BvD e.V.
DATENSCHUTZ GESTALTEN

Positionspapier zur Reform der EU-Datenschutz-Grundverordnung (DSGVO)

24. Juni 2025

Die Datenschutz-Grundverordnung (DSGVO) gilt seit 2018 und setzt seitdem hohe Standards für den Schutz personenbezogener Daten in Europa. Sie ist Ausdruck eines europäischen Grundrechtsverständnisses und dient als globaler Maßstab für den Datenschutz. Gleichzeitig zeigt die Anwendungs- und Aufsichtspraxis in Europa, dass Anpassungen erforderlich sind, um unnötige Bürokratie abzubauen, Rechtsunsicherheit zu verringern und Datenschutz und digitale Innovation miteinander zu verbinden.

In Zeiten zunehmender Digitalisierung, immer komplexer werdender Technologien, stark wachsender Risiken für die Cybersicherheit und zunehmender Regulierung kommt den Datenschutzbeauftragten insbesondere in kleinen und mittleren Unternehmen eine wichtige Beratungsfunktion zu. In Unternehmen fehlt es vielfach an der erforderlichen Kompetenz, um diese Themen angemessen zu behandeln. Qualifizierte Datenschutzbeauftragte können in diesem und anderen Bereichen zum Wegbereiter für eine sichere und rechtskonforme digitale Transformation werden, sofern sie angemessen eingebunden werden und ihr Mehrwert erkannt wird.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. setzt sich daher für einen Paradigmenwechsel ein. Hersteller dürfen nur digitale Lösungen anbieten, die datenschutzkonform nutzbar sind. Durch verpflichtende Konformitätsnachweise können Unternehmen und öffentliche Stellen darauf vertrauen, dass die von ihnen eingesetzten Produkte die Anforderungen der DSGVO erfüllen. Dies schafft Rechtssicherheit und entlastet insbesondere kleine und mittlere Unternehmen.

Unsere Kernforderungen

Risikobasierter Datenschutz mit einheitlicher Anwendung und praxisnaher Umsetzung durch **"Privacy by Design"** als Herstellerpflicht:

- **Beteiligung des Herstellers an der Compliance-Verantwortung des Verantwortlichen und Auftragsverarbeiters.**
- **Hersteller dürfen Produkte und Dienstleistungen nur anbieten, wenn sie datenschutzkonform einsetzbar sind („Privacy by Design").**
- **Diese Konformität muss durch den Hersteller nachgewiesen werden.**
- **Hersteller sollen ihre Produkte und Dienstleitungen datenschutzkonform vorkonfigurieren, soweit möglich („Privacy by Default").**
- **Einbindung des Datenschutzbeauftragten erweitern, um insbesondere kleine und mittlere Unternehmen bei Pflichten und Risiken zu entlasten.**

Wir fordern eine zielgerichtete Weiterentwicklung der DSGVO, die durch klare und verständliche Vorgaben für mehr Rechtssicherheit sorgt. Die aktuelle Fassung leidet unter komplexen Formulierungen und weitreichenden Interpretationsspielräumen. Diese führen zu Unsicherheit und einem übermäßigen Beratungsbedarf. Notwendig sind:

- Eine sprachliche Überarbeitung mit eindeutigen, praxistauglichen Formulierungen.
- Konkrete Handlungsanweisungen statt unklarer Rechtsvorgaben.
- Standardisierte Prozesse und Vorlagen für häufige Anwendungsfälle.
- Verbindliche Auslegungsrichtlinien der Aufsichtsbehörden.
- Eine risikoorientierte Abstufung der Anforderungen, die sich an der tatsächlichen Gefährdung der Betroffenenrechte orientiert.

Die DSGVO muss auch für Nicht-Juristen verständlich und umsetzbar sein, statt interpretationsbedürftige Rechtsgrundsätze aufzustellen. Nur so können Verantwortliche Datenschutz effektiv und rechtssicher umsetzen und Betroffene ihre Rechte wahrnehmen.

