Bundesverband
Kooperierender Mittelstand

BKM

Digital-Omnibus & DSGVO:

Europäischen Datenschutz risikobasiert und innovationsfreundlich gestalten

Stellungnahme

Brüssel, der 22. Mai 2026

Am 19. November hat die Europäische Kommission ihren Vorschlag für die sogenannte Digital-Omnibus-Verordnung 2025/0360 (COD) (in der Folge „Digi-Omnibus“) vorgelegt, mit dem insbesondere Innovationshemmnisse abgebaut und bürokratische Belastungen für Unternehmen im Digitalbereich reduziert werden sollen.

Ein wesentlicher Teil des Pakets zielt auf die Vereinfachung der Datenschutzgrundverordnung (DSGVO) ab. Diese stellt für viele Unternehmen weiterhin eine erhebliche administrative Belastung dar und gerät vor dem Hintergrund datengetriebener Geschäftsmodelle sowie aktueller Entwicklungen im Bereich der Künstlichen Intelligenz zunehmend an ihre Grenzen. Vor diesem Hintergrund hat der Bundesverband Kooperierender Mittelstand (BKM) wiederholt eine grundlegende Überarbeitung des europäischen Datenschutzrahmens gefordert. Der durch die Europäische Kommission angestoßene Reformprozess ist daher im Grundsatz zu begrüßen.

Die bevorstehenden Positionierungen im Rat und im Europäischen Parlament nimmt der Bundesverband Kooperierender Mittelstand (BKM) zum Anlass, um erneut auf seine zentralen Positionen zur Datenschutzgrundverordnung hinzuweisen.

Für den Verband ist klar: Ziel der Reform muss ein innovationsfreundlicher, risikobasierter Datenschutz sein, ohne das bestehende Rechte- und Schutzniveau abzusenken.

Bundesverband Kooperierender Mittelstand e.V. (BKM) | Unter den Linden 17 | 10117 Berlin | Tel.: +49 30 318 7309 0
info@bkm-verband.de | www.bkm-verband.de | Vereinsregister: Amtsgericht Berlin-Charlottenburg VR 22795 B
Vorstand i.S.d. § 26 BGB: Günter Althaus (Präsident), Julia Graeber, Dr. Stefan Müller, Dr. Andreas Trautwein
Hauptgeschäftsführer: Dr. Henning Bergmann | Lobbyregister Dt. Bundestag: R001283 | EU-Transparenzregister: 196997510883-76

1. Zur Änderung von Artikel Artikel 4 & 5 DSGVO: Stärkung des risikobasierten Ansatzes

Der Schutz natürlicher Personen bei der Verarbeitung von Daten ist ein in der Charta der Grundrechte der EU verankertes hohes Gut, das ständig gegenüber konkurrierenden Interessen abgewogen werden muss. Dieser Schutz wurde dich die DSGVO konkretisiert - das Prinzip der Interessenabwägung findet sich allerdings ihrer derzeitigen Ausformung aus unserer Überzeugung nicht wieder. So besagt Erwägungsgrund 4 der DSGVO, dass der Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht sei, im Hinblick auf seine gesellschaftlichen Funktionen gesehen werden muss, zu denen unter anderem auch die unternehmerische Freiheit zählt.

Allerdings wird in Abweichung hierzu dem Datenschutz häufig ein unverhältnismäßig hoher Stellenwert eingeräumt, was unter anderem darin Ausdruck findet, dass die DSGVO alle personenbezogenen Daten gleichermaßen schützt – unabhängig davon, ob sie für den Betroffenen oder Dritten bedeutsam, geheim oder in einer anderen Form von besonderem Wert sind. Diese mangelnde Differenzierung nach Sensibilität und wirtschaftlicher Relevanz im bestehenden Rechtsrahmen schränkt die Nutzungsmöglichkeit der Daten unverhältnismäßig stark ein.

Für uns steht daher fest: Datenschutz muss risikobasiert ausgestaltet und in ein ausgewogenes Verhältnis zu Innovationsfähigkeit, Wettbewerbsfähigkeit und praktikabler Datenverwendung im Mittelstand gebracht werden. Im Sinne dieses Grundsatzes bedarf es einer gezielten Anpassung einzelner Artikel der DSGVO, auf die im Folgenden eingegangen werden soll.

a. Änderung der Definition „personenbezogener Daten“ in Artikel 3 Nummer 1 Buchstabe a Digi-Omnibus zur Änderung von Artikel 4 Nummer 1 DSGVO

Im Lichte des risikobasierten Ansatzes ist die in Artikel 3 Absatz 1 von der Kommission vorgeschlagene Änderung der Definition der „personenbezogenen Daten“ in Artikel 4 DSGVO positiv zu betrachten: Hierdurch soll klargestellt werden, dass Daten nicht mehr als „personenbezogen“ einzustufen sind, wenn das verarbeitende Unternehmen nicht über die Mittel verfügt, die betroffene Person zu identifizieren. Maßgeblich für die Einordnung als personenbezogene Daten wäre damit die tatsächliche Re-Identifizierbarkeit der Daten durch den jeweiligen Verantwortlichen, was dem Grundprinzip des risikobasierten Ansatzes folgt.

