Der AI Act im Spannungsfeld von digitaler und sektoraler Regulierung

BertelsmannStiftung

Impressum

© Bertelsmann Stiftung, Gütersloh
Dezember 2024

Herausgeber
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0
www.bertelsmann-stiftung.de

Autoren
Prof. Dr. Philipp Hacker

Verantwortlich
Asena Soydaş

Lektorat
Rudolf Jan Gajdacz, München

Grafikdesign
Nicole Meyerholz, Bielefeld

Bildrechte
Titelfoto: © utoi – stock.adobe.com
S. 7: © Ansichtssache_Britta Schröder

Zitiervorschlag
Hacker, Philipp (2024). Der AI Act im Spannungsfeld von digitaler und sektoraler Regulierung.
Hrsg. Bertelsmann Stiftung. Gütersloh.

DOI 10.11586/2024189

Der AI Act im Spannungsfeld von digitaler und sektoraler Regulierung

Prof. Dr. Philipp Hacker

BertelsmannStiftung

Inhalt

Vorwort

Mit dem Inkrafttreten der Verordnung zur Künstlichen Intelligenz (AI Act) im Sommer 2024 hat Europa einen entscheidenden Schritt für die Regulierung von KI-Systemen unternommen. Dieses erste umfassende, demokratisch legitimierte Regelwerk stellt die Weichen für eine sicherere Nutzung von KI im Einklang mit europäischen Werten. Als weiteres Puzzlestück ergänzt der AI Act die europäischen Bestrebungen der letzten Legislaturperioden, die Europäische Union und insbesondere den europäischen Binnenmarkt „fit für das digitale Zeitalter“ zu machen.

Bis August 2026 steht die Aufgabe an, den AI Act bestmöglich Stück für Stück umzusetzen und konkret zu definieren, was seine Vorgaben in der Praxis bedeuten. Doch wie bei jedem komplexen Vorhaben zeigt sich bereits: Einzelne Teile passen noch nicht nahtlos ineinander. Inkonsistenzen, Überschneidungen und Unklarheiten könnten die reibungslose Umsetzung behindern und zu den Unsicherheiten führen, die eigentlich vermieden werden sollten.

Ein zentrales Problem ist, dass viele Gesetze bei ihrer Entstehung isoliert betrachtet werden, obwohl sie im Zusammenspiel mit anderen Regelungen ein Gesamtbild ergeben müssen. So auch beim AI Act, dessen horizontaler Ansatz ihn in engen Zusammenhang mit bestehenden digitalen und sektoralen Regelungen stellt. Er verweist vielfach auf andere Rechtsakte, deren praktische Bedeutung jedoch noch analysiert, getestet und umgesetzt werden muss.

Dabei geht es nicht nur um juristische Präzision. Die Auswirkungen des AI Act betreffen zentrale Wirtschafts- und Gesellschaftsbereiche. Regulatorische Widersprüche können Innovationen bremsen und Unsicherheiten den Einsatz neuer Technologien erschweren. Diese Unklarheiten könnten nicht nur die Effizienz der Regulierung beeinträchtigen, sondern auch zu einer Fragmentierung der Auslegungen und Zuständigkeiten führen. Gleichzeitig kann es zu Regulierungsarbitrage kommen, bei der Unternehmen uneinheitliche Vorgaben ausnutzen, um sich strengeren Anforderungen zu entziehen. Aus den Herausforderungen bei der Umsetzung der Datenschutz-Grundverordnung lässt sich hier besonders viel lernen, um die Durchsetzung des AI Act noch effektiver zu gestalten.

Es ist notwendig, zeitnah den Diskurs darüber zu führen, wie die europäischen digitalen und sektoralen Rechtsakte in ihrer Umsetzung besser aufeinander abgestimmt werden können. Diese Frage erfordert weitere wissenschaftliche Einsichten und politische Debattenräume, um sowohl die Kohärenz der Regulierung als auch ihre langfristige Wirksamkeit sicherzustellen.

Mit unserer Studie im Projekt reframe[Tech] – Algorithmen fürs Gemeinwohl möchten wir genau an dieser Stelle ansetzen und einen Impuls zur Schaffung einer fundierten wissenschaftlichen Grundlage geben. Für die rechtswissenschaftliche Analyse haben wir Prof. Dr. Philipp Hacker von der Europa-Universität Viadrina Frankfurt (Oder) gewonnen. Die Studie gibt eine erste Übersicht darüber, wie der AI Act mit bestehenden digitalen Regelungen wie der Datenschutz-Grundverordnung und dem Digital Services

Act sowie mit sektoralen Vorschriften interagiert. Anhand exemplarisch ausgewählter Sektoren – der Finanz-, Medizin- und Automobilbranche – werden die aktuellen Herausforderungen in Bezug auf den AI Act beleuchtet.

Jeder dieser Bereiche zeigt, dass der Anpassungsbedarf sowie die Notwendigkeit von Nachjustierungen je nach digitalem und sektoralem Rechtsakt unterschiedlich stark ausgeprägt sind.

Dennoch lassen sich über alle Sektoren hinweg gemeinsame strukturelle Maßnahmen identifizieren: Kurzfristig muss eine bessere Verzahnung bestehender Regelwerke erfolgen, um Doppelungen zu vermeiden und die Effizienz zu steigern. Langfristig sind sowohl nationale als auch europäische Ansätze erforderlich, um die KI-Regulierung mit anderen Rechtsakten zu harmonisieren und regulatorische Widersprüche nachhaltig zu beseitigen. Darüber hinaus sollte eine regelmäßige Überprüfung der regulatorischen Rahmenwerke erfolgen, um sicherzustellen, dass technologische und gesellschaftliche Entwicklungen angemessen berücksichtigt werden.

Wir befinden uns in einem entscheidenden Zeitfenster, das gemeinsame Anstrengungen erfordert: Die Umsetzung und Durchsetzung des AI Act kann nur dann erfolgreich sein, wenn alle relevanten Akteur:innen in Europa und den Mitgliedstaaten – von Gesetzgebern und Aufsichtsbehörden bis hin zu Unternehmen und der Zivilgesellschaft – gemeinsam am Puzzlebild arbeiten. Gemeinsam können wir sicherstellen, dass dieses Regelwerk, klarer abgestimmt, seine volle Wirkung entfaltet – für eine rechtssichere, innovative und verantwortungsvolle KI-Landschaft.

Unser Dank gilt Prof. Dr. Philipp Hacker für seinen wichtigen Beitrag zur Analyse des AI Act im Kontext der digitalen und sektoralen Rechtsakte sowie den Teilnehmenden des Dialogtreffens für die tiefgehende und erkenntnisreiche Diskussion. Wir freuen uns auf Ihre Rückmeldungen und selbstverständlich über jede Form konstruktiver Kritik.

Asena Soydaş
Project Manager
reframe[Tech]
Bertelsmann Stiftung

Martin Hullin
Direktor Digitalisierung
und Gemeinwohl
Bertelsmann Stiftung

Executive Summary

Diese Studie analysiert den AI Act im Kontext der bestehenden EU-Digitalregulierungen sowie sektoralen Vorschriften und zeigt die relevanten Schnittstellen und möglichen Konflikte auf. Der AI Act, der im August 2024 in Kraft trat, ist Teil einer umfassenden EU-Regulierung digitaler Technologien, zu der auch die Datenschutz-Grundverordnung (DS-GVO) und der Digital Services Act (DSA) zählen. Der horizontale, risikobasierte Ansatz des AI Act zielt darauf ab, KI-Anwendungen nach ihrem Risikopotenzial zu kategorisieren und für besonders risikoreiche Systeme strenge Anforderungen zu schaffen. Er ist dabei nicht auf Unternehmen in der EU beschränkt, sondern betrifft auch außerhalb der EU ansässige Unternehmen, deren KI-Systeme in der EU angeboten oder deren Output dort genutzt wird.

Friktionen und Synergien

Die Studie identifiziert Friktionen und Synergien zwischen dem AI Act und anderen Rechtsakten:

- **Konflikte mit der Digitalregulierung:** Mehrere EU-Rechtsakte aus dem Digitalbereich interagieren auf komplexe Weise mit dem AI Act.

  _ **Friktionen mit dem DSA:** Es bestehen Überschneidungen bei den Anforderungen an Risikoanalysen für große Plattformen (z. B. VLOPs) und generative KI-Systeme, die sowohl unter den DSA als auch den AI Act fallen. Wenngleich mit unterschiedlicher Akzentuierung, stehen jeweils systemische Risiken im Vordergrund. Diese Analysen sollten intelligent kombiniert werden, gerade wenn hybride Plattformen zunehmend generative KI integrieren.

  _ **Interaktionen mit der DS-GVO:** Der AI Act und die DS-GVO stehen in einem systematischen Spannungsverhältnis, da primär der Anbieter eines KI-Systems nach dem AI Act haftet, während die DS-GVO grundsätzlich den Betreiber für die Datenverarbeitung verantwortlich macht. Zudem erlaubt der AI Act in Hochrisiko-KI-Systemen die Verarbeitung sensibler Daten zur Diskriminierungsvermeidung, was nach der DS-GVO sonst verboten ist. Diese Ausnahme gilt jedoch, trotz ihrer großen Relevanz, nicht für generative KI. Daher besteht für das KI-Training mit personenbezogenen und sensitiven Daten Regelungsbedarf.

- **Sektorale Konflikte:** Der AI Act steht zudem in einem Spannungsverhältnis zu mehreren sektoralen Regulierungen, insbesondere aufgrund seiner horizontalen Natur (d. h. branchenübergreifend), die über bereits existierende, spezialisierte Regelungswerke hinausgehen.

  _ **Finanzprodukte (Anhang III AI Act):** Kreditbewertungssysteme und andere KI-basierte Finanzanwendungen sind bereits stark reguliert. Der AI Act fügt zusätzliche Vorschriften hinzu. Während Compliance-Systeme explizit integriert werden sollen, ist das Verhältnis zahlreicher anderer Vorschriften, welche dieselben Risiken adressieren, ungeklärt, etwa im Bereich der Datengovernance und Modellleistung.

_ **Medizinprodukte (Anhang I Abschnitt A AI Act):** Hier entstehen Doppelverpflichtungen nach AI Act und der Medizinprodukteverordnung (MDR), insbesondere bei Hochrisiko-KI-Systemen wie der Krebsdiagnose. Diese Systeme unterliegen sowohl den MDR- als auch den strengen Anforderungen des AI Act für Risikomanagement und Dokumentation. Dies kann insbesondere zu Kapazitätsproblemen bei den Konformitätsbewertungsstellen führen.

_ **Automobilsektor (Anhang I Abschnitt B AI Act):** Die hergebrachte Bewertungsmethodik (sog. Typgenehmigung) bleibt das zentrale Zulassungsverfahren für Fahrzeuge, das sicherstellt, dass technische und sicherheitsrelevante Normen eingehalten werden. Der AI Act bringt zusätzliche Anforderungen nur für KI-Systeme, die nicht als hochriskant eingestuft werden. Für hochriskante Systeme, wie etwa sicherheitskritische autonome Fahrsysteme, bleibt die sektorale Regulierung maßgeblich. Diese Systeme sind zwar von den spezifischen Anforderungen des AI Act ausgenommen, jedoch müssen die sektoralen Vorschriften künftig unter Berücksichtigung der Hochrisiko-Prinzipien des AI Act angepasst werden.

Handlungsempfehlungen

Der AI Act als horizontaler Rechtsrahmen ergänzt sektorale Regelungen und weitere Digitalgesetze, ist jedoch nur unzureichend auf diese abgestimmt. Daraus leiten sich Handlungsempfehlungen für verschiedene Akteure in kurz-, mittel- und langfristiger Perspektive ab. In den meisten Fällen handelt es sich dabei um Maßnahmen, welche die Umsetzung des AI Act vereinfachen, Spannungsverhältnisse klären, Kooperationen verstärken und evidenzbasierte Evaluationen ermöglichen. Sie bieten damit die Möglichkeit, das regulatorische Umfeld für KI nachhaltig zu verbessern, ohne den Grundrechtsschutz abzusenken.

1. Kurzfristige Maßnahmen

- **Ausweisung eines „Lead Act“ (Europäischer Gesetzgeber):** Ein „Lead Act“ könnte als vorrangiger Rechtsrahmen zur Konfliktminimierung zwischen dem AI Act und sektorspezifischen Vorschriften etabliert werden. Dieser Lead Act könnte je nach Sektor der AI Act selbst oder zentrale sektorale Regelungen sein. Wenn die Anforderungen des Lead Act erfüllt sind, wird vermutet, dass auch die Anforderungen der anderen Regelwerke eingehalten sind, wodurch Rechtsunsicherheiten verringert werden.

