damit das Amt der bzw. des BfDI stärken würden. Das laufende Gesetzgebungsverfahren zum BDSG bietet dafür eine schnelle Gelegenheit.

Bonn, den 18.06.2024

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)453

Die Wirtschaftsauskunfteien e. V.
Stellvertretende Geschäftsleitung
Natascha Reifert

Kormoranweg 5
65201 Wiesbaden

Telefon 0611 / 9278-320
Geschaeftsleitung@die-wirtschaftsauskunfteien.de
www.die-wirtschaftsauskunfteien.de

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache 20(4) 446

Per Mail: Innenausschuss@bundestag.de

Wiesbaden, 15. April 2024

Stellungnahme zum Ersten BDSG-Änderungsgesetz

Sehr geehrte Damen und Herren,

wir möchten nochmals die Gelegenheit ergreifen, unsere Überlegungen zum aktuellen Entwurf zum Ersten BDSG Änderungsgesetzes vorzutragen.

A) Einleitung:

Ausweislich der Gesetzesbegründung soll durch den Gesetzentwurf einerseits der Koalitionsvertrag und andererseits das Urteil des Europäischen Gerichtshofes vom 7. Dezember 2023 – C634/21 „SCHUFA Holding (Scoring)“ aufgreifend, § 31 durch einen neuen § 37a BDSG ersetzt werden.[1] Sowohl der Koalitionsvertrag, als auch die Entscheidung des Europäische Gerichtshof (EuGH) sind durch das Bestreben nach Erhöhung von Transparenz beim Scoring/Profiling motiviert. Es erscheint im Gesamtzusammenhang nicht unwichtig daran zu erinnern, dass das dem Vorlageverfahren zu Grunde liegende Ausgangsverfahren nicht etwa gegen die SCHUFA Holding AG geführt wurde, sondern gegen den Hessischen Datenschutzbeauftragten (HBDI). Zu der gegen ihn beim Verwaltungsgericht

[1] S. Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, S. 1

Wiesbaden (VG Wiesbaden) eingereichten Klage war es nur gekommen, weil dieser die ursprünglich von der SCHUFA Holding AG der Klägerin erteilte Auskunft nach Art. 15 DSGVO auch bezüglich der darin enthaltenen Angaben zum Scoring als grundsätzlich ausreichend angesehen hatte.[2] Im Zeitpunkt der Klage konnten also die Auskunfteien von der grundsätzlichen Rechtmäßigkeit der durch sie im Rahmen von Auskunftsersuchen nach Art. 15 DSGVO erteilten Auskünfte auch hinsichtlich der Angaben zum Scoring/Profiling in Übereinstimmung zumindest eines für sie wesentlichen Teils der Datenschutzkonferenz (DSK) ausgehen. Ein Regelungsbedürfnis bestand also nicht. Erst das VG Wiesbaden hatte daran Zweifel und legte entsprechende Fragen dem EuGH vor. Dabei fragte das VG Wiesbaden aber nicht schlicht nach der Reichweite des Art. 15 Abs. Buchst. h) DSGVO[3], sondern knüpfte – etwas konstruiert - an Art. 22 DSGVO. Das VG Wiesbaden war offensichtlich der Meinung, dass Art. 15 Abs. 1 Buchst. h) DSGVO keinen allgemeinen Transparenzanspruch beim Scoring enthält[4]. Nur deshalb kam es dann zur vermeintlich bestehenden Regelungslücke, die im Verhältnis zum Entscheider nach Art. 22 DSGVO und dem externen Dienstleister vermeintlich besteht. Der EuGH hat die Vorlage seinerseits nicht wegen Unzulässigkeit zurückgewiesen, sondern die Überlegungen des VG Wiesbaden aufgegriffen. Es kam dann zu dem Ergebnis, dass es nur gelingt den externen Scoringdienstleister zur Transparenz nach Art. 15 Abs. 1 Buchst. h) DSGVO zu verpflichten, indem man ihn in den Anwendungsbereich des Art. 22 DSGVO „hineinzieht“. Dies soll dann erforderlich sein, wenn der durch den Dienstleister gelieferte Wahrscheinlichkeitswert für den letztendlich (über den Vertrag) befindenden Entscheider „maßgeblich“ ist.

