bankenverband

Positionspapier

des Bankenverbandes zu einem KI-förderlichen Rechtsrahmen

Juli 2025

Lobbyregister-Nr. R001458
EU-Transparenzregister-Nr. 0764199368-97

Bundesverband deutscher Banken e. V.
Burgstraße 28
10178 Berlin
Telefon: +49 30 1663-0
www.bankenverband.de

USt.-IdNr. DE201591882

Einleitung

Mit der Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung)[1] hat die Europäische Union einen umfassenden rechtlichen Rahmen geschaffen, der darauf abzielt, Künstliche Intelligenz vertrauensvoll und sicher einzusetzen. Damit nimmt die EU eine weltweite Vorreiterrolle in der Regulierung von KI ein. Während andere Regionen bei der Entwicklung und der gewinnbringenden Verwendung von KI führend sind, ist es nun entscheidend, den bestehenden Rechtsrahmen möglichst innovations- und wirtschaftsfreundlich anzuwenden. Dies ist notwendig, damit Deutschland und Europa die Chancen von KI konsequent nutzen können. Dazu gehört, dass

1. die Umsetzung der Verordnung im Rahmen noch ausstehenden Konkretisierungen durch die EU-Kommission sowie die nationalen Gesetzgeber möglichst praxisgerecht, rechtssicher und EU-weit einheitlich für die Unternehmen ausgestaltet wird,

2. ein konsistentes Zusammenspiel mit bereits bestehende aufsichtsrechtliche Anforderungen für Banken sichergestellt und eine Doppelregulierung vermieden werden sowie

3. eine kohärente Verzahnung der datenschutzrechtlichen Anforderungen mit den regulatorischen Vorgaben der KI-Verordnung gewährleistet wird.

Die nachfolgenden Vorschläge der privaten Banken sollen einen Beitrag dazu leisten, die Verordnung zukunftsorientiert umzusetzen.

1 Anforderungen an die Umsetzung der KI-Verordnung

Die Verordnung gilt in Teilen bereits ab Februar 2025, weitere Vorschriften werden bis August 2027 folgen, sofern der gesetzliche Zeitplan nicht noch einmal angepasst wird. Zu vielen Aspekten sind noch Konkretisierungen in Form von Leitlinien, harmonisierten Standards und nationalen Durchführungsgesetzen und Ähnliches geplant, die in den nächsten Monaten erfolgen sollen. Bei deren Ausgestaltung und Anwendung gilt es insbesondere Folgendes zu beachten.

Einheitliche Interpretation der KI-Definition

Die Definition von Künstlicher Intelligenz ist für den Anwendungsbereich der KI-Regulierung entscheidend. Eine zu weit gefasste Definition, die konventionelle IT-Systeme miterfasst, würde die Wirtschaft unnötig belasten. Eine zu eng gefasste Definition hingegen würde Spielräum für

[1] VERORDNUNG (EU) 2024/1689 vom 13. Juni 2024.

Umgehungsmöglichkeiten schaffen, was die politische Zielsetzung der Verordnung und deren Technologieneutralität gefährden würde. Dennoch lässt die KI-Definition der Verordnung einige Fragen offen, die es im Sinne der Rechtssicherheit für Akteure aufzulösen gilt.

Eine sachgemäße und zugleich möglichst trennscharfe Definition für den europäischen Wirtschaftsraum zu haben, ist ein wichtiges Anliegen der Kreditwirtschaft. Denn in kaum einer anderen Branche spiegelt sich die IT-gestützte Analyse und Verarbeitung von Daten in einer so vielfältigen Softwarelandschaft quer durch alle Funktionen und Geschäftsbereiche wider. Diese überwiegend konventionellen IT-Systeme, die keine Form des maschinellen Lernens oder der Selbstoptimierung beinhalten, fallen gemäß der KI-Verordnung nicht unter die KI-Definition. Weniger eindeutig für ist die Bewertung für grundlegende statistische Verfahren, wie lineare und logistische Regressionen, die eine sehr begrenzte Lernfähigkeit aufweisen und uneingeschränkt nachvollziehbar sind, und damit nicht die KI-spezifischen Risiken aufweisen, die der Gesetzgeber mit der Verordnung adressieren wollte.