- **Stärkere Verzahnung von Regulierungen (Europäische Kommission, insbesondere AI Office):** Die bestehende sektorspezifische Gesetzgebung sollte besser mit dem AI Act verknüpft werden, um Doppelregulierungen zu vermeiden. Insbesondere in den Bereichen Finanzdienstleistungen und Medizinprodukte sollten klare Abgrenzungen definiert werden, die die Vorgaben des AI Act im Verhältnis zu den sektorspezifischen Vorschriften präzisieren. Diese Verzahnung kann weitgehend durch Durchführungsverordnungen erreicht werden, ohne dass der AI Act selbst geändert werden muss. Strukturell hat Art. 17 Abs. 4 AI Act Vorbildcharakter: Der Absatz ist ein Beispiel für eine gelungene Verzahnung, da spezifisch und sehr konkret geregelt ist, welche Teile des AI Act durch bestehendes Regulierungsrecht automatisch erfüllt werden und welche Maßnahmen darüber hinaus noch getroffen werden müssen. Leider ist diese Vorschrift auch die einzige im AI Act, die eine derartige Klarheit und Präzision hinsichtlich der sektoralen Verschränkung bietet. Auch hier gilt: Durch derartiges Gesetzgebungshandwerk ließen sich KI-Entwicklung und -Einsatz in der EU erheblich vereinfachen, ohne dass beim Grundrechtsschutz irgend Abstriche gemacht werden müssten.

- **Festlegung von Praxisleitlinien und Content Moderation (Europäische Kommission, insbesondere AI Office):** Es sollten Leitlinien erstellt werden, die aufzeigen, wie Content Moderation auf Modell-

ebene gestaltet werden kann, um systemische Risiken zu minimieren, die auch durch die Verquickung von Plattformen mit generativer KI verstärkt werden. Diese Leitlinien sollten zugleich sicherstellen, dass die Moderation nicht unverhältnismäßig in die Meinungsfreiheit eingreift und die Vielfalt der KI-Ergebnisse gewahrt bleibt.

- **Durchführung ganzheitlicher Risikoanalysen (AI Office und Kommissionsaufsicht über VLOPs/ VLOSEs):** Bei großen Plattformen, die generative KI einsetzen, sollten umfassende Risikoanalysen durchgeführt werden, um sowohl plattform- als auch KI-spezifische Risiken zu bewerten. Dies erfordert eine verstärkte Zusammenarbeit zwischen den Aufsichtsbehörden gemäß dem Digital Services Act und dem AI Act.

- **Entwicklung spezifischer Leitlinien (Europäischer Datenschutzausschuss):** Es sollten spezifische Leitlinien zum Umgang mit personenbezogenen Daten in KI-Trainings entwickelt werden, um Rechtsunsicherheiten bei der Harmonisierung mit der DS-GVO zu verringern. Diese Leitlinien sollten klare Vorgaben für die Wiederverwendung solcher Daten enthalten und in enger Abstimmung mit dem AI Office erfolgen.

- **Institutionelle Verzahnung der Aufsicht (Nationaler Gesetzgeber):** Die Zusammenarbeit zwischen der nationalen KI-Aufsichtsbehörde und sektorspezifischen Regulierungsbehörden sollte verstärkt werden, etwa durch die Abordnung von Fachleuten aus sektorspezifischen Behörden. Sie können eine Scharnierfunktion einnehmen und helfen, Expertise sektorspezifisch und projektbezogen bereitzustellen. Zugleich ist der Austausch mit dem AI Office wichtig, damit ein dauerhafter AI Enforcement Hub mit entsprechender Expertise, Feedback und strukturierten Lernprozessen entstehen kann.

- **Einrichtung eines zentralen Datenzugangsportals (Nationaler Gesetzgeber):** Ein zentrales Portal für den Zugang zu KI-Daten sollte geschaffen werden, um Forscher:innen und Regulierungsbehörden eine leichtere Überwachung von generativen und Hochrisiko-KI-Systemen zu ermöglichen.

- **Einführung staatlicher Stipendienprogramme (Nationaler Gesetzgeber):** Unternehmen in regulierten Sektoren, insbesondere kleine und mittlere Unternehmen (KMU), sollten durch staatliche Stipendienprogramme unterstützt werden, um die Anforderungen des AI Act und sektorspezifischer Regulierungen besser zu verstehen und umzusetzen. Diese Programme könnten z. B. die Teilnahme an spezialisierten Schulungsprogrammen fördern, um die betriebliche Compliance zu stärken.

- **Erarbeitung detaillierter Leitlinien (Nationale Aufsichtsbehörden):** Nationale Aufsichtsbehörden sollten Leitlinien zur Anwendung des AI Act in spezifischen sektoralen Kontexten entwickeln. Diese Guidelines könnten dann auf die Besonderheiten einzelner Sektoren eingehen und eine präzise Handhabung des AI Act im Wechselspiel mit sektoralen Vorschriften ermöglichen.

- **Einrichtung verstärkter Kooperationsmechanismen (Nationale Aufsichtsbehörden):** Die nationale KI-Aufsicht sollte enger mit Datenschutzbehörden kooperieren, um eine kohärente Umsetzung von AI Act und DS-GVO zu gewährleisten. Durch regelmäßige Konsultationen und Absprachen könnten Friktionen zwischen den Regelwerken gemindert werden.

- **Einrichtung sektorspezifischer Expertengremien (Nationale Aufsichtsbehörden):** Sektorspezifische Expertengremien sollten innerhalb der nationalen KI-Aufsichtsbehörde etabliert werden, die aus Wissenschaft, Zivilgesellschaft und Industrie zusammengesetzt sind. Diese Gremien könnten sektorspezifische Risiken und Besonderheiten bei der Umsetzung des AI Act berücksichtigen.

- **Etablierung übergreifender technischer Normen (Standardisierungsorganisationen):** Standardisierungsorganisationen sollten technische Normen

entwickeln, die als Safe-Harbor-Mechanismen dienen und die Anforderungen des AI Act und der sektorspezifischen Regulierung erfüllen. Ferner sollten derartige Normen auch für AI Act und DS-GVO gemeinsam entwickelt werden. Dies kann Unternehmen helfen, die regulatorischen Anforderungen übergreifend effektiv umzusetzen.

- **Entwicklung von Praxisleitfäden (Unternehmen):** Die Unternehmen sollten Praxisleitfäden (Codes of Practice) gemäß Art. 56 AI Act entwickeln, um die Umsetzung des AI Act auf branchenspezifischer Ebene zu fördern und die Zusammenarbeit zwischen Unternehmen und Regulierern zu stärken.

- **Klärung der Systematik (Rechtswissenschaft):** In der Rechtswissenschaft sollten verstärkt auch die Systematik von und das Verhältnis zwischen Instrumenten der Digitalgesetzgebung in den Blick genommen werden. Das Prinzip der Spezialregelung zur Klärung von Vorrangfragen (lex specialis) kann hier ein erster Ansatzpunkt sein. Derartige Systematisierung kann dann eine Grundlage für Behördenleitlinien oder Gerichtsurteile bilden.

2. Mittelfristige Maßnahmen

- **Stärkere Nutzung spezifischer Verweise im Rechtstext (Europäischer Gesetzgeber):** Der AI Act sollte durch explizite Verweise auf andere relevante Regulierungen klarer gestaltet werden, um Überlappungen zu vermeiden und die kohärente Anwendung der betroffenen Rechtsakte zu erleichtern.

- **Harmonisierung mit der DS-GVO (Europäischer Gesetzgeber):** Um die Nutzung von personenbezogenen Daten in KI-Modellen und -Systemen zu ermöglichen, sollten die Regelungen im AI Act und in der DS-GVO besser aufeinander abgestimmt werden. Dies könnte durch spezifische Ausnahmen und Verknüpfungen im AI Act erreicht werden, für die Art. 10 Abs. 5 AI Act, der sich mit der Verwendung von sensitiven Daten für Fairnessanalysen beschäftigt, eine Vorlage abgeben kann.

- **Rechtsrahmen für KI-Training (Europäischer Gesetzgeber):** Der AI Act sollte mittelfristig um eine explizite Ausnahme für die Nutzung von Daten zu Trainingszwecken mit entsprechenden Schutzvorkehrungen ergänzt werden, ähnlich der bestehenden Text- und Data-Mining-Ausnahme im Urheberrecht.

- **Content Moderation auf Modellebene (Europäischer Gesetzgeber):** Der Digital Services Act sollte so erweitert werden, dass vertrauenswürdige Hinweisgeber schädliche Eingabeaufforderungen und illegale KI-Ausgaben melden können, um plattform- und KI-spezifische Risiken umfassend abzudecken.

- **Verknüpfung von Durchführungsgesetzen (Nationaler Gesetzgeber):** Die nationalen Durchführungsgesetze zum AI Act, Digital Services Act und der DS-GVO sollten besser verknüpft werden, um Synergien zu schaffen, insbesondere im Bereich des Datenzugangs und des Risikomanagements.

3. Langfristige Maßnahmen

- **Evaluation AI-Act-Regulierung (Europäischer Gesetzgeber):** Der AI Act sollte nach einer angemessenen Anwendungszeit grundlegend extern evaluiert und überarbeitet werden. Diese Fassung könnte z. B. Haftungsregelungen, Vorschriften für Basismodelle und Transparenzanforderungen kombinieren, ggf. ohne Berücksichtigung der spezifischen prozeduralen und substanziellen Regelungen für Hochrisiko-KI (z. B. Art. 8 bis 27 AI Act), und so für eine flexiblere Compliance in Hochrisiko-Bereichen sorgen.

- **Aufsichtsarchitektur (Nationaler Gesetzgeber):** Die Zusammenarbeit zwischen den sektoralen und KI-spezifischen Aufsichtsbehörden sollte langfristig institutionalisiert und in einen klaren gesetzli-

chen Rahmen eingebettet werden. Dieser Rahmen muss Zuständigkeiten, Kommunikationskanäle und Entscheidungsprozesse definieren, um eine kohärente und effiziente Überwachung sicherzustellen.

- **Entwicklung eines Frameworks für Kooperation und Evaluation (Aufsichtsbehörden):** Die Aufsichtsbehörden sollten evidenzgestützte Mechanismen zur Evaluation ihrer Kooperationen einführen. Dieses Framework sollte regelmäßige Bewertungen der Zusammenarbeit anhand definierter Kriterien wie Geschwindigkeit, Konsistenz und Vollständigkeit des Informationsaustauschs ermöglichen. Die Ergebnisse der Evaluierungen sollten zur kontinuierlichen Anpassung und Optimierung der Kooperationsstrukturen und -prozesse genutzt werden, um die Effizienz und Wirkung der Aufsicht langfristig zu steigern.

Mit diesen Maßnahmen können, so die Hoffnung, der AI Act effizienter umgesetzt, regulatorische Konflikte vermieden und gleichzeitig die Innovationskraft in der EU gestärkt werden.

