BvD e.V.
DATENSCHUTZ GESTALTEN

Stellungnahme zum öffentlichen Entwurf (v. 0.9) Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim Einsatz von KI (The Bridge Blueprint)

27. September 2025

Die Tätigkeit von betrieblichen und behördlichen Datenschutzbeauftragten basiert auf deren tiefgehenden und fundierten Kenntnissen der datenschutzrechtlichen Vorschriften. Diese Kenntnisse sind elementar, um die Verantwortlichen und Auftragsverarbeiter bei der Einführung neuer Verarbeitungen von personenbezogenen Daten oder der Änderung bereits vorhandener Verarbeitungstätigkeiten hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften zu beraten und deren Einhaltung zu überwachen. Dabei sollte die Einhaltung des Datenschutzes jedoch nicht als Verhinderung von Innovationen betrachtet werden, sondern als Garant für einen verantwortungsvollen Fortschritt.

In der Diskussion um die Etablierung eines funktionierenden und vertrauenswürdigen Rahmenwerks für den Einsatz von Künstlicher Intelligenz (KI) ist zu beachten, dass regelmäßig personenbezogene Daten sowohl auf Modellebene als auch auf Systemebene verarbeitet werden. Daher sind die Datenschutzbeauftragten aufgrund ihrer umfassenden Erfahrung wichtige Akteure, da sie in ihrer beruflichen Praxis bereits von Anfang an mit KI-Projekten konfrontiert wurden und diese aus datenschutzrechtlicher Perspektive begleiten und analysieren.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. begrüßt die Thesen zur einheitlichen Anwendung von Datenschutz und KI-Regulierung beim Einsatz von KI.

I. Die Notwendigkeit des Brückenschlags

Der gesetzliche Auftrag der Datenschutzbeauftragten, die verarbeitenden Stellen im Hinblick auf die Einhaltung der datenschutzrechtlichen Vorschriften zu beraten, basiert auf einem lösungsorientierten Vorgehen bei der

Einführung und Änderung der Verarbeitung personenbezogener Daten im betrieblichen und behördlichen Alltag. Dies beinhaltet auch eine fachkundige Beratung bei der Integration von KI in die Verarbeitungstätigkeiten. Um dieser Aufgabe mit der gebotenen Verantwortung gerecht zu werden, ist es für aus Sicht des BvD unerlässlich, sich mit verändernden Rahmenbedingungen für Verarbeitungstätigkeiten auseinanderzusetzen und deren Auswirkungen auf die DSGVO aktuell zu bewerten.

II. Datenschutzgrundsätze als Qualitätsauftrag

Die wachsende Bedeutung von KI in Unternehmen, Organisationen und Behörden sowie die neuen europäischen Rechtsakte machen deutlich, dass sich insbesondere die Bewertung der Erforderlichkeit mit den sich verändernden Rahmenbedingungen weiterentwickelt werden muss.

Aus den Anforderungen von Art. 32 DSGVO und dem daraus resultierenden technischen Fortschritt ergibt sich zwangsläufig die Notwendigkeit, auch KI-unterstützte Maßnahmen zur Abwehr von Risiken zu integrieren. Diese Maßnahmen sind durch weitere Maßnahmen zum Schutz der betroffenen Personen zu ergänzen, die durch den KI-Einsatz neu entstehen.

Wenn der Datenschutz von Anfang an in die Projektplanung integriert wird, verliert er seine unberechtigt zugeschriebene Rolle als Innovationshemmnis. Vielmehr schafft er Vertrauen in den Einsatz von KI, indem er notwendige Schutzmaßnahmen verankert und die Sicherheit der Verarbeitung mittels KI stärkt.

Voraussetzung dafür ist, dass der Gesetzgeber klare Verbote und Befugnisse für die Verarbeitung personenbezogener Daten in öffentlichen und nicht-öffentlichen Stellen festlegt und Aufsichtsbehörden sowie die Rechtsprechung das Zusammenspiel der DSGVO, der KI-Verordnung und weiterer europäischer Rechtsakte konkret auslegen.