Datenschutz ist keine Innovationsbremse, sondern Teil jeder nachhaltigen Digitalstrategie.

1. Bürokratie abbauen, Datenschutzwirkung stärken

Bei der Ausgestaltung der datenschutzrechtlichen Dokumentationspflichten und Nachweiserfordernisse besteht die Möglichkeit, diese insbesondere für Klein- und Kleinstunternehmen praktikabel und ressourcenschonend zu gestalten. Dabei ist jedoch stets zu gewährleisten, dass das durch die Datenschutz-Grundverordnung vorgegebene Schutzniveau für die Rechte und Freiheiten der betroffenen Personen in vollem Umfang erhalten bleibt und nicht abgesenkt wird. Deshalb fordern wir:

1. Risikobasierte Ausgestaltung der DSGVO als Leitprinzip konsequent stärken: Die DSGVO enthält bereits risikobasierte Elemente, wie etwa in Art. 24, 25, 30, 32 und 35 DSGVO angelegt. In der Praxis fehlt jedoch häufig eine konsequente, rechtssichere Umsetzung dieses Grundsatzes, insbesondere durch eine mangelnde Differenzierung bei regulatorischen Anforderungen an Verarbeitungen mit unterschiedlichem Risikopotenzial.
   Wir fordern daher eine Klarstellung und Weiterentwicklung des risikobasierten Ansatzes in der DSGVO und ihrer Anwendungspraxis. Die Aufsichtsbehörden sollten in ihren Leitlinien, Prüfstandards und Auslegungen stärker zwischen risikoarmen und risikobehafteten Verarbeitungen differenzieren. Die DSGVO darf nicht als "One-Size-Fits-All"-Regelwerk verstanden werden. Vielmehr muss eine risikoadäquate Umsetzung datenschutzrechtlicher Pflichten ermöglicht und gefördert werden, beispielsweise durch vereinfachte Verfahren für risikoarme Verarbeitungen, abgestufte Rechenschaftspflichten sowie pragmatische Prüfmaßstäbe.
   Dies dient nicht nur der Entlastung insbesondere kleiner und mittlerer Unternehmen, sondern auch der zielgerichteten Stärkung des Grundrechtsschutzes – dort, wo er am dringendsten gebraucht wird.
2. Verpflichtung der Hersteller von digitalen Produkten und Dienstleistungen zu Privacy bei Design und Default sowie die Bereitstellung der für das Risikomanagement der Produkte entsprechend der vom Hersteller vorgesehenen Zweckbestimmung des Produkts erforderlichen Konformitätsnachweise (inkl. Muster-VVT, Muster-DSFA, Musterschreiben zur Beantwortung von Betroffenenrechten)
3. Durch die bereits gesetzlich verankerten Zertifizierungen können Hersteller und Dienstleister diese Konformitätsnachweise erbringen. Die organisatorischen Strukturen, die derzeit umgesetzt sind, um diese Zertifizierungen zu ermöglichen, haben sich als nicht effektiv erwiesen. Hier ist ein Neustart erforderlich.
4. Orientierung des EDSA am rechtlich erforderlichen Mindestmaß bei der Interpretation des Datenschutzrechts im Rahmen der Veröffentlichung von Guidelines und anderer Hilfen.
5. Verständlichere Ausgestaltung der Betroffenenrechte im Sinne der Bürgerinnen und Bürger bei gleichzeitiger Einschränkung von missbräuchlichen oder exzessiven Auskunftsrechten, insbesondere in Art. 15 DSGVO.

Dazu ist eine klare Regelung zur Benennung von Datenschutzbeauftragten zu treffen, wie es einige Mitgliedsstaaten bereits getan haben:

- Risikoorientierung bei der Benennungspflicht
- Benennung, wenn Art. 9 DSGVO-Daten (z.B. Gesundheitsdaten) geschäftsmäßig verarbeitet werden und die Verarbeitung über die bloße Erfüllung von Rechtspflichten (z.B. durch den Arbeitgeber) hinausgeht,
- Benennung, wenn Verantwortliche Technologien einsetzen, die ein hohes Risiko für Betroffene begründen können,
- Benennung, wenn personenbezogene Daten in Drittstaaten übermittelt werden.