Abkürzungsverzeichnis

ABl	Amtsblatt
Abs.	Absatz
ADS	Automated Driving System (automatisiertes Fahrsystem)
AI	Artificial Intelligence
Art.	Artikel
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
CEN	Comité Européen de Normalisation (Europäisches Komitee für Normung)
CENELEC	Comité Européen de Normalisation Électrotechnique (Europäisches Komitee für elektrotechnische Normung)
CRA	Cyber Resilience Act
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
CTR	Clinical Trials Regulation
DMA	Digital Markets Act
DORA	Digital Operational Resilience Act
DSA	Digital Services Act
DS-GVO	Datenschutz-Grundverordnung
EG	Erwägungsgrund
ENISA	European Network and Information Security Agency (Agentur der Europäischen Union für Cybersicherheit)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDA	Food and Drug Administration
GA	Gerichtsakte
GDNG	Gesundheitsdatennutzungsgesetz
GPAI	General-Purpose AI Models (generative KI-Technologien)
IVDR	In Vitro Diagnostic Medical Devices Regulation
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KWG	Kreditwesengesetz
MaRisk	Mindestanforderungen an das Risiko-managementsystem von Banken
MDR	Medizinprodukteverordnung
Rn	Randnote, Randnummer
Rs	Rechtssache
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
StVZO	Straßenverkehrs-Zulassungs-Ordnung
UAbs.	Unterabsatz
UrhG	Urheberrechtsgesetz
VLOPs	Very Large Online Platforms
VLOSEs	Very Large Online Search Engines

I. Einleitung

Der AI Act, in Kraft getreten am 2.8.2024,[1] steht im Zentrum des Diskurses um den rechtlichen Rahmen für Künstliche Intelligenz (KI). Dabei wird jedoch bisweilen ausgeblendet, dass er nicht in ein rechtliches Vakuum gestoßen ist. Vielmehr waren und sind Produkte, die KI nutzen, schon seit langer Zeit reguliert – durch sektorspezifische Instrumente, technologieneutrale Rechtsakte und jüngst nun auch durch weitere Digitalgesetze. Die EU hat in den letzten Jahren eine Reihe bedeutender Rechtsakte erlassen, um die Aufsicht über digitale Technologien voranzutreiben und zentrale Risiken gesetzlich zu adressieren. Zu den wesentlichen Instrumenten zählen unter anderem die Datenschutz-Grundverordnung (DS-GVO),[2] der Digital Services Act (DSA)[3] und das Haftungsrecht für KI.[4]

Ferner spielen im sektoralen Bereich das Bank-, Medizinprodukte- und Automotive-Recht eine besondere Rolle, die jeweils unterschiedlich auf digitale Entwicklungen eingehen. Diese Regelungen zielen allesamt darauf ab, eine Balance zwischen technologischer Innovation und dem Schutz von Grundrechten und Wettbewerb zu schaffen.

Der AI Act stößt nun in dieses regulatorische Gefüge hinein, indem er einen horizontalen, risikobasierten Ansatz verfolgt. Er klassifiziert Anwendungen von KI-Systemen sowie bestimmte KI-Modelle mit allgemeinem Verwendungszweck (z. B. GPT-4) anhand ihres Risikopotenzials für die Gesellschaft, wobei besonders hochriskante Systeme strengen Vorschriften unterliegen (z. B. in Medizin, Kreditvergabe oder der Personalauswahl). Seine Reichweite ist nicht zu unterschätzen: Er ist nicht nur anwendbar auf Unternehmen mit Sitz in der EU, sondern auch auf solche außerhalb der Union, sofern ihre KI-Modelle in der EU angeboten oder deren Ergebnisse in der EU genutzt werden. Eine ähnliche globale Wirkung entfaltet auch die DS-GVO.

Ein aus wissenschaftlicher und praktischer Sicht zentrales Thema in der Regulierung von Künstlicher Intelligenz, das in der bisherigen Debatte jedoch noch nicht hinreichend beleuchtet wurde, ist die Schnittstelle des AI Act zu bestehenden sektorspezifischen und digitalen Regulierungen. Diese Schnittstellen müssen klar benannt und adressiert werden, um die Ausnutzung von Schlupflöchern (Regulierungsarbitrage) zu vermeiden und eine höhere Rechtssicherheit für Unternehmen und Nutzer:innen zu ge-

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024, http://data.europa.eu/eli/reg/2024/1689/oj.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1, http://data.europa.eu/eli/reg/2016/679/oj.

3 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277 vom 27.10.2022, S. 1, http://data.europa.eu/eli/reg/2022/2065/oj.

4 Dies betrifft insbesondere die überarbeitete und nunmehr verabschiedete Produkthaftungsrichtlinie sowie den Vorschlag zu einer KI-Haftungsrichtlinie, siehe dazu etwa Wagner 2023; Hacker 2023; De Bruyne, Dheu und Ducuing 2023; Novelli et al. 2024.

währleisten. Nur so kann sichergestellt werden, dass Innovationen nicht durch unnötige Bürokratie behindert werden, gleichzeitig aber hohe Standards für Grundrechte gewahrt bleiben.

Ziel dieser Studie ist es daher, anhand von Fallbeispielen die rechtlichen Überschneidungen, Lücken und Synergien des AI Act mit bestehenden Regelungen zu untersuchen (Abschnitt II.). Daraus werden übergreifende Erkenntnisse (Abschnitt III.) und schließlich konkrete Handlungsempfehlungen abgeleitet (Abschnitt IV.), die zur Steigerung der regulatorischen Kohärenz, zum proaktiven Schutz von Grundrechten und zur Förderung von Innovation beitragen sollen.

II. AI Act und Digitalgesetze

Wie viele andere Rechtsakte auch, so betont der AI Act eingangs pflichtgemäß, bestimmte verwandte Rechtsakte, so etwa die Datenschutz-Grundverordnung (DS-GVO) und die Teile des Digital Services Act (DSA) zur Haftung der Anbieter von Vermittlungsdiensten, nicht zu berühren. Dass der AI Act sich so lapidar selbst zurücknimmt, löst jedoch die Sachprobleme im Schnittbereich von AI Act und weiterer Digitalregulierung keineswegs; vielmehr wird dadurch lediglich das Spannungsverhältnis zu den genannten und weiteren Rechtsakten offensichtlich. Diesen Überschneidungsbereichen und den sich daraus ergebenden Herausforderungen, aber auch Chancen, wird im Folgenden nachgespürt.

Dabei wird insbesondere auf den DSA und die DS-GVO eingegangen. Ausgespart werden dabei weitestgehend das Haftungsrecht und gänzlich der Digital Markets Act (DMA). Dieser setzt erstens mit wettbewerbsrechtlichen Vorschriften einen deutlich anderen Schwerpunkt, da er nicht auf die Governance von KI abzielt. Zudem betrifft er vor allem Gatekeeper im Bereich E-Commerce und Suchmaschinen. Diese Bereiche sind vom AI Act jedoch gerade nicht als Hochrisiko-Anwendungen ausgewiesen, sodass die Überschneidungen begrenzt sind.

Erwähnt werden sollte zudem, dass der AI Act noch nicht komplett ist. Anders als in den übrigen Digitalgesetzen sollen die Regelungen des AI Act noch weiter konkretisiert werden durch sogenannte technische Standards. Das sind Normen, die durch Expertengremien – angesiedelt etwa bei den europäischen Standardsetzungsorganisationen Comité Européen de Normalisation (CEN) und Comité Européen de Normalisation Électrotechnique (CENELEC) – ausgearbeitet werden. Diese Standards werden gegenwärtig entwickelt und sollen bis spätestens Anfang/Mitte 2026 veröffentlicht sein. Sie bieten z. B. weitere Definitionen von Schlüsselbegriffen oder beschreiben Verfahren und zum Teil auch konkrete quantitative Schwellen, die unbestimmte Rechtsbegriffe für KI-Entwickler und -Anbieter übersetzen und implementierbar machen sollen.

Werden diese Standards eingehalten, so wird vermutet, dass auch die entsprechende Norm des AI Act erfüllt ist (Art. 40 Abs. 1 AI Act). Richtig formuliert, können sie daher eine Art „sicheren Hafen“ (safe harbor) für KI-Entwickler und Anwender bieten. Darauf wird im Rahmen der Handlungsempfehlungen noch zurückzukommen sein.

Safe-Harbor-Mechanismus

Ein Safe-Harbor-Mechanismus ist ein rechtlicher Rahmen, der Unternehmen oder Organisationen Rechtssicherheit in verschiedenen Regulierungsbereichen bietet. Er funktioniert wie folgt:

1. ***Definition:*** Der Gesetzgeber oder eine Regulierungsbehörde legt konkrete Kriterien oder Verhaltensweisen fest.
2. ***Freiwillige Einhaltung:*** Unternehmen können sich freiwillig dazu entscheiden, diese Kriterien zu erfüllen.
3. ***Rechtssicherheit:*** Wenn ein Unternehmen nachweislich alle Kriterien des Safe Harbor erfüllt, gilt es automatisch als rechtskonform in dem betreffenden Bereich.
4. ***Flexibilität:*** Die Nutzung eines Safe Harbor ist optional. Unternehmen können auch auf andere Weise Rechtskonformität erreichen.
5. ***Beispiele:*** Safe-Harbor-Regelungen finden sich in verschiedenen Rechtsbereichen, z. B. im Datenschutz- oder im Kapitalmarktrecht.

Der Vorteil eines Safe Harbor liegt in der Schaffung klarer Leitlinien und der Reduzierung rechtlicher Unsicherheiten. Er bietet einen „sicheren Hafen" für Unternehmen, die sich an die vorgegebenen Regeln halten, schließt aber alternative Wege zur Rechtskonformität nicht aus.

1. Digital Services Act

Der Digital Services Act (DSA) und der AI Act überschneiden sich in verschiedenen Bereichen, jedoch existieren auch deutliche Abgrenzungen und Lücken zwischen den beiden Regelwerken. Dies beginnt schon bei den erfassten Technologien und Systemen.

Während der DSA primär die Pflichten von Onlineplattformen und Onlinesuchmaschinen (insbesondere von Very Large Online Platforms, VLOPs, und Very Large Online Search Engines, VLOSEs) regelt, konzentriert sich der AI Act auf die Regulierung spezifischer Risiko- und Entwicklungskategorien von Künstlicher Intelligenz (z. B. Hochrisiko-KI und KI-Modelle mit allgemeinem Verwendungszweck = General-Purpose AI Models, GPAI). Mit General-Purpose AI meint der AI Act breit einsetzbare Modelle, etwa generative KI-Modelle wie ChatGPT, Claude, Gemini u. Ä.

Auch die Stoßrichtung scheint sich zunächst erheblich zu unterscheiden: Der AI Act adressiert spezifische KI-Risiken wie Intransparenz, Diskriminierung, Unvorhersehbarkeit und Autonomie, stellt Leitplanken für hinreichende Performanz, Robustheit und IT-Sicherheit auf und versucht, Informationsasymmetrien entlang der KI-Wertschöpfungskette sowie zwischen Anbietern und Behörden abzubauen. Dies entspricht dem produktsicherheitsrechtlichen Ansatz, durch spezifische Vorgaben den Markt und die jeweils Betroffenen vor potenziell gefährlichen, qualitativ minderwertigen Produkten zu schützen.

Demgegenüber geht es dem DSA nicht um die Qualität der Plattformen an sich; vielmehr nutzt er diese Intermediäre als Einfallstor, um im gesamtgesellschaftlichen Interesse besseren Zugriff auf illegale oder sonst riskante Inhalte, die auf diesen Plattformen geteilt werden, zu erlangen und deren Verbreitung zu unterbinden. Die eigentlichen Anforderungen an diese Inhalte (vor allem bei Illegalität) finden sich denn auch nicht im DSA selbst, sondern in verschiedenen, zum Teil europäischen, zum Teil nationalen Spezialgesetzen (z. B. Strafgesetzbuch, Jugendschutzrecht).

Beiden Rechtsakten gemein ist jedoch eine stark prozedurale Komponente: Beide halten die jeweiligen Regulierungsadressaten – Plattformen und KI-Anbieter/-Betreiber – dazu an, Compliance-Systeme aufzusetzen, um bestimmte Risiken für Individuen und die Allgemeinheit zu verringern. Dies weist auf einen wichtigen Schnittbereich hin. Denn nach beiden Rechtsakten müssen Risikoanalysen durch die Regulierungsadressaten nicht erst nach Schadenseintritt (ex post), sondern bereits zuvor (ex ante) durchgeführt werden, um entsprechende Maßnahmen zur Minimierung dieser Risiken zu ergreifen – möglichst, bevor sie sich realisiert haben.

a | Zugriffsbereiche: VLOPs/ VLOSEs vs. High-Risk/GPAI

Die Anwendungsbereiche und Ziele der beiden Gesetze sind demnach nicht deckungsgleich. Dennoch ergeben sich Schnittmengen, insbesondere bei hybriden Plattformen, die sowohl als VLOPs/ VLOSEs im Sinne des DSA agieren als auch generative KI in ihre Plattform integrieren. Dies ist ein sowohl wirtschaftlich als auch rechtlich überaus relevantes Phänomen – und in beiden Fällen sind systemische Risikoanalysen verpflichtend.

VLOPs und VLOSEs wie Google, Meta, Microsoft, Linkedin oder X/Twitter[5] nutzen in ihren Diensten schon seit geraumer Zeit klassische KI, um Anfragen von Nutzer:innen zu beantworten und Rankings zu erstellen. In aller Regel bewegen sich diese KI-Applikationen

5 https://digital-strategy.ec.europa.eu/de/policies/list-designated-vlops-and-vloses.