B) Gesetzentwurf enthält keine Ausführungen zum Begriff der Maßgeblichkeit

Der EuGH schafft mit dem Kriterium der Maßgeblichkeit einen neuen unbestimmten Rechtsbegriff, ohne nähere Hinweise wie dieser ggf. durch den nationalen Gesetzgeber oder die Datenschutzaufsichtsbehörden auszuformen wäre. Etwas überraschend greift der vorliegende Gesetzentwurf dieses Thema nicht auf, sondern formuliert im Rahmen des Art. 22 Abs. 2 Buchst. b DSGVO einen Ausnahmetatbestand für Art. 22 Abs. 1 DSGVO. Der Gesetzentwurf übergeht dabei

[2] S. Sachverhaltsfeststellungen EuGH Rs. C634/21, Rn. 14ff
[3] Vgl. dagegen EuGH Rs.C-203/22
[4] Zum Streitstand s. Gola/Heckmann-Franck, DSGVO, Art. 15, Rn. 17ff

die für die Anwendung des Ausnahmetatbestandes des Art. 22 Abs. 2 Buchst. b) DSGVO relevante Frage, ob überhaupt der Anwendungsbereich des Art. 22 Abs. 1 DSGVO eröffnet ist. Es verbleibt damit bei der Rechtsunsicherheit, die durch das Maßgeblichkeitskriterium entstanden ist. Sowohl für die Wirtschaft als auch für die betroffenen Personen wäre es für die Rechtsklarheit aber wünschenswert, durch den Gesetzgeber Hinweise zur praktischen Ausformung des Maßgeblichkeitskriteriums zu erhalten. Es macht auch keinen Sinn, diese Ausformung den Parteien des Entscheidungsprozesses zu überlassen, wenn nicht zumindest eine hinreichende Konkretisierung erfolgt.

Ein Vorbild hierfür könnte dem aktuell noch bestehenden § 31 BDSG entnommen werden, der (noch) bei der Verwendung von Anschriftendaten formuliert, dass Anschriftendaten „nicht ausschließlich“ zur Berechnung von Wahrscheinlichkeitswerten genutzt werden dürfen. Dabei ist zu bedenken, dass die Auskunfteien einen Wahrscheinlichkeitswert nur auf solchen Daten ermitteln können, die sie zulässigerweise verarbeiten. Die Definition des Maßgeblichkeitskriteriums muss daher bei der Weiterverwendung der gelieferten Entscheidungshilfe ansetzen. Der Einleitungssatz des § 37a BDSG-E knüpft aber an die Erstellung und Verwendung gleichermaßen an, sodass eine entsprechende Konkretisierung des Maßgeblichkeitskriteriums dort nicht verankert werden kann. Dies kann wahrscheinlich nur durch die Schaffung eines neuen Absatzes und damit Neukonzepetion der gesamten Vorschrift gelingen, die die Voraussetzungen für die Erstellung und die sich dann ggf. anschließende Verwendung von Wahrscheinlichkeitswerten strikt trennt. Ohne dem bleibt jedoch die durch den neuen unbestimmten Rechtsbegriff entstandene Rechtsunsicherheit bestehen.

C) Der Anwendungsbereich der geplanten Vorschrift ist unklar

Der Anwendungsbereich des § 37a Abs. 2 BDSG-E ist offen und bietet daher erhebliche Rechtsunsicherheit. Die Vorschrift könnte auch als Verbot bestimmter Datenverarbeitungen verstanden werden. Eine Regelung über die Rechtmäßigkeit einer Datenverarbeitung ist aber nicht von Art. 22 Abs. 2 lit. b DSGVO gerade nicht gedeckt. Der Gesetzgeber läuft mithin Gefahr, eine offensichtlich europarechtswidrige Formulierung aufzunehmen. Auch der Bundesrat hat hierauf bereits hingewiesen.

§ 37a Abs. 3 BDSG kann als Verbot bestimmter Datenverarbeitungen verstanden werden. Gemäß Wortlaut dürften für das Kreditscoring nur noch besonders qualifizierte Negativdaten verwendet werden. Nach dieser Auslegung wäre die Verwendung sonstiger Daten (z.B. Positivdaten, Daten aus öffentlichen Registern, etc.) auch bei Vorliegen einer Einwilligung oder der Verwendung der Daten zur Erfüllung eines Vertrages ausgeschlossen. Diese Auslegung würde gegen Europarecht verstoßen, da die vom Gesetzgeber vorgesehene Öffnungsklausel – Art. 22 Abs. 2 lit. b DSGVO – eine solche Regelungswirkung nicht erlaubt.