Daher begrüßen wir, dass die EU-Kommission in ihren Leitlinien aus Februar 2025 die KI-Definition weiter präzisiert hat.[2] Dies fördert nicht nur ein EU-weit einheitliches Verständnis, sondern konkretisiert auch anhand ausgewählter Beispiele, welche Systeme als Künstliche Intelligenz gelten und welche nicht dazu zu zählen sind. Die Leitlinien stellen unter anderem klar, dass die langjährig in der Kreditvergabeprüfung der Banken etablierten Regressionsverfahren nicht als KI-Systeme zu bewerten sind.

Allerdings haben Leitlinien der EU-Kommission keinen rechtsverbindlichen Charakter, sondern dienen als Orientierung für die Akteure und die Aufsicht. Daher spricht sich der Bankenverband für eine konsistente Anwendung innerhalb der EU und durch die Mitgliedstaaten aus. Nur so ist eine harmonisierte Aufsichtspraxis zu erreichen, die Rechtssicherheit und gleiche Standortbedingungen für alle Marktteilnehmenden sicherstellt. Nicht zuletzt würde eine zu weite KI-Definition den Blick von den wirklich risikoreichen KI-Anwendungen ablenken, für die es zurecht gesetzlicher Leitplanken und einer dedizierten Aufsicht bedarf. Der Fokus muss darauf liegen, die charakteristischen Herausforderungen und Risiken fortgeschrittener KI-Technologien zu bewältigen, einschließlich Fragen der Verzerrung, der Undurchsichtigkeit und der autonomen Entscheidungsfindung.

Klare und enge Abgrenzung von Hochrisiko-KI-Anwendungen

Neben dem Verbot von KI-Praktiken, die mit dem europäischen Recht und den gemeinsamen Werten nicht vereinbar sind, steht die Regulierung von Hochrisiko-KI-Systemen im Zentrum der

[2] Commission Guidelines on the defintion of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)", C (2025) 924 final, 2. Februar 2025.

KI-Verordnung. Anbieter und Betreiber von Hochrisiko-KI-Systemen müssen künftig vor deren Einsatz nachweisen können, dass die KI-Systeme die Anforderungen der Verordnung erfüllen. So soll einer Schädigung der Gesundheit und Sicherheit oder der Grundrechte von Personen in der EU vorgebeugt werden.

Die KI-Verordnung legt in Anhang III fest, für welche Anwendungszwecke eines KI-Systems ein hohes Risiko angenommen werden muss.[3] Anbieter von KI-Systemen müssen prüfen, ob ihre KI-Systeme in den Hochrisikobereich fallen und für eine Konformität mit den Anforderungen der Verordnung sorgen. Für unsere Mitglieder könnten insbesondere KI-Systeme, die im Prozess der Bonitätsbewertung natürlicher Personen (Anhang III Nr. 5 b) sowie im Bereich des Personalmanagements (Anhang III Nr. 4) zum Einsatz kommen, in den Hochrisikobereich fallen.

Von den unter Anhang III Nr. 5 b) der Verordnung genannten Hochrisiko-KI-Systemen zur Bonitätsbewertung sind ausdrücklich solche KI-Systeme ausgenommen, die zur Aufdeckung von Finanzbetrug verwendet werden. Unserem Verständnis nach umfasst dies KI-Systeme, die der Prävention von Geldwäsche und Terrorismusfinanzierung, dem Sanktionsscreening oder der Identifizierung von betrügerischen Zahlungstransaktionen dienen. Dies sollte die EU-Kommission in ihren angekündigten Leitlinien zu Hochrisiko-KI-Systemen klarstellen. Zudem sollten die Leitlinien konkrete Anwendungsfälle von Hochrisiko-KI-Systemen beinhalten und möglichst zeitnah – vor dem angekündigten Termin im Februar 2026 – veröffentlicht werden.