In einer sich verändernden Welt entwickeln sich auch die vernünftigen Erwartungen der betroffenen Personen weiter. Der Einsatz von KI in der Verarbeitung personenbezogener Daten dürfte daher zunehmend zur Regel werden. In dieser Hinsicht sollte auch der datenschutzrechtliche Grundsatz der Transparenz betrachtet werden. Der Einsatz von KI ist bekanntlich damit verbunden, dass eine Restunsicherheit bezüglich des Modells auch für den Betreiber, also den datenschutzrechtlich Verantwortlichen, verbleibt. Sowohl Verantwortliche als auch betroffene Personen sind sich dieser Eigenschaft bewusst. Dies ist bei der Erfüllung der Informationspflichten und der Bewertung der Verarbeitung zu berücksichtigen.

III. Eine verlässliche Rechtsgrundlage für den KI-Einsatz

Datenschutzbeauftragte sind bei ihrer Beratung darauf angewiesen, dass bezüglich der Rechtsgrundlagen für den Einsatz von KI Klarheit besteht. Vor diesem Hintergrund begrüßt der BvD die Ausführungen zu den Rechts-

grundlagen in den Thesen zur einheitlichen Anwendung von Datenschutz und KI-Regulierung beim Einsatz von KI ausdrücklich.

Hinsichtlich der These zur Nutzung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO öffentlichen Interesse auch von nicht-öffentlichen Stellen sollte allerdings nicht unerwähnt bleiben, dass sich die Erlaubnisnorm in Art. 10 Abs. 5 KI-VO lediglich auf die unbedingte Erforderlichkeit zur Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen bezieht. Darüber hinaus stellt sie strenge zusätzliche Bedingungen an diese Verarbeitung der Daten gemäß Art. 9 DSGVO. Dazu gehören unter anderem modernste Sicherheits- und Datenschutzmaßnahmen, ein Verbot der Übermittlung an oder des Zugangs für Dritte sowie Lösch- und Dokumentationspflichten.

Gerade im Zusammenhang mit der Nutzung des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO sehen sich Verantwortliche mit erheblicher Rechtsunsicherheit konfrontiert. Der Bridge Blueprint bezieht sich zu Recht auf die „vernünftigen Erwartungen der betroffenen Personen", die sich durch die KI-Verordnung und weitere unionsrechtliche Vorgaben neu konturieren. Aus Sicht der Datenschutzbeauftragten ist es besonders wichtig, dass Verantwortliche frühzeitig eine strukturierte Abwägung vornehmen und dokumentieren, wie diese Erwartungen im konkreten KI-Einsatz berücksichtigt werden.

Die Datenschutzbeauftragten unterstützen die Verantwortlichen, indem sie den Prozess kritisch begleiten, die Angemessenheit der Abwägung prüfen und darauf hinwirken, dass Risiken für die betroffenen Personen transparent erfasst und minimiert werden. Damit tragen sie zur Rechtssicherheit bei und schaffen zugleich eine belastbare Grundlage für innovative, aber verantwortungsvolle KI-Anwendungen.

IV. Automatisierte Entscheidungen und Betroffenenrechte

Automatisierte Entscheidungen und die wirksame Ausübung von Betroffenenrechten stellen zentrale Herausforderungen beim Einsatz von KI-Systemen dar. Maßgeblich ist dabei die Sicherstellung von Verfahrensgerechtigkeit. Die DSGVO enthält mit Artikel 22 bereits einen spezifischen Rahmen, der durch die Vorgaben der KI-Verordnung ergänzt und konkretisiert wird.

Für die Praxis bleibt ein wesentliches Risiko bestehen, dass Einzelpersonen erheblichen, potenziell schädlichen Ergebnissen ohne hinreichende Transparenz oder wirksame Rechtsbehelfe ausgesetzt sind. Entscheidend ist daher die Schaffung nachvollziehbarer Entscheidungsprozesse, die eine Überprüfung und Anfechtung ermöglichen. Die Verknüpfung von Transparenz, menschlicher Aufsicht und Protokollierung bildet hierfür eine zentrale Grundlage.