Um diesen Grundsatz insgesamt in der DSGVO zu verankern, bedarf es auch einer Änderung der Vorschriften über die Auftragsdatenverarbeitung. Es muss klar sein, dass in Fällen, in denen aus Sicht des Empfängers keine personenbezogenen Daten vorliegen, kein Grund besteht, eine Auftragsverarbeitungsvertrag gemäß Artikel 28 DGSVO abzuschließen, wenn der Empfänger selbst keinen Personenbezug herstellen kann. Analog zur Logik des

Änderungsvorschlags gilt gleiches, wenn personenbezogene Daten nur beim Auftragsverarbeiter verbleiben, während der Verantwortliche selbst den Personenbezug nicht mehr (oder gar nicht) herstellen kann.

Die vorgeschlagenen Änderungen hätten das Potenzial, eine gemeinschaftliche Nutzung von Daten innerhalb von Kooperationen zu vereinfachen und deren Wettbewerbsfähigkeit damit zu stärken. Aktuell steht der rechtssicheren Nutzung von Kundendaten der Anschlusshäuser durch die Kooperation auch in anonymisierter und pseudonymisierter Form oftmals die Vorschriften der DSGVO entgegen bzw. der rechtliche Erklärungsaufwand ist durch diese mittelständischen Kooperationen wirtschaftlich nicht darstellbar. Damit bleiben die Skaleneffekte dieser Kooperationen mit Blick auf digitale Geschäftsmodelle aktuell ungenutzt.

b. Erweiterung der legitimen Zwecke einer personenbezogenen Datenverarbeitung (Artikel 3 Nummer 2 Digi-Omnibus zur Änderung von Artikel 5 Absatz 1 Buchstabe b DSGVO)

Der Kommissionsvorschlag will durch die Änderung des Artikels 5 Absatz 1 Buchstabe b DSGVO in Artikel 3 Nummer 2 Digi-Omnibus den Kreis personenbezogener Datenverarbeitungen, die automatisch als mit dem ursprünglichen Erhebungszweck vereinbar gelten, erweitern. Künftig sollen darunter insbesondere auch Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken fallen. Aus Sicht des Bundesverbands Kooperierender Mittelstand (BKM) sollte dieser Katalog ausdrücklich um Verarbeitungsvorgänge zum Zwecke der Anonymisierung und Pseudonymisierung ergänzt werden.

Anonymisierung und Pseudonymisierung stellen keine eigenständigen Zwecke dar, die unabhängig von der ursprünglichen Datenerhebung bestehen. Durch diese Prozesse wird nicht das Ziel der Verarbeitung verändert, sondern schlicht der Personenbezug entfernt. Diese Praxis schützt für sich genommen die Interessen betroffener Personen – es entspräche also einem risikobasierten Ansatz, jede mit diesen Prozessen verbundene Zweckänderung stets als mit dem ursprünglichen Zweck vereinbar anzusehen.

c. Kodifizierung des risikobasierten Ansatzes in Artikel 5 Absatz 3 DSGVO

Im derzeitigen Datenschutzregime lässt sich der risikobasierte Ansatz in verschiedenen Artikeln der Datenschutzgrundverordnung verstreut finden. So werden unter anderem in Artikel 9 (Verarbeitung besonderer Kategorien personenbezogener Daten), Artikel 32 (Vorgaben zur Datensicherheit), Artikel 33 (Meldungen an die Aufsichtsbehörde) oder in Artikel 35 (Datenschutzfolgeabschätzung) die Pflichten des Verantwortlichen in

Abhängigkeit zu den mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen gebracht. Was fehlt, ist jedoch ein grundsätzliches Bekenntnis zum risikobasierten Ansatz in der DSGVO. Um die Innovations- und Wettbewerbsfähigkeit mittelständischer Unternehmen nicht auszubremsen, ist es jedoch von zentraler Bedeutung, datenrechtliche Standards nur dort hoch anzusetzen, wo die Verarbeitung personenbezogener Daten mit einem Risiko für die betroffene Person einhergehen könnte. Maßgeblich sind dabei insbesondere die Wahrscheinlichkeit und Schwere eines möglichen Schadens, der aus der Verarbeitung resultieren kann.

Aus diesem Grund fordern wir, den risikobasierten Ansatz als Grundsatz in der DSGVO zu verankern. Hierzu wäre die Schaffung eines neuen Absatz 3 des Artikels 5 DSGVO nötig, der besagt, dass „die Grundsätze dieser Verordnung zum Schutz personenbezogener Daten so auszulegen sind, dass die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos einer Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden."

Die Kodifizierung des risikobasierten Ansatzes als übergreifendes Leitprinzip statt in vereinzelten Ansätzen würde nicht nur eine Reduzierung unnötiger Belastungen für Unternehmen bei risikoarmen Verarbeitungen nach sich ziehen. Auch hätte solch eine systematische Aufwertung eine Lenkungswirkung für Aufsichtsbehörden zur Folge, die in der Folge ihre Anforderungen verstärkt risikoorientiert begründen müssten. Dies würde auch zu einer Reduzierung divergierender Vollzugspraktiken und damit zu einer Harmonisierung datenschutzrechtlicher Standards in der EU führen.

Forderungen:

- Dem Vorschlag der Europäischen Kommission zur Änderung der Definition personenbezogener Daten in Artikel 4 DSGVO ist zu folgen.
- Darüber hinaus bedarf es einer Klarstellung, dass kein Auftragsverarbeitungsvertrag gemäß Artikel 28 DSGVO erforderlich ist, wenn der Verantwortliche bzw. Auftragsverarbeiter keinen Personenbezug (mehr) herstellen kann.
- Artikel 5 Absatz 1 Buchstabe b sollte im Bereich der Anwendungsmöglichkeiten personenbezogener Datenverarbeitung, die als vereinbar mit dem ursprünglichen Verwendungszweck gelten, um den Tatbestand der Anonymisierung und Pseudonymisierung erweitert werden.
- Zusätzlich sollte der risikobasierte Ansatz in Artikel 5 Absatz 3 DSGVO kodifiziert werden.