Schärfung der Rollenabgrenzung und Ausweitung des Bestandschutzes auf Anbieter

Die KI-Verordnung reguliert die verschiedenen Akteure in der KI-Wertschöpfungskette anhand ihrer jeweiligen Rolle (z. B. Anbieter, Betreiber, Händler, etc.). Jedoch bestehen weiterhin Unklarheiten bei der Trennung zwischen der Rolle des Anbieters und der des Betreibers, u. a. wenn ein Finanzinstitut mit einem anderen Unternehmen kooperiert oder ein KI-System innerhalb von Konzernstrukturen von mehreren Banken genutzt wird. Dies beeinträchtigt die Rechtssicherheit und könnte so Fortschritt hemmen. Daher sollte das AI-Office die Rollenabgrenzung nachschärfen.

Von besonderer Bedeutung ist dies für die Frage, ob ein Bestandsschutz für bereits im Einsatz befindliche KI-Systeme besteht. Der Rechtstext nimmt die Rolle des Betreibers von Hochrisiko-KI-Systemen von den Pflichten der Verordnung aus, sofern das System vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurde und danach in seiner Konzeption nicht erheblich verändert wird.

[3] Vgl. Artikel 6 Abs. 2 der KI-Verordnung.

Eine Bank, die ein Hochrisiko-KI-System z. B. zur Erstellung von Arbeitszeugnissen selbst entwickelt und ausschließlich zum Eigengebrauch in Betrieb genommen hat, gilt laut dem Verordnungstext nicht nur als Betreiber, sondern auch als Anbieter dieses Systems und wäre somit ab August 2026 voll von den Anforderungen betroffen. Angesichts des strengen Sanktionsregimes könnten die betroffenen Akteure sich genötigt sehen, ein solches KI-System vorsichtshalber nicht weiter zu betreiben. Gleichzeitig weist die EU-Kommission in ihren Leitlinien zur KI-Definition vom Februar 2025 in einer Fußnote darauf hin, dass für sämtliche Systeme, die vor dem 2. August in Verkehr gebracht oder in Betrieb genommen wurden, die Bestandsschutzregel des Artikel 111 Abs. 2 gilt. Diesen Widerspruch sollte die Kommission auflösen und klarstellen, dass der Bestandschutz für Betreiber *und* Anbieter gilt.

Auch zur Rolle des „nachgelagerten Anbieters" sind weiterhin Fragen offen. Besonders relevant wird dies im Kontext von generativer KI auf Basis großer Sprachmodelle, wie sie zumeist außereuropäische Anbieter bereitstellen. Die Verordnung erfasst diese als KI-Modelle mit allgemeinem Verwendungszweck (GPAI-Modelle). Banken könnten zu nachgelagerten Anbietern werden, wenn sie ein solches Modell in ihr eigenes KI-System integrieren.

Die KI-Verordnung nennt nachgelagerte Anbieter als Begünstigte der Transparenzinformationen von GPAI-Anbietern (in Anhang XII). Es ist jedoch unklar, ob der nachgelagerte Anbieter auch die rechtliche Verantwortung für die Anbieterpflichten trägt. Denn für diese Verantwortung würden die Informationen, die dem nachgelagerten Anbieter zustehen, nicht ausreichen. Dies gilt insbesondere für die Integration eines GPAI-Modells in ein Hochrisikosystem. Da die Erfüllung der Anbieterplichten nur in Kooperation mit dem eigentlichen Anbieter des GPAI-Modells möglich wäre, würde die Nutzung von generativer KI für Hochrisikoanwendungen praktisch unmöglich werden. Zudem ist fraglich, ob zusätzliche Meldepflichten für Banken als nachgelagerte Anbieter gegenüber dem AI-Office erwachsen, da sie als Folge womöglich zum Anbieter eines KI-Systems mit allgemeinem Verwendungszweck werden würden.

Der Bankenverband würde daher eine klarere Rollenabgrenzung durch das AI-Office begrüßen.

Gewährleistung eines Level-Playing-Field und effizienter Aufsichtsstrukturen

Wie eingangs erwähnt, sieht die KI-Verordnung an vielen Stellen weitere Konkretisierungen vor, zum Teil durch die Europäische Kommission oder das darunter geschaffene Büro für Künstliche Intelligenz (AI-Office), zum Teil durch die einzelnen Mitgliedstaaten.

