bitkom

Bitkom Stellung-nahme

Bundesdatenschutz-gesetz 2023

Bitkom Stellungnahme zum BDSG-Änderungsgesetz

Auf einen Blick

BDSG-Änderungsgesetz

Ausgangslage

Das Bundesministerium des Inneren und für Heimat (BMI) veröffentlichte im August den (noch nicht ressortabgestimmten) Entwurf des Bundesdatenschutz-Änderungsgesetzes. Mit dem Gesetz werden Strukturreformen für die deutschen Datenschutzaufsichtsbehörden nach den Vorgaben des Koalitionsvertrags angestoßen und das Bundesdatenschutzgesetz (BDSG) aufgrund der Ergebnisse der Evaluierung in 2021 angepasst.

Bitkom-Bewertung

Geht in die richtige Richtung – Es ist richtig, dass das BDSG überarbeitet wird. Harmonisierung der Rechtsauslegung durch eine Strukturreform der Aufsichtsbehörden, mehr Rechtssicherheit und die Korrektur von missglückten BDSG-Regelungen sind dringend notwendig. Das Änderungsgesetz springt dabei jedoch noch deutlich zu kurz.

Das Wichtigste

Im Bitkom versammelt sich das größte und zugleich über alle Branchen erstreckende Datenschutz-Expertengremium Deutschlands. Unser Papier zeichnet daher mögliche Kompromisslinien vor und bildet die Industriepraxisperspektiven und -erfahrung ab:

- **Aufsichtsstruktur**
  Das derzeitige System aus 18 Datenschutzaufsichtsbehörden, die zu wenig untereinander abgestimmt sind, ist in Deutschland nicht tragfähig. Aus den unterschiedlichen Interpretationen der Landesaufsichtsbehörden resultiert eine Komplexität, die sowohl für kleine und mittelständische Unternehmen (KMU) als auch Unternehmen mit Niederlassungen bzw. Kundinnen und Kunden in mehreren Bundesländern enorme Herausforderungen bedeuten. Das BDSG-Änderungsgesetz enthält zwar einige Erleichterungen, aber nicht die benötigten strukturellen Änderungen, die für mehr Harmonisierung, Rechtssicherheit für Unternehmen und Entlastung der Aufsichtsbehörden sorgen würden.
- **Gesetzliche Änderungen aus einem Guss**
  Das BDSG-Änderungsgesetz enthält bereits einige richtige und wichtige Anpassungen, wie z. B. Klarstellungen zum Auskunftsanspruch. Jedoch sind weitere Änderungen notwendig. Das BMI führt in seiner Gesetzesbegründung aus, dass ein weiteres Änderungsgesetz geplant sei. Im Sinne der Effizienz und um schnellstmöglich die dringend benötigte Rechtssicherheit herzustellen, sollten die Änderungen jedoch schon in den nun vorliegenden Entwurf eingearbeitet werden.

65%

der Unternehmen sehen in der uneinheitlichen Auslegung des Datenschutzrechts in Deutschland ein Digitalisierungshemmnis (lt. einer Studie von Bitkom Research)

Bitkom-Zahl

65 Prozent

65 Prozent der Unternehmen sehen in der uneinheitlichen Datenschutzauslegung ein Digitalisierungshemmnis. 52 Prozent beklagen zudem die mangelnde Beratung durch Aufsichtsbehörden (lt. einer Studie von Bitkom Research).

Inhalt

1 Überblick und grundsätzliche Anmerkungen

Institutionalisierung der Datenschutzkonferenz

Bitkom steht der geplanten stärkeren Institutionalisierung der Datenschutzkonferenz als Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern im BDSG grundsätzlich positiv gegenüber. Dies sollte durch die Schaffung einer gemeinsamen Geschäftsstelle erfolgen, die die Kollaboration unterstützt, als einheitliche Ansprechstelle dient und beispielsweise bei der gemeinsamen Entwicklung von Formularen, Meldewegen etc. unterstützend tätig werden kann. Insbesondere die gemeinsame Positionsfindung ist essenziell, um Rechtsunsicherheiten zu reduzieren. Durch verbesserten (Erfahrungs-)Austausch zwischen den Datenschutzaufsichtsbehörden innerhalb der Datenschutzkonferenz (DSK) könnten unterschiedliche Auslegungen zukünftig verhindert und so mehr Harmonisierung erreicht werden. Rechtssicherheit und Vertrauen in den Datenschutzrahmen können so erhöht und der interne Compliance-Aufwand in Unternehmen deutlich verringert werden.

Aus unterschiedlichen Interpretationen der Landesaufsichtsbehörden resultiert bisher eine Komplexität, die sowohl für kleine und mittelständische Unternehmen (KMU) als auch Unternehmen mit Niederlassungen bzw. Kunden in mehreren Bundesländern Herausforderungen bedeuten. Die unterschiedliche Interpretation der DS-GVO durch die Behörden behindert Wachstum, da für jeden Geltungsbereich rechtlicher Rat eingeholt werden muss und evtl. Produkte verändert werden müssen. Rechtsunsicherheit führt zudem dazu, dass innovative Projekte gar nicht erst angegangen werden.