2. Artikel 3 Nummer 7 Digi-Omnibus zur Änderung des Artikels 22 Absatz 1 & 2 DSGVO: Wegfall der Notwendigkeit der Einwilligung, wenn die Datenverarbeitung für die Erbringung einer Dienstleistung notwendig ist

Mit einem Anpassungsvorschlag des Artikels 22 DSGVO in Artikel 3 Nummer 7 Digi-Omnibus verfolgt die Europäische Kommission das Ziel, Klarstellungen in Bezug auf automatisierte Entscheidungen mit erheblicher Wirkung auf betroffene Personen erreichen.

So wird einerseits die Systematik des Artikel 22 Absatz 1 und 2 angepasst: Während die bestehende Systematik des Artikel 22 DSGVO als Verbot automatisierter Entscheidungen mit erheblicher Beeinträchtigung (Absatz 1) mit eng begrenzten Ausnahmen (Absatz 2: Vertragserfüllung, gesetzliche Erlaubnis, Zustimmung des Betroffenen) konzipiert ist, soll nun ein Erlaubnistatbestand unter den in Absatz 2 genannten Voraussetzungen etabliert werden. Insofern stellt diese Neufassung eine Abkehr von einem Schutzrecht des Betroffenen hin zu einer zulässigkeitsorientierten Regelung für Unternehmen dar, was prinzipiell zu begrüßen ist.

Insbesondere kommt der Klarstellung in Artikel 22 Absatz 1(a) DSGVO-neu eine zentrale Bedeutung zu. Indem klargestellt wird, dass das Kriterium der Notwendigkeit zur Vertragserfüllung unabhängig davon zu beurteilen ist, ob die Entscheidung auch auf andere Weise als durch ausschließlich automatisierte Mittel getroffen werden könnte, wird ein zentraler Streitpunkt der bisherigen Auslegungspraxis adressiert. Insofern ist auch der Erwägungsgrund 38 des Kommissionsvorschlags zum Digi-Omnibus von erheblicher Bedeutung, da er klarstellt, dass die bloße Möglichkeit einer menschlichen Entscheidungsfindung den Verantwortlichen nicht daran hindert, sich für eine ausschließlich automatisierte Verarbeitung zu entscheiden.

Diese Neufassung ist von großem Nutzen für datengetriebene Geschäftsmodelle und den Einsatz KI-gestützter Entscheidungsverfahren Diese entfalten ihre größten Effizienzpotenziale regelmäßig gerade dort, wo eine menschliche Entscheidung zwar möglich, jedoch mit einem unverhältnismäßigen Ressourcenaufwand verbunden wäre. Die Entkopplung des Einsatzes automatisierter Verfahren von einer restriktiven Erforderlichkeitsprüfung sowie von der bloßen Möglichkeit menschlicher Alternativen erweitert den Handlungsspielraum für skalierbare und wirtschaftlich effiziente Automatisierungslösungen erheblich und ist daher im Kern innovationsfördernd.

Forderung:

- Dem Vorschlag der Kommission zur Neustrukturierung der Einwilligungsvoraussetzungen bei automatisierter Entscheidungsfindung gemäß Artikel 22 Absatz 1 und 2 DSGVO ist zu folgen.

3. Artikel 3 Nummer 9 Buchstabe a Digi-Omnibus zur Änderung des Artikel 35 Absatz 4 DSGVO: Erstellung einer harmonisierten Liste von Datenverarbeitungsaktivitäten, für die eine Datenschutz-Folgeabschätzung (nicht) erforderlich ist

Mit dem Artikel 3 Nummer 9 Buchstabe a Digi-Omnibus zur Änderung des Artikels 35 Absatz 4 DSGVO will die Kommission die Liste an Verarbeitungsvorgängen, für die gemäß Absatz 1 desselben Artikels eine Datenschutz-Folgeabschätzung (DSFA) zwingend durchzuführen ist, auf den Europäischen Datenschutzausschuss übertragen.

Nach derzeitiger Rechtslage sind die nationalen Aufsichtsbehörden nach Absatz 4 verpflichtet, eine solche Liste zu erstellen. Hierdurch ist jedoch im Laufe der Zeit ein europaweiter Flickenteppich an unterschiedlichen Listen für nicht-öffentliche Einrichtungen entstanden. Je nach Mitgliedstaat, in dem ein Unternehmen eine Verarbeitungstätigkeit durchführt, sind unterschiedliche Regelungsstile (technologiebezogen vs. funktionsbezogen/ fallbezogen vs. Sektoral), Schwellen für die Kumulation der gelisteten Kriterien (einzelne Treffer vs. Kriterienkombination) sowie sich hieraus ergebende Prüfarchitekturen zu beachten.

Die vorgeschlagene Änderung des Artikel 35 Absatz 4 DSGVO, wonach die Kompetenz zur Erstellung von Listen der Verarbeitungsvorgänge, für die eine DSFA durchzuführen ist, auf den Europäischen Datenschutzausschuss übertragen werden soll, ist im Grundsatz zu begrüßen, da sie zu einer Harmonisierung dieser Listen beitragen würde. Dabei ist jedoch sicherzustellen, dass sich der Ausschuss weiterhin an den Kriterien des WP 248 orientiert und das bislang bestehende Schutzniveau nicht über das derzeitige Maß hinaus verschärft.