Eine interne Abfrage unter unseren Mitgliedern hat ergeben, dass die Umsetzungsreife des vorliegenden Regelwerkes in den allermeisten Punkten noch nicht gegeben ist. Zu den zahlreichen Level 2- und Level 3-Regulierungen kommen harmonisierte europäische Normen hinzu, deren Zeitplan stark gefährdet ist. Letztere sollen Möglichkeiten aufzeigen, wie die

Anforderungen an Hochrisiko-KI-Systeme – z. B. das vorgeschriebene Risiko- oder Qualitätsmanagementsystem – in der Praxis umgesetzt werden können.

Diese Konkretisierungen sind für Marktteilnehmende essenziell, damit sie die Vorgaben der Verordnung rechtssicher umsetzen können. Angesichts der im Detail relevanten Sachverhalte und der mitunter weitreichenden Auswirkungen sollten die Marktakteuere möglichst früh und eng eingebunden werden. Zudem benötigen die Unternehmen angemessen Zeit für die Umsetzung. Allein die Fülle der noch ausstehenden Konkretisierungen lässt Zweifel an einer hinreichenden Marktkonsultation. Daher sollte die Kommission den Zeitplan noch einmal kritisch prüfen und gegebenenfalls verlängern.

Zudem ist eine maximale Harmonisierung innerhalb der EU wünschenswert. Ein Auseinanderlaufen oder gar ein Flickenteppich an unterschiedlichen nationalen Interpretationen würde wettbewerbsverzerrend wirken und muss unbedingt vermieden werden. Daher ist eine enge Abstimmung unter den Mitgliedsstaaten im europäischen KI-Gremium bzw. seinen Untergruppen wichtig. In gleicher Weise sollten sich auch die auf nationaler Ebene mit der Überwachung der Verordnung betrauten Fachbehörden möglichst eng koordinieren und einer einheitlichen Rechtsauslegung folgen.

Die Bundesregierung muss bis August dieses Jahres eine zuständige Aufsichtsbehörde für die Zwecke der KI-Verordnung benennen oder einrichten. Dem Vernehmen nach beabsichtigt sie, die Zuständigkeit für die Marktüberwachung für KI im Finanzsektor auf mehrere Behörden zu verteilen. Neben den bestehenden Finanzaufsichtsbehörden, die für solche KI-Systeme zuständig sein sollen, die in direktem Bezug zu Finanzdienstleistungen stehen, soll die Aufsicht für alle anderen KI-Systeme in den Finanzinstituten bei der Bundesnetzagentur liegen. Diese geteilte Verantwortlichkeit würde dem grundlegenden Ziel einer effizienten und bürokratiearmen Aufsicht ohne Doppelstrukturen entgegenstehen. Es drohen Abgrenzungsfragen, Konflikte und Redundanzen. Daher sollten allein die Finanzaufsichtsbehörden die KI-Systeme in Banken überwachen, unabhängig davon, um welche Anwendung es im Einzelfall geht. Die Bundesnetzagentur kann dabei die Rolle als zentrales Koordinierungs- und Kompetenzzentrum übernehmen und über die Abstimmung mit der Finanzaufsicht, wie auch den zuständigen Fachbehörden in anderen regulierten Sektoren, eine konsistente Aufsichtspraxis sicherstellen.

2. Verzahnung mit bestehendem Bankaufsichtsrecht

Im Hinblick auf die Anforderungen an das Risikomanagement und an die Einrichtung eines Qualitätsmanagementsystems erkennt die Verordnung zurecht die hohen Standards im

Finanzsektor aufgrund bereits bestehender regulatorischer und aufsichtlicher Anforderungen an.[4] Das bestehende umfangreiche bankaufsichtsrechtliche Regelwerk ist technologieagnostisch und gilt auch für KI-Systeme. Daher dürften die Anforderungen der KI-Verordnung in weiten Teilen bereits von bestehenden Vorgaben an Banken abgedeckt sind.

