

Dokumentation als Schlüssel für gelebten Datenschutz

Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zu den Vorschlägen der Europäischen Kommission zur Änderung von Artikel 30 Absatz 5 DSGVO im Rahmen der IV. Omnibus-Verordnung (COM(2025) 501 final).

4. August 2025

Inhalt

I. Verbraucherrelevanz.....	3
II. Zusammenfassung.....	3
III. Einleitung.....	4
IV. Allgemeine Anmerkungen.....	4
V. Zu den konkreten Vorschlägen	7
1. Dokumentation als Instrument der Risikoprävention.....	7
2. Dokumentation als Voraussetzung gelebter Datenschutzpraxis.....	8
3. Dokumentation als Grundlage wirksamer Rechenschaft und Aufsicht	9
VI. Stärkung der Anwendung durch Unterstützung und Durchsetzung.....	9
Impressum	11

I. Verbraucherrelevanz

Verbraucher:innen sind tagtäglich von der Verarbeitung ihrer personenbezogenen Daten betroffen – etwa beim Arztbesuch, im Kontakt mit ihrer Anwältin oder beim Abschluss alltäglicher Verträge. Dabei werden ihre grundrechtlich verankerten Rechte von den Regelungen der Datenschutz-Grundverordnung (DSGVO) geschützt. Wenn die datenverarbeitende Stellen künftig jedoch ihre Verarbeitungstätigkeiten nicht mehr systematisch dokumentieren müssen, fehlt eine zentrale Grundlage, um Risiken frühzeitig zu erkennen und Datenschutzverletzungen wirksam vorzubeugen. Die Pflicht zur Dokumentation stärkt somit unmittelbar die Sicherheit für Verbraucher:innen.

Zugleich sind die Verfahrensverzeichnisse eine Voraussetzung dafür, dass Verbraucher:innen ihre Datenschutzrechte wirksam ausüben können. Denn ohne eine strukturierte Dokumentation können Unternehmen beispielsweise nur schwer ihren Informationspflichten nachkommen oder Auskunftersuchen nachvollziehbar beantworten. Die geplante Reform würde damit die praktische Durchsetzbarkeit zentraler Rechte erheblich schwächen – und das Vertrauen sowohl in das europäische Rechtssystem als auch in die digitale Wirtschaft untergraben.

II. Zusammenfassung

- Die von der Europäischen Kommission vorgeschlagene Einschränkung der Dokumentationspflicht nach Artikel 30 Absatz 5 DSGVO lehnt der Verbraucherzentrale Bundesverband (vzbv) ab. Die geplante Begrenzung auf „hochriskante“ Verarbeitungen für Unternehmen mit bis zu 750 Beschäftigten untergräbt zentrale Prinzipien der DSGVO und gefährdet die Rechte betroffener Personen. Jede Öffnung der Verordnung birgt zudem das Risiko, das sorgsam austarierte Schutzniveau des europäischen Datenschutzrechts strukturell zu schwächen – ohne dass hierfür eine belastbare Notwendigkeit oder Folgenabschätzung vorliegt.
- Verzeichnisse von Verarbeitungstätigkeiten sind kein bürokratischer Selbstzweck, sondern ein zentrales Instrument der Risikoprävention. Sie ermöglichen eine systematische Erfassung, Bewertung und Steuerung datenschutzrechtlicher Risiken. Gerade die Einschätzung, ob ein hohes Risiko vorliegt, erfordert ihrerseits bereits eine strukturierte Dokumentation.
- Darüber hinaus bilden diese Verzeichnisse die Grundlage für eine reflektierte und überprüfbare Datenschutzpraxis. Ohne sie fehlt Unternehmen ein zentrales Werkzeug, um ihre rechtlichen Pflichten wirksam umzusetzen.
- Verfahrensverzeichnisse sind zudem unverzichtbar für die Rechenschaftspflicht und die effektive Aufsicht. Sie schaffen Rechtssicherheit für Verantwortliche, Auftragsverarbeiter und Dritte und ermöglichen es Aufsichtsbehörden, risikoreiche Verfahren zu identifizieren und gezielt zu prüfen.
- Statt zentrale Rechenschaftspflichten abzubauen, sollte der europäische Gesetzgeber gezielt in Aufklärung, technische Unterstützung und konsequente Durchsetzung investieren – um einen digitalen Ordnungsrahmen zu stärken, der Wettbewerbsfähigkeit, Innovation und Grundrechtsschutz gleichermaßen gewährleistet.