Bitkom hat bereits 2020 Vorschläge vorgelegt, wie mehr Harmonisierung, Arbeitsentlastung für die Datenschutzaufsichtsbehörden sowie mehr Rechtssicherheit für die DSK zu erreichen wären. Im Rahmen der nun mit dem BDSG angestoßenen Strukturreform, sollte die DSK sich eine neue Geschäftsordnung[1] geben, die beispielsweise die Schaffung (durch Zuweisung) thematischer Schwerpunktaufsichten und strukturierte Beratung der Verantwortlichen vorsieht.

65%

der Unternehmen halten die uneinheitliche Auslegung in Deutschland für ein Digitalisierungshemmnis.

Gemeinsame Vertretung im Europäischen Datenschutzausschuss

Eine gestärkte Position des Bundesbeauftragten für den Datenschutz als Vertreter im Europäischen Datenschutzausschuss (EDSA) und damit als einheitliche und zentrale Anlaufstelle für den Datenschutz in Deutschland ist grundsätzlich zu begrüßen.

[1] https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_09-2022.pdf

Eine gemeinsame Vertretung verliert aber dort ihre erzielte Wirkung, wo Landes-Datenschutzbehörden für ihr jeweiliges Bundesland das Datenschutzrecht weiterhin unterschiedlich auslegen und unterschiedliche Maßstäbe innerhalb Deutschlands gelten. Zudem ist fraglich, was bei einem Widerspruch zwischen den Positionen der DSK und dem EDSA gelten soll.

Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

In § 18 Abs. 2 BDSG wird künftig die Zusammenarbeit zwischen den Aufsichtsbehörden des Bundes und der Länder geregelt. Sie sollen „Einvernehmen über einen gemeinsamen Standpunkt erzielen, bevor sie diesen an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Europäische Kommission oder den Europäischen Datenschutzausschuss übermitteln“. Unklar bleibt jedoch aus den vorgeschlagenen Änderungen, wie eine Zusammenarbeit zwischen den einzelnen Aufsichtsbehörden in der Datenschutzkonferenz erfolgen soll und wie im Einzelnen einheitliche Entscheidungen sichergestellt werden sollen. Auch ein zeitlicher Aspekt ist nicht erfasst und trägt weiter zur Unsicherheit bei. Unternehmen können nicht mehrere Monate warten, bis sich die Datenschutzkonferenz abstimmt, um dann das eigentliche in der Datenschutz-Grundverordnung (DS-GVO) vorgesehene Abstimmungsverfahren abwarten zu müssen.

Nur wenn ein solcher Prozess zur einheitlichen Entscheidungsfindung und der Umsetzung solcher gemeinsam getroffenen Entscheidungen geregelt ist, kann dies zu mehr Transparenz und Einheitlichkeit bei der Anwendung des europäischen und deutschen Datenschutzrechts führen.

Es fehlen jedoch weitgehendere, mutige Schritte, um eine echte Aufsichtsreform und mehr Rechtssicherheit zu erreichen. Von besonderer Bedeutung ist bereits jetzt – und wir zukünftig noch stärker sein – die Beratungstätigkeit der Aufsichtsbehörden. In einer immer komplexer werdenden Datenregulierungslandschaft stehen Unternehmen (und Behörden und die Wissenschaft) vor immer größeren Herausforderungen. Ein umfangreiches Hilfe- und Beratungsangebot ist daher unerlässlich, um das Vertrauen in den Rechtsrahmen zu erhalten, Datenschutz sinnvoll um- und durchzusetzen und als Industrienation wettbewerbsfähig und innovativ zu bleiben. Auch im Interesse der Aufsichtsbehörden und deren (z.T. fehlenden personellen und finanziellen) Kapazitäten sollte über Schwerpunktzuweisungen nachgedacht werden. Dies kann Doppel- bzw. Mehrfacharbeit vermeiden und für gesteigerten Expertisenaufbau in den jeweiligen Schwerpunktaufsichten sorgen.

Ausnahme Auskunftsrecht

Begrüßenswert ist der Vorschlag in § 34 Abs. 1 BDSG eine Klarstellung zum Auskunftsanspruch der Betroffenen gem. Art. 15 DS-GVO für den Fall zu ergänzen, dass die erfragte Information Betriebs- oder Geschäftsgeheimnissen des Verantwortlichen oder einer Dritten betreffen. Diese Regelung ist für Unternehmen sehr bedeutend, wenn eine Auskunftsanfrage sensible Informationen des Unternehmens oder einer Dritten betrifft. Es sollte darüber hinaus im Gesetz klargestellt werden, dass die Ausnahmen vom Auskunftsrecht nach Art. 15 DS-GVO

auch für die Informationen nach Art. 15 Abs. 1 lit. a)-h) DS-GVO gelten. Nach den EDSA-Guidelines 01/2022 on data subject rights – Right of access, Version 2.0, 28 March 2023, Rn. 169, gilt Art. 15 Abs. 4 DS-GVO, welcher u. a. Betriebs- und Geschäftsgeheimnisse schützt, nicht für Art. 15 Abs. 1 lit. a)-h) DS-GVO. Dies ist widersprüchlich und sollte durch die Ausnahme im BDSG klargestellt werden. Das BDSG sollte zudem um eine eindeutige Ausnahme zum Schutz der Rechte und Freiheiten Dritter (vgl. Art. 23 Abs. 1 lit. i) DS-GVO) ergänzt werden, da auch hier durch die Auslegung des Art. 15 Abs. 4 DS-GVO durch den EDSA eine Lücke entstanden ist