Aus Sicht der Datenschutzbeauftragten ist es von besonderer Bedeutung, die Regulierung und Umsetzung von Schutzmaßnahmen auf der Systemebene zu verankern. Eingriffe auf Modellebene sind für Verantwortliche in der Praxis kaum steuerbar, da sie häufig bei den Anbietern, Herstellern oder Entwicklern liegen und nicht im Einflussbereich der betreibenden Stelle. Auf der Systemebene hingegen können Verantwortliche durch nachvollziehbare Prozesse, Protokollierungen und organisatorische Vorkehrungen konkret sicherstellen, dass die Rechte der Betroffenen wirksam gewahrt bleiben. Datenschutzbeauftragte leisten hier einen wesentlichen Beitrag, indem sie die Dokumentation begleiten, Kontrollmechanismen einfordern und die Verknüpfung zwischen den technischen Vorgaben der KI-Verordnung und den Transparenz- und Rechenschaftspflichten der DSGVO herstellen.

Von besonderer Bedeutung ist, dass die Anforderungen nicht auf der Modellebene, sondern auf der Ebene der eingesetzten Systeme wirksam werden, da Eingriffe auf Modellebene in vielen Fällen technisch weder verlässlich noch praktikabel sind. Zudem betreffen sie häufig Akteure in der Wertschöpfungskette, die nicht in der unmittelbaren Verantwortung des Betreibers stehen. Ein Fokus auf die Systemebene ermöglicht es dem Verantwortlichen hingegen, die Einhaltung der Betroffenenrechte wirksam sicherzustellen.

Dies führt zu einer Stärkung der Rechenschaftspflicht: Die Anforderungen der KI-Verordnung übersetzen den datenschutzrechtlichen Grundsatz der Verantwortlichkeit in überprüfbare Systemanforderungen im Sinne der Produktsicherheit. Für Verantwortliche im praktischen Einsatz bedeutet dies, dass sie geeignete systemseitige Maßnahmen vorhalten müssen, die nachweislich unzulässige Ergebnisse verhindern und die Rechte der betroffenen Personen effektiv absichern.

Auch in diesem Zusammenhang sind Datenschutzbeauftragte frühzeitig einzubinden. Sie sollten den Prozess ebenso wie die Dokumentation begleiten. Sie haben darauf zu achten, dass die Systeme im Unternehmen nicht nur auf ihre technische Funktionsfähigkeit geprüft werden, sondern dass die Verfahren um Transparenz, Nachvollziehbarkeit und geeignete Kontrollmechanismen ergänzt werden, um eine Verarbeitungsgerechtigkeit zu gewährleisten. Der Verantwortliche, also der Betreiber, ist auf seine datenschutzrechtliche Pflicht hinzuweisen, systemseitige Maßnahmen nachweisbar zu dokumentieren und interne Abläufe so zu gestalten, dass betroffene Personen ihre Rechte wirksam wahrnehmen können.

V. DSFA: Ein strategisches Instrument zur Risikobeherrschung

Die Datenschutz-Folgenabschätzung (DSFA) ist ein strategisches Instrument zur Risikobeherrschung und ein wesentliches Element im Umgang mit personenbezogenen Daten und KI-Systemen. Ihre Wirkung entfaltet sie jedoch nur, wenn sie frühzeitig in den Projektverlauf integriert und kontinuierlich begleitet wird. Eine Einbindung erst am Ende des Prozesses kann auch hier diesem Anspruch keinesfalls gerecht werden.

Erforderlich ist zudem eine enge Verzahnung mit den Vorgaben der KI-Verordnung. Während die DSFA den Raum für die Bewertung kontextabhängiger Risiken eröffnet, sollte sie mit den dort vorgesehenen Risikobewertungen abgestimmt werden, um Redundanzen zu vermeiden und Synergien nutzbar zu machen.

Die Identifikation von Risiken wie Fehlinformationen, Manipulation oder die unbeabsichtigte Offenlegung von Trainingsdaten ist korrekt. Im Mittelpunkt muss dabei jedoch stehen, dass die DSFA dokumentiert, wie diesen Risiken praktisch begegnet wird, welche Schutzmaßnahmen für betroffene Personen vorgesehen sind und ob diese ausreichen.

