BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 55/2025
November 2025

zum

Bridge Blueprint
Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz[1]

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Malte Dedden
RA Michael Dreßler
RA Peter Hense,
RA Prof. Dr. Armin Herb, (Vorsitzender)
RAin Heike Kraus, MLE, LL.M
RA Jörg Martin Mathis
RAin Simone Rosenthal
RA Dr. Hendrik Schöttle
RA Sebastian Schulz
RA Dr. Volker Schumacher

RA André Haug, Vizepräsident, Bundesrechtsanwaltskammer
RA Sebastian Aurich, LL.M., Bundesrechtsanwaltskammer
Ass. jur. Frederic Boog, LL.M., Bundesrechtsanwaltskammer, Brüssel

[1] Vorgelegt von Thomas Fuchs (HmbBfDI), Dr. Markus Wünschelbaum, Dr. h.c. Marit Hansen (ULD) und Benjamin Walczak in der Fassung des öffentlichen Beteiligungs-Entwurfs „v. 0.9“

Verteiler: Europäische Kommission
Bundeskanzleramt
Bundesministerium für Justiz und Verbraucherschutz
Bundesministerium des Innern und für Heimat
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte der Länder
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer (BRAK) ist die Dachorganisation der anwaltlichen Selbstverwaltung in Deutschland. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten[2] gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Sie nimmt zum Entwurf des Bridge Blueprints wie folgt Stellung:

Kurzbewertung

Die Vorschläge sind grundsätzlich zu begrüßen. Ihre Berücksichtigung in der Rechtsanwendung – aber, soweit einschlägig auch bei der Rechtssetzung – wäre zu begrüßen.

Die Vorschläge greifen etablierte Auslegungsgrundsätze auf und wenden diese konsequent, nachvollziehbar und praxistauglich auf jüngere technische und rechtliche Entwicklungen (insbesondere) im Bereich der künstlichen Intelligenz an. Damit wird, vorausgesetzt, dass die Aufsichts- und Rechtsprechungspraxis den gesetzten Beispielen folgen wird, ein Beitrag zu einem rechtssicheren und funktionierenden KI-Einsatz geleistet.

Kurzfristige Umsetzbarkeit und Technikneutralität

Vorteile des gewählten Ansatzes, die Probleme im Wesentlichen auf der Ebene der Rechtsauslegung bzw. Anwendung zu adressieren anstatt regulatorische Klarstellungen zu fordern, sind dessen kurzfristige Umsetzbarkeit und weitgehende Technologieoffenheit. Beides ist angesichts der rasant fortschreitenden Entwicklungen vonnöten und auf regulatorischem Wege schwerlich zu erreichen.

Grundrechtsgarantien

Ein weiterer Vorteil besteht darin, dass er die primär-, konventions- und verfassungsrechtlich gebotenen Grundrechtsgarantien, die vielfach Grund für die bisweilen als ausufernd empfundene Daten-, Digital-, und KI-Gesetzgebung der europäischen Union und ihrer Mitgliedsstaaten – nach hiesigem Verständnis – nicht aufgibt, wie dies bei vielen derzeit diskutierten regulatorischen Ansätzen – hier zumeist mit dem Ziel der Bürokratiebegrenzung – zumindest in Teilen der Fall ist. Vielmehr wird ein echter Grundrechtsausgleich angestrebt und in weiten Teilen erreicht.

Stärkere Betonung unantastbarer Verfahrensgarantien geboten

Indes kann und sollte der Grundrechtsschutz in Teilen stärker betont werden. Begrüßenswerter Weise verzichtet der Vorschlag auf kleinteilige Regelungen. Umso wichtiger ist es jedoch, die zu beachtenden Grundsätze klar und vollständig zu benennen, damit in der weiteren Betrachtung und insbesondere der Rechtsanwendung nicht versehentlich doch einige Grund- und Verfassungsrechte „auf der Strecke bleiben." Dies gilt umso mehr für Rechte und Grundsätze, die in allgemeinen Debatten zu den Themen Datenschutz, Datennutzung, künstliche Intelligenz, Gefahrenabwehr und Strafverfolgung regelmäßig unterbelichtet bleiben – etwa der Zugang zum Recht und das anwaltliche Berufsgeheimnis. Um Überfrachtungen und unbeabsichtigte Auslassungen zu vermeiden, sollte die Benennung abstrakt und ohne

[2] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden willkürlich gewählte weibliche oder männliche Form schließt alle Geschlechter gleichberechtigt ein.