Die laufenden Bemühungen der Europäischen Bankenaufsichtsbehörde, die Anforderungen der Verordnung mit den bestehende bankaufsichtlichen Vorgaben abzugleichen, sind grundsätzlich zu begrüßen. Hierbei sollten insbesondere die Vorgaben der KI-Verordnung identifiziert werden, die Banken bereits erfüllen und somit nicht noch einmal gesondert umsetzen müssen. Falls Widersprüche zwischen der KI-Verordnung und dem bestehenden Rechtsrahmen für Banken zutage treten sollten, müsste der Gesetzgeber gegebenenfalls klarstellen, welche Regelung Vorrang hat. Auf keinen Fall sollten die Aufsichtsbehörden oder Regulatoren in solchen Fällen vermeintliche Klarstellungen in Form von *zusätzlichen* Regulierungen und Standards anstreben. Die Erfahrung zeigt, dass diese Vorgehensweise im Gegenteil resultiert. Sie erhöht die Komplexität der Regulierung zu Lasten der Verständlichkeit und wirft letztlich eher noch zusätzliche Fragen auf, als dass sie Unklarheiten beseitigt. Banken dürfen nicht vor die Situation gestellt werden, dass sie Vorgaben aus der KI-Regulierung erfüllen müssen, die dem bestehenden bankaufsichtlichen Regelwerk entgegenstehen.

Einer Anpassung des bestehenden bankaufsichtsrechtlichen Regelwerks bedarf es nicht. Dies wäre auch hinsichtlich der von der Politik bekräftigten Bestrebens zur Stärkung der Wettbewerbsfähigkeit und Vereinfachung des Rechtsrahmens nicht vertretbar.

Zudem bedarf es eines EU-weit einheitlichen Verständnisses und einer harmonisierten Aufsichtspraxis über die jeweiligen Mitgliedstaaten und die involvierten Aufsichtsbehörden hinweg. Denn die größten europäischen Banken werden bereits heute einheitlich in gemeinsamen Aufsichtsteams (Joint Supervisory Teams) unter Federführung der Europäische Zentralbank überwacht. Dies unterstreicht die Notwendigkeit einer engen Abstimmung unter den Europäischen und nationalen Aufsehern und spricht zusätzlich dafür, die Marktüberwachung in die Hände der Behörden zu geben, die bereits mit der Finanzaufsicht betraut sind (siehe Abschnitt oben zu Aufsichtsstrukturen). Dies würde den Rückgriff auf etablierte Prüfungspraktiken und die Nutzung vorhandener Erfahrungen und Kenntnisse ermöglichen.

Mit Blick auf die Meldung von schwerwiegenden Vorfällen sprechen wir uns dafür aus, bereits etablierte Meldewege und Meldeplattformen (MVP) zu nutzen, die bereits im Kontext der Zahlungsdienste-Richtlinie (PSD) und dem Digital Operational Resiliance Act (DORA) für Finanzinstitute genutzt werden. Dies würde zu einem möglichst schlanken und effizienten

[4] Vgl. unter anderem Artikel 17 Abs. 4 (Qualitätsmanagementsystem) und Artikel 26 Abs. 5 Satz 5 (Pflichten der Betreiber von Hochrisiko-KI-Systemen) sowie Erwägungsgrund 158 der Verordnung.

Meldeprozess beitragen, der Aufwand und Nutzen in einem praxisnahen Rahmen hält. Im Zusammenhang mit der Meldepflicht von schwerwiegenden Vorfällen sollte zudem aus Gründen der Rechtsklarheit der Tatbestand der „Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte" gemäß Art. 3 Nr. 49 lit. c) KI-VO präzisiert werden, um das damit verfolgte Ziel der der Vermeidung einer Dopplung von Meldepflichten für bereits regulierte Anbieter wirksam zu erreichen.

3 Weiterentwicklung der DSGVO zur Förderung des KI-Einsatzes

Die zunehmende Verbreitung und Relevanz von KI-Technologien stellt das bestehende Datenschutzrecht vor strukturelle und normative Herausforderungen. Die EU-Datenschutz-Grundverordnung (DSGVO) bietet zwar einen europaweit einheitlichen Rahmen für den Schutz personenbezogener Daten, ist jedoch aufgrund ihrer Entstehung vor einem Jahrzehnt bislang nicht in allen Aspekten auf die besonderen technischen und funktionalen Eigenheiten von KI-Systemen ausgerichtet. Im Zusammenspiel mit der KI-Verordnung stellen sich in der Praxis eine Vielzahl von Einzelfragen. Es besteht daher ein erhöhter Bedarf an klarstellenden Regelungen und an einer kohärenten Verzahnung der datenschutzrechtlichen Anforderungen mit den regulatorischen Vorgaben der KI-Verordnung.