In der Praxis besteht ein Bedarf an einheitlichen Leitlinien. Insbesondere kleine und mittlere Unternehmen sehen sich mit Herausforderungen bei der Durchführung einer DSFA im Zusammenhang mit KI-Systemen konfrontiert. Einheitliche Handreichungen und branchenspezifische Beispiele der Aufsichtsbehörden oder von den Aufsichtsbehörden genehmigte Verhaltensregeln von Wirtschaftsverbänden könnten die Umsetzung erleichtern.

Schließlich ist eine klare Abgrenzung zur Grundrechte-Folgenabschätzung (FRIA) gemäß der KI-Verordnung erforderlich. Verantwortliche benötigen Orientierung darüber, wie beide Instrumente ineinandergreifen und wie sich Überschneidungen vermeiden lassen.

Für die Praxis ist es von entscheidender Bedeutung, dass die Abgrenzung zwischen Datenschutz-Folgenabschätzung (DSFA) und Grundrechte-Folgenabschätzung (FRIA) nicht nur formal beschrieben, sondern auch in der Praxis umsetzbar ist. Während sich die DSFA auf die Risiken der Verarbeitung personenbezogener Daten konzentriert, berücksichtigt die FRIA darüberhinausgehende gesellschaftliche und grundrechtliche Implikationen. Verantwortliche benötigen hier eine klare Orientierung darüber, wie beide Verfahren ineinandergreifen, ohne dass Doppelprüfungen entstehen oder relevante Risiken übersehen werden.

Datenschutzbeauftragte übernehmen dabei eine koordinierende Rolle: Sie können die Schnittstellen beider Verfahren identifizieren, Synergien nutzbar machen und sicherstellen, dass die Ergebnisse in einem konsistenten Risikomanagement zusammengeführt werden. So wird verhindert, dass Verantwortliche durch parallele Prozesse unnötig belastet werden, und zugleich wird gewährleistet, dass Betroffene wirksam geschützt bleiben.

VI. Zusammenfassung

Der BvD begrüßt die Themen des „The Bridge Blueprint“ ausdrücklich als wichtigen Beitrag zur Schaffung eines kohärenten Rahmens für den Einsatz von KI im Einklang mit der Datenschutz-Grundverordnung.

Aus Sicht der Datenschutzbeauftragten ist es entscheidend, dass Datenschutz und Innovation nicht als Gegensätze verstanden werden. Vielmehr sollten die Grundprinzipien des Datenschutzes als Qualitätsmaßstab für den

vertrauenswürdigen Einsatz von Künstlicher Intelligenz dienen. Datenschutzbeauftragte bringen hier ihre Erfahrung und ihre unabhängige Expertise ein. Sie unterstützen Verantwortliche dabei, Rechtsunsicherheiten zu verringern, die notwendigen Abwägungen zu dokumentieren, die Rechte der Betroffenen wirksam auszugestalten und die Vorgaben der KI-Verordnung mit den Anforderungen der DSGVO in Einklang zu bringen. Damit leisten sie einen wichtigen Beitrag dazu, technologische Entwicklungen verantwortungsvoll, transparent und rechtssicher zu gestalten.

VII. Ausblick

Der BvD e. V. sieht in den Thesen des „The Bridge Blueprint" eine wertvolle Grundlage, die nun in die Praxis überführt werden muss. In den kommenden Jahren wird es entscheidend sein, dass Aufsichtsbehörden, Rechtsprechung und Gesetzgeber klare Leitlinien entwickeln, um Verantwortlichen und Betroffenen Orientierung zu geben. Insbesondere kleine und mittlere Unter-nehmen benötigen praxisgerechte Hilfestellungen, um die Anforderungen der DSGVO und der KI-Verordnung effizient und rechtssicher umsetzen zu können. Darüber hinaus sollten regulatorische Reallabore genutzt werden, um Erfahrungen zu sammeln, Rückmeldungen aus der Praxis einzubeziehen und Innovationen in einem kontrollierten Rahmen zu erproben.

Datenschutzbeauftragte können mit ihrer Beratungskompetenz und ihren Erfahrungen aus der täglichen Praxis einen wesentlichen Beitrag dazu leisten, technologische Innovation mit datenschutzrechtlicher Verlässlichkeit zu verbinden.

Die Autorinnen: Andrea Backer-Heuveldop, Regina Mühlich

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

Stand

Oktober 2025

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.