VLOPs und VLOSEs im Digital Services Act (DSA)

Der Digital Services Act führt spezielle Kategorien für sehr große Onlineplattformen (VLOPs) und sehr große Onlinesuchmaschinen (VLOSEs) ein, die besonders strengen Regelungen unterliegen:

1. ***Definition:***
   - VLOPs: Onlineplattformen mit durchschnittlich mehr als 45 Millionen monatlich aktiven Nutzer:innen in der EU
   - VLOSEs: Onlinesuchmaschinen mit durchschnittlich mehr als 45 Millionen monatlich aktiven Nutzer:innen in der EU

2. ***Einstufung:*** Die EU-Kommission benennt Plattformen und Suchmaschinen als VLOPs/VLOSEs basierend auf den gemeldeten Nutzerzahlen. Die Anbieter müssen die Zahlen alle sechs Monate aktualisieren.

3. ***Zusätzliche Pflichten:*** VLOPs/VLOSEs müssen die strengsten Regeln des DSA einhalten, unter anderem:
   - regelmäßige Bewertung systemischer Risiken (Art. 34 DSA)
   - Ergreifen von Risikominderungsmaßnahmen (Art. 35 DSA)
   - Durchführung unabhängiger Compliance-Prüfungen (Art. 37 DSA)
   - Einrichtung einer unabhängigen Compliance-Abteilung (Art. 41 DSA)

4. ***Aufsicht:*** Die EU-Kommission beaufsichtigt die Einhaltung der DSA-Pflichten durch VLOPs/VLOSEs.

5. ***Benannte VLOPs und VLOSEs:*** Die EU-Kommission hat z. B. folgende Dienste offiziell als VLOPs oder VLOSEs eingestuft:
   - VLOPs: Amazon Marketplace, Apple AppStore, Booking.com, Facebook und Instagram, Google Play, Google Maps, LinkedIn, X/Twitter
   - VLOSEs: Bing, Google Search

Der DSA schafft mit den Sonderregeln für VLOPs/VLOSEs einen risikobasierten Regulierungsrahmen, der den besonderen Herausforderungen und Auswirkungen sehr großer Plattformen und Suchmaschinen Rechnung trägt.

jedoch außerhalb des Hochrisiko-Bereichs des AI Act, da dieser E-Commerce und Suchmaschinen grundsätzlich ausspart. In jüngerer Zeit ist jedoch zu beobachten, dass gerade im Bereich der Onlinesuche (search) große Anbieter generative KI in ihre klassische Suchfunktion integrieren. Dies lässt sich etwa beobachten bei Bing, Google oder X (ehemals Twitter). Auch im Rahmen anderer VLOPs werden generative Funktionen zunehmend verbaut, um etwa Posts zu generieren, umzuschreiben oder zu illustrieren (Facebook, LinkedIn). Diese neuen KI-Modelle sind jedoch regelmäßig als generative KI-Technologien (GPAI) im Sinne des AI Act zu qualifizieren, für die dort spezifische Pflichten gelten. Art. 53 AI Act enthält etwa Vorschriften über Transparenz und Urheberrecht für GPAI-Modelle und Art. 55 AI Act ordnet für besonders mächtige GPAI-Modelle etwa die Überprüfung und Verringerung von systemischen Risiken an.

Bei hybriden Plattformen, die neben klassischer auch generative KI nutzen, treffen also die Pflichten des Digital Services Act (DSA) auf die Anforderungen des AI Act, was neue Herausforderungen bei der Einordnung und Regulierung solcher Plattformen mit sich bringt.

b | Systemische Risikoanalyse

Eine zentrale Schnittstelle zwischen dem DSA und dem AI Act ist die Verpflichtung zur Durchführung systemischer Risikoanalysen. Beide Regelwerke sehen vor, dass spezifische Risiken, die durch digitale Plattformen oder KI-Systeme entstehen, regelmäßig identifiziert, bewertet und gemindert werden müssen. Diese Anforderungen sind für hybride Plattformen, die sowohl als große Onlineplattformen im Sinne des DSA (VLOPs/VLOSEs) fungieren als auch KI-Systeme integrieren, besonders relevant.

(1) Systemische Risiken nach AI Act und DSA

Nach dem DSA müssen Very Large Online Platforms (VLOPs) und Very Large Online Search Engines (VLOSEs) systemische Risiken analysieren, die durch die Nutzung ihrer Plattformen entstehen. Zu diesen Risiken zählen unter anderem die Verbreitung illegaler Inhalte, die Unterminierung demokratischer Prozesse durch Falschinformationen, die Beeinträchtigung der Meinungsfreiheit, Gesundheit, öffentlichen Sicherheit oder der Schutz der Privatsphäre der Nutzer:innen (Art. 34 Abs. 1 DSA). Die Plattformbetreiber sind verpflichtet, Maßnahmen zu ergreifen, um diese Risiken zu minimieren und eine regelmäßige Überprüfung der Wirksamkeit dieser Maßnahmen durchzuführen (Art. 35 DSA).

Der AI Act verlangt von den Anbietern von großen generativen KI-Modellen (GPAI mit systemischen Risiken) ebenfalls, systemische Risiken zu identifizieren, zu bewerten und zu reduzieren, die durch den Einsatz solcher KI entstehen (Art. 55 Abs. 1 AI Act).[6] Dies umfasst Risiken für die Gesundheit, Sicherheit und Grundrechte sowie den Umweltschutz. Insbesondere dann, wenn diese Systeme in großem Umfang oder in sensiblen Kontexten verwendet und die Risiken entlang der KI-Wertschöpfungskette weitergereicht werden können, ist die Schwelle zu systemischen Risiken schnell erreicht (Art. 3 Abs. 65 AI Act).

Zwar sind in beiden Fällen sogenannte systemische Risiken betroffen; sie werden jedoch in den Rechtsakten jeweils leicht unterschiedlich akzentuiert. Der DSA legt ein stärkeres Augenmerk auf Informationsfreiheiten, während der AI Act die öffentliche Gesundheit und Sicherheit in den Vordergrund rückt. In beiden Fällen müssen jedoch im Grundsatz alle besonderen, sich aus dem Einsatz der jeweiligen Technologie (große Plattform; KI) ergebenden Risiken für jegliche Grundrechte analysiert werden.

(2) Konsolidierte und technologieübergreifende Risikoanalyse

Bei hybriden Plattformen, die generative KI-Technologien einsetzen (z. B. Bing mit eingebetteter generativer KI, LinkedIn mit KI-verbesserten Posts oder X mit KI-generierten Inhalten), überschneiden sich die Pflichten aus dem DSA und dem AI Act

6 Für Hochrisiko-Anbieter gilt Art. 9 Abs. 1 AI Act, der ähnliche Pflichten vorsieht.

zumindest teilweise. Dabei – und das ist bislang kaum untersucht worden – müsste nach hier vertretener Auffassung im Rahmen der Risikobewertung der einen Technologie dem Umstand Rechnung getragen werden, dass diese mit der jeweils anderen Technologie verknüpft ist.

Die generative KI sollte im Rahmen des AI Act nicht nur auf typische systemische Risiken wie Verzerrungen oder Diskriminierungen in den erzeugten Informationen geprüft werden. Es muss auch berücksichtigt werden, dass solche verzerrten Inhalte oder andere Risiken durch die Verbindung von KI mit großen Plattformen noch ungleich weiterverbreitet werden können. Beispielsweise muss bei der Prüfung systemischer Risiken des KI-Modells, das Bing zugrunde liegt, dem Umstand Rechnung getragen werden, dass dessen Ergebnisse in eine klassische Internetsuche integriert werden.

Umgekehrt sollte im Rahmen des DSA geprüft werden, inwiefern der Einsatz solcher KI-Technologien die systemischen Risiken der Plattform insgesamt beeinflusst, wie z. B. in Bezug auf die Verbreitung falscher Informationen oder den Schutz der Meinungsfreiheit. Dies betrifft etwa den Einsatz von klassischer, besonders aber von generativer KI auf Plattformen wie Facebook, X/Twitter, aber auch LinkedIn.

Diese Verquickungen lassen eine integrative, umfassende Risikoanalyse sinnvoll erscheinen (wechselseitige Risikoanalyse). Eine solche Analyse sollte dreierlei umfassen: 1) die plattformspezifischen Risiken, die der DSA in den Vordergrund rückt, 2) die KI-spezifischen Risiken, die der AI Act adressiert, und 3) zusätzlich die aus der technologischen Verschränkung resultierenden Effekte. So können alle wesentlichen Punkte in einem konsolidierten Prozess gebündelt werden.

Um es noch einmal zu betonen: Besonders wichtig ist im Rahmen dieser wechselseitigen, technologieübergreifenden Risikoanalyse, dass bei der Risikobewertung nach dem DSA die Nutzung von generativer KI berücksichtigt wird, da dies neue systemische Risiken für die Plattform schaffen kann. Umgekehrt muss bei der Risikoanalyse gemäß AI Act ebenfalls die Tatsache einfließen, dass die KI auf einer großen Plattform eingesetzt wird, was die Verbreitung der KI-Ausgaben und deren potenzielle Risiken verstärkt.

Anbieter müssen diese Risiken reduzieren. Die dafür getroffenen Maßnahmen müssen dann diese Verschränkung und ihr Verstärkungspotenzial abbilden. So kann es z. B. nicht genügen, lediglich die Trainingsdatenbasis mit diversen Datenpunkten anzureichern und Filter zu implementieren, um diskriminierende Ergebnisse zu reduzieren; sondern es müssen auch Anstrengungen unternommen werden, die Reichweite derartiger KI-Ergebnisse auf der Plattform zu verringern. Der zumutbare Aufwand, der für das Risikomanagement von KI und Plattform jeweils betrieben werden muss, ist dadurch in aller Regel höher, als wenn die Technologien jeweils isoliert eingesetzt würden (identische KI ohne Plattform oder die identische Plattform ohne generative KI).

Eine solche konsolidierte Analyse würde sicherstellen, dass sowohl die systemischen Risiken der Plattform als auch die durch den Einsatz von KI hervorgerufenen Risiken ganzheitlich bewertet und effektiv gemindert werden.

c | Zugang für Wissenschaftler:innen: Art. 40 Abs. 8 DSA

Ein weiterer zentraler Unterschied zwischen dem Digital Services Act (DSA) und dem AI Act betrifft den Zugang zu Daten und Modellen durch Forscher:innen. Art. 40 Abs. 8 des DSA gewährt Forscher:innen, die einen überprüften Status erhalten (zugelassene Forscher:innen, vetted researchers), ein Recht auf Zugang zu Daten von sehr großen Onlineplattformen (VLOPs) und Suchmaschinen (VLOSEs).[7] Dieser Zugang dient dazu, die Einhaltung der Vorschriften des DSA zu überwachen und systemische Risiken zu analysieren, etwa die Verbreitung illegaler Inhalte, von Falschinformationen oder negative Auswirkungen auf Grundrechte. Diese Regelung stellt, jedenfalls in der Theorie, eine bedeutende Maßnahme zur Erhöhung

7 Siehe auch Harrington und Vermeulen.

der Transparenz und zur Ermöglichung unabhängiger Forschung im Bereich der digitalen Plattformen dar.

Ein vergleichbarer Mechanismus fehlt jedoch im AI Act, der keine expliziten Bestimmungen enthält, die den Zugang zu Daten für die Überprüfung von KI-Systemen durch Forscher:innen regeln. Diese Lücke erschwert es, unabhängige, wissenschaftsgetriebene oder durch die Zivilgesellschaft verantwortete Einsicht in die Funktionsweise von KI-Systemen zu gewinnen. Dies schränkt die Transparenz und die Fähigkeit zur externen Überprüfung von Risiken erheblich ein. Insbesondere könnte dies problematisch sein, da viele hybride Plattformen sowohl als VLOPs/VLOSEs als auch als Anbieter von generativer KI (GPAI) agieren, was eine detaillierte und vom jeweiligen Anbieter unabhängige Risikobewertung für beide Aspekte erfordert.