Eine Bindung an die Größe einer Organisation ist ein analoger Denkansatz, der den Anforderungen der neuen Verarbeitungsrealitäten nicht mehr gerecht wird. Mittels neuer Technologien spielt die Größe einer Organisation kaum noch eine Rolle.

2. Einheitliche Auslegung und Beratung in der EU sicherstellen

Unternehmen und öffentliche Stellen stehen bei der Anwendung der DSGVO häufig vor erheblichen Unsicherheiten. Diese resultieren vor allem aus den unterschiedlichen Interpretationen der Verordnung durch die Aufsichtsbehörden in den EU-Mitgliedstaaten. Gerade für europaweit tätige Organisationen führt dies zu erheblichen Rechtsunsicherheiten und erschwert die rechtssichere Umsetzung der Vorschriften. Zwar bietet die DSGVO einen grundsätzlichen Rahmen, der durch Leitlinien und Entscheidungen der Behörden weiter konkretisiert werden kann – doch genau hier fehlt es bislang an einheitlichen, verbindlichen Vorgaben. Deshalb besteht ein Bedarf an harmonisierten Auslegungsstandards sowie an praxisnahen Leitlinien und Beratung, um die Rechtsklarheit und Planungssicherheit für Verantwortliche in der gesamten EU zu verbessern.

3. Datenschutz und Innovation verbinden

Neue Technologien sind für die Wettbewerbsfähigkeit Europas von zentraler Bedeutung. Die DSGVO schafft Rahmenbedingungen, in denen datenschutzkonforme Innovationen technologieneutral möglich sind.
Ein Schlüssel hierzu ist die rechtssichere Nutzung anonymisierter Daten. Der BvD fordert daher:

- **Eine eigenständige Rechtsgrundlage für die Anonymisierung personenbezogener Daten.**
- **Standardisierte, rechtlich anerkannte Anonymisierungsverfahren.**
- **Klare Privilegierung der Datennutzung nach erfolgreicher Anonymisierung.**

- **Rechtssicherheit für Unternehmen und öffentliche Stellen bei der Weiterverarbeitung anonymisierter Datensätze.**
- **Vereinfachte Prozesse für Forschung und Entwicklung mit anonymisierten Daten.**
- **Schaffung von Anreizen für datenschutzkonforme Technologien durch Privilegierung der Anonymisierung.**

Diese Maßnahmen würden insbesondere die Entwicklung datengetriebener Innovationen wie KI-Systeme erleichtern, ohne den Schutz personenbezogener Daten zu gefährden. Anonymisierte Daten fallen nicht in den Anwendungsbereich der DSGVO - diese Klarstellung muss jedoch durch eindeutige Regelungen zur Anonymisierung ergänzt werden.

4. Sanktionen transparent gestalten

Die aktuelle Vollzugspraxis der Aufsichtsbehörden variiert zwischen den EU-Mitgliedstaaten. Dies führt zu Rechtsunsicherheit und Wettbewerbsverzerrungen im europäischen Binnenmarkt. Für einen fairen und effektiven Vollzug der DSGVO fordern wir:

- Harmonisierung des Vollzugs:
- Verbindliche EU-weite Standards für Bußgeldverfahren
- Einheitliche Bewertungsmaßstäbe in allen Mitgliedstaaten
- Koordinierte Durchsetzungsstrategie der Aufsichtsbehörden
- Vermeidung von regulatorischer Arbitrage und Standortvorteilen
- Stärkung der Durchsetzung gegenüber internationalen Konzernen durch das Führen von Bußgeldverfahren durch bspw. den EDSA

Ein einheitliches und transparentes Sanktionsregime schafft Rechtssicherheit für Unternehmen und stärkt das Vertrauen in den europäischen Datenschutz. Die Durchsetzung der DSGVO darf jedoch nicht zu einem Standortwettbewerb zwischen den Mitgliedstaaten führen.