Ziel muss es sein, einerseits den effektiven Schutz personenbezogener Daten sowie die Sicherung der Grundrechte auch im Kontext datengetriebener KI-Anwendungen uneingeschränkt zu gewährleisten. Gleichzeitig gilt es, innovationsfreundliche Rahmenbedingungen zu schaffen, die die technologische Wettbewerbsfähigkeit und die Entwicklung vertrauenswürdiger KI-Systeme sowohl auf nationaler als auch auf europäischer Ebene nachhaltig fördern. Eine präzisierende Fortentwicklung der DSGVO in zentralen Anwendungsfeldern erscheint daher erforderlich, um regulatorische Klarheit zu schaffen und rechtssichere sowie verantwortungsvolle KI-Anwendungen zu ermöglichen. Zwar versuchen die Datenschutzaufsichtsbehörden bereits Unterstützung zu Auslegungsfragen zu geben[5], doch besteht hier weiterer Unterstützungs- und Klärungsbedarf durch den Gesetzgeber und die nach der KI-Verordnung und DSGVO zuständigen Aufsichtsbehörden. Sowohl die gesetzlichen Vorgaben als auch die Aufsichtspraxis sollten einen widerspruchsfreien Handlungsrahmen bilden. Dies soll an folgenden Beispielen gezeigt werden.

Schaffung von mehr Rechtssicherheit beim Anlernen von KI-Systemen mit Trainingsdaten

Die Entwicklung und das Training von KI-Systemen im Bankensektor setzen regelmäßig den Rückgriff auf umfangreiche Datenbestände voraus. Neben öffentlich zugänglichen Informationen

[5] Vgl. u.a. https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

greifen Institute dabei auch auf interne Datenquellen zurück, etwa aus dem operativen Betrieb oder der Kundenkommunikation. Um datenschutzrechtlichen Anforderungen zu genügen, erscheint es vielfach als besserer Weg, die verwendeten Daten vor ihrer Verwendung im KI-Training zu anonymisieren oder zumindest zu pseudonymisieren.

Beide Verfahren – sowohl Anonymisierung als auch Pseudonymisierung – stellen jedoch selbst Verarbeitungsvorgänge im Sinne der DSGVO dar. In der Praxis fehlt es bislang an der erforderlichen Rechtssicherheit, in welcher Weise diese Maßnahmen datenschutzkonform durchgeführt werden können. Positiv zu vermerken ist, dass sich u.a. der EU-Datenschutzausschuss bereits mit Fragen der Pseudonymisierung und Anonymisierung im KI-Kontext befasst hat.[6]

Darüber hinaus stellt sich die Folgefrage, ob die so vorbereiteten Datensätze im weiteren Verlauf des Trainingsprozesses rechtlich als anonymisiert oder pseudonymisiert zu qualifizieren sind. Dies ist insofern von Bedeutung, als anonymisierte Daten nicht mehr in den Anwendungsbereich der DSGVO fallen. Pseudonymisierte Daten hingegen bleiben grundsätzlich datenschutzrechtlich relevant, auch wenn ein Rückschluss auf die betroffene Person ohne Zusatzwissen faktisch ausgeschlossen ist.

Gerade im Kontext automatisierter Trainingsprozesse innerhalb von KI-Systemen stellt sich auch die Frage, inwieweit klassische Betroffenenrechte – etwa auf Auskunft oder Löschung gemäß Art. 15 ff. DSGVO – von der verantwortlichen Stelle überhaupt sinnvoll und verhältnismäßig umgesetzt werden können. Denn KI-Modelle verarbeiten Trainingsdaten in der Regel nicht in einer Weise, die eine nachträgliche personenbezogene Rückverfolgbarkeit ohne erhebliche Zusatzinformationen ermöglicht.