Detailauflistungen erfolgen. Die Bundesrechtsanwaltskammer schlägt vor diesem Hintergrund die in der Anlage unter III. 2, IV. und V. hervorgehobenen Ergänzungen des Blueprints vor.

Regulatorische Anerkennung der Grundsätze wünschenswert

Naturgemäß fehlt dem Vorschlag die für ein Höchstmaß an Rechtssicherheit anzustrebende rechtliche Bedingungswirkung. Vielmehr kann er nur vermittels rechtswissenschaftlicher Kommentierungen wirken. Für mehr Rechtssicherheit sollte die Gesetzgeber eine Anerkennung der Auslegungsgrundsätze in regulatorischer Form in Betracht ziehen – namentlich bei den derzeit ohnehin anstehenden Reformüberlegungen in der Digital- und Datengesetzgebung. Ausreichen könnten insoweit bereits anerkennende Erwähnungen in Gesetzesbegründungen und Erwägungsgründen. Derartige Normierungen würden sich nach Auffassung der Bundesrechtsanwaltskammer zwanglos in das bestehende Daten- und KI-Regime einfügen, wären überschaubar und anwenderfreundlich. Der vielfach gefürchteter „Regelungstsunami“ würde damit vermieden bzw. begrenzt (vgl. Ergänzungsvorschlag der BRAK am Ende der Ziffer VI. der Anlage).

Verbleibender Regelungsbedarf sollte benannt werden

Vielfach wird mit den beschriebenen Ansätzen bereits auf Ebene der Rechtsanwendung ein Brückenschluss für einen praktikablen, rechtssicheren und grundrechtskonformen KI-Einsatz ermöglicht. Soweit dies angesichts normativer Grenzen nicht der Fall ist – etwa weil mit Blick auf Nichthochrisikosysteme eine Lösung unmittelbar unter Rückgriff auf Art. 10 Abs. 5 KI-VO ausscheidet – sollte dies nach Ansicht der Bundesrechtsanwaltskammer im Bridge Blueprint klar benannt und somit auf entsprechende gesetzliche Regelungen im Geist des Papiers hingewirkt werden (vgl. Ergänzungsvorschlag der BRAK am Ende der Ziffer VI.).

****

The Bridge-Blueprint

Thesen zur einheitlichen Anwendung von

Datenschutz- und KI-Regulierung

beim KI-Einsatz

Ergänzungsvorschläge der BRAK in Blau

I. Die Notwendigkeit eines Brückenschlags

Die europäische Debatte über künstliche Intelligenz scheint in einer Sackgasse festzustecken. Sie reduziert die Thematik auf einen Zielkonflikt zwischen technologischem Fortschritt und dem Schutz von Grundrechten. Das Resultat ist ein strategisches Zögern und das Gefühl, dass wesentliche Fortschritte ausbleiben.

Die Ursache hierfür ist jedoch nicht auf einen Fehler in der europäischen Wertearchitektur im Datenschutzrecht zurückzuführen. Vielmehr ist sie die Folge einer Rechtsunsicherheit: Es mangelt an einem gemeinsamen Verständnis, wie die zentralen Ziele der DSGVO praxistauglich ins Werk gesetzt werden können, um für innovative Unternehmen eine verlässliche Grundlage zu schaffen und Aufsichtsbehörden eine skalierbare Rechtsdurchsetzung zu ermöglichen. Diese Interpretationslücke trägt zur Stagnation bei. Sie schließt sich aber, wenn man die DSGVO als das versteht, was sie ist: ein Brückenrecht, das allgemeine Prinzipien mit konkreten oftmals technischen Anforderungen des Fachrechts verbindet. Der Grundsatz, die DSGVO bliebe von anderer Digitalregulierung „unberührt“, dient der Klarstellung ihrer Geltung, begründet aber keine isolierte Auslegung. Die DSGVO bleibt nicht unbeeinflusst.