Negativ zu bewerten ist jedoch, dass diese Ausnahme nur dann greift, wenn das Interesse an der Geheimhaltung der Betriebs- und Geschäftsgeheimnisse das Interesse der betroffenen Person an der Information überwiegt. Der Wortlaut des neuen Satzes in § 34 Abs. 1 BDSG spricht für eine durchzuführende Interessenabwägung im Rahmen der Auskunftsanfrage, legt jedoch nicht näher dar, wann besonders bedeutende Interessen des Unternehmens betroffen sein können. Art. 23 DS-GVO enthält dagegen lediglich die Maßgabe, dass die Beschränkung eine notwendige und verhältnismäßige Maßnahme darstellen muss. Eine Beschränkung auf eine Interessenabwägung zwischen den Interessen des Betroffenen und der Verantwortlichen bzw. Dritten ist jedoch zu eng und wird dieser Anforderung nicht gerecht.

Aufsichtsbehörde Joint Controller

Die Neuregelung in § 40a BDSG zu einer gemeinsamen Aufsichtsbehörde bei gemeinsam verantwortlichen Unternehmen ist positiv zu bewerten. Diese Regelung vereinfacht die Zusammenarbeit von Unternehmen in der Praxis. Die Zuständigkeit für die gemeinsame Datenverarbeitung soll jedoch auf die Aufsichtsbehörde festgelegt werden, die für das Unternehmen zuständig ist, dass in dem der Antragstellung vorausgegangenen Geschäftsjahres umsatzstärker war. Besonders bei der Zusammenarbeit mit großen Unternehmen wäre die zuständige Aufsichtsbehörde ohne großen zusätzlichen Verwaltungsaufwand bestimmbar. Allerdings halten wir grundsätzlich das Kriterium des Umsatzes zur Bestimmung der Aufsichtszuständigkeit für nicht tauglich. Allein aus dem Umsatz lässt sich noch nicht auf die (Macht)Position eines Unternehmens innerhalb der Verantwortlichkeit schließen. Zudem sollte das Gesetz klarer formulieren, welche Wirkung die Vorgabe des § 40a BDSG für Aufsichtsbehörden hat.

2 Detailanmerkungen

Zu Artikel 1 Nummer 2 a) – Änderung des § 1 BDSG

Das gesamte Konstrukt der Regelungen zum territorialen Anwendungsbereich ist (wie auch schon in der derzeit geltenden Fassung des BDSG) wenig verständlich.

Der Anwendungsbereich von § 1 Abs. 4 S. 2 Nr. 1: „personenbezogene Daten im Inland verarbeitet“ ist nach wie vor unglücklich, da er nicht den Grundsätzen des Art. 3 DS-GVO und den dort genannten Anknüpfungspunkten für Verantwortliche und Auftragsverarbeiter folgt. Praktisch dürften damit auch Fälle von Verantwortlichen außerhalb der EU/EWR erfasst sein, die z. B. Daten auf einem hiesigen Rechenzentrum betreiben, auch wenn keine weiteren Anknüpfungspunkte für Inlandsbezug bestehen. Wären dadurch auch Konstellationen erfasst, in denen Verantwortliche gar nicht der DS-GVO unterliegen, aber dem BDSG? Die Regelung sollte aufgrund dieser Lücke nochmals überarbeitet werden.

Ebenso wie in der derzeit geltenden Fassung des BDSG ist die Regelung des § 1 Abs. 4 Satz 3 völlig unklar. Danach finden gewisse Regelungen des BDSG (§§ 8 bis 21, 39 bis 44) auf nicht öffentliche Stellen Anwendung, obwohl das BDSG nach Satz 2 gar nicht anwendbar ist. Konkret sollen bestimmte Regelungen anwendbar sein, wenn

- keine personenbezogenen Daten im Inland verarbeitet werden,
- keine Niederlassung im Inland vorhanden ist, oder
- keine Niederlassung im Inland oder Europäischen Wirtschaftsraum (EWR) vorhanden ist, und der Verantwortliche/ Auftragsverarbeiter keine Waren/ Dienstleistungen im Inland anbietet oder das Verhalten von betroffenen Personen im Inland überwacht.

Ergo: Auch wenn jeglicher Bezug zu Deutschland fehlt, soll das BDSG mit gewissen Regelungen dennoch Anwendung finden - also auf jedes beliebige Unternehmen in einem Land auf der Welt. Dies scheint weder sinnvoll noch durchsetzbar. Wie stellt sich die Bundesregierung hier die entsprechende Kontrolle und Durchsetzung vor? Was ist der genaue Zweck dieser Regelung, auch in Hinblick auf die in Bezug genommenen Normen?

Zu Artikel 1 Nummer 3 c) – Änderungen an Kapitel 2 BDSG

Der neue Absatz 1 von § 4 BDSG könnte europarechtswidrig sein, dass die Videoüberwachung durch öffentliche Stellen (= Verarbeitung personenbezogener Daten) allein auf Basis der Aufgabenerfüllung gestattet wird („ist nur zulässig, soweit“).