Eine wichtige Überlegung gerade für hybride Plattformen ist, dass Wissenschaftler:innen die Regelungen des Art. 40 DSA möglicherweise nutzen könnten, um Zugang zu Daten über KI-Systeme zu erhalten, die in diese Plattformen integriert sind. Da diese KI-Systeme, wie oben erwähnt, eng mit den systemischen Risiken der Plattformen verknüpft sind, könnte eine umfassende Risikoanalyse die KI-Daten (Training, Validierung, Output) als notwendiges Element umfassen. So könnte ein Forscherteam die Risikobewertung der Plattform (nach DSA) mit der Bewertung der Risiken der eingesetzten KI (nach AI Act) verbinden und so relevante Einsichten gewinnen. Dies setzt zugleich jedoch erhebliche Ressourcen und Kompetenzen aufseiten (zivilgesellschaftlicher) Forscher:innen voraus, die erst langsam und unter Wahrung ihrer Unabhängigkeit aufgebaut werden müssen.

Es wäre insgesamt sinnvoll, auch die Zugangsmöglichkeiten zu Plattform- und KI-Daten enger zu verzahnen, um eine einheitliche, umfassende Risikoanalyse durchzuführen. Dies würde Forscher:innen und Zivilgesellschaft ermöglichen, nicht nur plattformspezifische Risiken zu bewerten, sondern auch den Einfluss von KI-Technologien auf diese Risiken zu untersuchen. Auch darüber hinausgehende Forschung zur generellen Wirkweise von besonders mächtigen Modellen würde dadurch ermöglicht – bis zur Grenze der legitimen Geschäftsgeheimnisse, auch zur Verhinderung von Industriespionage –, was nicht nur für die KI-Sicherheit, sondern auch die Entwicklung weiterer Systeme und Architekturen bedeutsam wäre.

d | Content Moderation und Art. 55 AI Act

Nach dem AI Act besteht keine ausdrückliche Pflicht zur Moderation von KI-Ausgaben. Im Rahmen des DSA jedoch wird den Anbietern von Hosting-Diensten eine bedeutende Verantwortung bei der Moderation von Inhalten auferlegt. Hosting-Dienste zeichnen sich dadurch aus, dass sie von Nutzer:innen bereitgestellte Informationen speichern. Dies umfasst praktisch alle Plattformen, auf denen Inhalte gespeichert und verbreitet werden können, einschließlich der sehr großen Onlineplattformen (VLOPs). Art. 16 DSA verpflichtet die Anbieter von Hosting-Diensten, Verfahren zur Meldung von rechtswidrigen Inhalten bereitzustellen. Diese Verfahren müssen einfach zugänglich, elektronisch und benutzerfreundlich sein. Zudem wird erwartet, dass gemeldete Inhalte schnell und objektiv geprüft werden.

Schließlich führt Art. 22 DSA den Status der „vertrauenswürdigen Hinweisgeber“ ein, die vorrangig zu behandelnde Meldungen übermitteln können. Diese Funktion zielt darauf ab, das Risiko von systematischen Missständen (z. B. häufige illegale Inhalte, falsche Gesundheitsinformationen) auf Plattformen effizient zu mindern und sicherzustellen, dass Spezialist:innen in ihrem Fachgebiet gezielt auf die Moderation von Inhalten einwirken. Dadurch wird ein dezentrales Monitoring forciert.

Im Gegensatz dazu sieht der AI Act zwar keine spezifischen Verpflichtungen zur Moderation von KI-generierten Inhalten vor. Anbieter und Betreiber von KI-Systemen, insbesondere auch von generativer KI (GPAI), sind nicht ausdrücklich zur Moderation der von ihren Systemen erzeugten Inhalte verpflichtet. Dennoch kann KI in z. T. auch strafrechtlich relevanten Bereichen wie dem Urheberrecht oder dem Äuße-

rungsrecht illegale Inhalte erzeugen. Dies berührt zumindest auch Grundrechte, die im Rahmen von Art. 55 AI Act berücksichtigt werden müssen. Nach hier vertretener Auffassung müssen daher Anbieter von GPAI-Modellen mit systemischen Risiken zumutbare technische und organisatorische Maßnahmen ergreifen, um die Generierung illegaler Inhalte (z. B. rassistische Beleidigungen) bereits auf technischer Ebene zu verhindern. Die technischen und die spezifisch rechtlichen Details müssen jedoch noch genau geklärt und geprüft werden.

Diese proaktive Maßnahme würde darauf abzielen, rechtswidrige oder unter systemisches Risiko fallende Inhalte zu blockieren, bevor sie auf Plattformen verbreitet werden können. Damit könnte das Übel gewissermaßen an der technischen Wurzel gepackt werden: Nicht erst dann, wenn ein KI-generierter, illegaler Post auf einer Plattform erscheint, sondern bereits dann, wenn er generiert werden soll, erfolgt eine technische und organisatorische Risikominderung. Die dafür notwendigen Strategien und Techniken müssten regelmäßig auf den Prüfstand gestellt und überarbeitet werden. Dabei ist sicherzustellen, dass eine übermäßige Moderation weder die Meinungsfreiheit noch die Vielfalt der Perspektiven beeinträchtigt. Dass illegale Posts und Falschmeldungen natürlich auch ohne KI geschrieben werden können, hebt die möglichen Pflichten auf Modellebene keineswegs auf.

Hinzu kommt, dass auch eventuell durch Plattformen zur Moderation von Inhalten eingesetzte KI-Modelle unter Art. 53 und 55 AI Act fallen können. Dies hätte zur Folge, dass umfängliche Informationen über diese Systeme bereitgestellt und Risiken für die Meinungsfreiheit und andere Grundrechte in die Risikoanalyse dieser spezifischen KI-Systeme einbezogen werden müssen.

e | Zwischenergebnis zu AI Act und DSA

Es besteht eine zunehmende Überschneidung zwischen den Pflichten aus dem Digital Services Act (DSA) und dem AI Act, insbesondere bei hybriden Plattformen, die sowohl als sehr große Onlineplattformen (VLOPs/VLOSEs) agieren als auch generative KI-Technologien (GPAI) integrieren. Diese Plattformen müssen sowohl die systemischen Risiken, die aus ihrer Größe und Reichweite resultieren (nach DSA), als auch die spezifischen Risiken durch KI-Systeme (nach AI Act) analysieren und mindern.

Ein zentrales Problem sind die Verknüpfung dieser beiden Technologien und die daraus entstehenden neuen Risiken. Hier ist eine konsolidierte, technologieübergreifende Risikoanalyse angezeigt, die sowohl die plattformspezifischen als auch die KI-spezifischen Risiken und deren gegenseitige Verstärkung einbezieht.

Zusätzlich gibt es eine Diskrepanz zwischen den Regelungen des DSA und des AI Act bezüglich des Zugangs zu Daten für Forscher:innen. Während der DSA Wissenschaftler:innen expliziten Zugang zu Plattformdaten gewährt, fehlt eine solche Bestimmung im AI Act, was die Überprüfung von KI-Systemen erschwert. Ein einheitlicher Zugang zu Daten von Plattformen und KI-Systemen für Wissenschaftler:innen und Zivilgesellschaft wäre notwendig, um unabhängige, dezentrale und umfassende Risikoanalysen zu ermöglichen.

Schließlich besteht eine ausdrückliche Pflicht zur Inhaltemoderation nach dem DSA nur für Hosting-Plattformen. Der AI Act lässt sich aber so interpretieren, dass in Einzelfällen auch als Folge der systematischen Risikoanalyse KI-Ausgaben moderiert werden müssen, wenn dies zur Reduzierung erheblicher Gefahren für Individuen oder demokratische Prozesse erforderlich ist.

2. Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DS-GVO) bietet einen umfassenden Rechtsrahmen für die Verarbeitung personenbezogener Daten durch private und öffentliche Stellen mit Bezug zur EU. Sie bleibt nach Art. 2 Abs. 7 AI Act grundsätzlich unabhängig vom AI Act. Jedoch gibt es mehrere Bereiche, in denen der AI Act die DS-GVO beeinflussen kann.[8] Ein zentraler Aspekt ist die Frage, wie die beiden Regelwerke in der Praxis miteinander interagieren, insbesondere in Bezug auf Interessenabwägungen, Risikobewertungen und Haftungsfragen. Hier werden zunächst allgemeine Auswirkungen des AI Act auf die DS-GVO betrachtet, bevor konkrete Friktionen diskutiert und Lösungswege aufgezeigt werden.

a | Auswirkungen des AI Act auf die DS-GVO

Eine wichtige Schnittstelle betrifft die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO.[9] Demnach können personenbezogene Daten auch dann verarbeitet werden, wenn der Verantwortliche – regelmäßig die Daten verarbeitende Stelle – ein berechtigtes Interesse daran hat und die Grundrechte und Interessen der betroffenen Personen nicht überwiegen. Auch kommerzielle Interessen wie die Nutzung für Werbung können grundsätzlich ein berechtigtes Interesse darstellen.

Geboten ist in jedem Fall eine umfassende Interessenabwägung. In der Literatur wird zu Recht teilweise wie folgt argumentiert: Die Befolgung des AI Act sollte die Interessenabwägung zugunsten, eine Verletzung des AI Act zulasten des Verantwortlichen beeinflussen.[10] Der AI Act indiziert insoweit ein berechtigtes Interesse oder dessen Fehlen. Nach hier vertretener Ansicht geht diese Verknüpfung noch weiter: Eine Verletzung des AI Act führt in der Regel dazu, dass kein legitimes Interesse für die Verarbeitung von Daten durch das rechtswidrige KI-System vorliegt,[11] es sei denn, es handelt sich um eine Verletzung reiner Formvorschriften, wie z. B. Dokumentationspflichten. Anbieter und Betreiber müssen dann vielmehr auf eine wirksame Einwilligung der betroffenen Personen setzen. Die Verletzung des AI Act selbst dürfte, von Ausnahmefällen abgesehen, die Wirksamkeit einer etwaigen Einwilligung jedoch nicht tangieren.[12]

Eine weitere zentrale Schnittstelle betrifft die Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO. Sie sind dann verpflichtend von dem oder den datenschutzrechtlich Verantwortlichen durchzuführen, wenn die Verarbeitung mit einem hohen Risiko für die Rechte der betroffenen Personen einhergeht. Wichtig ist jedoch: Hochrisiko-Anwendungen nach dem AI Act sind nicht deckungsgleich mit Hochrisiko-Anwendungen nach der DS-GVO. Ein Beispiel dafür ist die personenbezogene Profilerstellung (profiling) mithilfe von KI, die nach der DS-GVO fast immer als Hochrisiko-Anwendung eingestuft wird, während es nach dem AI Act nicht zwingend in diese Kategorie fällt. So ist ein KI-basiertes Profiling zu Werbe- oder Empfehlungszwecken grundsätzlich nach der DS-GVO, nicht aber nach dem AI Act als Hochrisiko-Tätigkeit zu verstehen.

Umgekehrt wohnt jedoch Hochrisiko-Applikationen nach dem AI Act häufig zugleich ein hohes Risiko im Sinne von Art. 35 DS-GVO inne.[13] Danach ist eine Datenschutz-Folgenabschätzung verpflichtend, wenn die Datenverarbeitung mit einem hohen Risiko für Betroffene einhergeht. Der AI Act hat eine ähnliche Vorgabe: Betreiber müssen in einer Reihe von Hochrisiko-Fällen – insbesondere, wenn es sich um Behörden, Kreditinstitute oder Versicherungen handelt –

8 Siehe auch Hüger 2024: 263; Engeler und Rolfes 2024: 423; Radtke 2024: 353; Hense 2024: 449; Braegelmann 2024: 39, 41.

9 Siehe etwa Reichert, Radtke und Eske 2024: 483, 485; Hacker 2021: 257, 291 ff.

10 Siehe etwa Hüger 2024: 263, 283 f.

11 Vgl. GA Bobek, Schlussanträge v. 19.12.2018, Rs. C-40/17, Fashion ID, Rn. 122; Hacker 2020: 273.

12 Zu diesem Problemkomplex ausführlich, z. B. der Verletzung der DS-GVO, siehe Hacker 2020: 397 ff.

13 Zu den Kriterien im Einzelnen Hacker 2020: 304; siehe auch Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, Künstliche Intelligenz und Datenschutz, Version 1.0 Rn. 38–40, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

zusätzlich eine Grundrechte-Folgenabschätzung nach dem AI Act durchführen. Allerdings kann eine Grundrechte-Folgenabschätzung im Rahmen des AI Act durchaus in eine Datenschutz-Folgenabschätzung nach der DS-GVO integriert werden, um die Anforderungen beider Regelwerke zu erfüllen.[14]

Ein dritter Überschneidungsbereich betrifft die IT-Sicherheit. Art. 32 der DS-GVO und Art. 15 des AI Act gehen Hand in Hand, da beide von den Verantwortlichen verlangen, geeignete Sicherheitsmaßnahmen zu treffen. Nach Art. 32 DS-GVO müssen Verantwortliche geeignete technische und organisatorische Maßnahmen zur Wahrung der IT-Sicherheit treffen, in Abhängigkeit von den jeweiligen Risiken und dem Stand der Technik. In ähnlicher Weise hält Art. 15 Abs. 5 AI Act fest, dass technische Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen den jeweiligen Umständen und Risiken angemessen sein müssen. Hier kann man also einen Gleichlauf der Kriterien konstatieren.