Aufbauend auf diesem Verständnis, stellt dieses Papier die praxistaugliche Blaupause für den notwendigen Brückenschlag vor („Bridge Blueprint“). Es bietet eine Interpretation der DSGVO im Zusammenspiel mit der KI-Verordnung an, die sich gezielt auf den Einsatz von Systemen konzentriert – den Punkt, an dem die Vorteile der Innovation und die Risiken für Individuen gleichermaßen entstehen. Es ist nicht das Ziel, die DSGVO- Grundsätze zugunsten der Innovation aufzuweichen. Es geht darum, eine tragfähige Brücke zu bauen, die unsere europäischen Werte mit dem Fortschritt verbindet.

II. Datenschutz-Grundsätze als Qualitätsauftrag

Dieser Ansatz interpretiert die Grundsätze der DSGVO gerade nicht als Innovationshemmnisse, sondern als Auftrag für die Qualität und Sicherheit beim Einsatz von KI-Systemen zu sorgen. Dies spiegelt sich insbesondere in den Grundsätzen der Datenminimierung und der Datenrichtigkeit wider.

Primär dienen die Grundsätze der DSGVO dem Schutz des Einzelnen. Insbesondere der Grundsatz der Datenminimierung wird jedoch häufig als pauschales Gebot missverstanden, „weniger Daten zu nutzen“. Dieser Grundsatz wirkt aber nicht pauschal; es kommt vielmehr darauf an, welche Verarbeitung von Daten für einen konkreten Zweck erforderlich ist. Die KI-Verordnung hilft, diesen Zweck im Kontext von KI zu konturieren: Der Einsatz von KI-Systemen, die fair, hinreichend präzise sowie sicher sind und nicht unzulässig diskriminieren. Folglich ist die Verarbeitung umfangreicher Datensätze zur Mitigation schädlicher, diskriminierender Ergebnisse kein Verstoß gegen die Datenminimierung, wenn dies der Erfüllung von Pflichten zum Schutz betroffener Personen dient. In gleicher Weise schafft der Grundsatz der Richtigkeit eine positive Verpflichtung, Einzelpersonen vor den Schäden fehlerhafter Systeme zu schützen – wenn notwendig auch durch die Verarbeitung personenbezogener Daten. Aus den Grundsätzen der Datenminimierung und der Richtigkeit kann sich daher eine positive Rechtspflicht zur Datenverarbeitung ergeben, sofern diese zur Gewährleistung von Fairness und Datenintegrität im System erforderlich ist.

Diese Synergie wird durch den Grundsatz „Datenschutz durch Technikgestaltung“ aus Artikel 25 DSGVO verdeutlicht. Er betont die Integration rechtlicher Vorgaben in Systeme von Beginn an, bei der Entwicklung oder Auswahl von Mitteln zur Verarbeitung personenbezogener Daten. Diese Anforderung gewinnt durch die spezifischen Design- Anforderungen für Hochrisiko-KI-Systeme in der KI-Verordnung an Bedeutung. Indem Schutzmaßnahmen während der Phasen der Entwicklung und des Einsatzes verankert werden, stellt dieser gemeinsame „By-Design“-Ansatz sicher, dass Datenschutz und ethische Erwägungen nicht erst nachträglich berücksichtigt, sondern von Anfang an in die Architektur von KI-Systemen integriert werden.

III. Eine verlässliche Rechtsgrundlage für den KI-Einsatz

Eine Hauptursache für die Stagnation ist die Frage nach einer geeigneten Rechtsgrundlage, insbesondere wenn für den Betrieb eines KI-Systems personenbezogene Daten verarbeitet werden sollen. Diese Herausforderung verschärft sich bei der Verarbeitung besonders sensibler Daten. Eine enge Auslegung der DSGVO birgt die Gefahr eines gefährlichen Paradoxons: Dieselben Vorgaben, die den Einzelnen vor unzulässiger Datenverarbeitung schützen sollen, könnten es verhindern, die notwendigen Schritte zu unternehmen, um die Sicherheit, Richtigkeit und Fairness des KI-Einsatzes zu gewährleisten.