Vor diesem Hintergrund erscheint eine gesetzliche Klarstellung erforderlich, die folgende Punkte adressiert:

- Zulässigkeit von Vorverarbeitungsschritten: Die Durchführung von Anonymisierungs- und Pseudonymisierungsmaßnahmen sollte ausdrücklich als zulässiger Verarbeitungsschritt anerkannt werden, sofern geeignete technische und organisatorische Schutzmaßnahmen vorliegen.

- Klarheit über den datenschutzrechtlichen Status vorbereiteter Datensätze: Es bedarf unionsweit einheitlicher Kriterien zur Abgrenzung zwischen anonymisierten, pseudonymisierten und personenbezogenen Daten im Kontext des maschinellen Lernens.

[6] https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation_de.

- Anpassung der Betroffenenrechte bei pseudonymisierten Trainingsdaten: In Konstellationen, in denen ein Rückschluss auf identifizierbare Personen praktisch ausgeschlossen ist, sollte geprüft werden, inwieweit sich Betroffenenrechte sachgerecht anpassen lassen, um eine funktionale Umsetzung von KI-Anwendungen nicht unverhältnismäßig zu erschweren.

Datenschutzfolgenabschätzung nach DSGVO und Grundrechtsfolgenabschätzung nach KI-Verordnung synchronisieren

Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO sowie die in der KI-Verordnung unter Artikel 27 vorgesehene Grundrechtsfolgenabschätzung für Hochrisiko-KI-Systeme verfolgen übereinstimmend das Ziel, potenzielle Risiken für die Rechte und Freiheiten natürlicher Personen im Vorfeld technischer Systementwicklungen systematisch zu identifizieren, zu bewerten und – soweit möglich – zu minimieren. Beide Instrumente beruhen auf dem präventiven Risikomanagementansatz des europäischen Grundrechtsschutzes, sind bislang jedoch weder inhaltlich noch methodisch aufeinander abgestimmt.

Vor diesem Hintergrund erscheint eine systematische Koordinierung beider Prüfregime geboten. Die gegenwärtige Parallelität der Anforderungen birgt das Risiko redundanter Prüfprozesse sowie potenziell widersprüchlicher Wertungen in Bezug auf die Schutzbedürftigkeit betroffener Rechtsgüter. Zur Vermeidung doppelten Verwaltungsaufwands und zur Steigerung der rechtspraktischen Kohärenz ist eine stärkere inhaltliche und strukturelle Verzahnung von Datenschutzfolgenabschätzung und Grundrechtsfolgenabschätzung erforderlich.

Empfehlenswert ist insoweit die Entwicklung standardisierter, aufeinander abgestimmter Prüf- und Dokumentationsformate (Templates), die eine konsistente Bewertung ermöglichen und überflüssige Prüfhandlungen vermeiden. Die Einbindung konkreter Prüfkriterien und klarer Abgrenzungen zwischen datenschutz- und grundrechtsspezifischen Prüfaspekten ist hierbei unerlässlich.

Zugleich sollte geprüft werden, ob und inwieweit bei Implementierung wirksamer risikominimierender Maßnahmen – etwa durch technische Verfahren der Pseudonymisierung oder Anonymisierung – eine Einschränkung oder Modulation der Prüfungspflichten sachlich gerechtfertigt ist. Dies könnte etwa durch eine risikoadaptive Ausgestaltung der Prüfpflichten erfolgen, welche den Einsatz datenschutzfreundlicher Gestaltungstechniken im Sinne des Art. 25 DSGVO incentiviert.

Eine solche Systematisierung und Flexibilisierung würde nicht nur zu einer Vereinfachung der regulatorischen Anforderungen beitragen, sondern auch die rechtssichere Implementierung der KI-Verordnung in datenschutzrelevanten Anwendungsfeldern befördern. Die Herstellung von Kohärenz zwischen bestehenden datenschutzrechtlichen Instrumenten und den neu eingeführten

Mechanismen der KI-Regulierung ist aus Sicht einer grundrechtsorientierten und praktikablen Normanwendung unabdingbar.

Technische Ausgestaltung der Betroffenenrechte im Anwendungsbereich der KI-Verordnung

Die in der Datenschutz-Grundverordnung (DSGVO) normierten Betroffenenrechte – insbesondere das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) sowie Widerspruch (Art. 21 DSGVO) – behalten auch im Kontext von KI-Systemen ihre uneingeschränkte Geltung. Sie sind Ausprägungen grundrechtlich geschützter Rechtspositionen, deren effektive Wahrung durch die Anwendung der KI-Verordnung sichergestellt werden muss.