Dies schränkt die Handlungsfähigkeit öffentlicher Stellen zu weit ein. Eine Videoüberwachung mit dem Zweck der Aufgabenerfüllung begründen zu können, wird, wenn überhaupt, nur einen sehr kleinen Teilbereich erfassen. Eine Videoüberwachung z. B. in Zügen wird damit ausgeschlossen, da die Durchführung des ÖP(N)Vs auch ohne eine Videoüberwachung möglich ist. Sicherheit und Sicherheitsgefühls der betroffenen Personen müssen jedoch ebenfalls in der Abwägung zur Rechtmäßigkeit berücksichtigt werden.

Mit der neuen Regelung würden öffentlichen Stellen alle anderen Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO verwehrt. Nach der Regelung dürften öffentliche Stellen etwa keine Einwilligung für eine Videoüberwachung einholen (Art. 6 Abs. 1 lit. a DS-GVO) oder sich auf ein Anstellungsverhältnis oder andere vertragliche Grundlage stützen (Art. 6 Abs. 1 lit. b DS-GVO).

Dieser Ausschluss sämtlicher Erlaubnistatbestände dürfte gegen die zwingenden Vorgaben der DS-GVO und die Rechtsprechung. des Gerichtshofes der Europäischen Union (EuGH) verstoßen.

So hat der EuGH, noch zur Richtlinie 95/46/EG, entschieden, dass Mitgliedstaaten daran gehindert sind, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen (C-708/18, Rz. 53).

Zu Art. 6 Abs. 1 DS-GVO hat der EuGH in ständischer Rechtsprechung entschieden, dass Art. 6 Abs. 1 DS-GVO eine erschöpfende und abschließende Liste der Fälle enthält, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann (C-252/21, Rz. 90).

Daher muss eine Verarbeitung unter einen der in dieser Bestimmung vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können (C-252/21, Rz. 90).

Genau diese Möglichkeit wird öffentlichen Stellen mit der vorgeschlagenen Regelung in Artikel 1 Nummer 3 jedoch genommen, da die Verarbeitung per Videoüberwachung allein unter den dort genannten Bedingungen zulässig sein soll.

Sofern eine Überarbeitung der Regelungen zur Videoüberwachung des öffentlich-zugänglichen Raums durch nicht-öffentliche Stellen stattfinden soll, sind außerdem klare Regelungen zu folgenden Fällen wünschenswert:

- zu Verantwortlichkeiten im Fall einer Verbindung nicht öffentlicher-Stellen zu Behörden z. B. im ÖPNV (Bundespolizei, BMI, etc.)
- zur Videoüberwachung im ÖPNV
- zum Einsatz von Bodycams bei Mitarbeitenden des ÖPNV; ggf. in Form von Regelungen im Zusammenhang mit Gefährdungslagen

Zu Artikel 1 Nummer 7 – Änderung des § 19 BDSG

Die aktuelle Änderung geht in die richtige Richtung. Insbesondere die Klarstellung der Notwendigkeit einer einheitlichen Rechtsauffassung ist begrüßenswert. Vorteilhaft wäre die Schaffung einer noch klareren Regelung, die es erlaubt, dass bei einem inländischen Unternehmen, das im gesamten Bundesgebiet mit Tochterunternehmen und Mehrheitsbeteiligungen vertreten- und auch über Landesgrenzen hinweg tätig ist, vorrangig die für die Muttergesellschaft zuständige Aufsichtsbehörde federführend ist. Die Umsatzstärke, wie aktuell im Referentenentwurf vorgesehen, sollte kein entscheidendes Kriterium sein.

Zu Artikel 1 Nummer 8 b) – Änderung des § 27 BDSG

Die Regelung bedarf u. a. sprachlicher Anpassung. „Unternehmen“ sollte im Sinne der Einheitlichkeit in „nicht öffentliche Stellen“ geändert werden.

Die Formulierung im § 27 „nicht ausschließlich“ ist zu unbestimmt. Erläuterungen, auch im Begründungsteil des Gesetzes, wären hier wünschenswert.

Wenn es hierbei um die Rechtsformen ginge, kämen entweder privatrechtliche oder öffentlich-rechtliche in Betracht. Wenn sich der Absatz auf eine Gruppe gemeinsam Verantwortlicher bezieht (z. B. zwei Behörden und eine privatwirtschaftliche Einheit) sollte dies aber klarer formuliert werden. Die Klarstellung könnte beispielsweise wie folgt lauten: „Für gemeinsam Verantwortliche, bei denen mindestens ein Verantwortlicher eine öffentliche Stelle ist, […]“

Die Formulierung sollte auch hinsichtlich der Begrifflichkeit „Behörde“ angepasst werden, da hier die Aufsichtsbehörden gemeint sind.

Beispiel: Aufsichtsbehörde des Bundes und der Länder

Die Formulierung „die den Verantwortlichen beaufsichtigt“ sollte ebenfalls klarer gefasst werden, da eine „Beaufsichtigung“ durchaus von mehreren Behörden erfolgt. Klarstellend könnte z. B. die „federführende Aufsicht“ genannt werden.