Analog dazu soll die Behörde gemäß Artikel 35 Absatz 5 künftig auch eine harmonisierte „weiße“ Liste für Verarbeitungsvorgänge erstellen, für die keine DSFA erforderlich ist. Dies ist vor allem vor dem Hintergrund zu begrüßen, dass nach derzeitiger Rechtslage nationale Datenschutzbehörden nicht verpflichtet sind, eine solche Liste zu erstellen, und dem in den meisten Fällen bisher auch nicht nachgekommen sind (etwa in Deutschland). Dies führt dazu, dass Unternehmen, die eigentlich keine aufwändige DSFA erstellen müssten, aus Gründen der fehlenden Rechtssicherheit dennoch tun. Eine harmonisierte Liste mit „weißen“ Praktiken kann hier erhebliche Abhilfe schaffen.

Zu begrüßen ist ferner eine unionsweit einheitliche Methodik für Datenschutz-Folgeabschätzungen. Gerade bei grenzüberschreitenden Verarbeitungsvorgängen ließen sich hierdurch Mehrfachbewertungen für ein- und dieselben Vorgang vermeiden. Jedoch sollte auch hier darauf geachtet werden, dass diese einem möglichst schlanken und praxistauglichem Zuschnitt folgen, der Unternehmen nicht überfordert und nicht über die bestehende Praxis der Erstellung und Dokumentation von DSFA hinausgeht.

Forderungen

- Dem Vorschlag der Kommission, in Artikel 35 DSGVO die Zuständigkeit für die Erstellung von Listen DSFA-pflichtiger Verarbeitungsvorgänge auf den Europäischen Datenschutzausschuss zu übertragen, ist zu folgen, sofern dabei das bestehende Schutzniveau nicht erhöht wird.
- Dem Vorschlag der Kommission, Rechtssicherheit durch eine unionsweit einheitliche „weiße Liste“ nicht DSFA-pflichtiger Verarbeitungsvorgänge zu schaffen, ist zu folgen.

4. Artikel 3 Nummer 15 Absätze 1 bis 7 zur Neuschaffung der Artikel 88a & 88b: Neuregelung der Endgerätezugriffe und Einführung von maschinenlesbaren Signalen

Der Verordnungsentwurf der Europäischen Kommission zum Digital-Omnibus greift die Aufforderung des Europäischen Rates auf, den bestehenden EU-Besitzstand einer umfassenden Überprüfung und einem „Stresstest“ zu unterziehen, um Potenziale zur Vereinfachung und Konsolidierung bestehender Rechtsvorschriften zu identifizieren. Der Entwurf steht damit insbesondere im Kontext des erklärten Ziels der Europäischen Kommission, die bürokratischen Belastungen für Unternehmen jährlich um 25 Prozent zu reduzieren.

Vor diesem Hintergrund erscheint es aus Sicht des Bundesverbands Kooperierender Mittelstand (BKM) nur schwer nachvollziehbar, dass der Entwurf mit Artikel 3 Nummer 15 und der Einführung der neuen Artikel 88a und 88b DSGVO zusätzliche regulatorische Anforderungen vorsieht, die diesem Ziel erkennbar zuwiderlaufen. Statt bestehende Belastungen abzubauen, drohen die vorgeschlagenen Regelungen insbesondere kleine und mittlere Unternehmen vor neue bürokratische und technische Herausforderungen zu stellen. Inwiefern die vorgeschlagenen Regelungen den kooperierenden Mittelstand belasten, wird im Folgenden näher dargestellt.

a. Artikel 88a DSGVO-neu

Durch die vorgeschlagene Neuregelung der Endgerätezugriffe im Artikel 88a DSGVO-neu verfolgt die Kommission zwei Ziele: Einerseits soll hierdurch die verpflichtende Zustimmung Endgerätezugriffe in Bezug auf personenbezogene Daten aus der e-Privacy-Verordnung in die DSGVO integriert werden. Diese ist zwar aus dem Gedanken der Entschlackung des Digital-Acquis heraus richtig gedacht, führt jedoch in der Praxis zu parallelen Anforderungskatalogen, etwa in Bezug auf Einwilligungsregelungen und Aufsichtssysteme.

Andererseits will die Kommission durch den neuen Artikel 88a DSGVO-neu der Problematik der sogenannten „Consent-Fatigue“ entgegenwirken, wonach durch eine Überforderung ständiger Cookie-Einwilligungsanfragen bei Websitezugriffen leichtfertig Einwilligungen

erteilen – ein Ziel, das der Bundesverband Kooperierender Mittelstand (BKM) ausdrücklich unterstützt. Zu diesem Zweck wird in Absatz 4 die Regelung vorgeschlagen, dass betroffene Personen die Möglichkeit haben sollen, mit einem einzigen Klick oder gleichwertigen Mitteln abzulehnen (Buchstabe a), sowie diese Entscheidung für einen Zeitraum von sechs Monaten vom Verantwortlichen respektiert wird.

Aus Sicht des BKM stellt solch eine Anforderung Unternehmen vor erhebliche technische Herausforderung. Bereits ein Wechsel des Endgeräts oder das Löschen des Browser Caches lassen den Nutzer aus technischer Sicht als neuen Nutzer erscheinen. Somit wird es Unternehmen unmöglich gemacht, eine Cookie-Präferenz über diesen langen Zeitraum zu respektieren. Eine vorgesehene „Single-Click-Ablehnung“ gewährt darüber hinaus faktisch ein Recht auf kostenlosen Zugang zu Dienstleistungen ohne Gegenleistungen und stellt einen unzumutbaren und invasiven Eingriff in Geschäftsmodellen von Digitalen Diensten dar, denen somit ihre wirtschaftliche Basis entzogen wird.