Vor dem Hintergrund der spezifischen technischen Eigenheiten vieler KI-Systeme – etwa nicht-lineare Modellarchitekturen, hohe Datenvolumina sowie datengetriebene Trainingsmechanismen – ergibt sich ein erheblicher Konkretisierungsbedarf hinsichtlich der technischen Umsetzung dieser Rechte im Rahmen der KI-Verordnung. Insbesondere stellt sich die Frage, unter welchen technischen Bedingungen die Löschung personenbezogener Daten im Sinne des Art. 17 DSGVO als rechtlich wirksam anzusehen ist.

Eine besondere Herausforderung ergibt sich in Fällen, in denen personenbezogene Daten nicht lediglich verarbeitet, sondern zur Modellbildung und -anpassung verwendet werden. Die vollständige Entfernung einzelner Datenpunkte kann hier erhebliche Auswirkungen auf die Modellintegrität, Systemstabilität oder sogar auf die operative Nutzbarkeit des KI-Systems haben. In der Praxis zeigt sich, dass bestehende Modellarchitekturen bislang nur bedingt in der Lage sind, den Anforderungen der DSGVO vollumfänglich gerecht zu werden.

Vor diesem Hintergrund rückt die Notwendigkeit klarer, technischer Umsetzungsstrategien zur Wahrung datenschutzrechtlicher Ansprüche zunehmend in den regulatorischen Fokus. Ziel muss es sein, einen Ausgleich zwischen der praktischen Durchsetzbarkeit der Betroffenenrechte einerseits und der Aufrechterhaltung innovationsfreundlicher Rahmenbedingungen andererseits zu schaffen.

Aus technischer Sicht sind dabei insbesondere folgende Lösungsansätze Gegenstand aktueller Diskussionen:

- „Machine Unlearning“: Verfahren zur gezielten Entfernung spezifischer Informationen aus trainierten Modellen ohne vollständiges Retraining.
- Federated Learning: Dezentralisierte Lernansätze, bei denen Daten lokal verarbeitet werden und eine verbesserte Kontrolle durch die betroffenen Personen möglich ist.

- Granulare Zugriffskontrollen: Differenzierte Zugriffskonzepte, welche selektive Datenlöschungen oder -einschränkungen ermöglichen, ohne die Gesamtfunktionalität zu beeinträchtigen.

- Modulare Systemarchitekturen: Strukturelle Trennung von Modellkomponenten zur besseren Rückverfolgbarkeit und gezielten Interventionsfähigkeit.

- Pseudonymisierung und Datenmaskierung: Techniken zur Risikominimierung, deren Einsatz allerdings mit Blick auf die verbleibende Personenbeziehbarkeit rechtlich sorgfältig abzuwägen ist.

Trotz der beschriebenen technischen Fortschritte bleibt festzuhalten, dass auf operativer Ebene bislang keine einheitlichen Standards existieren, die eine rechtskonforme Umsetzung datenschutzrechtlicher Vorgaben im KI-Kontext verbindlich festlegen. Diese Rechtsunsicherheit stellt insbesondere kleine und mittlere Unternehmen sowie Forschungseinrichtungen vor praktische und ökonomische Herausforderungen.

Im Lichte des schrittweisen Inkrafttretens der KI-Verordnung erscheint es aus Sicht der Praxis unabdingbar, dass der europäische und nationale Gesetzgeber – gegebenenfalls flankiert durch Aufsichtsbehörden und Standardisierungsinstitutionen – technische Leitlinien und Mindestanforderungen zur effektiven Wahrung von Betroffenenrechten formuliert. Andernfalls drohen Verzögerungen bei der Markteinführung innovativer KI-Lösungen sowie Investitionszurückhaltung aufgrund regulatorischer Unklarheit.

Eine unterlassene Klärung würde letztlich das Ziel der KI-Verordnung – die Förderung von Innovation unter gleichzeitiger Wahrung grundrechtlicher Schutzstandards – erheblich beeinträchtigen.