Das Kriterium zur Zuweisung von Zuständigkeit über die Beschäftigtenzahl („[…] der die meisten Personen beschäftigt, welche ständig personenbezogene Daten automatisiert verarbeiten.“) ist ungeeignet. Allein die Anzahl an Beschäftigten sagt noch nichts über die Rolle des Verantwortlichen im Rahmen der gemeinsamen Verantwortlichkeit aus.

So zielt etwa die DS-GVO bei der Feststellung der Federführung auf die „Hauptniederlassung“ ab (Art. 4 Nr. 16 DS-GVO). Hier geht es gerade nicht um die reine Anzahl an Beschäftigten, sondern um den Sitz der Hauptverwaltung/ des Managements, jener Ebene, die über die Zwecke und Mittel der Verarbeitung entscheidet. Dies erscheint gerade im Hinblick auf die Festlegung der Zuständigkeit bei einer gemeinsamen Verantwortlichkeit sinnvoll, in der es ebenfalls um die Entscheidung hinsichtlich Zwecke und Mittel der Verarbeitung geht.

Es wäre wünschenswert, eine Klarstellung im Kontext des § 27 BDSG einzufügen, dass die Verarbeitung von besonderen Kategorien personenbezogener Daten auch für statistische Zwecke im Unternehmen möglich ist, ungeachtet eines etwaigen

wissenschaftlichen Auftrags bzw. Zweckes. Unter statistische Zwecke sollten unter den neuen Begebenheiten auch Verarbeitungen im Rahmen von Data Analytics fallen, z. B. im Rahmen von Künstlicher Intelligenz (KI)-Anwendungen, solange der Wesensgehalt einer statistischen Auswertung (aggregierte Ergebnisse, die ohne Personenbezug weiterverarbeitet werden) erhalten bleibt.

Zu Artikel 1 Nummer 10 - Änderung des § 34 BDSG

Die Möglichkeit, das Auskunftsrecht aufgrund von privaten Satzungen einzuschränken, soll bestehen bleiben. Hier gibt es legitime Anwendungsfälle, die eine Einschränkung rechtfertigen.

Die Möglichkeit der Begrenzung aufgrund von Geheimhaltungsinteressen wird begrüßt. Die Anpassung liegt auf der Linie der Interpretation des Art. 15 DS-GVO durch die europäischen Datenschutzbehörden. So geht der EDSA in seinen Leitlinien zu Art. 15 DS-GVO (Leitlinien 01/2022, 28. März 2023) davon aus, dass im Rahmen der Ausnahmeregelung des Art. 15 Abs. 4 DS-GVO zum einen der Verantwortliche selbst unter „andere Personen“ fällt und sich der Verantwortliche auf Geschäftsgeheimnisse als schützenswerte Rechte berufen kann (Rz. 171). Vorteilhaft wäre die zusätzliche Klarstellung der weiten Auslegung von Geheimhaltungsinteressen. Zudem sollten eine weitere Klarstellung und Ausnahme zum Schutze der Rechte und Freiheiten anderer Personen aufgenommen werden.

Zu Artikel 1 Nummer 13 –Einfügung des § 40a BDSG

Die Formulierung „Unternehmen“ sollte im Sinne der Einheitlichkeit in „nicht öffentliche Stellen“ geändert werden.

Die Formulierung „zuständig“ ist ebenfalls anzupassen, da die genaue Bedeutung unklar bleibt. Soll es in der Regelung um federführende Zuständigkeit gehen, also mehrere federführende Aufsichtsbehörden vorhanden sein und dann die Regelung des § 40a greifen? Dies würde unserem Verständnis der Regelung entsprechen, sollte aber klargestellt werden. Denn allein „zuständig“ sind in der Praxis oft mehrere Aufsichtsbehörden.

Die Umsetzung der entsprechenden Anzeige durch die Unternehmen ist zu unbestimmt. Wenn dies nicht klar vorgegeben wird, werden sich erfahrungsgemäß mehrere unterschiedliche Meldeverfahren etablieren, die die Unternehmen dann je nach Konstellation verwenden müssen. Sinnvoll wäre hier auch die Einrichtung eines einheitlichen Portals o. ä. Die Rechtsfolgen der Nichtmeldung sind bisher nicht ersichtlich. Gilt die Zuweisung von Zuständigkeit nur nach der entsprechenden Meldung oder auch ohne sie? Und entstünden nichtmeldenden Unternehmen Nachteile?

Bitkom hält das Kriterium zur Bestimmung der Zuständigkeit („in deren Zuständigkeitsbereich das Unternehmen fällt, das in dem der Antragstellung vorangegangenen Geschäftsjahr den größten Jahresumsatz erzielt hat“) für ungeeignet. Allein aus dem Umsatz lässt sich noch nicht auf die (Macht)Position eines Unternehmens innerhalb der Verantwortlichkeit schließen.

Zudem sollte das Gesetz klarer formulieren, welche Wirkung die Vorgabe des § 40a BDSG für Aufsichtsbehörden hat.

3 Weitere Änderungsbedarfe

Das BMI sollte die jetzige Gelegenheit der Änderung des BDSG nutzen, um zugleich weitere Anpassungen vorzunehmen. Ein weiteres, späteres Änderungsgesetz wäre ineffizient und verzögert wichtige Klarstellungen und die notwendige Rechtssicherheit noch weiter. Bitkom schlägt im Folgenden einige wichtige Änderungen vor, die im BDSG-Änderungsgesetz aufgegriffen werden sollten. Hiermit würde ebenfalls dem Koalitionsvertrag entsprochen, da die Änderung nationaler Sonderregeln auch die europäische Zusammenarbeit vereinfacht und Harmonisierung fördert.