Nicht zuletzt können Verbraucher berechtigte Interessen haben, differenzierte Entscheidungen über die Verwendung ihrer Daten zu treffen – etwa im Hinblick auf Tracking, personalisierte Werbung oder die Weitergabe an Dritte. Auf der anderen Seite verfolgen Websitebetreiber nicht nur kommerzielle, sondern auch legitime funktionale Interessen, etwa die Gewährleistung von IT-Sicherheit oder die Betrugsprävention. Diese Zwecke setzen die Speicherung und Verarbeitung bestimmter Daten auf dem Endgerät regelmäßig voraus und dienen letztlich auch dem Schutz der Nutzer selbst.

Eine pauschale Single-Click-Lösung wird diesen unterschiedlichen Präferenzen nicht gerecht. Sie reduziert die Entscheidung auf ein binäres „Alles oder Nichts“ und verhindert damit eine sachgerechte Abwägung zwischen unterschiedlichen Datenverarbeitungszwecken. Insbesondere werden notwendige oder sicherheitsrelevante Verarbeitungen faktisch mit optionalen, etwa werblichen Zwecken gleichgesetzt. Dies widerspricht dem Grundgedanken einer informierten und spezifischen Einwilligung, die gerade eine differenzierte Entscheidung ermöglichen soll.

Die vorgesehenen Ausnahmen in Artikel 88a Absatz 3 hingegen laufen ins Leere: so legt die Aggregationsausnahme fest, dass bestimmte Datenverarbeitungen ohne Einwilligungen erlaubt sein sollen, wenn Daten aggregiert werden und der Verantwortliche diese ausschließlich für eigene Zwecke nutzt. Dies verkennt jedoch die praktische Realität der arbeitsteiligen Datenverarbeitungsstrukturen, wo unterschiedliche Akteure zur Messung, Verifizierung und zur Analyse von Daten zusammenwirken.

Aus diesem Grund fordern wir eine ersatzlose Streichung des Artikel 88a DSGVO-neu.

b. Artikel 88b DSGVO-neu

Artikel 88b DSGVO-neu soll darüber hinaus eine weitere Compliance-Schicht für Unternehmen schaffen, indem zentralisierte und verbindliche Mechanismen zur Verwaltung von Einwilligungen vorgeschlagen werden.

Die in Artikel 88a vorgesehene Single-Click-Lösung greift bereits erheblich in bestehende Geschäftsmodelle ein. Eine darüberhinausgehende gesetzliche Festlegung ihrer konkreten Ausgestaltung in Artikel 88b verstärkt diesen Eingriff und ist aus Sicht des Bundesverbands Kooperierender Mittelstand (BKM) in seiner Gesamtheit unverhältnismäßig invasiv.

Darüber hinaus konterkariert Artikel 88b das im Digitalen Omnibus angelegte Prinzip der Vereinfachung. Anstelle einer Entlastung werden Unternehmen mit zusätzlichen bürokratischen Anforderungen konfrontiert, die mit einem komplexen Umbau bestehender Front-End-Strukturen verbunden sind.

Zugleich verkennt die Regelung die tatsächliche Nutzerrealität: Einwilligungen zur Verwendung und Erhebung von Endgerätedaten werden in der Praxis kontextbezogen erteilt. Eine zentralisierte Voreinstellung ist nicht geeignet, dieses differenzierte und situative Entscheidungsverhalten abzubilden. Ohne konkreten Nutzungskontext werden Einwilligungen tendenziell pauschal verweigert – selbst in Fällen, in denen Nutzer personalisierte Angebote ausdrücklich wünschen. Dies führt langfristig zu einer spürbaren Minderung von Qualität und Relevanz digitaler Dienste.

Die daraus resultierenden Einschränkungen bei der Datenverfügbarkeit haben zudem unmittelbare ökonomische Folgen. Das frei zugängliche Internet basiert maßgeblich auf datengetriebenen Geschäftsmodellen. Ohne Personalisierung verlieren digitale Werbeangebote an Wirksamkeit und Nutzerrelevanz, wodurch der Wert von Werbeplätzen erheblich sinkt. Entstehende Umsatzeinbußen müssten durch eine Intensivierung von Werbeschaltungen kompensiert werden, was wiederum die Nutzerfreundlichkeit beeinträchtigt.

Vor diesem Hintergrund ist auch die übergeordnete Zielrichtung der europäischen Datenpolitik insgesamt zu hinterfragen. Gute Ansätze im Rahmen des Digital-Omnibus – die sich beispielsweise an der Flexibilisierung des e-Governance-Frameworks erkennen lassen, würden durch Maßnahmen wie Artikel 88b, die mit erheblichen Einbrüchen bei der Datennutzung einhergehen, unterlaufen.

Aus den genannten Gründen fordert der Bundesverband Kooperierender Mittelstand (BKM) die vollständige Streichung des Artikel 88b-neu.

Forderung

- Die von der Kommission vorgeschlagene Neuregelung der Endgerätezugriffe in Artikel 88a und 88b. DSGVO-neu ist ersatzlos zu streichen.