5. Datenschutzbeauftragte stärken, Qualifikation sichern

Die erfolgreiche Umsetzung der DSGVO erfordert spezialisiertes Fachwissen, das insbesondere in KMU häufig nicht verfügbar ist. Anstatt kostenintensive Parallelstrukturen zu schaffen, sollte edie Rolle des Datenschutzbeauftragten gesetzlich gestärkt werden – als unabhängige und qualifizierte Fachinstanz mit klarer Verankerung in den Compliance-Strukturen des Unternehmens.

1. Gesetzliche Verankerung erweiterter DSB-Kompetenzen:
   - Verbindliche Übertragung der operativen Datenschutzsteuerung an Datenschutzbeauftragte
   - Klare Definition der DSB-Rolle des Datenschutzbeauftragtenals primärer Datenschutz-Manager
   - Rechtliche Aufwertung der Position des Datenschutzbeauftragten bei gleichzeitiger Beibehaltung der Letztverantwortung der obersten Unternehmensleitung

2. Konkrete Kompetenzzuweisung in Kernprozessen:
   - Federführung bei Datenschutz-Folgenabschätzungen (DSFA)
   - Zentrale Steuerung des Datenschutz-Risikomanagements
   - Führung und Pflege der Verarbeitungsverzeichnisse
   - Management von Datenpannen mit verpflichtender DSB-Einbindung
   - Koordination bei Betroffenenanfragen
   - Qualitätssicherung bei technisch-organisatorischen Maßnahmen

3. Effiziente Ressourcennutzung durch:
   - Vermeidung von Doppelstrukturen in Unternehmen
   - Nutzung der Expertise des Datenschutzbeauftragten als „Single Point of Contact“
   - Standardisierte Prozesse und Workflows

4. Flankierende Maßnahmen:
   - Entwicklung einheitlicher Qualifikationsstandards für DSBs
   - Zertifizierte Aus- und Weiterbildungsprogramme
   - Ausbau behördlicher Unterstützungsangebote

Impressum

Herausgeber

Berufsverband der Datenschutz-
beauftragten Deutschlands (BvD) e. V.

Budapester Straße 31
10787 Berlin

T 030 26 36 77 60
F 030 26 36 77 63

bvd-gs@bvdnet.de
www.bvdnet.de

Eingetragen im Lobbyregister des
Deutschen Bundestages und der
Bundesregierung:
Registernummer R000841

Genderhinweis

Auf die gleichzeitige Verwendung der Sprachformen weiblich, divers und männlich (w/d/m) wird in diesem Text verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Über den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Mit über 30 Jahren Erfahrung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die älteste Interessenvertretung für betriebliche und behördliche Datenschutzbeauftragte und -berater. BvD-Mitglieder sind in allen Branchen vertreten, insbesondere IT und IKT, Industrie/Produktion, Handel/Vertrieb, Beratung sowie Gesundheits- und Sozialwesen. Als erster Ansprechpartner der Betroffenen sind die BvD-Mitglieder Anlaufstelle für etwa fünf Millionen Arbeitnehmer sowie einen Großteil der Bürger und Konsumenten. Zudem sind sie als konstruktiv lösungsorientierte Datenschutzexperten ein wichtiger Partner für die verantwortliche Unternehmensleitung. Die Verbandsvorstände, alle Leiter von Arbeitskreisen, Ausschüssen und Regionalgruppen des BvD bringen ihre praktische Erfahrung unentgeltlich in die Verbandsarbeit ein. Mit der Gründung des Europäischen Dachverbandes EFDPO (www.efdpo.eu) hat der BvD die Weichen für die verstärkte Vernetzung und Kommunikation auf EU-Ebene gestellt.