III. Einleitung

Im Rahmen der IV. Omnibus-Verordnung schlägt die Europäische Kommission unter anderem vor, Artikel 30 Absatz 5 DSGVO zu ändern. Künftig soll die Pflicht zur Führung von Verzeichnissen von Verarbeitungstätigkeiten auf Prozesse mit „hohem Risiko“ im Sinne von Artikel 35 DSGVO beschränkt werden. Die Beurteilung, ob ein solches Risiko vorliegt, soll sich an den Leitlinien der Artikel-29-Gruppe zur Datenschutz-Folgenabschätzung orientieren.¹ Derzeit gilt die Ausnahme lediglich, wenn die Verarbeitung nur gelegentlich erfolgt, kein voraussichtliches Risiko für betroffene Personen birgt und keine besonderen Kategorien personenbezogener Daten umfasst.

Zudem soll die Ausnahme nicht mehr nur für kleine und mittlere Unternehmen (KMU) mit bis zu 250 Mitarbeitenden gelten, sondern auch auf sogenannte „small mid-caps“ (SMC) ausgeweitet werden – also Unternehmen mit weniger als 750 Beschäftigten, einem Jahresumsatz von höchstens 150 Millionen Euro und einer Bilanzsumme von maximal 129 Millionen Euro.

Der vzbv lehnt die vorgelegten Reformvorschläge ab. Eine Öffnung der DSGVO zum jetzigen Zeitpunkt birgt erhebliche Risiken für die in der Europäischen Grundrechtecharta verankerten Rechte und Freiheiten natürlicher Personen. Der vzbv begrüßt daher, dass die Europäische Kommission den Dialog mit Interessengruppen sucht, und bedankt sich für die Gelegenheit zur Stellungnahme.

IV. Allgemeine Anmerkungen

Die DSGVO ist eine Erfolgsgeschichte und bildet ein zentrales Fundament der europäischen Digitalregulierung. Sie ist das Ergebnis eines intensiven, mehrjährigen Aushandlungsprozesses, an dem Gesetzgeber, Zivilgesellschaft, Wirtschaft und Wissenschaft gleichermaßen beteiligt waren. Die DSGVO stellt damit einen sorgfältig austarierten Kompromiss dar, der unterschiedliche, teils widerstreitende Interessen in Einklang bringt. Dem folgend war sie in zahlreichen Drittstaaten Referenzmodell für eigene Datenschutzgesetze.

Aus Sicht des vzbv ist es verfehlt, Datenschutz pauschal als Hemmnis für Wettbewerbsfähigkeit und technologische Innovation darzustellen. Es fehlen belastbare empirische Nachweise für innovationshemmende Effekte eines strengen Datenschutzes.² Im Gegenteil zeigen unter anderem die Evaluationsberichte der Europäischen Kommission aus den Jahren 2020 und 2024 sowie das dazu eingeholte Stakeholder-Feedback, dass kein struktureller Reformbedarf im Hinblick auf die DSGVO besteht. Die Europäische Kommission betonte vielmehr, dass die Grundsätze und

¹ Artikel-29-Datenschutzgruppe: Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“. WP 248 rev.01, 2017, <https://ec.europa.eu/newsroom/article29/items/611236>, 29.07.2025.

² Siehe Bernd Beckert u. a.: Die Digitalisierung aus Innovationsperspektive. Faktencheck und Handlungsbedarf. Policy Brief 01/2021, S. 13, https://www.isi.fraunhofer.de/content/dam/isi/dokumente/policy-briefs/policy_brief_digitalisierung.pdf, 29.07.2025.