Neben wichtigen spezifischen Änderungen muss zunächst ein generelles Problem adressiert werden. Das aus dem letzten Jahrtausend stammende Verbotsprinzip erschwert konzeptionell den Großteil der zukunftsorientierten Datenpolitik in Deutschland und der EU, da die Aufsichtsbehörden gesetzlich auf dieses Prinzip verpflichtet wurden. In nicht eindeutigen Sachverhalten wird sich daher formell häufig hierauf bezogen. Die neuen Datennutzungs-Offensiven in Deutschland und Europa laufen damit zum Teil ins Leere, denn auch Sonderregulierungen können sich neu darstellende, vielfältige Anwendungen nicht abschließend kategorisieren. Als Konsequenz zeigen sich bereits heute Innovationshemmnisse und die Abwanderung von entsprechend technologieorientierten Unternehmen.[2]

Pflicht zur DSB-Bestellung bei Notwendigkeit der Durchführung einer Datenschutz-Folgeabschätzung (DSFA)

Die nationale Sonderregelung zur Bestellpflicht des Datenschutzbeauftragten sollte abgeschafft werden.

Kommt ein Verantwortlicher zu dem Schluss, dass für eine Verarbeitung personenbezogener Daten eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen ist, hat dies zur Folge, dass er gemäß der nationalen Regelung in § 38 I 2 BDSG ausnahmslos verpflichtet ist, einen Datenschutzbeauftragten (DSB) zu bestellen.

Praktische Relevanz:

[2] https://www.bitkom.org/Bitkom/Publikationen/Datenschutz-als-Herausforderung-fuer-die-Digitalisierung

Beispiel 1: Der Einsatz von KI-basierten Lösungen durch Verantwortliche, die selbst nicht Anbieter der Lösung sind, jedoch Produkte nutzen, in denen KI verbaut ist. Allein die Nutzung kann eine DSFA-Pflicht auslösen und damit zwangsweise die Bestellpflicht eines DSB.

Beispiel 2: Die Nutzung von Online Office-Suiten (wie z. B. M365) durch KMU.

Die bestehende Regelung ist ein massiver Hemmschuh für Digitalisierungsvorhaben mit Machine Learning-Unterstützung für die kommenden Jahre und wird daher als innovationshemmend eingeschätzt. Die Regelung trägt der in Art. 16 Charta der Grundrechte der Europäischen Union (GrCH) verankerten unternehmerischen Freiheit nicht hinreichend Rechnung.

Die nationale Sonderregelung benachteiligt zudem Verantwortliche, die dem Anwendungsbereich des BDSG unterliegen, im Vergleich zu Verantwortlichen, die in Mitgliedsstaaten der EU agieren, welche keine entsprechende Regelung vorsehen. Dies stellt eine Diskriminierung der beschriebenen Adressatengruppe sowie eine Wettbewerbsverzerrung dar.

Zusätzliche Prüfungen beim Einsatz von KI werden zudem zeitnah ohnehin durch den EU-AI-Act gelten, sodass es der nationalen Sonderregelung nicht bedarf.

Bitkom hält daher die Streichung von § 38 Abs.1 Satz 2 1. Fall BDSG für erforderlich, um das Datenschutzrecht mit dem Recht auf unternehmerische Freiheit in eine angemessene Balance zu bringen, eine Gleichbehandlung von Verantwortlichen in der EU und Wettbewerbsgleichheit sicherzustellen sowie innovative Geschäftsmodelle im Zuge der digitalen Transformation zu unterstützen.

Klarstellungen zur Anonymisierung

Die Anonymisierung ist vor dem Hintergrund der strategischen Relevanz personenbezogener Daten für datengetriebene Geschäftsmodelle einerseits sowie für die sekundäre Nutzung im Rahmen der Digitalisierung anfallender (personenbezogener) Daten andererseits einer der zentralen Aspekte rund um die Anwendung der DS-GVO. Der Mehrwert anonymisierter Daten liegt auf der Hand: Im Bereich der Forschung, für das Trainieren von KI oder für die Entwicklung von Produkten können auch ohne personenbezogene Daten signifikante Fortschritte erzielt werden. Diese sind essenziell für die Datenökonomie und damit auch für das Gelingen der deutschen und europäischen Datenstrategie.

Ohne mehr Praktikabilität und Klarstellungen liegt die (weitere) Zurückhaltung gegenüber Investitionen in Anonymisierungsverfahren auf der Hand und die Innovation treibende Kraft hinter der Implementierung datenschutzfreundlicher Verfahren wird gehemmt. Denn ohne ausreichende Gewissheit darüber, (i) wann ein anonymisiertes Datum nach Ansicht der Aufsichtsbehörden vorliegt, (ii) wie eine Anonymisierung im Einklang mit der DS-GVO erreicht werden kann und (iii) welche Eigenschaften eine zulässige technische Realisierung der Anonymisierung beinhaltet, werden Investitionsentscheidungen nicht getroffen.