5. Verwendung personenbezogener Daten im Kontext der Künstlichen Intelligenz

Künstliche Intelligenz und andere datengetriebene Geschäftsmodelle haben heute eine deutlich größere wirtschaftliche und gesellschaftliche Bedeutung als noch im Jahr 2018, als die Datenschutz-Grundverordnung verabschiedet wurde. Vor diesem Hintergrund ist es ausdrücklich zu begrüßen, dass die Europäische Kommission im Rahmen des aktuellen Reformprozesses Ansätze verfolgt, den europäischen Datenschutzrahmen mit der dynamischen Entwicklung digitaler Schlüsseltechnologien in Einklang zu bringen.

Aus Sicht des Bundesverbands Kooperierender Mittelstand (BKM) darf Technologieoffenheit jedoch nicht auf Anwendungen der Künstlichen Intelligenz verengt werden. Vielmehr müssen auch andere datengetriebene Geschäftsmodelle und innovative Formen der Datenverarbeitung angemessen berücksichtigt werden.

a. Artikel 3 Nummer 15 Digi-Omnibus zur Neuschaffung des Artikel 88c: Verarbeitung zur Entwicklung und Betrieb von KI auf Basis einer neuen Rechtsgrundlage

Der von der Kommission vorgeschlagene neue Artikel 88c DSGVO sieht vor, die Verarbeitung personenbezogener Daten zur Entwicklung und zum Betrieb von KI-Systemen künftig ausdrücklich als „berechtigtes Interesse“ im Sinne von Artikel 6 Absatz 1 Buchstabe f DSGVO einzuordnen.

Nach der deutschen Rechtsprechung ist eine entsprechende Stützung bereits auf Grundlage der geltenden DSGVO möglich (vgl. OLG Köln, Beschl. v. 23.05.2025). In der bisherigen Praxis wird diese Möglichkeit jedoch vornehmlich von großen amerikanischen Technologieunternehmen genutzt. Dies lässt sich insbesondere dadurch erklären, dass diese Unternehmen typischerweise stärker datengetriebene Geschäftsmodelle verfolgen und zugleich eine höhere Bereitschaft zeigen, bestehende regulatorische Spielräume auszuschöpfen, während europäische Unternehmen häufig zurückhaltender agieren und den Vorgaben der Datenschutzaufsichtsbehörden ein höheres Gewicht beimessen.

Um diesen Wettbewerbsnachteil auszugleichen und für Unternehmen ein höheres Maß an Rechtssicherheit in der Verwendung personenbezogener Daten zu diesem Zwecke zu

schaffen, ist es grundsätzlich sinnvoll, die bisherige Praxis auch materiell-rechtlich in der DSGVO zu verankern.

Gleichwohl wirft die Verortung dieser Klarstellung in einem eigenständigen Artikel 88c DSGVO aus rechtsdogmatischer Sicht Fragen auf. Da es sich hier um eine Konkretisierung der Voraussetzungen des Artikel 6 Absatz 1 Buchstabe f DSGVO handelt, erschiene eine Einbettung in Artikel 6 selbst oder zumindest eine Klarstellung in den Erwägungsgründen aus systematischer Sicht überzeugender.

b. Artikel 3 Nummer 3 Buchstabe a Digi-Omnibus zur Schaffung einer KI-Ausnahme für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 2 (k) DSGVO

Die Kommission will mit Artikel 9 Absatz 2 Buchstabe k eine neue Ausnahme vom Verbot der Verarbeitung sensibler personenbezogener Daten einführen. Diese soll für die Entwicklung und den Betrieb von KI-Systemen gelten und durch zusätzliche Schutzmaßnahmen nach Artikel 9 Absatz 5 eingeschränkt werden. Im Grundsatz unterstützt der Bundesverband Kooperierender Mittelstand (BKM) dieses Vorhaben, da hierdurch ein zentraler Zielkonflikt adressiert wird: Innovationsfähigkeit vs. Datenschutz.

Allerdings ist zu kritisieren, dass der in Artikel 9 Absatz 2 Buchstabe k gewählte Ansatz zu kurz greift und nicht technologieoffen formuliert ist. So werden andere bestehende und entstehende datengetriebene Technologien hierbei vollständig außer Acht gelassen. Um eine Benachteiligung anderer datengetriebener Geschäftsmodelle zu vermeiden, sollten die Vorschriften technologieneutral formuliert werden.

Um eine verhältnismäßige Anwendung sicherzustellen, sollte unabhängig davon klargestellt werden, dass die vorgesehenen Rechtsgrundlagen nicht nur für datenintensive KI-Systeme gelten, sondern im Wege eines Erst-recht-Schlusses (a fortiori) auch weniger eingriffsintensive datengetriebene Anwendungen erfassen. Dies betrifft insbesondere Systeme zur Betrugs- und Missbrauchserkennung und zur Produktverbesserung, die regelmäßig auf klar zweckgebundene Analysen operativer Daten beschränkt sind und typischerweise geringere Risiken für die Rechte und Freiheiten betroffener Personen aufweisen.

Nicht zuletzt sollte sowohl im Artikel 88c-neu DSGVO, als auch im neuen Artikel 9 Absatz 2 Buchstabe k DSGVO klargestellt werden, dass die neuen Rechtsgrundlagen nicht nur für Verantwortliche, sondern auch für Auftragsverarbeiter gelten, die in deren Auftrag und Interesse handeln. Das Gesetz sollte daher hervorheben, dass Auftragsverarbeiter personenbezogene Daten und besondere Kategorien personenbezogener Daten im Rahmen dieser Vorschriften rechtmäßig verarbeiten können, wenn sie auf Grundlage eines Auftragsverarbeitungsvertrags gemäß Artikel 28 DSGVO tätig werden. Diese Klarstellung

ist entscheidend, um eine einheitliche Anwendbarkeit entlang der gesamten Datenverarbeitungskette sicherzustellen und Auslegungsunsicherheiten im komplexen KI-Ökosystem zu vermeiden.