Ergänzend müssen jedoch auch die Vorschriften der NIS-2-Richtlinie,[15] des geplanten Cyber Resilience Act (CRA)[16] und im Finanzbereich des Digital Operational Resilience Act (DORA)[17] beachtet werden, die zusätzliche Anforderungen an die IT-Sicherheit von manchen KI-Systemen stellen. Hier zeigt sich einmal mehr, dass der AI Act und auch die DS-GVO vom Zusammenspiel mit weiteren Digitalgesetzen leben.

14 Schemmel 2024: 321.

15 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022, S. 80, http://data.europa.eu/eli/dir/2022/2555/oj.

16 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM/2022/454 final.

17 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor, ABl. L 333 vom 27.12.2022, S. 1, http://data.europa.eu/eli/reg/2022/2554/oj.

b | Unterschiedliche Verantwortlichkeiten

Es besteht also eine Reihe von Überschneidungen zwischen dem AI Act und der DS-GVO. Ein erster echter Friktionspunkt zwischen beiden Akten entsteht durch die unterschiedliche Verantwortlichkeit der beteiligten Akteure. Während der Anbieter eines KI-Systems nach dem AI Act die Hauptpflichten trägt, ist nach der DS-GVO in aller Regel der Betreiber der KI-Anwendung der Verantwortliche für die Verarbeitung personenbezogener Daten. Dies führt zu einer unterschiedlichen Adressierung der Pflichten, was zu Unsicherheiten bei der Haftungsfrage führen kann. Wenn ein Fehler in einem Hochrisiko-KI-System auftritt, könnte der Anbieter nach dem AI Act haftbar gemacht werden, während die DS-GVO den Betreiber als Verantwortlichen sieht. Zudem ist etwa für die Durchführung einer Datenschutz-Folgenabschätzung der Verantwortliche zuständig, der dann dafür sorgen muss, dass der Anbieter die dafür erforderlichen Informationen bereitstellt.[18] In bestimmten Fällen kann jedoch auch eine gemeinsame datenschutzrechtliche Verantwortlichkeit vorliegen, sodass sowohl der Anbieter als auch der Betreiber nach der DS-GVO haften.[19] Insgesamt sind die Verantwortungssphären der beteiligten Akteure jedoch nicht aufeinander abgestimmt.

c | Datenerhebung und Reduktion von Bias

Ein weiteres Spannungsverhältnis besteht zwischen der Stoßrichtung des AI Act, Diskriminierung beim Einsatz von KI-Systemen zu reduzieren, und Art. 9 der DS-GVO. Danach dürfen besonders geschützte Daten, etwa zu Alter, Religionszugehörigkeit oder ethnischer Herkunft, gar nicht verarbeitet werden, es sei denn, es liegt eine explizite gesetzliche Ausnahme vor. Diese Regel ist nicht unproblematisch: Denn um Ungleichverteilungen zwischen geschützten Gruppen

18 Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, Künstliche Intelligenz und Datenschutz, Version 1.0 Rn. 40, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf; vgl. a. Art. 25 Abs. 2 AI Act.

19 Dazu ausführlich etwa Gierschmann 2020: 69; Hacker 2020: 130 ff.

im Output zu entdecken und zu beheben, muss man zunächst einmal wissen, welche Individuen überhaupt welcher Gruppe angehören (z. B. Religion, Alter, ethnische Herkunft). Viele dieser geschützten Merkmale sind jedoch zugleich eben sensitive Daten im Sinne von Art. 9 Abs. 1 DS-GVO, deren Verarbeitung grundsätzlich verboten ist. So verhält es sich z. B. gerade bei den Attributen „Religion", „Alter" und „ethnische Herkunft". Zwar enthält Art. 9 Abs. 2 DS-GVO eine Ausnahme für Datenverarbeitungen im öffentlichen Interesse; ob diese jedoch durchweg greift, ist ungeklärt und darf bezweifelt werden.[20] KI-Entwickler, die diese Daten erheben, setzen sich daher einem erheblichen datenschutzrechtlichen Haftungsrisiko aus.[21]

Dies hat der europäische Gesetzgeber erkannt. Der AI Act sieht nun in Art. 10 Abs. 5 zur Erkennung und Verringerung von Verzerrungen in Hochrisiko-KI-Systemen eine Ausnahme für die Verarbeitung sensibler Daten vor. Zugleich müssen Maßnahmen zur Wahrung der datenschutzrechtlichen Interessen der betroffenen Personen getroffen und die Verarbeitung zu Zwecken der Diskriminierungsreduzierung auf das Notwendige begrenzt werden. Diese an sich sinnvolle Ausnahme gilt jedoch nur für Hochrisiko-KI und nicht für generative KI oder Nicht-Hochrisiko-Systeme – obwohl auch hier erhebliches Diskriminierungspotenzial besteht.

d | Datenerhebung und Performanz

Schließlich existiert ein weiterer potenzieller Konflikt zwischen den Performanzanforderungen des AI Act (Art. 15) und den Bestimmungen der DS-GVO (Art. 9). Art. 15 Abs. 1 AI Act fordert für Hochrisiko-Systeme ein „angemessenes Maß an Genauigkeit", wobei Genauigkeit richtigerweise als Performanz bzw. Leistungsfähigkeit i. S. v. technischen Gütemaßen zu lesen ist. Art. 9 DS-GVO hingegen verbietet, wie gerade gesehen, die Nutzung bestimmter Kategorien von sensitiven Daten.

20 Siehe auch Hacker 2021: 257, 294.

21 Siehe auch van Bekkum und Borgesius 2023: 263, 280.

Gesundheitsdatennutzungsgesetz (GDNG)

Inkrafttreten: 26. März 2024

Ziel: Erleichterung der Nutzung von Gesundheitsdaten für Forschung und Verbesserung der Versorgung

Wichtige Punkte: In Deutschland zielt das Gesundheitsdatennutzungsgesetz (GDNG) darauf ab, die Nutzung von Gesundheitsdaten für Forschung und Versorgungsverbesserung zu erleichtern, indem es eine neue Gesundheitsdateninfrastruktur mit einer zentralen Datenzugangs- und Koordinierungsstelle schafft.[1] Das Gesetz ergänzt die DS-GVO, indem es neue Regelungen für Datennutzung, Datenschutz und Forschungsprozesse etabliert. Es ermöglicht eine effizientere Verknüpfung von Gesundheitsdaten und vereinfacht länderübergreifende Forschungsprojekte.[2]

Herausforderungen: Zugleich bleiben etliche Herausforderungen im datenschutzrechtlichen Bereich durch dessen Zersplitterung zwischen verschiedenen Ländern und Krankenhausgesetzen bestehen.[3] Ferner wird die erleichterte Nutzung von Gesundheitsdaten durch Krankenkassen auch ohne Einwilligung der Betroffenen vielfach – nicht ohne Grund – kritisch gesehen.[4]

1 Siehe etwa Rauch, Richters und Naucke 2024: 218.

2 Schneider und Katzenstein 2024: 196.

3 Rauch, Richters und Naucke 2024: 218, 220.

4 Siehe etwa Weichert 2023; Theisen 2024: 54.

Für die Entwicklung leistungsfähiger KI-Modelle, insbesondere im medizinischen Bereich, ist jedoch teilweise die Verarbeitung sensibler Daten notwendig (z. B. Gesundheitsdaten). Die Nutzung solche Daten könnte nach dem AI Act erforderlich sein, um die hinreichende Leistung und auch die Abdeckung diverser Bevölkerungsgruppen durch das KI-Modell zu gewährleisten. Art. 9 DS-GVO verhindert dies jedoch grundsätzlich. Hier sind neue Ansätze notwendig. In Deutschland weist das Gesundheitsdatennutzungsgesetz (GDNG) in diese Richtung. Hier könnte eine Regelung auf europäischer Ebene für erheblichen Fortschritt und Klärung sorgen. Der europäische Gesundheitsdatenraum ist ein erster Schritt in diese Richtung.[22]

e | KI-Training nach der DS-GVO

Tritt man einen Schritt zurück, zeigt sich ein grundsätzliches Problem. Derzeit besteht eine Rechtslücke hinsichtlich der Wiederverwendung personenbezogener Daten zu KI-Trainingszwecken, die durch neue rechtliche Instrumente oder eine Revision bestehender Gesetze geschlossen werden sollte. Insbesondere die Frage, wie personenbezogene Daten unter Berücksichtigung des Datenschutzrechts erneut genutzt werden dürfen, muss in diesem Kontext geklärt werden.[23]

Unter der DS-GVO existiert keine eindeutige Grenze zwischen legaler und illegaler Wiederverwendung von Daten zu KI-Trainingszwecken. Vieles hängt von den konkreten Umständen des Einzelfalls ab.[24] Für eine rechtliche Analyse sind jedoch insbesondere die Art. 6 Abs. 1 lit. f, Art. 6 Abs. 4 und Art. 9 DS-GVO entscheidend. Dazu im Einzelnen:

Gemäß Art. 6 Abs. 1 lit. f DS-GVO ist die Verarbeitung personenbezogener Daten für das Training von KI-Modellen zulässig, wenn die berechtigten Interessen des Verantwortlichen oder Dritter nicht von den Rechten und Interessen der betroffenen Personen überwogen werden. Dabei sind Faktoren wie der Grad der Anonymisierung, die gesellschaftlichen Vorteile des Modells, die Dauer der Datenspeicherung und die Nähe der Daten zu sensiblen Kategorien zu berücksichtigen. Da die nachträgliche Einholung individueller Einwilligungen oft mit unverhältnismäßig hohen Transaktionskosten verbunden wäre, wird Art. 6 Abs. 1 lit. f DS-GVO häufig die zentrale rechtliche Grundlage für das KI-Training mit personenbezogenen Daten darstellen.[25]

Art. 6 Abs. 4 DS-GVO stellt zusätzliche Anforderungen an die sekundäre Nutzung von Daten und beinhaltet einen Kompatibilitätstest, der mehrere Faktoren berücksichtigt. Dies sind unter anderem die Verbindung zwischen der ursprünglichen und der sekundären Nutzung, der Erhebungskontext, die Nähe zu sensiblen Datenkategorien, die Auswirkungen auf die Betroffenen sowie das Vorhandensein von Schutzmaßnahmen wie Verschlüsselung und Pseudonymisierung.

Im Hinblick auf sensible Daten wird es noch komplexer. So existiert unter Art. 9 DS-GVO kein allgemeiner Abwägungstatbestand wie nach Art. 6 Abs. 1 lit. f DS-GVO. Vielmehr ist die Verarbeitung sensibler Daten (z. B. Gesundheitsdaten), wie gesehen, verboten, wenn nicht eine Ausnahme nach Art. 9 Abs. 2 DS-GVO eingreift. Allerdings könnten Entwickler in Fällen, in denen das Training selbst relativ geringe Risiken birgt, ggf. die Ausnahme des öffentlichen Interesses gemäß Art. 9 Abs. 2 lit. g DS-GVO in Anspruch nehmen, etwa wenn das Modell gezielt auf die Förderung rechtlicher Gleichheit und Nichtdiskriminierung ausgerichtet ist.[26] Dies gilt jedoch nur für den Trainingsprozess, nicht für die Anwendung des Modells im Feld, und ist auch für das Training durchaus nicht immer gesichert.

22 Siehe dazu etwa Werry und Ntanas 2024: 641.

23 Siehe etwa die aktuellen Debatten um die Verwendung von Nutzerdaten zu Trainingszwecken durch Plattformen wie X/Twitter oder Meta: Gkritsi 2024; Weatherbed 2024.