Dieses Papier plädiert für einen klaren, verlässlichen Standard, indem es das Interesse an der Datenverarbeitung zur Erfüllung der durch die KI-Verordnung vorgeschriebenen Pflichten eng mit dem Konzept der vernünftigen Erwartungen der betroffenen Personen und erheblicher öffentlicher Interessen verknüpft. Dieser Ansatz verleiht mehreren einschlägigen Grundsätzen der DSGVO im Zeitalter der KI eine konkrete Bedeutung, ohne das Regelwerk als Ganzes zu schwächen.

1. Berechtigtes Interesse als Rechtsgrundlage (Artikel 6 DSGVO)

Die Verarbeitung personenbezogener Daten erfordert nach Artikel 6 DSGVO eine Rechtsgrundlage. Das berechtigte Interesse als flexibelste Rechtsgrundlage der DSGVO wurde als austariertes Instrument geschaffen, um notwendige Datenverarbeitungen jenseits von Vertrag oder Einwilligung zu ermöglichen. Im KI-Kontext hat diese Flexibilität jedoch zu erheblicher Rechtsunsicherheit geführt: Das berechtigte Interesse wird zugleich als notwendiger Wegbereiter für Innovation und als riskantes Einfallstor für eine „Move fast, break things“-Mentalität dargestellt.

Diese Zuspitzung geht jedoch am Kern der Sache vorbei. Entscheidend ist ein konkreter Maßstab der Rechtsgrundlage des berechtigten Interesses: die vernünftigen Erwartungen des Einzelnen – geprägt durch einschlägige Vorgaben des Unionsrechts, wie die KI- Verordnung. Während die Prüfung des berechtigten Interesses im Kern auf den typisierten Einzelfall abstellt, verändert die KI-Verordnung den Rahmen dieser Bewertung für KI-Systeme. Sie verschiebt den Maßstab von einer impliziten, rein kontextbezogenen Einschätzung dessen, was eine betroffene Person erwarten könnte, hin zu einem konkreten, in Rechtspflichten verankerten Maßstab. Die berechtigte Erwartung eines Betroffenen entwickelt sich damit von der singulären Bewertung eines Datenverarbeitungsprozesses zu einem allgemeinen, systembezogenen Standard: die

Erwartung, dass ein KI-Produkt auf dem europäischen Markt dem geltenden Recht entspricht und die damit verbundenen KI-Praktiken rechtskonform sind.

Konkret schafft dies eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die zur Entwicklung und Validierung des Qualitäts- und Risikomanagementsystems eines Systems erforderlich sind, wie es die KI-Verordnung für Hochrisiko-KI-Systeme vorschreibt. Diese Logik ist jedoch nicht auf Hochrisiko-KI- Systeme beschränkt. Jeder für den KI-Einsatz Verantwortliche hat ein berechtigtes Interesse daran, Daten zu verarbeiten, um die Einhaltung der KI-Verordnung zu gewährleisten. Dies umfasst die Prüfung, ob ein System als hochriskant einzustufen ist, unter ein Verbot fällt oder Transparenzpflichten unterliegt – eine Bewertung, die für jedes KI-System erforderlich ist.

2. Erhebliches öffentliches Interesse (Artikel 9 DSGVO)

Artikel 9 setzt hohe Hürden für die Verarbeitung besonderer Kategorien von Daten und gestattet diese nur ausnahmsweise. Das primäre Ziel dieser Schutzvorschrift ist es, die Rechte und Freiheiten von Betroffenen zu schützen, insbesondere um Diskriminierung aufgrund von Merkmalen wie Gesundheit, Herkunft oder Weltanschauung zu verhindern. Doch im Kontext der von KI-Systemen droht eine paradoxe Wirkung: Diese Einschränkung von Datenverarbeitungen, die Diskriminierung verhindern soll, kann bei KI-Systemen dazu führen, dass derartige Benachteiligungen gefördert werden.

Indem ein KI-System aus historischen Mustern in Daten lernt, kann es gesellschaftliche Verzerrungen (Bias) aus Trainingsdatensätzen perpetuieren und so auf der Grundlage geschützter Merkmale diskriminieren, ohne jemals explizit dazu angewiesen worden zu sein. Dies führt zu einer unbeabsichtigten und gefährlichen Konsequenz: Artikel 9 DSGVO, der Diskriminierung verhindern soll, könnte das Risiko einer neuen, automatisierten Form dieser Diskriminierung erhöhen, wenn Verantwortliche daran gehindert werden, ebenjene Verzerrungen zu identifizieren und zu korrigieren und ihren Auswirkungen entgegenzuwirken.