Forderungen

- Dem Vorschlag der Kommission in Artikel 88c, die Verarbeitung personenbezogener Daten zur Entwicklung und zum Betrieb von KI-Systemen ausdrücklich als berechtigtes Interesse anzuerkennen, ist ausdrücklich zu unterstützen.
- Anpassung des Artikel 9 Absatz 2 Buchstabe k: „die Verarbeitung erfolgt im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells unter den in Absatz 5 genannten Bedingungen ***oder eines vergleichbaren datengetriebenen Systems mit gleichwertiger Zielsetzung und Risikostruktur.“***
- Klarstellung in den Erwägungsgründen, dass im Sinne des Arguments a fortiori die Rechtsgrundlage des Artikel 9 Absatz 2 Buchstabe k ebenso für weniger eingriffsintensive und datengetriebene Anwendungen gilt.
- Klarstellung in den Erwägungsgründen, dass die Rechtsgrundlage des Artikel 88 Buchstabe c sowie Artikel 9 Absatz 2 Buchstabe k ebenfalls für Auftragsverarbeiter gelten, die im Rahmen eines Auftragsverarbeitungsverhältnisses nach Artikel 28 DSGVO tätig werden.

6. Artikel 3 Nummer 8 Buchstabe a zur Anpassung des Artikel 33: Angleichung der Meldefristen von NIS-2 und DSGVO

Mithilfe einer Anpassung des Artikel 33 DSGVO sollen Meldungen künftig über den in Artikel 23a der NIS-2-Richtlinie (2022/2555) vorgesehenen „Single Entry Point“ erfolgen. Zudem ist eine Verlängerung der Meldefrist von bislang 72 auf 96 Stunden vorgesehen.

Der Bundesverband Kooperierender Mittelstand (BKM) begrüßt ausdrücklich die Einführung einer zentralen Anlaufstelle für digitale Meldepflichten. Eine Bündelung IT-sicherheitsrelevanter Eingaben über einen „Single Entry Point“ reduziert die Komplexität in Krisensituationen erheblich und ermöglicht es Unternehmen, sich auf die Bewältigung des Vorfalls zu konzentrieren, anstatt parallele Meldeprozesse bedienen zu müssen.

Auch die Anpassung der Satzkonstruktion, wonach künftig nur noch ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ eine Meldepflicht auslöst, ist sachgerecht. Sie stärkt den risikobasierten Ansatz der DSGVO und trägt dazu bei, Meldepflichten auf tatsächlich relevante Vorfälle zu konzentrieren.

Die Verlängerung der Meldefrist auf 96 Stunden ist im Grundsatz ebenfalls zu begrüßen, da sie Unternehmen in Grenzsituationen den notwendigen Handlungsspielraum verschafft, um Vorfälle zunächst zu analysieren und fundierte Meldungen abzugeben.

Diese Anpassung greift jedoch zu kurz, solange keine analoge Harmonisierung mit den Meldefristen der NIS-2-Richtlinie erfolgt. In der Praxis können bestimmte NIS-2-relevante IT-Sicherheitsvorfälle ebenfalls in den Anwendungsbereich von Artikel 33 DSGVO gelangen – etwa, wenn diese mit einem Leak personenbezogener Daten verbunden sind. Unterschiedliche Fristen würden faktisch zu parallelen Meldepflichten führen – genau das, was durch die Einführung eines „Single Entry Point“ eigentlich vermieden werden soll.

Ohne eine Angleichung der Meldefristen droht die Reform daher, ihr eigenes Ziel zu unterlaufen und zusätzliche Komplexität zu schaffen, anstatt sie zu reduzieren. Eine konsequente Angleichung der Meldefristen ist deshalb zwingend erforderlich.

In diesem Zusammenhang sollte ebenfalls klargestellt werden, dass eine getätigte Meldung über den Single-Entry-Point von jeder zusätzlichen Meldungspflicht, beispielsweise gegenüber (Landes-)Datenschutzaufsichtsbehörden, entbindet.

Parallel stellen sich Fragen bezüglich der praktischen Umsetzung einer zentralen Meldestelle. So ist fraglich, wie sichergestellt werden soll, dass ein einheitliches System auf technischer Ebene grenzüberschreitend funktionieren kann. Auch stellt sich die Frage nach der Verantwortlichkeit, sollten Meldungen aus verschiedenen Gründen nicht rechtzeitig die zuständige Stelle erreichen.

Forderungen

- Dem Vorschlag der Kommission, Meldungen nach Artikel 33 DSGVO über einen „Single Entry Point“ zu bündeln und die Meldefrist auf 96 Stunden zu verlängern, ist zu folgen
- Zugleich ist eine vollständige Harmonisierung mit den Meldefristen der NIS-2-Richtlinie sicherzustellen.

7. Anpassung des Artikel 28 Absatz 1 i.V.m Artikel 32

Die aus Artikel 28 Absatz 1 i. V. m. Absatz 3 Buchstabe a und Artikel 32 DSGVO abgeleitete Pflicht zur Kontrolle von Auftragsverarbeitern ist für viele Betriebe faktisch nicht umsetzbar und aus datenschutzrechtlicher Sicht unpraktikabel.