24 Hüger 2024: 263, 284.

25 Dies ist z. T. anders im Fall von Plattformen, welche die Daten ihrer Nutzer:innen, mit denen sie ohnehin in vertraglichem Austausch stehen, für KI-Training verwenden wollen. Hier kann die Einwilligung durchaus ein Instrument sein, das jedoch auch keine Pauschallösung bietet, siehe dazu nur die zahlreichen Beiträge zur Kritik des Einwilligungsmechanismus, Überblick etwa in Hermstrüwer 2016: Kapitel 5; Hacker 2020: 577 ff.

26 Hacker 2021: 257, 294.

Für den Fall, dass das KI-Modell lediglich für Forschungszwecke entwickelt wird, bieten Art. 9 Abs. 2 lit. j und Art. 89 DS-GVO den Mitgliedstaaten Spielraum, spezifische Regeln für die Verarbeitung sensibler Daten in der Forschung zu erlassen. So hat etwa der deutsche Gesetzgeber in § 27 BDSG einen spezifischen Abwägungstest für die Verwendung sensibler Daten in Forschungskontexten eingeführt, der allerdings strenger als Art. 6 Abs. 1 lit. f DS-GVO ist.

Zusammenfassend besteht mithin ein klarer Bedarf an einer neuen Bestimmung zur Verarbeitung sensibler und nicht sensibler personenbezogener Daten für das Training von KI, insbesondere im Hinblick auf Art. 6 und 9 DS-GVO.

f | Zwischenergebnis zu DS-GVO und AI Act

Der AI Act und die DS-GVO stehen in einem komplexen Wechselverhältnis zueinander, insbesondere im Hinblick auf Interessenabwägungen, Risikobewertungen und Haftungsfragen. Während die DS-GVO eigenständig bleibt, können Anforderungen des AI Act dennoch wesentliche Auswirkungen auf den Datenschutzrahmen haben. Besonders relevant sind hierbei die Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO, die sich häufig mit den Hochrisiko-Anwendungen des AI Act überschneiden, jedoch nicht deckungsgleich sind. In solchen Fällen wird eine Integration der Risikoabschätzungen beider Regelwerke vorgeschlagen.

Zudem gibt es Spannungen zwischen den beiden Regelwerken, insbesondere hinsichtlich der Verantwortlichkeit der Akteure (Anbieter vs. Betreiber) sowie bei der Verarbeitung sensibler Daten zur Diskriminierungsreduzierung im Rahmen von KI-Anwendungen. Hier besteht Reformbedarf, wie etwa die Ausweitung von Ausnahmen für die Verarbeitung sensibler Daten auf Nicht-Hochrisiko-KI-Systeme, z. B. generative KI (siehe im Einzelnen unten, Abschnitt IV.).

Ganz allgemein besteht ein dringender Bedarf an einem klaren Rechtsrahmen zur Wiederverwendung personenbezogener Daten für KI-Trainingszwecke, da es bislang keine eindeutigen Regelungen dazu gibt.

AI Act und Haftungsrecht

Das digitale Produkthaftungsrecht im Kontext von Künstlicher Intelligenz ist ein komplexes und aktuelles Thema, das durch verschiedene EU-Rechtsakte, wie die neue Produkthaftungsrichtlinie, die geplante AI Liability Directive und den AI Act, geregelt wird.[1]

Verhältnis von AI Act und Produkthaftungsrecht:

- Verletzt ein Unternehmen den AI Act, ist es typischerweise auch nach Produkthaftungsrecht oder Deliktsrecht haftbar.
- Allerdings könnten Unternehmen in Einzelfällen auch trotz Erfüllung des AI Act haftbar sein.
- Dies hätte doppelte, ggf. divergierende Anforderungen an Unternehmen zur Folge.
- Lösungsansatz: Harmonisierung technischer Standards als Safe-Harbor-Regelungen für AI Act und Produkthaftungsrecht

1 Siehe dazu etwa Hacker 2024; Novelli et al. 2024; Wachter 2024: 671; Wagner 2023; Hacker 2023.

III. AI Act und sektorale Regulierung

Der AI Act interagiert nicht nur mit neuen Digitalgesetzen der EU, sondern insbesondere auch mit bestehender sektoraler Regulierung. Dafür wurden spezifische Sektoren in Anhängen zum AI Act ausdrücklich aufgeführt, die zum Großteil bereits jetzt spezifischem Produktsicherheitsrecht unterliegen. Die verschiedenen sektoralen Regulierungen werden in drei verschiedenen Abschnitten erwähnt: sektorale Regulierung von Produkten nach Anhang I Abschnitt A AI Act, nach Anhang I Abschnitt B und nach Anhang III.

Im Folgenden werden stellvertretend drei Sektoren untersucht: Medizinprodukte (Anhang I Abschnitt A), Automotive (Anhang I Abschnitt B) und Finanzprodukte (Anhang III). Eine ganze Klasse von Hochrisiko-Applikationen bezieht sich direkt auf das bestehende Produktsicherheitsrecht (wie in Anhang I Abschnitt A AI Act aufgeführt). Dazu zählen beispielsweise der Bereich der Maschinen, Medizinprodukte und Spielzeuge (unter c). Allerdings sind die Querverbindungen zwischen AI Act und diesen spezifischen Rechtsbereichen trotz Nachbesserungen in der finalen Version des AI Act gegenüber dem ursprünglichen Kommissionsentwurf nur unvollständig ausgeprägt. Dies gilt zumal für Hochrisiko-Systeme aus Anhang III AI Act, die etwa im Bereich der Kreditvergabe und der Versicherung ebenfalls einem komplexen, bereits bestehenden Regulierungsrecht unterliegen (unter b). Deutlich klarer abgegrenzt sind solche Produkte, die dem alten Produktsicherheitsrecht unterfallen und in Anhang I Abschnitt B AI Act aufgelistet sind, etwa aus dem Automotive-Bereich (unter d). Hier gilt vorrangig das spezifische Produktsicherheitsrecht, nicht der AI Act. Bevor diese konkreten Abgrenzungen in den Blick kommen, sollen jedoch allgemeine Formen der Verschränkung von AI Act und sektoraler Regulierung behandelt werden (unter a).

1. Allgemeine Verschränkung

Dass der AI Act überhaupt zusätzlich zu sektoralen Regulierungsinstrumenten angewendet wird, ist insoweit nachvollziehbar, als diese bestehenden sektorspezifischen Akte regelmäßig auf die klassischen Gefahren der jeweiligen Produkte, vor allem für Gesundheit und Sicherheit, nicht aber weitergehende KI-Risiken wie etwa Diskriminierung oder Intransparenz eingehen.

Grundsätzlich betont daher Erwägungsgrund 64 AI Act, dass sektorale Regulierung und AI Act parallel anwendbar sind und die Vorschriften aller Akte erfüllt werden müssen. Zugleich wird eingeräumt, dass Anbieter von Produkten mit Hochrisiko-KI-Systemen, die sowohl dem AI Act als auch weiteren sektoralen Rechtsvorschriften unterliegen, flexibel bei der Umsetzung der Konformitätsanforderungen sein können. Auch haben sektorspezifische Regelungen zur Erforderlichkeit einer neuen Konformitätsbewertung nach einer Änderung des KI-Modells Priorität (EG 84 AI Act). Wird z. B. nur die Verpackung eines Medizinprodukts geändert, so muss nach der Medizinprodukteverordnung (MDR) nicht das Produkt selbst neu bewertet werden. Dieses Ergebnis übernimmt der AI Act. Dies soll unnötigen Verwaltungsaufwand und Kosten vermeiden.

Die Flexibilität betrifft insbesondere die Integration von Test- und Berichterstattungsverfahren in bestehende Dokumentationen und Compliance- sowie Qualitätsmanagementsysteme, solange alle Anforderungen der verschiedenen Rechtsakte erfüllt werden.[27] Erwägungsgrund 158 führt dies für regulierte Kreditinstitute und bestimmte Versicherungen weiter aus. Ferner kann die Kommission „Initiativen, auch sektoraler Art, ergreifen, um den Abbau technischer Hindernisse zu erleichtern, die den grenzüberschreitenden Datenaustausch im Zusammenhang mit der KI-Entwicklung behindern“ (Erwägungsgrund 165 AI Act). Auch die so wichtigen −die Implementierung zentral leitenden − technischen Normen müssen mit den bestehenden, sektorspezifischen Normen kompatibel sein (Art. 40 Abs. 2 AI Act). Diese Verschränkung wird auch aufsichtsrechtlich nachvollzogen, indem grundsätzlich die sektorale Marktüberwachungsbehörde auch für die Einhaltung des AI Act zuständig ist (Art. 74 Abs. 3 UAbs. 1 AI Act). So wird in Deutschland wohl die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die Aufsicht über Finanzprodukte auch nach dem AI Act zuständig sein. Die Mitgliedstaaten können von dieser Regel zugunsten sektoraler Behörden zwar abweichen, doch dann muss eine enge Koordination zwischen der zentralen Marktüberwachungsbehörde und den sektoralen Behörden sichergestellt sein (Art. 74 Abs. 3 UAbs. 2 AI Act). Dies gilt auch für die jeweiligen Verfahrensordnungen, mithin die Art und Weise, wie die Behörden ihre Aufgaben ausüben und wie Betroffene ihre Rechte geltend machen können (Art. 74 Abs. 4 AI Act).

Ein genauer Blick auf die betroffenen Sektoren zeigt jedoch, dass signifikante Abgrenzungsprobleme fortbestehen. Dies wird im Folgenden anhand von Beispielen aus dem Finanzbereich (Anhang III), der Medizinprodukte (Anhang I Abschnitt A) sowie Automotive (Anhang I Abschnitt B) exemplarisch erörtert.

2. Finanzprodukte

Finanzprodukte sind nicht grundsätzlich der Hochrisiko-Kategorie des AI Act zugeordnet. Vielmehr betrifft dies nach Anhang III Nr. 5 AI Act lediglich Systeme, die

- zur Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen oder
- bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen.

Kreditbewertungssysteme, die auf statistischen Modellen, Heuristiken und KI-basierten Entscheidungsprozessen beruhen, sind also explizit als Hochrisiko-Anwendungen im AI Act klassifiziert (Anhang III Ziff. 5 lit. b AI Act). Zwar fallen Einsätze von KI-Systemen, die lediglich vorbereitende Maßnahmen umfassen, aus den Hochrisiko-Kategorien des Anhangs III wieder heraus (Art. 6 Abs. 3 AI Act). Kreditscores fließen jedoch regelmäßig maßgeblich in die Kreditentscheidung ein, was der EuGH richtigerweise in der SCHUFA-Entscheidung klargestellt hat,[28] sodass diese KI-Systeme nicht unter die genannte Ausnahme fallen.[29] Daher unterliegen diese Systeme den Hochrisiko-Anforderungen des AI Act in Bezug auf Datenqualität, Transparenz und Überwachung. Dies betrifft sowohl traditionelle Banken als auch Fintech-Unternehmen, die zunehmend KI-gestützte Kreditentscheidungen treffen. Dabei ist entscheidend, dass der KI-Begriff des AI Act sehr breit ist und neben avancierten Modellen auch klassische Methoden des maschinellen Lernens erfasst, die zum Teil bereits seit Jahrzehnten in der Finanzwirtschaft genutzt werden, etwa statistische Modellierung, lineare oder logistische Regression.[30] Dasselbe gilt für Bonitätsbewertungssysteme.

27 Siehe auch EG 81 und Art. 9 Abs. 10, Art. 11 Abs. 2 sowie Art. 17 Abs. 3 AI Act.

28 EuGH, Rs. C-634/21, SCHUFA, Rn. 75.

29 Radtke 2024: 353, 359 f.

30 Siehe etwa Hacker 2024: 10; Woesch und Vogt 2024: 689, 691.

Eine Ausnahme stellt die Nutzung von KI-Systemen zur Betrugserkennung dar. Während Kreditbewertungssysteme streng reguliert werden, sind KI-Systeme, die ausschließlich zur Erkennung von Finanzbetrug eingesetzt werden, von den Hochrisiko-Bestimmungen des AI Act ausgenommen. Dem Wortlaut von Anhang III zufolge betrifft dies allerdings nur Erkennungssysteme im Bereich der Kredit- und Bonitätsbewertung. Man wird diese Ausnahme jedoch, da ein sachlicher Differenzierungsgrund nicht ersichtlich ist, auch analog auf die Betrugsbekämpfung im Bereich der Lebens- und Krankenversicherungen anwenden müssen.