Regelungen der DSGVO wirksam, zukunftsfähig und verhältnismäßig sind.³ Auch der Rat der Europäischen Union bezeichnet in seinem Bericht⁴ aus dem Jahr 2023 die DSGVO als Erfolg. Sie habe zu positiven Ergebnissen bei der Harmonisierung des EU-Rechts und der Stärkung einer Datenschutzkultur auf EU- und globaler Ebene geführt. Ihre Anwendung hätte Vertrauen und Rechtssicherheit gestärkt, den grenzüberschreitenden Datenverkehr innerhalb der EU erleichtert und damit den Binnenmarkt sowie die Entwicklung der digitalen Wirtschaft gefördert. Der Fokus sollte daher künftig auf kohärenter Auslegung und wirksamer Durchsetzung liegen – statt auf Deregulierung.

Nicht Datenschutz oder Verbraucherschutz hemmen Wettbewerbsfähigkeit und Innovationskraft in Europa, sondern strukturelle Defizite: etwa die unzureichende Digitalisierung der Verwaltung, der schleppende Ausbau digitaler Infrastrukturen (insbesondere Glasfaser- und 5G-Netze), der anhaltende Fachkräftemangel sowie fehlende Investitionen in Forschung, Entwicklung und Start-up-Förderung. Starker Datenschutz ist hingegen eine tragende Säule einer wertebasierten digitalen Ökonomie und ein europäisches Qualitätsversprechen. Zahlreiche europäische Unternehmen – etwa im Bereich datenschutzfreundlicher KI-Anwendungen – sind damit erfolgreich am Markt positioniert.⁵ Von einem niedrigen Datenschutzniveau profitieren vor allem datenreiche, marktmächtige Großkonzerne auf Kosten mittelständischer Anbieter.

Für Verbraucher:innen bedeutet Datenschutz Vereinfachung und Entbürokratisierung im Alltag, etwa wenn sie sich bei der Verwendung digitaler Dienste auf ein hohes Schutzniveau verlassen können. Gleichzeitig ist dieses Vertrauen der Verbraucher:innen eine essenzielle Voraussetzung für die Nutzung digitaler Dienste und für eine starke Markenbindung. Demgegenüber belegen Studien, dass Datenschutzbedenken zu den Hauptgründen zählen, wenn Verbraucher:innen bestimmte digitale Angebote meiden.⁶ Auch das Consumer Conditions Scoreboard (CCS) 2023 zeigt deutlich, wie stark Datenschutzbedenken das Vertrauen beeinträchtigen können: 70 % der Verbraucher:innen äußerten sich besorgt darüber, wie ihre personenbezogenen Daten verwendet und weitergegeben werden. 38 % berichteten in diesem Zusammenhang von einem Rückgang ihres Vertrauens in den elektronischen Handel.⁷

Eine Öffnung der DSGVO zum aktuellen Zeitpunkt birgt erhebliche Risiken für die in der Europäischen Grundrechtecharta verankerten Rechte und Freiheiten natürlicher Personen. In einer Sonderausgabe des Eurobarometers zur digitalen Dekade 2024 gaben 46 % der Befragten an, dass der Missbrauch personenbezogener Daten die größte persönliche Auswirkung im Bereich digitaler Technologien hat.⁸ Umso bedauerlicher ist es, dass die Europäische Kommission keine Folgenabschätzung vorgelegt hat, die nachweist, dass die Vorschläge im Sinne von Artikel 52

³ European Commission: Second Report on the application of the General Data Protection Regulation. COM(2024) 357 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357>, 29.07.2025.

⁴ Council of the European Union: Council position and findings on the application of the General Data Protection Regulation (GDPR). 15507/23, <https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf>, 29.07.2025.

⁵ Wie etwa Brighter AI oder Sordi.ai, nur um zwei Beispiele zu nennen.

⁶ Bitkom: Mehr als jeder Dritte hat Hemmungen, digitale Angebote zu nutzen, 2025, <https://www.bitkom.org/Presse/Presseinformation/Hemmungen-digitale-Angebote-Digitaltag-2025>, 29.07.2025.

⁷ European Commission: Consumer Conditions Scoreboard, 2023, S. 20, https://commission.europa.eu/system/files/2023-10/consumer_conditions_scoreboard_2023_v1.1.pdf, 29.07.2025.

⁸ Dass.: The Digital Decade. Special Eurobarometer 551, 2024, <https://europa.eu/eurobarometer/surveys/detail/3174>, 29.07.2025.

Absatz 1 der Charta erforderlich, verhältnismäßig und ausgewogen sind. Eine solche Prüfung ist Voraussetzung für jede Einschränkung von Grundrechten.

Besorgniserregend ist zudem, dass die vorgeschlagenen Anpassungen zu weitergehenden Aushöhlungen der DSGVO führen könnten. So wurden in der politischen Debatte – auch von Seiten der deutschen Bundesregierung – Vorschläge eingebracht, KMU vollständig vom Anwendungsbereich der DSGVO auszunehmen.⁹ Die dänische Ratspräsidentschaft schlägt bereits vor, die Informations- und Auskunftsrechte nach Artikel 13 bis 15 DSGVO einzuschränken und das Beschwerderecht nach Artikel 77 zu erschweren.¹⁰ Diese Initiativen zeigen, dass jede noch so kleine Anpassung als Einfallstor genutzt werden könnte, um das sorgsam austarierte Regulierungsgefüge der DSGVO massiv zu untergraben – mit der Folge einer tiefgreifenden Erosion des europäischen Datenschutzniveaus.

Hinzu kommt: Die DSGVO bildet gemeinsam mit dem Digital Services Act (DSA), dem Digital Markets Act (DMA) und weiteren Rechtsakten das Fundament eines kohärenten europäischen Ordnungsrahmens für den digitalen Raum. Dieser Rahmen schafft Vorhersehbarkeit und damit Rechts-, Planungs- und Investitionssicherheit für Unternehmen. Die Europäische Kommission hat jedoch keine Analyse vorgelegt, welche Auswirkungen mögliche Änderungen der DSGVO auf diese Regelwerke haben könnten. Es besteht die Gefahr, dass die Reform die Kohärenz dieses – noch nicht einmal vollständig angewendeten – Regelungsgefüges untergräbt und den erklärten Zielen der Vereinfachung und der Vorhersehbarkeit des EU-Rechts zuwiderläuft. Insbesondere würde das Prinzip eines abgestuften, aber einheitlichen Schutzniveaus für Grundrechte im digitalen Raum geschwächt.

Nur wenn die bestehenden Instrumente stark und konsistent sind und strikt durchgesetzt werden, kann die Europäische Union ihre Rolle als globale Standardsetzerin im Bereich digitaler Grundrechte behaupten. Sie stärken die Unabhängigkeit von außereuropäischen Plattformen – gerade vor dem Hintergrund wachsender geopolitischer Spannungen und internationaler Wettbewerbsdynamiken.

Die DSGVO ist ein bewährter Ordnungsrahmen für den digitalen Raum und bedarf keiner strukturellen Reform. Statt an ihrem Fundament zu rütteln, sollte die Europäische Kommission auf kohärente Auslegung und konsequente Durchsetzung setzen. Jede Öffnung birgt das Risiko einer schleichenden Erosion des Datenschutzniveaus – mit weitreichenden Folgen für Grundrechte, Rechtsklarheit und Vertrauen.

⁹ Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD. 21. Legislaturperiode, 2025, S. 65, <https://www.cdu.de/app/uploads/2025/04/Koalitionsvertrag-%E2%80%93-barrierefreie-Version.pdf>, 29.07.2025.

¹⁰ Danish presidency of the Council of the European Union: Securing better conditions for companies to comply with the data protection rules. DK Non-paper, 2025.

V. Zu den konkreten Vorschlägen

1. Dokumentation als Instrument der Risikoprävention

Die geplante Änderung von Artikel 30 Absatz 5 DSGVO greift tief in die Systematik des risikobasierten Datenschutzes ein. Sie reduziert die Dokumentation von Verarbeitungstätigkeiten auf einen vermeintlich verzichtbaren Verwaltungsakt – tatsächlich bildet sie jedoch die Grundlage jeder belastbaren Risikoabschätzung und ist ein zentrales Element effektiven Datenschutzmanagements.

Datenschutzrisiken lassen sich nicht abstrakt oder einmalig beurteilen. Sie entstehen aus konkreten, sich wandelnden Verarbeitungskontexten und erfordern eine kontinuierliche, kontextsensitive Bewertung.¹¹ Eine strukturierte Dokumentation ermöglicht es, Datenflüsse systematisch zu erfassen, zu analysieren und hinsichtlich ihrer Risiken zu bewerten. Ohne diese Grundlage drohen Fehleinschätzungen – insbesondere in sensiblen Bereichen wie der ärztlichen oder anwaltlichen Praxis. Der Vorschlag der Kommission würde jedoch dazu führen, dass selbst in solchen Fällen künftig kein Verzeichnis der Verarbeitungstätigkeiten mehr erforderlich wäre.¹²

Besonders problematisch ist, dass die Reform Verantwortlichen ermöglichen würde, die Einstufung ihrer Verarbeitung eigenständig vorzunehmen – ohne dass verbindliche, überprüfbare Kriterien für die Qualifikation als „hochriskant“ existieren. Die herangezogenen Leitlinien der Artikel-29-Gruppe sind unverbindlich und wurden für die Zwecke der Datenschutz-Folgenabschätzung konzipiert, nicht für die pauschale Bewertung von Dokumentationspflichten. Dies schafft erhebliche Unsicherheiten und eröffnet strukturelle Fehlanreize: Unternehmen könnten versucht sein, Risiken systematisch zu unterschätzen – sei es aus wirtschaftlichem Druck, mangelnder datenschutzrechtlicher Expertise oder verzerrter Risikowahrnehmung.

Für verantwortungsbewusste Unternehmen entsteht eine paradoxe Situation: Während bislang lediglich ein Verfahrensverzeichnis zu führen war, verlangt die neue Regelung nun eine eigenständige Risikobewertung – ohne belastbare Maßstäbe. Um ihrer Rechenschaftspflicht nachzukommen, müssten sie begründen können, warum ihre Verarbeitung kein „hohes Risiko“ darstellt. Doch genau diese Einschätzung setzt ihrerseits eine strukturierte Dokumentation voraus – etwa zur Art der Daten, den Verarbeitungszwecken, dem Umfang und den Schutzmaßnahmen. Ohne diese Grundlage ist eine belastbare Risikobewertung kaum möglich.

Verantwortungsbewusste Unternehmen werden daher weiterhin dokumentieren – auch wenn sie formal nicht mehr dazu verpflichtet sind. Gleichzeitig entfällt für weniger gewissenhafte Mitbewerber:innen der Anreiz zur strukturierten Risikoabschätzung. Dies führt zu einem systematischen Wettbewerbsungleichgewicht: Wer sich gesetzestreu verhält, trägt den Aufwand einer strukturierten Risikoabschätzung – während andere durch Regelvermeidung Wettbewerbsvorteile erlangen.

¹¹ Siehe Artikel-29-Datenschutzgruppe (WP29) (2017) (wie Anm. 1), S. 13f.

¹² Entsprechend Erwägungsgrund 91 DSGVO sowie den Leitlinien WP 248 rev.01 birgt die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder einen Rechtsanwalt kein hohes Risiko, da diese Verarbeitungen als nicht umfangreich gelten.

Ein risikobasierter Ansatz verlangt keine pauschalen Ausnahmen, sondern setzt voraus, dass Risiken systematisch erfasst und analysiert werden. Genau das leistet die Dokumentation der Verarbeitungstätigkeiten – sie ist damit nicht entbehrlich, sondern konstitutiv für wirksamen Datenschutz.

2. Dokumentation als Voraussetzung gelebter Datenschutzpraxis

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten ist weit mehr als eine formale Anforderung. Sie bildet den strukturellen Rahmen für eine reflektierte, systematische und rechtskonforme Datenverarbeitung – insbesondere für KMU. Der Wegfall dieser Pflicht würde Unternehmen nicht von der Verantwortung entbinden, ihre Prozesse datenschutzkonform zu gestalten. Ohne eine strukturierte Dokumentation fehlt jedoch ein zentrales Instrument, um dieser Verantwortung wirksam nachzukommen.

Verarbeitungsverzeichnisse ermöglichen es Verantwortlichen, ein belastbares Verständnis ihrer Datenverarbeitung und der zugrunde liegenden Rechtsgrundlagen zu entwickeln. Sie schaffen Transparenz über die Vielzahl datenschutzrechtlicher Verpflichtungen, erleichtern deren systematische Erfassung und unterstützen die Überführung in angemessene organisatorische Abläufe. Insbesondere tragen sie zur praktischen Umsetzung der Grundsätze des Datenschutzes nach Artikel 5 DSGVO bei – etwa hinsichtlich Zweckbindung, Datenminimierung und Speicherbegrenzung. Auch die Bestimmung einer tragfähigen Rechtsgrundlage gemäß Artikel 6 DSGVO sowie die Wahrung der Betroffenenrechte, etwa im Rahmen von Informationspflichten oder Auskunftersuchen, werden durch eine sorgfältige Dokumentation erheblich erleichtert. Nicht zuletzt bildet sie die Grundlage für die Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten. Der ersatzlose Wegfall dieser Pflicht birgt erhebliche Risiken: Ohne systematische Erfassung bleiben Schwachstellen in der Datenverarbeitung häufig unerkannt – mit potenziell gravierenden Folgen für die Rechte der betroffenen Personen.

Auch hier zeigt sich das regulatorische Fehlanreizsystem: Während verantwortungsbewusste Unternehmen ihre Dokumentationspraxis freiwillig fortführen werden, könnten gerade solche Akteure, die ohnehin über schwache Rechenschaftsstrukturen oder intransparente Geschäftsmodelle verfügen, sich einer systematischen Auseinandersetzung mit ihren Pflichten entziehen. Die Reform würde damit ausgerechnet dort auf Kontrolle verzichten, wo sie am dringendsten erforderlich ist und ein fatales Signal hinsichtlich der Verbindlichkeit datenschutzrechtlicher Mindeststandards senden.

Die Dokumentation von Verarbeitungstätigkeiten ist nicht bloß ein gesetzliches Erfordernis, sondern eine unverzichtbare Voraussetzung für eine wirksame, überprüfbare und nachhaltige Datenschutzpraxis. Ihr Wegfall würde nicht zur Entlastung, sondern zur Erosion gelebter Datenschutzverantwortung führen und damit auch die praktische Wirksamkeit der DSGVO insgesamt schwächen.

3. Dokumentation als Grundlage wirksamer Rechenschaft und Aufsicht

Die Dokumentation von Verarbeitungstätigkeiten ist eine tragende Säule der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DSGVO. Sie ersetzt das frühere – deutlich aufwendigere – System der Meldepflichten nach der Datenschutzrichtlinie 95/46/EG und bildet heute das zentrale Instrument, mit dem datenverarbeitende Stellen nachweisen können, dass sie die datenschutzrechtlichen Vorgaben aktiv, strukturiert und nachvollziehbar umsetzen. Dies betrifft nicht nur die Dokumentation von Risiko- und Interessenabwägungen, sondern auch die transparente Darstellung der Zweckbindung, Datenminimierung, Speicherbegrenzung sowie der getroffenen technischen und organisatorischen Maßnahmen.

Somit schafft die Dokumentation Rechtssicherheit – nicht nur für Verantwortliche selbst, sondern auch für Auftragsverarbeiter, gemeinsam Verantwortliche und weitere Dritte, die auf eine klare Dokumentation der Datenflüsse und Zuständigkeiten angewiesen sind. Ohne nachvollziehbare Verzeichnisse entstehen Unsicherheiten über Rollenverteilungen, Rechtsgrundlagen und Schutzmaßnahmen, was nicht nur die Zusammenarbeit erschwert, sondern auch die Haftungsrisiken erhöht. Die Dokumentation ist damit ein zentrales Instrument zur Sicherung rechtlicher Klarheit und operationaler Verlässlichkeit in komplexen Datenökosystemen.

Für Datenschutzaufsichtsbehörden bildet die Dokumentation eine unverzichtbare Prüfungsgrundlage. Nur auf Basis strukturierter Verzeichnisse lassen sich risikogeneigte Verarbeitungsvorgänge identifizieren, gezielte Prüfungen durchführen und wirksame aufsichtsrechtliche Maßnahmen ergreifen. Der Wegfall dieser Pflicht würde die Kontrollfähigkeit der Behörden erheblich schwächen und die effektive Durchsetzung der DSGVO in der Praxis substanziell beeinträchtigen.

Verarbeitungsverzeichnisse sind unverzichtbar für die Rechenschaftspflicht, die Rechtssicherheit aller Beteiligten und die effektive Aufsicht durch Datenschutzbehörden. Ohne sie fehlt die Grundlage für wirksame Nachvollziehbarkeit und Kontrolle und damit für eine belastbare Durchsetzung der DSGVO.

VI. Stärkung der Anwendung durch Unterstützung und Durchsetzung

Statt grundlegende Rechenschaftspflichten aufzugeben, sollte die Europäische Kommission vorrangig bestehende Instrumente ausschöpfen, um die wirksame Anwendung der DSGVO zu fördern. Dazu zählen praxisnahe Leitlinien zur Risikoeinschätzung und zur Klärung der Dokumentationspflichten für KMU. Ergänzend könnten für wenig risikobehaftete Verarbeitungsprozesse europaweit standardisierte Vorlagen und digitale Werkzeuge bereitgestellt

werden – etwa zur Erstellung von Verzeichnissen von Verarbeitungstätigkeiten, Auftragsverarbeitungsverträgen oder Datenschutzhinweisen sowie zur Auswahl grundlegender technischer und organisatorischer Maßnahmen. Initiativen nationaler Aufsichtsbehörden bieten hierfür bereits erprobte Vorbilder.¹³ Denkbar wäre auch, Schulungsangebote zu fördern, die Start-Ups und KMU gezielt unterstützen – wie sie etwa von der Berliner Datenschutzbeauftragten angeboten werden.¹⁴

Darüber hinaus sollte die Europäische Kommission die Nutzung standardisierter Symbole zur Vereinfachung von Datenschutzhinweisen durch einen delegierten Rechtsakt etablieren. Auch die Verbreitung von Verhaltensregeln und Zertifizierungsmechanismen sollte gezielt gestärkt werden, verbunden mit einer Analyse der Ursachen bestehender Hürden und deren gezielter Beseitigung.

Neben der Unterstützung durch solche Hilfsmittel ist die konsequente Durchsetzung des geltenden Rechts zentral. Sie stärkt nicht nur die Rechte der betroffenen Personen, sondern sorgt für faire Wettbewerbsbedingungen und schützt Unternehmen, die sich rechtskonform verhalten, vor strukturellen Nachteilen. Dabei ist hervorzuheben, dass zentrale Durchsetzungsinstrumente – etwa Klagebefugnisse von Verbraucherorganisationen oder Schadensersatzklagen – erst jüngst Wirkung entfalten konnten, nachdem ihre Reichweite über Jahre hinweg bestritten wurde, obwohl der Wortlaut der Vorschriften eindeutig war.

Der europäische Gesetzgeber sollte nicht auf eine Schwächung essenzieller Mechanismen zur Risikobewertung und Erfüllung der Rechenschaftspflicht setzen. Stattdessen gilt es, gezielt in Aufklärung, technische Unterstützung und effektive Durchsetzung zu investieren. Nur unter diesen Voraussetzungen lässt sich ein digitaler Ordnungsrahmen stärken, der sowohl Innovation als auch den Schutz der Grundrechte gewährleistet.

¹³ European Data Protection Board: Practical resources for SMEs, https://www.edpb.europa.eu/sme-data-protection-guide/practical-resources-for-smes_en, 29.07.2025.

¹⁴ Berliner Beauftragte für Datenschutz und Informationsfreiheit: Schulungen für Vereine, Start-ups und Kleinunternehmen, <https://www.datenschutz-berlin.de/service/starthilfe-datenschutz/>, 29.07.2025.

Impressum

Herausgegeben von:

Verbraucherzentrale Bundesverband e.V.

Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0

digitales@vzbv.de

vzbv.de

Stand:

August, 2025

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