Schon kleinste Aufträge – etwa an Werbeagenturen – erfordern regelmäßige Überprüfungen vonseiten auftraggebender Unternehmen. Da KMU meist selbst nicht über das nötige Personal oder Know-How verfügen, müssen sie externe Prüfer beauftragen – mit erheblichem Kostenaufwand.

Zudem haben sich seit 2018 die Rahmenbedingungen grundlegend geändert: Datenbanken und Cloud-Services sind in der Zwischenzeit der Standard. Anbieter regelmäßig zu auditieren, ist für mittelständische Unternehmen nicht leistbar – weder aus finanzieller noch aus organisatorischer Sicht. Zwar können hier Self-Assessments Abhilfe leisten, allerdings binden auch diese Ressourcen und erfordern spezielles Know-How, das in der Breite nicht vorhanden ist.

Zusätzlich fehlt an Klarheit, was unter einer „regelmäßigen Überprüfung“ nach Artikel 32 DSGVO überhaupt zu verstehen ist. Trotz dieser Unsicherheit drohen Unternehmen Bußgelder von bis zu 4% des Jahresumsatzes – auch wenn Datenlecks allein auf Versäumnisse der Auftragsverarbeiter zurückzuführen sind.

Anpassungen am europäischen Gesetzestext sind dringend geboten. Eine Wesentlichkeitsschwelle bei der Verarbeitung unkritischer Daten würde verhindern, dass Kleinstaufträge im Bürokratiedickicht ersticken. Für Kleinunternehmen sollte eine regelmäßige Auditierung nur freiwillig erfolgen – die Kostenbelastung stellt sich hier besonders unverhältnismäßig dar. Zudem braucht es klar normierte Vorgaben zu Prüfzyklen: Ein Intervall von 18 Monaten wäre aus datenschutzrechtlicher Perspektive völlig ausreichend und würde zugleich dringend benötigte Rechtssicherheit schaffen.

Forderungen

- Bei den v Kontrollpflichten gegenüber Auftragsverarbeitern gemäß Artikel 28 Absatz1 iVm Absatz 3 Buchstabe a und Artikel 32 DSGVO sollten starre Prüfzyklen von 18 Monaten eingeführt werden, um Rechtssicherheit zu gewährleisten.
- Es sollte klargestellt werden, dass regelmäßige Audits gemäß Artikel 32 DSGVO bei risikoarmen Verarbeitungen und Kleinstunternehmen auf freiwilliger Basis zu erfolgen haben

Fazit

Die im Rahmen des Digital-Omnibus-Pakets vorgesehene und überfällige Überarbeitung der Datenschutzgrundverordnung kann eine echte Reform des europäischen Datenschutzes darstellen – sofern es nicht bei kosmetischen Eingriffen bleibt, sondern eine echte strukturelle Anpassung hin zu einem risikobasierten und innovationsoffenen Ansatz erfolgt. Nur so lässt sich die digitale Wettbewerbsfähigkeit Europas stärken, ohne das bestehende Schutzniveau für natürliche Personen zu beeinträchtigen.

Wir fordern daher alle europäischen Gesetzgeber dazu auf, die vorgebrachten Petiten des Bundesverbands Kooperierender Mittelstand (BKM) im weiteren Verlauf des Gesetzgebungsprozess zu berücksichtigen.

Bundesverband Kooperierender Mittelstand e.V. (BKM) | Unter den Linden 17 | 10117 Berlin | Tel.: +49 30 318 7309 0
info@bkm-verband.de | www.bkm-verband.de | Vereinsregister: Amtsgericht Berlin-Charlottenburg VR 22795 B
Vorstand i.S.d. § 26 BGB: Günter Althaus (Präsident), Julia Graeber, Dr. Stefan Müller, Dr. Andreas Trautwein
Hauptgeschäftsführer: Dr. Henning Bergmann | Lobbyregister Dt. Bundestag: R001283 | EU-Transparenzregister: 196997510883-76

Bei Fragen zu den einzelnen Forderungen stehen wir gerne für einen vertieften Austausch bereit.

Der Bundesverband Kooperierender Mittelstand (BKM) vertritt als Spitzenverband der deutschen Wirtschaft in Berlin und Brüssel die Interessen von ca. 200.000 mittelständischen Unternehmen, die in über 250 Verbundgruppen organisiert sind. Einzelne Verbundgruppen treten unter einer Marke auf, z.B. EDEKA, REWE, INTERSPORT, EP: ElectronicPartner, expert und BÄKO. Alle fördern ihre Mitglieder durch eine Vielzahl von Angeboten wie etwa Einkaufsverhandlungen, Logistik, IT, Finanzdienstleistungen, Beratung, Marketing, Ladeneinrichtung und Trendforschung.

Bundesverband Kooperierender Mittelstand e.V. (BKM) | Unter den Linden 17 | 10117 Berlin | Tel.: +49 30 318 7309 0
info@bkm-verband.de | www.bkm-verband.de | Vereinsregister: Amtsgericht Berlin-Charlottenburg VR 22795 B
Vorstand i.S.d. § 26 BGB: Günter Althaus (Präsident), Julia Graeber, Dr. Stefan Müller, Dr. Andreas Trautwein
Hauptgeschäftsführer: Dr. Henning Bergmann | Lobbyregister Dt. Bundestag: R001283 | EU-Transparenzregister: 196997510883-76