Wir halten vor diesem Hintergrund einige Klarstellungen und Änderungen sowie ausdefinierte Kriterien für notwendig, die den Anwendern bei der Beantwortung der

Frage helfen, wann eine Anonymisierung vorliegt. Bitkom bringt sich seit Jahren konstruktiv mit Hilfestellungen und Empfehlungen[3] in die Debatte ein[4] und die Erfahrungsberichte zeigen deutlich, dass Klarstellungen notwendig sind.

Aus Praxissicht ist von besonderer Bedeutung, ob eine Anonymisierung eine Verarbeitung im Sinne der DS-GVO darstellt. Dies ist nach wie vor umstritten, da zum einen in den Regelbeispielen des Art. 4 Nr. 2 DS-GVO die Anonymisierung nicht erwähnt worden ist und eine Definition des Begriffes Anonymisierung in der DS-GVO nicht vorgenommen wurde. Trotz ihrer hohen praktischen Bedeutung wurde die Anonymisierung nur in den Sätzen vier und fünf von Erwägungsgrund 26 erwähnt. Eine Definition bleibt die DS-GVO somit schuldig. Dies führt zum einen zu streitbaren Ansichten in der Literatur und zum Teil in den Aufsichtsbehörden, ob die Anonymisierung einen Verarbeitungsvorgang darstellt und zum anderen um richtige Definition der Anonymisierung.

Es ist notwendig eine Klarstellung im BDSG aufzunehmen, die besagt, dass eine Anonymisierung bereits im Unternehmen verarbeiteter Daten keine Verarbeitung personenbezogener Daten darstellt.

Änderung des § 22 BDSG

In § 22 BDSG sollte eine eindeutige gesetzliche Erlaubnisgrundlage für die Verarbeitung von Gesundheitsdaten zum Abschluss und zur Durchführung von Verträgen (insbesondere explizite Versicherungsverträge, bei denen die Verarbeitung unumgänglich ist) aufgenommen werden. Zumindest sollte die Anwendbarkeit des Art. 9 Abs. 2 lit. f) DS-GVO auf die Durchführung von Versicherungsverträgen klargestellt werden.

Diese Anpassung ist notwendig, weil insbesondere in der Lebens-, Kranken- und Unfallversicherung Verträge nicht abgeschlossen und durchgeführt werden können, ohne dass Gesundheitsdaten verarbeitetet werden. Das gilt beispielsweise auch für die Rückversicherung. Die Verarbeitung von Gesundheitsdaten spielt aber auch in der Haftpflicht- und Rechtsschutzversicherung eine wichtige Rolle, wenn Ansprüche wegen Gesundheitsschäden geltend gemacht werden.

Die von Bitkom vertretende Auffassung, dass die zur Durchführung eines Versicherungsvertrages erforderliche Verarbeitung von Gesundheitsdaten nach Art. 9 Abs. 2 lit. f) DS-GVO erlaubt ist, ist nach wie vor aufgrund der Rechtslage strittig. Bei den deutschen Datenschutzbehörden gibt es uneinheitliche Auffassungen dazu. Die Datenschutzbehörden einiger EU-Länder, z. B. Dänemark und Tschechien, wenden ebenfalls Art. 9 Abs. 2 lit. f) DS-GVO an.

Andere EU-Länder verfügen über spezielle nationale Erlaubnisnormen unterschiedlichen Umfangs zur Verarbeitung von Gesundheitsdaten zum Abschluss

[3] https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung
[4] https://www.bitkom.org/Bitkom/Publikationen/Anonymisierung-und-Pseudonymisierung-von-Daten-fuer-Projekte-des-maschinellen-Lernens

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) DS-GVO oder sie werden auf Art. 9 Abs. 4 DS-GVO gestützt. Teils werden sie auch als Konkretisierungen des Art. 9 Abs. 2 lit. f) DS-GVO verstanden.

Greift keine gesetzliche Erlaubnis, muss die Verarbeitung der Gesundheitsdaten auf eine Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DS-GVO gestützt werden. Die Verhandlung einer Muster-Einwilligung zwischen der deutschen Versicherungswirtschaft und der Datenschutzkonferenz dauert inzwischen schon vier Jahre an. Die unklare Rechtslage führt zu kritischen Nachfragen von Geschädigten und ihren Rechtsanwälten, die die Einholung einer Einwilligung als nicht notwendig und vielmehr als Versuch der Versicherungswirtschaft ansehen, die Schadenregulierung zu verzögern. Es kommt auch zu erheblichen Behinderungen im grenzüberschreitenden Datenverkehr mit Ländern, in denen keine Einwilligung nötig ist, insbesondere im Rückversicherungsgeschäft.

Beispielhaft sei folgender Fall gebildet:

Ein Erstversicherer ist in einem EU-Mitgliedstaat mit landesgesetzlicher Erlaubnisnorm ansässig. Er benötigt daher für die Verarbeitung von Gesundheitsdaten für eine Lebensversicherung keine Einwilligung der betroffenen Person. Das Gleiche gilt für die Weitergabe der Daten an den Rückversicherer. Wenn der Rückversicherer seinen Sitz in Deutschland hat, kann er hingegen die Daten ohne Einwilligung des Betroffenen nicht entgegennehmen und verarbeiten. Er hat aber keinen direkten Kontakt zur betroffenen Person, um die Einwilligung einzuholen.