An dieser Stelle bewirkt die KI-Verordnung einen grundlegenden Wandel. Die Geltendmachung eines „erheblichen öffentlichen Interesses“, das die Verarbeitung sensibler Daten erlaubt, wurde bisher als hohe Hürde angesehen, die oft mit den Aufgaben öffentlicher Stellen verbunden ist. Nun definiert die KI-Verordnung z.B. in Art. 10 Abs. 5 ein neues, spezifisches und erhebliches öffentliches Interesse: das Interesse daran, sicherzustellen, dass eingesetzte KI-Systeme keine gesellschaftlichen Benachteiligungen perpetuieren. Um dafür zu sorgen, dass ein KI-System etwa nicht aufgrund des Gesundheitszustands oder der ethnischen Herkunft diskriminiert, müssen Maßnahmen ergriffen werden. Das umfasst auch, wenn unbedingt erforderlich, die gezielte Verarbeitung solcher Daten, um eben jene Risiken zu testen, zu messen und zu mitigieren. Wie sowohl die KI-Verordnung als auch die DSGVO betonen, müssen für besondere Datenkategorien geeignete Garantien vorgesehen werden, um weitere Risiken für die betroffenen Personen zu vermeiden.

Insofern handeln die Verantwortlichen nicht allein aus kommerziellem Eigeninteresse, sondern vollziehen eine Sicherheitsmaßnahme zur Mitigierung von Risken und erfüllen damit ein erhebliches öffentliches Interesse.

[Ergänzungs-Vorschlag BRAK: zu den gemäß Art. 10 Abs. 5 Satz 1 KI-VO zu treffenden angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen zählen auch das europarechtlich garantierte Recht auf einen wirksamen Rechtsbehelf und auf anwaltliche Vertretung (Art. 47 EU-Charta), die immer gewährleistet bleiben müssen.]

IV. Automatisierte Entscheidungen und Betroffenenrechte

Zwei der drängendsten Fragen beim KI-Einsatz sind der Umgang mit automatisierten Entscheidungen und die wirksame Ausübung der Betroffenenrechte. Beiden Themenkomplexen liegt eine ähnliche Problemstellung zugrunde: die Sicherstellung von Verfahrensgerechtigkeit bei automatisierten KI-Systemen. Hierfür bietet die DSGVO im Zusammenspiel mit der KI-Verordnung eine einheitliche Lösung.

Automatisierte Entscheidungen sind für zahlreiche Einsatzszenarien von KI-Systemen erforderlich. Sie bergen jedoch das inhärente Risiko, „Computer-sagt-nein"-Szenarien zu schaffen, in denen Einzelpersonen erheblichen, potenziell schädlichen Ergebnissen ohne Transparenz oder wirksame Rechtsbehelfe ausgesetzt sind. Die DSGVO hat diese Herausforderung vorhergesehen. Artikel 22 wurde nicht geschaffen, um die Automatisierung zu blockieren, sondern um sicherzustellen, dass sie nachprüfbar ist,
z.B. indem solche Praktiken erlaubt werden, wenn das Unionsrecht dies zulässt und geeignete Maßnahmen zum Schutz des Einzelnen vorhanden sind.

Ein wesentliches Hindernis ist bisher jedoch das Fehlen umfassender Gesetze, die solche Schutzmaßnahmen regeln. Die KI-Verordnung schafft hier Abhilfe. Sie liefert die geeigneten Maßnahmen, die im rechtlichen Rahmen bisher fehlten. Durch die Umsetzung der verbindlichen Anforderungen der KI-Verordnung, u.a. für aussagekräftige Transparenz, verpflichtende menschliche Aufsicht und robuste Überprüfbarkeit durch Protokollierung (Logging) gibt es einen rechtlich verbindlichen Standard für sichere und nachprüfbare automatisierte Systeme, der somit Artikel 22 erfüllen kann.

Der Wert dieser Anforderungen liegt in ihrem Fokus auf dem Prozess. Obschon die Transparenz eine zentrale Rolle einnimmt, ist es nicht erfolgversprechend, von einem „Blackbox"-Modell eine menschenähnliche „Erklärung" zu verlangen. Dies führt nur zu einer zweiten Blackbox – der Erklärung –, deren Verbindung zur ursprünglichen Entscheidung ungewiss ist. Ziel muss es sein, eine transparente und nachvollziehbare Kette des gesamten Entscheidungsprozesses zu schaffen. Dies ist die Grundlage dafür, dass betroffene Personen automatisierte Entscheidungen sinnvoll anfechten können ***[Ergänzungs-Vorschlag BRAK: und verfahrensrechtliche Garantien wie das Recht auf einen wirksamen Rechtsbehelf bzw. auf anwaltliche Vertretung eine Wirkung entfalten können].***

Die Erfüllung dieser Rechte durch direkte Eingriffe auf Modellebene ist technisch oft weder verlässlich noch machbar. Darüber hinaus richten sich rechtliche Anforderungen auf Modellebene oft an andere Akteure in der KI-Wertschöpfungskette als den Betreiber, was einen systembezogenen Fokus praxisgerechter und wirksamer macht. Die Überprüfbarkeit auf Systemebene ist daher ein vielversprechenderer Weg zur Durchsetzung der Betroffenenrechte im Vergleich zu nicht oder kaum wirksamen Eingriffen auf Modellebene.

Deshalb sprechen wir uns für eine Verlagerung des Fokus auf den Interaktionspunkt aus: eine Regulierung auf Systemebene, die Verantwortlichen beim KI-Einsatz zugänglich ist. In der Praxis bedeutet dies die Implementierung eines überprüfbaren Instrumentariums an systemseitigen Maßnahmen, die nachweislich unzulässige Ausgaben von Daten unterbindet. Somit entwickelt die KI-Verordnung die datenschutzrechtliche Rechenschaftspflicht von einem Grundsatz zu einer Systemanforderung fort.

V. Die DSFA: Ein strategisches Instrument zur Risikobeherrschung

Die Datenschutz-Folgenabschätzung (DSFA) nach Artikel 35 DSGVO und die notwendige Schwellenwertanalyse sollten nicht als letzte Hürde der Compliance betrachtet werden. Im Kontext von KI setzen sie die in diesem Papier dargelegten Ansätze operativ um. Anhand dieser Methodik weist der Verantwortliche den Übergang von abstrakten Grundsätzen zu einer konkreten, belastbaren Governance nach.

Während die Konformität mit der KI-Verordnung viele notwendige technische Standards liefert, können die Auswirkungen auf die Grundrechte nicht standardisiert werden, da sie stark kontextabhängig sind. Die DSFA ist damit der Raum für die Bewertung solcher kontextuellen und atypischen Risiken, die außerhalb standardisierter Rahmen fallen. Die wichtigsten Risiken, auf denen der Fokus liegen sollte, sind gesellschaftliche und individuelle Schäden, einschließlich des Potenzials für Fehlinformationen und Deepfakes, Falschdarstellung, Manipulation und Cybersicherheitsbedrohungen, die ein KI-System kompromittieren können. Auch beim Themenkomplex der Memorisierung von Trainingsdaten in KI-Systemen muss die Risikobewertung in der DSFA über die bloße Feststellung eines möglicherweise gefahrenträchtigen technischen Phänomens hinausgehen. Ein zentrales Risiko ist die unbeabsichtigte Preisgabe von Daten, wobei hohe Risiken für betroffene Personen insbesondere aus schädlichen oder unrichtigen Daten entstehen, die andernfalls nicht offengelegt worden wären– sei es aus dem Trainingsdatensatz oder aus früheren Nutzereingaben. ***[Ergänzungs-Vorschlag BRAK: Konkret zu betrachten sind dabei auch die Auswirkungen solcher Risiken auf bzw. für die Einhaltung rechtsstaatlicher Anforderungen der Überprüfung bzw. fairer Verfahren (Art. 6 EMRK) sein, die nicht unterlaufen werden dürfen.]***

Eine DSFA muss das effektive Management dieser Risiken für die betroffenen Personen dokumentieren, nicht abstrakte Gefahren. Während sich die DSFA auf Risiken aus der Verarbeitung personenbezogener Daten konzentriert, verfolgt die Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment, FRIA) der KI-Verordnung für öffentliche Stellen einen breiteren Ansatz, aber beide sind Teil des Nachweises einer umfassenden Risikobewertung.

VI. Ausblick und Aufruf

Dieses Papier präsentiert den Entwurf für einen kohärenten Weg zum Einsatz von KI. Die Realisierung dieses Potenzials erfordert jedoch mehr als nur eine juristische Interpretation; sie verlangt einen Mentalitätswandel. Der Diskurs muss sich verlagern: weg von einer müßigen Debatte darüber, ob die DSGVO Innovationen ermöglicht, hin zu einer zielgerichteten Diskussion darüber, wie wir einen verantwortungsvollen Fortschritt erreichen. Eine Diskussion, die in der Praxis verankert sein muss und Instrumente wie regulatorische Reallabore nutzt, um einen Dialog über die rechtskonforme Nutzung und Weiterentwicklung von künstlicher Intelligenz zu gestalten. Angesichts der globalen politischen Lage darf nicht übersehen werden, dass die digitale Souveränität Europas eine Schlüsselrolle bei der Gestaltung dieses Ökosystems für vertrauenswürdige KI spielen muss.

Dieser Wandel ist gerade deshalb möglich, weil das Datenschutzrecht nie dazu gedacht war, im luftleeren Raum zu existieren; es wurde konzipiert, um Individuen innerhalb einer gegebenen technologischen Realität zu schützen. Die KI-Verordnung beschreibt diese Realität für unsere Zeit. Sie liefert konkrete Governance-Anforderungen, die den abstrakten Grundsätzen der DSGVO Sinn und Durchschlagskraft verleihen. Diese Synergie ermöglicht

es, sich auf das zu konzentrieren, was wirklich zählt: die Qualität und Sicherheit der eingesetzten KI-Systeme, um Fairness und eine wirksame Mitigation von Risiken zu gewährleisten.

Die Etablierung eines funktionierenden, vertrauenswürdigen Rahmenwerks für den KI- Einsatz hängt von den Beiträgen aller relevanten Akteure ab, von nationalen und regionalen Regierungen, den europäischen Datenschutzbehörden, der europäischen Industrie, KI-Innovatoren, Datenschutzexperten und Datenschutzbeauftragten bis hin zur Zivilgesellschaft und NGOs. Es erfordert, über Silodenken hinauszugehen und dieses Konzept des Brückenschlags („Bridge Blueprint“) zu fördern, um die Grundsätze des Datenschutzes mit der Praxis des vertrauenswürdigen KI-Einsatzes zu verbinden.

[Ergänzungs-Vorschlag BRAK: Vielfach wird mit den beschriebenen Ansätzen bereits auf Ebene der Rechtsanwendung ein Brückenschluss für einen praktikablen, rechtssicheren und grundrechtskonformen KI-Einsatz möglich sein. Darüberhinausgehend wäre im Interesse größtmöglicher Rechtssicherheit deren regulatorische Anerkennung wünschenswert. Soweit der skizzierte Ansatz auf Anwendungseben normativen Grenzen begegnet - etwa soweit mit Blick auf Nichthochrisikosysteme eine Lösung unmittelbar unter Rückgriff auf Art. 10 Abs. 5 KI-VO ausscheidet – sollten entsprechende gesetzliche Regelungen im Geist dieses Papiers in Betracht gezogen werden].

Bei diesem Dokument handelt es sich um einen öffentlichen Entwurf (v. 0.9). Wir, die Autor:innen dieses Papiers, Thomas Fuchs, Dr. Markus Wünschelbaum, Dr. h.c. Marit Hansen und Benjamin Walczak laden alle Akteure ein, sich an diesem Dialog zu beteiligen und die Brücke zwischen Prinzip und Praxis mit uns zu bauen, indem Sie Ihr Feedback bis zum 15.11.2025 an folgende E-Mail-Adresse schicken:

aibridge@datenschutz.hamburg.de

Ihre Anmerkungen werden in die finale Version dieses Bridge Blueprints einfließen, dessen Veröffentlichung anschließend erfolgen wird.