D) Unzulässige Untersagung von Zweckänderungen: § 37a Abs. 2 Nr. 3 lit. b BDSG-E

Problem: Die Vorschrift kann so interpretiert werden, als wäre eine Zweckänderung von personenbezogenen Daten unzulässig, falls ein Verantwortlicher diese Daten zur Erstellung von Wahrscheinlichkeitswerten über eine Person verwendet. Dies würde die europarechtlich zwingende Vorschrift von Art. 6 Abs. 4 DSGVO verletzen.
Lösungsvorschlag: § 37a Abs. 2 Nr. 3 lit. b BDSG-E sollte gestrichen werden. Die in der DSGVO enthaltenen Regelungen sind abschließend, d.h. es gibt für nationales Recht keine Öffnungsklausel. Art. 6 Abs. 4 DSGVO löst die Problematik auch bereits abschließend und sinnvoll auf.
Die Stellungnahme des **Bundesrats** vom 22. März 2024 enthält diesbezüglich einen Ergänzungsvorschlag, der **nicht** übernommen werden sollte: Statt Streichung von § 37a Abs. 2 Nr. 3 lit. b BDSG-E schlägt der Bundesrat einen zusätzlichen Verweis auf die Grundsätze der Zweckbindung und Datenminimierung gem. Art. 5 Abs. 1 lit. b und c DSGVO vor. Dies würde die Europarechtswidrigkeit der Vorschrift nur verstärken.

E) § 37a BDSG-E erfasst auch Kreditscoring im B2B-Bereich

Problem: § 37a BDSG-E findet auch Anwendung auf das Erstellen von Wahrscheinlichkeitswerten im B2B-Bereich. Dies ist weder praktikabel, noch entspricht es der gesetzgeberischen Intention.
Lösungsvorschlag: Unternehmen im Sinne von § 14 BGB sollten ausdrücklich aus dem Anwendungsbereich ausgenommen werden.

F) Missverständnis bei der Regulierung von bestimmten Datenarten, z.B. Anschriftendaten oder Kontoinformationsdienstedaten

Problem: § 37a Abs. 2 Nr. 1 lit. d BDSG-E will die Nutzung von Anschriftendaten sowie Bankkontendaten untersagen, bzw. aus dem Anwendungsbereich der Erlaubnisvorschrift ausklammern. Dies steht nicht im Einklang mit den Schutzzielen von Art. 22 DSGVO. Ohne Anschriftendaten können z.B. eCommerce-Unternehmen keine Identitätsprüfung ihrer Kunden durchführen, um so z.B. Betrugsversuche zu erkennen. Auch der **Bundesrat** hat auf dieses Problem hingewiesen.
Sofern mit der Formulierung in § 37a Abs. 2 Nr. 1 Buchst. c) BDSG-E aus Kontoinformationsdiensten herrührende Daten gemeint sind, sollte dies auch so bezeichnet werden. Allerdings ist der Zugriff auf Kontoinformationen nach § 59 ZAG von der Zustimmung der betroffenen Person abhängig. Die Weiterverwendung solcher Informationen war nach bislang einhelliger Meinung nach den Regeln der DSGVO zu beurteilen. Sowohl der EDSA, als auch die LDI NRW kamen hierbei zu dem Ergebnis, dass eine Weiterverwendung unter Beachtung der Art. 6 und 7 DSGVO möglich ist.[5]
Es stellt sich daher die Frage, ob es einerseits nötig, andererseits zulässig ist, dies national zu regeln, ohne sich in Widerspruch zu Zulässigkeitsnormen der DSGVO zu setzen.

Ferner ist zu bedenken, dass nach der bisherigen Konzeption des § 37a BDSG-E nicht ausgeschlossen werden kann, dass der Anwendungsbereich weit über den der Auskunfteien reicht (s.o.). Instituten im Sinne des Finanzaufsichtsrechts wäre damit die Bildung von Wahrscheinlichkeitswerten unter Hinzunahme von Kontoinformationen verwehrt, obwohl die betroffene Person möglicherweise sogar Kunde des Hauses ist – und zwar sowohl im Kredit, als auch im Anlagebereich, der bekanntermaßen weitreichende Offenlegungspflichten kennt und auch im Kreditbereich schließt Art. 18 Abs. 3 Verbraucherkreditrichtlinie die Einbeziehung solcher Informationen vor. Aber selbst, wenn hier nur die Auskunfteien gemeint seien sollten, so würde sich auch dort die Frage stellen, warum diesen bei der Bildung von Wahrscheinlichkeitswerten bestimmte Parameter verwehrt werden sollen, die man der eigentlich vertragsschließenden Partei bei einer Beurteilung gerade zugesteht.

[5] 25. Tätigkeitsbericht LDI NRW, Ziffer 5.4

Wie die Gesetzesbegründung aufführt, wird § 37a Abs. 2 Nr. 1 Buchst. d) BDSG-E gegenüber § 31 dahingehend eingeschränkt, dass Anschriftendaten zur Erstellung und Verwendung von Wahrscheinlichkeitswerten überhaupt nicht mehr genutzt werden dürfen.[6] Mit der Begründungserwägung, wonach außerhalb des Anwendungsbereiches § 37a BDSG-E die Verarbeitung von Anschriftendaten stellt klar, dass sogn. Anschriftendaten zwar verarbeitet werden, aber nicht „gescored" werden dürfen. Das steht etwas im Widerspruch zu der vom Gesetzgeber selbst getätigten Feststellung, wonach § 37a BDSG-E keine Rechtsgrundlage, sondern nur eine Ausnahmevorschrift zu Art. 22 Abs. 1 DSGVO darstellt und sich die Zulässigkeit der Datenverarbeitung nach den allgemeinen Vorschriften, wie der des Art. 6 DSGVO richtet.[7] Dem entspricht auch die herrschende Meinung, wonach sich die Zulässigkeit des Profilings (zu dem die Erstellung und Verwendung von Wahrscheinlichkeitswerten ein Unterfall darstellen dürfte) im Wesentlichen nach Art. 6 Abs. 1 Buchst. f) DSGVO richtet. Es leuchtet nicht recht ein, warum sich die Zulässigkeit der Verarbeitung eines bestimmten Datums danach richten soll, ob sie nun Eingang in einen Wahrscheinlichkeitswert findet oder nicht. Dogmatisch wird durch § 37a BDSG-E über Art. 22 Abs. 2 DSGVO in die Zulässigkeitsvorschriften des Art. 6 DSGVO eingegriffen. Das ist aber – auch in Ansehung der dem Gesetzentwurf zugrunde liegenden EuGH-Entscheidung – unzulässig und europarechtswidrig.[8]

§ 37a Abs. 3 BDSG-E definiert zusätzlich für die Fälle des Abs. 1 Nr. 2 quasi im Sinne eines „Positivkataloges", welche Forderungsdaten berücksichtigt werden dürfen. Auch hier greifen die soeben ausgeführten Bedenken, dass mit der Begrenzung auf einen bestimmten Katalog die Verarbeitung anderer personenbezogener Daten bei der Erstellung und Verwendung von Wahrscheinlichkeitswerten ausgeschlossen werden soll, obwohl die Verarbeitung dieser Daten als „Klardatum" möglicherweise zulässig wäre und Art. 22 Abs. 2 Buchst. b) DSGVO gerade keine Begrenzung von Art. 6 DSGVO zulässt, es sei denn dies ergibt sich aus der DSGVO selbst, wie beispielsweise bei den Daten nach Art. 9 DSGVO.[9] Die immer wieder in der

[6] S. Gesetzesbegründung
[7] S. Gesetzesbegründung S. 23
[8] EuGH Rs. C-634/21, Rn. 68
[9] Die Einschränkung von Art. 6 DSGVO ergibt sich dort aus Art. 9 DSGVO selbst und im Rahmen von Art. 22 DSGVO aus dessen Abs. 4.

Gesetzesbegründung referenzierten „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person (Art. 22 Abs. 2 Buchst. b) DSGVO) lassen darüber hinaus nur Verfahrensrechte der betroffenen Personen zu, wie sie in Art. 22 Abs. 3 DSGVO erwähnt und in § 37a Abs. 6 DSGVO angelegt sind.[10] Eine weitere Ausformung dieser erscheint dagegen denkbar.

Lösungsvorschlag: Der Absatz II sollte gestrichen werden.

G) § 34 Abs. 1 S. 2 und § 37a Abs. 5 BDSG-E: Unverhältnismäßige Beeinträchtigung des Schutzes von Geschäftsgeheimnissen

Problem: § 34 Abs. 1 S. 2 und Abs. 5 BDSG-E werfen sowohl für sich genommen als auch gemeinsam gelesen rechtliche Bedenken auf: § 34 BDSG-E stellt die Wahrung von Geschäftsgeheimnissen unter den Vorbehalt der Interessenabwägung und erzeugt einen systematischen Bruch zu Art. 15 Abs. 4 DSGVO. § 37 Abs. 5 BDSG-E ist sehr wahrscheinlich unvereinbar mit Art. 15 Abs. 1 lit. h DSGVO.

Lösungsvorschlag: § 34 Abs. 1 S. 2 und § 37 Abs. 5 BDSG-E sollten gestrichen werden. Auf Empfehlung seiner Ausschüsse hat auch der **Bundesrat** gebeten, zu prüfen, ob § 34 Abs. 1 S. 2 BDSG-E gestrichen werden sollte.

Mit freundlichen Grüßen

[redacted]

Natascha Reifert

[10] EuGH Rs. C-634/21, Rn 67 f