Eine eindeutige gesetzliche Erlaubnisgrundlage für die Datenverarbeitung 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 Standortnachteile deutscher Erst- und Rückversicherer verhindern. Zudem würde die Regelung verhindern, dass bei einem Widerruf der Einwilligung Vertragsrecht und Datenschutzrecht auseinanderlaufen.

Hilfreich wäre aber auch schon im BDSG klarzustellen, dass die Verarbeitung von Gesundheitsdaten, die zur Durchführung von Versicherungsverträgen (einschließlich der Rückversicherung, der Schadenregulierung in der Haftpflichtversicherung sowie der Einschaltung von Gutachtern) erforderlich ist, unter Art. 9 Abs. 2 lit. f) DS-GVO fällt.

Dies sollte auch klarstellen, dass die Verarbeitung von Gesundheitsdaten zur Gesundheitsvorsorge gem. Art. 9 Abs. 2 lit. h) DS-GVO generell für die Krankenversicherungen gilt (privat wie gesetzlich). Art. 9 Abs. 2 lit. h) DS-GVO bzw. § 22 Abs. 1 lit. b) BDSG beschreibt die Verarbeitung von Gesundheitsdaten zum Zweck der Gesundheitsvorsorge, (...) die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich. Die privaten Krankenversicherer haben einen vergleichbaren Versorgungsauftrag wie die gesetzlichen Krankenversicherungen, die jedoch insbesondere über Regelungen aus dem Sozialgesetzbuch privilegiert sind.

Änderung des § 37 BDSG

§ 37 Abs. 1 und Abs. 2 sollten vollautomatisierte Entscheidungen im Rahmen des Abschlusses und der Durchführung von Versicherungsverträgen ermöglichen.

Im Zuge zunehmender Digitalisierung müssen Versicherer heutzutage in der Lage sein, vollautomatisiert über Anträge auf Versicherungsschutz und Leistungen aus Versicherungsverträgen zu entscheiden. Damit kann dem Begehren der Kundinnen und Kunden, die eine schnelle Bearbeitung ihrer Anliegen erwarten, besser Rechnung getragen werden.

Beispiele hierfür sind:

- Ein Antrag auf Abschluss eines Lebensversicherungsvertrages mit Gesundheitsangaben wird vom Versicherungsvermittler bei seinem Gespräch mit der Kundin oder dem Kunden elektronisch aufgenommen und direkt an das Versicherungsunternehmen geleitet. Dieses prüft den Antrag automatisiert und teilt dem Vermittler noch während des Gesprächs mit, dass der Vertrag angenommen wird. Der Vermittler informiert die Kundin oder den Kunden sofort darüber.
- Eine Kundin oder 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. Die Kundin oder der Kunde beantragt Tagegeld für elf Tage, legt aber eine Bescheinigung vor, aus der hervorgeht, dass er nur zehn Tage lang im Krankenhaus war. Die Bescheinigung wird automatisiert ausgelesen, der Bescheid wird automatisiert erstellt und verschickt und die Kundin oder der Kunde erhält sofort Krankentagegeld für 10 Tage. Wegen des verbleibenden Tages kann sie oder er sich mit seinem Versicherer in Verbindung setzen, sofern sie oder er weiterhin der Ansicht ist, hierfür Ersatz beanspruchen zu können.

In den beiden zuerst genannten Beispielen wären nach § 37 BDSG keine vollautomatisierten Entscheidungen möglich, weil § 37 BDSG das Antragsverfahren nicht abdeckt. Im dritten Beispiel wäre ebenfalls keine vollautomatisierte Entscheidung möglich, weil dem Begehren nicht im Sinne von Nr. 1 vollumfänglich stattgegeben wird und der in Nr. 2 genannte Sonderfall nicht vorliegt.

Die in Art. 22 Abs. 2 lit. a) und c) sowie Art. 22 Abs. 4 DS-GVO enthaltenen Ausnahmen werden von den Datenschutzbehörden sehr eng ausgelegt. Die Behörden betrachten vollautomatisierte Entscheidungen als nicht „erforderlich“ für den Versicherungsvertrag im Sinne von 22 Abs. 2 lit. a) DS-GVO, da der Vertrag auch nicht automatisiert abgeschlossen und durchgeführt werden könne. Eine Einwilligung im Sinne von Art. 22 Abs. 2 lit. c) und Art. 22 Abs. 4 DS-GVO sehen sie 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 DS-GVO ohnehin vorgesehene menschliche Prüfung auf Wunsch der Kundin oder des Kunden nach der Entscheidung (also sozusagen auf zweiter Stufe) reicht den Datenschutzbehörden nicht aus.

Dem Bedarf könnte mit einer Änderung des § 37 BDSG Rechnung getragen werden. Die dazu erforderlichen Öffnungen enthält die DS-GVO in Art. 22 Abs. 2 lit. b und Art. 22 Abs. 4 in Verbindung mit Art. 9 Abs. 2 lit. g) DS-GVO.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Rebekka Weiß, LL.M. | Leiterin Vertrauen & Sicherheit
T 030 27576-161 | r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenschutz