Verbraucherzentrale
Bundesverband

DSGVO: Entlastung ja – Aufweichung nein

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).

28. August 2025

Inhalt

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 Auskunftsersuchen 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.

- Dazu gehören etwa:

- Die Europäische Kommission sollte gemeinsam mit den europäischen Aufsichtsbehörden darauf hinarbeiten, leicht verständliche, europaweit harmonisierte Handreichungen, Muster und Checklisten speziell für KMU zu entwickeln und aktiv zu verbreiten.
- Die Bundesregierung sollte sich auf EU-Ebene dafür einsetzen, dass der risikobasierte Ansatz der DSGVO klarer verankert wird und Unternehmen bei Datenverarbeitungen mit geringem Risiko von vereinfachten Dokumentationsanforderungen profitieren können.
- Die Europäische Kommission sollte geprüfte Musterverträge und Standardtexte (z.B. für Auftragsverarbeitung) bereitstellen, die Unternehmen unmittelbar nutzen können, um Rechtssicherheit zu erlangen und Bürokratiekosten zu senken.
- Die Europäische Kommission sollte einheitliche Kurztexte und Piktogramme für typische Verarbeitungsvorgänge entwickeln und freigeben, damit KMU ihre Informationspflichten effizienter erfüllen können – bei gleichzeitiger Stärkung der Transparenz für Verbraucher:innen.
- Die Bundesregierung sollte die Entwicklung branchenspezifischer Verhaltenskodizes und KMU-geeigneter Zertifikate aktiv fördern und auf europäischer Ebene für eine pragmatische Anerkennungspraxis eintreten.
- Bund und Länder sollten die Datenschutzaufsichtsbehörden personell und finanziell so ausstatten, dass diese ihre Unterstützungsangebote für KMU – etwa durch Schulungen – deutlich ausbauen können.

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.

[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.

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 Regelungen der DSGVO wirksam, zukunftsfähig und verhältnismäßig sind.[3] Ebenso wurde im Rahmen des von Michael McGrath, Europäischer Kommissar für Demokratie, Justiz, Rechtsstaatlichkeit und Verbraucherschutz, geleiteten GDPR Implementation Dialogs[4] im Juli 2025 deutlich, dass die DSGVO von Stakeholdern insgesamt als ausgewogener Rechtsrahmen wahrgenommen wird, der ihre Ziele erreicht hat. Europäische Wirtschaftsverbände unterstrichen im Rahmen des Dialogs, dass sie erheblich in DSGVO-Compliance investiert haben und eine grundlegende Neuöffnung des Rechtsrahmens neue Unsicherheiten schaffen würde.

Zu einem vergleichbaren Ergebnis kam auch der Rat der Europäischen Union: in seinem Bericht[5] aus dem Jahr 2023 bezeichnet er 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

---

[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.

[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] Dass.: GDPR Implementation Dialogue: Summary Conclusions, 2025, https://commission.europa.eu/document/download/835dfd02-a38c-4cc3-ba53-5b0499e2b8b9_en?filename=Summary%20Conclusions%20Implementation%20Dialogue%20on%20the%20GDPR.pdf, 12.08.2025.

[5] 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.

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.[6] Von einem niedrigen Datenschutzniveau profitieren vor allem datenreiche, marktmächtige Großkonzerne auf Kosten mittelständischer Anbieter.

Für Verbraucher:innen bedeutet Datenschutz Vereinfachung und Entbürokatisierung 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.[7] 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.[8]

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.[9] Umso bedauerlicher ist es, dass die Europäische Kommission keine Folgenabschätzung vorgelegt hat, die nachweist, dass die Vorschläge im Sinne von Artikel 52 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.[10] 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.[11] Diese Initiativen zeigen, dass jede noch so kleine

---

[6] Wie etwa Brighter AI oder Sordi.ai, nur um zwei Beispiele zu nennen.

[7] 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.

[8] 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.

[9] Dass.: The Digital Decade. Special Eurobarometer 551, 2024, https://europa.eu/eurobarometer/surveys/detail/3174, 29.07.2025.

[10] 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.

[11] 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.

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.

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.[12] Eine strukturierte Dokumentation ermöglicht es, Datenflüsse

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

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.[13]

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.

> 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

[13] 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.

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 Auskunftsersuchen, 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 Mechanismen zur Risikobewertung und Erfüllung der Rechenschaftspflicht aufzugeben, sollten die Europäische Kommission und die Bundesregierung vorrangig bestehende Instrumente ausschöpfen und gezielt in Aufklärung, technische Unterstützung und effektive Durchsetzung investieren. Nur unter diesen Voraussetzungen lässt sich ein digitaler Ordnungsrahmen stärken, der sowohl Innovation als auch den Schutz der Grundrechte gewährleistet.

1. Praxisnahe Leitlinien und Checklisten für Unternehmen (insb. KMU)

Viele KMU stehen vor der Herausforderung, die komplexen Anforderungen der DSGVO im betrieblichen Alltag umzusetzen – oft ohne eigene Rechtsabteilung oder spezialisierte Datenschutzexpert:innen. Der Gesetzestext allein liefert hierfür wenig konkrete Handlungsanweisungen. Bisherige Unterstützungsangebote der Aufsichtsbehörden sind zudem oft sehr juristisch formuliert, umfangreich und nicht auf die Abläufe kleiner Betriebe zugeschnitten. In manchen Mitgliedstaaten gibt es bereits gute Hilfsmaterialien, in anderen fühlen sich Unternehmen

jedoch weitgehend allein gelassen.[14] Das führt zu Unsicherheiten, unnötigem Zeit- und Kostenaufwand und in der Folge zu übervorsichtigen, bürokratisch belastenden Prozessen.

Ein Ansatz, um dies zu verbessern, sind verbindliche Leitlinien, Checklisten und Musterformulare, die vom Europäischen Datenschutzausschuss (EDSA) zentral bereitgestellt werden sollten.[15] Der 2023 veröffentlichte KMU-Leitfaden des EDSA[16] zeigt, dass solche Angebote wirken können: kompakte, auf die Praxis zugeschnittene Erläuterungen, ergänzt durch Beispiele, die rechtliche Vorgaben in konkrete Handlungsschritte übersetzen. Entscheidend ist jedoch, diese Materialien noch stärker auf typische KMU-Szenarien auszurichten, juristische Fachsprache zu reduzieren und verbindliche, leicht adaptierbare Vorlagen bereitzustellen – etwa für Datenschutzhinweise, Einwilligungstexte oder Verarbeitungsverzeichnisse. Einheitliche, EU-weit abgestimmte Hilfsmittel würden zudem für mehr Rechtssicherheit bei grenzüberschreitender Tätigkeit sorgen.

Damit dies gelingt, müssen die Aufsichtsbehörden ihre internen Arbeitsweisen anpassen und den Anspruch verankern, für die Unternehmenspraxis zu schreiben – nicht nur für juristische Fachkreise. Vor diesem Hintergrund begrüßt der vzbv, dass sich der EDSA darauf verständigt hat, seine Arbeitsweise zu aktualisieren und ergänzende Formate für Leitlinien zu entwickeln.[17] Die Angebote müssen aktiv beworben und in bestehende Informationskanäle der Wirtschaft integriert werden, damit gerade vielbeschäftigte Mittelständler sie kennen und nutzen.

Der Nutzen liegt auf der Hand: Weniger Zeitverlust durch unnötige Rechtsrecherche, geringere Abhängigkeit von externer Beratung und ein Abbau von Unsicherheiten, die bisher zu ineffizienten oder übervorsichtigen Lösungen geführt haben. Durch eine gezielte Stärkung und Vereinheitlichung solcher praxisnahen Instrumente lässt sich die Umsetzung der DSGVO ohne Änderung des Verordnungstextes spürbar vereinfachen – eine lohnende Investition in Verwaltungseffizienz und Praxistauglichkeit. So wird die Wirtschaft gestärkt, ohne beim Datenschutz Abstriche zu machen – ein pragmatischer Weg, um Rechtssicherheit und Wettbewerbsfähigkeit zu verbinden.

> Die Europäische Kommission sollte gemeinsam mit den europäischen Aufsichtsbehörden darauf hinarbeiten, leicht verständliche, europaweit harmonisierte Handreichungen, Muster und Checklisten speziell für KMU zu entwickeln und aktiv zu verbreiten.

2. Vereinfachte Dokumentations- und Nachweispflichten

Für viele KMU stellen die umfangreichen Dokumentations- und Nachweispflichten der DSGVO eine Herausforderung dar. Ob etwa Verarbeitungsverzeichnis nach Artikel 30 oder die Dokumentation

---

[14] Vgl. European Commission (wie Anm. 3).

[15] Deutsche Industrie und Handelskammer: Unternehmen von EU-Bürokratie entlasten und europäische Wettbewerbsfähigkeit stärken. DIHK-Lösungsansätze, 2024, S. 6, https://www.dihk.de/resource/blob/124340/8aa17491616c2ce5801ddb22d61dc55f/dihk-vorschlaege-eu-buerokratieabbau-2024-data.pdf, 29.07.2025.

[16] Europäischer Datenschutzausschuss: Der EDSA-Datenschutzleitfaden für kleine Unternehmen, https://www.edpb.europa.eu/sme-data-protection-guide/home_de, 29.07.2025.

[17] European Data Protection Board: The Helsinki Statement on enhanced clarity, support and engagement, 2025, https://www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf, 29.07.2025.

von Datenschutz-Folgenabschätzungen – diese Pflichten sind für Betriebe ohne eigene Rechtsabteilung oft nur mit großem Aufwand zu bewältigen. Zwar sieht die DSGVO selbst bereits Erleichterungen vor, etwa für Unternehmen mit weniger als 250 Beschäftigten, die Daten nur gelegentlich und ohne Risiko verarbeiten. In der Praxis greifen diese Ausnahmen jedoch kaum, weil unklar bleibt, was Begriffe wie „gelegentlich“ oder „nicht risikohaft“ konkret bedeuten. So entsteht ein Klima der Unsicherheit.

Ein Ausweg besteht darin, den risikobasierten Ansatz der DSGVO konsequent in der Praxis umzusetzen. Unternehmen, die lediglich Standarddaten mit geringem Risiko verarbeiten - wie Kunden- und Mitarbeiterangaben in überschaubarem Umfang -, könnten auf vereinfachte Dokumentationsinstrumente zurückgreifen. Der EDSA und die nationalen Aufsichtsbehörden könnten hierfür europaweit einheitliche Muster und Vorlagen (und/oder ensprechende Online-Generatoren) bereitstellen, die den Nachweis der Einhaltung auf schlanke Weise ermöglichen.[18] Ein vereinfachtes Verarbeitungsverzeichnis mit den wichtigsten Angaben anstelle seitenlanger Tabellen, würde für viele KMU eine spürbare Entlastung bedeuten.

Herausfordernd bliebe, einen einheitlichen europäischen Standard sicherzustellen. Wenn Mitgliedstaaten unterschiedliche Maßstäbe für „geringes Risiko“ anlegen, droht erneut Unsicherheit. Entscheidend – auch für die Unternehmen in der praktischen Anwendung – ist, dass klare Kriterien veröffentlicht werden, wann eine vereinfachte Form genügt. Positiv- und Negativlisten könnten Orientierung bieten und verhindern, dass Unternehmen irrtümlich zu wenig dokumentieren. Daher ist eine Koordinierung auf Ebene des EDSA notwendig. Ebenso wichtig ist, dass die Erleichterungen nicht mit einem völligen Verzicht auf Dokumentation verwechselt werden: Auch bei vereinfachten Verfahren muss ein Mindestmaß an Aufzeichnungen gewährleistet sein.

Damit wird Bürokratie dort reduziert, wo sie offenkundig unverhältnismäßig ist, ohne das materielle Schutzniveau der DSGVO zu verändern. Ein Handwerksbetrieb mit fünf Angestellten müsste nicht denselben Dokumentationsapparat pflegen wie ein internationaler Konzern mit datenintensiven Analyseverfahren. Gleichzeitig bliebe die Dokumentationspflicht in risikoreichen Bereichen bestehen, sodass der Schutz der Betroffenenrechte unangetastet bleibt. Weniger formaler Ballast bedeutet zudem, dass die relevanten Unterlagen aktuell und verlässlich geführt werden können, anstatt Ressourcen in reine Papierarbeit zu investieren. Das Ergebnis ist eine pragmatische Balance zwischen Bürokratieabbau und Datenschutz, die Vertrauen bei Unternehmen wie auch Verbraucher:innen schafft.

> Die Bundesregierung sollte sich auf EU-Ebene dafür einsetzen, dass der risikobasierte Ansatz der DSGVO klarer verankert wird und Unternehmen bei Datenverarbeitungen mit geringem Risiko von vereinfachten Dokumentationsanforderungen profitieren können.

3. Standardisierte Verträge und Mustertexte

Ein erheblicher Aufwand im Datenschutzalltag vieler Unternehmen entsteht durch wiederkehrende juristische Detailarbeit. Die DSGVO verlangt etwa, dass Verantwortliche und ihre Auftragsverarbeiter einen Vertrag nach Artikel 28 schließen, der eine Vielzahl von Punkten regelt. In

[18] Wie es teilweise durch nationale Datenschutzbehörden bereits gehandhabt wird, siehe beispielsweise https://www.lda.bayern.de/de/thema_kleine_unternehmen.html

der Praxis bedeutet das: Für jeden Dienstleister müssen Unternehmen eigene Vereinbarungen prüfen oder verhandeln, oft unter Hinzuziehung externer Beratung. Gerade für KMU ist dieser Prozess kostenintensiv und zeitaufwendig. Dabei gibt es Möglichkeiten zur Vereinfachung: die stärkere Nutzung von Standardvertragsklauseln und geprüften Mustertexten, etwa auch durch den Einsatz von Online-Generatoren oder ähnlichen digitalen Hilfsmitteln. Die Europäische Kommission verfügt über die Kompetenz, solche Vorlagen bereitzustellen, und hat dies bereits für internationale Datentransfers getan. Auch Initiativen nationaler Aufsichtsbehörden bieten hierfür bereits erprobte Vorbilder.[19] Würden solche Standardtexte von der Europäischen Kommission, von Aufsichtsbehörden oder anerkannten Institutionen veröffentlicht und EU-weit akzeptiert, könnten Unternehmen diese direkt übernehmen und sicher sein, DSGVO-konforme Regelungen zu nutzen.

Natürlich sind Standardtexte kein Allheilmittel. Sie müssen unterschiedlichste Konstellationen abdecken, regelmäßig aktualisiert und von den Aufsichtsbehörden koordiniert werden. Auch ist Akzeptanz bei großen Marktakteuren nötig, die bislang eigene Vertragsmuster bevorzugen. Dennoch sind diese Hürden vergleichsweise gering.

Der Nutzen für KMU wäre erheblich. Standardisierte und verbindliche Verträge würden die Verhandlungslast deutlich reduzieren und für mehr Rechtssicherheit sorgen. Statt jeden Vertrag individuell zu entwerfen, könnten Unternehmen auf geprüfte Vorlagen zurückgreifen, die alle wesentlichen Anforderungen abdecken. Gerade bei Cloud- und IT-Dienstleistungen, wo kleine Betriebe häufig den Vertragsbedingungen großer Anbieter gegenüberstehen, würde dies für Augenhöhe sorgen.[20] Auch andere wiederkehrende Texte wie Einwilligungserklärungen, Datenschutzhinweise für typische Geschäftssituationen oder Antwortschreiben auf Auskunftsersuchen ließen sich standardisieren. So könnten KMU ihre Ressourcen gezielt für ihr Kerngeschäft einsetzen, anstatt immer wieder ähnliche juristische Dokumente zu erstellen. Zudem hätten Unternehmen bei Prüfungen oder Beschwerden ein starkes Argument, wenn sie auf offiziell empfohlene Muster verweisen können.

Weniger Vertragsflut bedeutet weniger Bürokratie, ohne dass Datenschutzrechte eingeschränkt werden. Standardisierte Verträge schaffen europaweit Einheitlichkeit, was insbesondere mittelständischen Exporteuren zugutekommt. Der Vorschlag schafft so einen pragmatischen Beitrag zur Entlastung der Wirtschaft, der Bürokratieabbau und Rechtsklarheit miteinander verbindet.

> Die Europäische Kommission sollte geprüfte Musterverträge und Standardtexte (z.B. für Auftragsverarbeitung) bereitstellen, die Unternehmen unmittelbar nutzen können, um Rechtssicherheit zu erlangen und Bürokratiekosten zu senken.

[19] Europäischer Datenschutzausschuss: Praktische Mittel für KMU, https://www.edpb.europa.eu/sme-data-protection-guide/practical-resources-for-smes_de, 29.07.2025.

[20] Siehe auch Lachenmann, Matthias: Die DS-GVO-Reformpläne der EU-Kommission: Nutzen für Unternehmen oder Schaden des großen Ganzen? - beck-online, 2025, in: Zeitschrift für Datenschutz (ZD), S. 365f., S. 366, https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2025-S-365-N-1, 01.07.2025.

4. Vereinfachte Datenschutzhinweise (Standardtexte und Piktogramme)

Datenschutzerklärungen und Informationspflichten gelten in der Praxis oft als schwerfällig, da sie umfangreich sind und viele wiederkehrende Informationen enthalten. Für KMU bedeutet das einen beträchtlichen Aufwand: Immer wieder müssen ähnliche Texte formuliert und angepasst werden. Eine pragmatische Lösung bestünde darin, verstärkt auf standardisierte Texte oder leicht verständliche Piktogramme zurückzugreifen. Für typische Verarbeitungsvorgänge – etwa beim Versand von Newslettern – könnten kurze Standardtexte bereitgestellt werden, ergänzt durch einheitliche Symbole, die bestimmte Datenverarbeitungen auf einen Blick erkennbar machen. Die Europäische Kommission verfügt bereits über die Möglichkeit, solche Piktogramme über einen delegierten Rechtsakt einzuführen.[21] Diese Befugnis sollte konsequent genutzt werden.

Für Unternehmen würde sich der Aufwand spürbar verringern: Statt lange Erklärungen auszuformulieren, könnten sie oft auf geprüfte Bausteine zurückgreifen. Gleichzeitig profitieren die betroffenen Personen. Kürzere und visuell unterstützte Hinweise sind leichter verständlich, das Wesentliche sticht hervor und wird nicht in seitenlangen Textblöcken verborgen. Auf diese Weise steigt die Transparenz, ohne dass inhaltlich Abstriche gemacht werden. Studien und Praxisberichte verweisen darauf, dass gerade standardisierte Icons einen echten Mehrwert schaffen können, weil sie wiederkehrende Informationen klar und prägnant darstellen.

Natürlich müssen auch hier Hürden bedacht werden. Einheitliche Piktogramme setzen voraus, dass ihre Bedeutung europaweit eindeutig verstanden wird. Auch muss gewährleistet sein, dass die Verwendung von Symbolen die rechtlich geforderte Information vollständig abdeckt. Verbraucherpanels könnten ein geeignetes Instrument sein, um zuvor offene Fragen zur Verständlichkeit und Akzeptanz solcher Formate zu beantworten. Entscheidend ist außerdem, dass Unternehmen die neuen Formate akzeptieren und in ihre Praxis übernehmen.

Das Ergebnis wäre ein deutlicher Gewinn an Verständlichkeit und Effizienz. Datenschutzhinweise würden kürzer, klarer und leichter zugänglich, ohne dass die Schutzstandards der DSGVO verwässert werden. Für KMU bedeutet das weniger Papierkram, für Verbraucher:innen mehr Transparenz. Der Datenschutz wird so zugleich unternehmensfreundlicher und verbrauchernäher ausgestaltet – ein Beispiel dafür, wie Bürokratieabbau und effektiver Grundrechtsschutz zusammengeführt werden können.

> Die Europäische Kommission sollte einheitliche Kurztexte und Piktogramme für typische Verarbeitungsvorgänge entwickeln und freigeben, damit KMU ihre Informationspflichten effizienter erfüllen können – bei gleichzeitiger Stärkung der Transparenz für Verbraucher:innen.

5. Branchenspezifische Verhaltenskodizes und Datenschutz-Zertifizierungen

Die DSGVO selbst bietet Instrumente, um ihre Anforderungen praxisnäher und für Unternehmen besser handhabbar zu gestalten: branchenspezifische Verhaltenskodizes (Art. 40) und

[21] Artikel 12 Abs. 8 DSGVO

Zertifizierungen oder Siegel (Art. 42). Ein Kodex ist ein von einer Branche oder einem Verband entwickeltes Regelwerk, das die allgemeinen Vorgaben der DSGVO auf konkrete branchentypische Abläufe herunterbricht. Wird ein solcher Kodex von einer Aufsichtsbehörde oder vom EDSA genehmigt, können sich Unternehmen anschließen und dessen Einhaltung zusagen – ein starkes Signal, das zugleich als Nachweis der Konformität gilt. Bislang gibt es jedoch nur wenige genehmigte Kodizes, und gerade KMU sind selten direkt beteiligt. Hier liegt erhebliches Potenzial: Kodizes könnten gezielt so ausgestaltet werden, dass sie die Bedürfnisse kleinerer Unternehmen berücksichtigen. Ähnliches gilt für Zertifizierungen: Ein Datenschutzsiegel bestätigt, dass ein Unternehmen zentrale Anforderungen einhält. Für KMU könnte ein eigenes, zugeschnittenes Gütesiegel entwickelt werden, das Kernstandards sichtbar macht und bei Kontrollen oder im Wettbewerb Vertrauen schafft. Behörden und Politik können diese Entwicklung durch Förderprojekte, Pilotprogramme oder vereinfachte Prüfverfahren unterstützen.

Auch hier gibt es Hürden. Die Erarbeitung eines Kodex erfordert Zeit, Ressourcen und Koordination zwischen Unternehmen und Behörden. Bisher verlief die Anerkennung schleppend, unter anderem wegen komplexer Verfahren. Finanzierungsfragen stellen sich ebenfalls: KMU dürfen nicht durch Mitgliedsbeiträge oder Überwachungskosten überfordert werden. Auch Zertifizierungen müssen klare Kriterien und unabhängige Prüfstellen haben – in vielen Mitgliedstaaten sind diese noch aufzubauen. Unternehmen könnten zudem zurückhaltend reagieren, weil sie zusätzliche Pflichten oder eine erhöhte Sichtbarkeit fürchten. Deshalb braucht es Vertrauen, dass Kodizes und Siegel tatsächlich entlasten, statt neue Bürokratie zu schaffen. Politische Unterstützung – etwa durch Fördermittel und eine pragmatische Anerkennungspraxis – kann diese Anfangshürden deutlich senken.

Der praktische Nutzen für Unternehmen ist vielfältig. Ein genehmigter Branchenkodex übersetzt abstrakte Regelungen in konkrete Handlungsanweisungen, etwa welche technischen und organisatorischen Maßnahmen in einem Sektor als ausreichend gelten oder wie Einwilligungen praxisgerecht eingeholt werden. So müssen KMU nicht jede Auslegungsfrage mit Jurist:innen oder Aufsichtsbehörden klären, sondern können sich am Kodex orientieren. Die Kosten verteilen sich zudem: Ein Verband erarbeitet Musterlösungen, anstatt dass jedes Unternehmen einzeln investiert. Für die Aufsichtsbehörden bedeutet dies, dass ganze Branchen erkennbar Standards einhalten – was Vertrauen schafft und die Prüfbelastung reduziert. Zertifizierungen erfüllen eine ähnliche Funktion: Sie verschaffen Unternehmen einen Wettbewerbsvorteil, indem sie Verbraucher:innen und Geschäftspartnern sichtbar machen, dass Datenschutz ernst genommen wird. Dadurch kann Datenschutz noch stärker als Qualitätsmerkmal herausgestellt werden. Branchen erhalten die Möglichkeit, praxisnahe Lösungen selbst zu entwickeln, anstatt staatlich detailliert reguliert zu werden.

Der hohe Standard der DSGVO bleibt durch diese Instrumente gewahrt, wird aber durch konkrete Vorgaben leichter einhaltbar. So entsteht Ordnung, Verlässlichkeit und Fairness: Unternehmen werden entlastet, Verbraucher:innen erhalten mehr Transparenz und Vertrauen. Verhaltenskodizes und Zertifizierungen sind damit eine Win-Win-Maßnahme, die Bürokratie senkt und Qualität sichert.

> Die Bundesregierung sollte die Entwicklung branchenspezifischer Verhaltenskodizes und KMU-geeigneter Zertifikate aktiv fördern und auf europäischer Ebene für eine pragmatische Anerkennungspraxis eintreten.

6. Mehr behördlicher Support und Beratung für KMU

Eine weitere Maßnahme im vorhandenen Rechtsrahmen ist, die Rolle der Datenschutzbehörden stärker auch als Unterstützer der Wirtschaft auszubauen. Anstatt Unternehmen ausschließlich zu kontrollieren und zu sanktionieren, sollten Aufsichtsbehörden – ohne ihre Unabhängigkeit aufzugeben – proaktiv Hilfestellung leisten. Konkret umfasst dies etwa praxisorientierte Workshops oder leicht zugängliche Online-Ressourcen wie FAQ oder Erklärvideos – wie sie etwa von der Berliner Datenschutzbeauftragten angeboten werden.[22].Diese Ansätze könnten flächendeckend ausgebaut werden.

Ein niedrigschwelliges Unterstützungsangebot sorgt dafür, dass Unternehmen Probleme schneller und unbürokratischer lösen können. Das verhindert auch Over-Compliance: Manche Firmen treffen aus Unsicherheit übervorsichtige Maßnahmen, die gar nicht nötig wären und Ressourcen binden. Wenn Aufsichtsbehörden proaktiv auf Unternehmen zugehen – etwa über Infoveranstaltungen oder Newsletter mit Praxistipps – verbessert das die gesamte Compliance-Kultur: Unternehmen fühlen sich nicht gegängelt, sondern unterstützt, und neigen eher dazu, kooperativ zu agieren. Letztlich profitieren auch die Betroffenen: Gut beratene Unternehmen können Prozesse wie Auskunftsersuchen effizienter umsetzen. Aus wirtschaftlicher Sicht steigert behördlicher Support die Wettbewerbsfähigkeit, da gerade kleine Betriebe ohne eigene Datenschutzexpert:innen auf diese Weise Zugang zu praxisnahem Wissen erhalten. Die Aufsicht würde so weniger als Strafinstanz, sondern stärker als Partner für rechtssichere Digitalisierung wahrgenommen. Das könnte auch die Anzahl formaler Verfahren senken, weil viele Fragen im Vorfeld geklärt werden. Erfahrungen aus Mitgliedstaaten, in denen Aufsichtsbehörden KMU gezielt helfen, zeigen, dass DSGVO-Compliance dort als weniger komplex wahrgenommen wird. Ein flächendeckend starker Support könnte die Kritik an Bürokratie spürbar dämpfen.

Potenzielle Hürden bestehen vor allem in den Ressourcen. Datenschutzbehörden sind vielerorts knapp besetzt und müssen ihre vielfältigen Aufgaben bewältigen. Zusätzliche Hilfsangebote setzen voraus, dass die Politik den Aufsichtsbehörden ausreichend Budget und Personal zur Verfügung stellt. Die Europäische Kommission hat wiederholt betont, dass Mitgliedstaaten ihre Aufsichtsbehörden personell stärken müssen. Zudem gilt es, die Unabhängigkeit zu wahren: Beratung darf nicht zur einseitigen Interessenvertretung werden. Manche Unternehmen könnten zögern, Probleme offen anzusprechen, wenn sie befürchten, dadurch eine Prüfung auszulösen. Klare Grenzen und transparente Kommunikation sind daher erforderlich, damit Beratung nicht mit Sanktionierung verwechselt wird. Auch ein Kulturwandel ist nötig – sowohl bei Behörden als auch bei Unternehmen. Mit gezielten Vorgaben und Schulungen ist dieser jedoch steuerbar. Werden diese Vorgaben umgesetzt, sind die Hürden eher organisatorisch als grundsätzlich.

Gut informierte Unternehmen setzen die Vorgaben verlässlicher um, wodurch auch die Rechte der Verbraucher:innen gestärkt werden. So entsteht eine klassische Win-Win-Situation: Unternehmen profitieren von Entlastung und Klarheit, Verbraucher:innen von besser umgesetztem Datenschutz. Unterstützung durch Behörden fördert Eigenverantwortung statt Misstrauen und beweist, dass Datenschutz praxisnah und wirtschaftsfreundlich ausgestaltet werden kann.

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

> Bund und Länder sollten die Datenschutzaufsichtsbehörden personell und finanziell so ausstatten, dass diese ihre Unterstützungsangebote für KMU – etwa durch Schulungen – deutlich ausbauen können.

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