Bei der Regulierung dieser Aktivitäten durch den AI Act kommt es jedoch zu verschiedenen Konflikten und Unstimmigkeiten mit bestehenden bank- und versicherungsrechtlichen Vorschriften.[31] Der Fokus liegt im Folgenden auf der Koordination mit dem Bankenrecht; ähnliche Erwägungen gelten jedoch auch für das Versicherungsrecht.[32]

a | Teilweise Integration

Einige Regelungen des AI Act sind mit den Anforderungen des bestehenden Finanzaufsichtsregimes kompatibel und durchaus verzahnt, wie bereits die allgemeinen Erwägungen oben zeigten. Art. 9 AI Act beispielsweise behandelt das Risikomanagement, ein Bereich, der seit geraumer Zeit ebenfalls durch das Bankrecht geregelt ist. Finanzinstitute sind schon jetzt verpflichtet, interne Kontroll- und Risikomanagementsysteme zu implementieren, um die sichere Verwendung von KI-Systemen zu gewährleisten. Ebenso fordert Art. 17 AI Act ein Qualitätsmanagementsystem von Hochrisiko-AI-Systemen, was in der Finanzbranche ebenfalls bereits geregelt ist.

Daher verweist Art. 9 Abs. 10 AI Act richtigerweise darauf, dass regulierte Kreditinstitute, wie auch andere sektoral regulierte Entitäten, die bestehenden Risikomanagementsysteme mit dem nach dem AI Act geforderten System kombinieren dürfen. In Deutschland werden die Anforderungen an das bankseitige Risikomanagementsystem durch zwei zentrale Mechanismen näher bestimmt: einerseits im Bereich der IT-Sicherheit den DORA (Digital Operational Resilience Act)[33] und andererseits ein mehrfach novelliertes Rundschreiben der BaFin (Mindestanforderungen an das Risikomanagementsystem, MaRisk).[34] Letzteres beruht auf gesetzlichen Vorgaben[35] sowie entsprechenden Leitlinien der Europäischen Bankenaufsicht und gilt ausdrücklich auch bei Verwendung von KI.[36] Vor allem die seit der letzten Novelle aufgenommene KI-Erweiterung der Modellvalidierung bietet große Überschneidungen mit der unter dem AI Act erforderlichen Konformitätsbewertung, also dem Testen der KI im Hinblick auf die Erfüllung der Vorgaben aus dem AI Act. Das nächste Update der MaRisk sollte daher möglichst klar die Verschränkung von bankaufsichtsrechtlichen Vorgaben und jenen des AI Act explizieren.

Art. 17 Abs. 4 AI Act geht sogar noch weiter: Er sieht vor, dass die Pflicht zur Einrichtung eines Qualitätsmanagementsystems für regulierte Finanzdienstleister, mit wenigen Ausnahmen, durch ein rechtskonformes Qualitätsmanagementsystem im Sinne des Finanzdienstleistungsrechts als erfüllt gilt. Es müssen lediglich noch die Komponenten des entsprechend neu aufgestellten Risikomanagements, des Marktbeobachtungssystems und des Systems zur Meldung von schweren Verstößen, die jeweils nach dem AI Act erforderlich sind, integriert werden.

31 Siehe dazu etwa Eber und Hacker (i. E.); Feldkamp et al. 2024: 60; Woesch und Vogt 2024: 689.

32 Siehe etwa Marano und Li 2023: 12.

33 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor, ABl. L 333 vom 27.12.2022, S. 1, http://data.europa.eu/eli/reg/2022/2554/oj.

34 BaFin, Rundschreiben 06/2024 (BA) vom 29.5.2024, Mindestanforderungen an das Risikomanagement – MaRisk, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_06_2024_MaRisk_pdf_BA.html.

35 Art. 97 Abs. 1 CRD IV, § 25a Abs. 1 KWG.

36 MaRisk, AT 4.3.5, Rn. 1.

Art. 17 Abs. 4 AI Act – Harmonisierung mit sektoraler Regulierung

Art. 17 Abs. 4 AI Act ist ein Paradebeispiel für die Harmonisierung zwischen dem AI Act und bestehenden sektoralen Regulierungen:

1. ***Grundprinzip:*** Finanzinstitute, die bereits Anforderungen an interne Governance, Arrangements oder Prozesse nach EU-Finanzdienstleistungsrecht unterliegen, gelten für einen Großteil der Qualitätsmanagementanforderungen des AI Act als konform.

2. ***Abgedeckte Bereiche:*** Die meisten Aspekte des Qualitätsmanagementsystems nach Art. 17 Abs. 1 werden durch bestehendes Finanzrecht erfüllt.

3. ***Zusätzliche AI-Act-Anforderungen:*** Drei spezifische Bereiche müssen Finanzinstitute zusätzlich implementieren:
   - Risikomanagementsystem (Art. 17 Abs. 1 Punkt g)
   - Post-Market-Überwachungssystem (Art. 17 Abs. 1 Punkt h)
   - Vorfallberichterstattungssystem (Art. 17 Abs. 1 Punkt i)

4. ***Klare Abgrenzung:*** Der Artikel schafft Rechtssicherheit, indem er präzise definiert, welche Anforderungen durch bestehende Regulierungen erfüllt sind und welche zusätzlich umgesetzt werden müssen.

5. ***Einschränkung:*** Diese klare Harmonisierung ist bisher auf das Qualitätsmanagementsystem im Finanzbereich beschränkt. Für andere Anforderungen des AI Act oder andere Sektoren fehlen ähnlich detaillierte Regelungen.

Diese Regelung zeigt also, wie sektorübergreifende und sektorspezifische Regulierungen effektiv harmonisiert werden können, um Doppelregulierungen zu vermeiden und gleichzeitig spezifische KI-Risiken abzudecken.

Art. 17 Abs. 4 AI Act hat damit Vorbildcharakter: Der Absatz ist ein Beispiel für eine gelungene Verzahnung, da spezifisch und sehr konkret geregelt ist, welche Teile des AI Act durch bestehendes Regulierungsrecht automatisch erfüllt werden und welche Maßnahmen darüber hinaus noch getroffen werden müssen. Leider ist diese Vorschrift auch die einzige im AI Act, die eine derartige Klarheit und Präzision hinsichtlich der sektoralen Verschränkung bietet.

b | Lücken und potenzielle Doppelregelungen

Bekannt ist, dass der AI Act neue Anforderungen einführt, die über die bisherigen bankrechtlichen Vorschriften hinausgehen bzw. diese zum Teil auch doppeln. Ein zentrales Beispiel hierfür ist die Datengovernance. Art. 10 AI Act legt strenge Standards für die Qualität der verwendeten Daten fest. Unternehmen müssen sicherstellen, dass die Trainingsdaten ihrer KI-Systeme vollständig, fehlerfrei, repräsentativ und nicht diskriminierend sind.

Diese Anforderungen ergänzen bestehende Vorgaben aus dem Bankaufsichtsrecht. Die Capital Requirements Directive IV 2013/36/EU (CRD IV) legt in Art. 76 CRD IV fest, dass Finanzinstitute robuste Risikomanagementsysteme benötigen, die auf hochwertigen und regelmäßig überprüften Daten basieren. Ein weiteres zentrales Instrument des Bankrechts wiederum, die Capital Requirements Regulation (EU) Nr. 575/2013 (CRR), fordert von Finanzinstituten die Verwendung qualitativ hochwertiger, vollständiger und aktueller Daten zur Berechnung und Modellierung von Risiken. Art. 185 CRR

verpflichtet Banken, die Qualität der Scoring-Modelle („Genauigkeit und Konsistenz“) für interne Ratings und Risikobewertungen kontinuierlich zu überprüfen. Dies geschieht unter anderem durch ein fortlaufendes Monitoring der Funktionsweise dieser Modelle. Darüber hinaus legt Art. 174 CRR fest, dass statistische Modelle und „andere mechanische Methoden“ zur Risikobewertung eine hohe Vorhersagekraft haben müssen (Buchstabe a). Die Eingabedaten müssen wiederum auf ihre Genauigkeit, Vollständigkeit, Angemessenheit und Repräsentativität überprüft werden (Buchstaben b, c). Zudem müssen die Modelle regelmäßig validiert (Buchstabe d) und unter menschlicher Aufsicht betrieben werden (Buchstabe e).

Somit zeigt sich, dass die Vorgaben von Art. 174 CRR und Art. 10 AI Act weitgehend identisch sind, sogar teilweise dieselben Begriffe verwenden (Vollständigkeit, Repräsentativität). Es fehlt jedoch an einer Norm, die wie Art. 17 Abs. 4 AI Act genau regeln würde, welche Elemente von Art. 10 AI Act als durch Art. 174 CRR abgedeckt gelten sollen und welche nicht. Man wird bei vergleichender Betrachtung jedoch feststellen können, dass vor allem die Verpflichtung, Verzerrungen in Trainingsdaten zu minimieren (Art. 10 Abs. 2 lit. g AI Act), durch Art. 174 CRR jedenfalls nicht ausdrücklich abgebildet wird, auch wenn man dies in die allgemeinen Qualitätsanforderungen hineinlesen kann.[37] Insgesamt lässt sich damit sagen, dass die Erfüllung von Art. 174 CRR in der Regel dazu führen sollte, dass die zentralen, im AI Act festgehaltenen Datenqualitätsmerkmale wie Repräsentativität, Relevanz, Fehlerfreiheit, Vollständigkeit, statistische Geeignetheit und ggf. auch die Minimierung von Verzerrungen ebenfalls erfüllt werden.

Zusätzlich gibt es im AI Act jedoch auch neue Verpflichtungen, z. B. in Bezug auf Transparenz und Dokumentation. Finanzunternehmen, die Hochrisiko-KI-Systeme wie Kreditbewertungssysteme einsetzen, müssen umfangreiche Dokumentationen führen und sicherstellen, dass eine geeignete menschliche Aufsicht über diese Systeme gewährleistet ist. Diese Anforderungen führen ggf. zu einer zusätzlichen Belastung, da Finanzinstitutionen bereits bestehenden Dokumentations- und Transparenzanforderungen unterliegen. Hier hilft lediglich der bereits erwähnte 64. Erwägungsgrund des AI Act, wonach insbesondere Dokumentationspflichten aus mehreren Rechtsakten kombiniert und flexibel gehandhabt werden dürfen, solange insgesamt alle Pflichten erfüllt werden. Die MaRisk weist bereits jetzt darauf hin, dass Modelle, insbesondere wenn sie mit KI operieren, eine hinreichende Erklärbarkeit aufweisen müssen.[38]

Auch in Bezug auf Gütemaße und Cybersicherheit schafft der AI Act zusätzliche Vorgaben (Art. 15 AI Act). Wie schon erwähnt, muss nach Art. 15 Abs. 1 AI Act ein angemessenes Maß an Leistung i. S. v. technischen Gütemaßen eingehalten werden; und die Cybersicherheit muss, wie ebenfalls erwähnt, risikoadäquat sein. Banken müssen nicht nur die bereits bestehenden Sicherheitsvorkehrungen einhalten, sondern zudem die vom AI Act geforderten Anforderungen an Robustheit und IT-Sicherheit erfüllen. Auch diese dürften sich jedoch weitgehend mit den bestehenden Vorgaben des Bankenrechts decken.[39] So fordert z. B. Art. 174 lit. a CRR bereits jetzt eine gute Prognosefähigkeit der eingesetzten Modelle und der DORA enthält sehr spezifische Regeln zur erforderlichen IT-Sicherheit.

Der Mangel an expliziter Koordination zwischen den sektoralen Vorschriften des Bankensektors und den neuen Regelungen des AI Act führt zu regulatorischen Doppelungen, die gesetzestechnisch nicht gelöst wurden. Finanzinstitutionen müssen daher in weiten Bereichen gewissermaßen einen „educated guess“ vornehmen, inwiefern die Vorgaben des AI Act ggf. über einzelne Anforderungen des Bankenrechts hinausgehen. Dass dies ein unbefriedigender Zustand ist, liegt auf der Hand.

37 Das Modell darf nach Art. 174 lit. a CRR keine wesentlichen systematischen Fehler enthalten, wozu man diskriminierende Verzerrungen durchaus zählen kann.

38 MaRisk, AT 4.3.5, Rn. 6.

39 Siehe dazu etwa MaRisk, AT 4.3.5, Rn. 5 (Stabilität) und AT 7.2 (IT-Sicherheit) sowie den DORA.

c | Zwischenergebnis zu Finanzprodukten

Die Einführung des AI Act führt zu einem komplexen Spannungsfeld zwischen den neuen Anforderungen an Hochrisiko-AI-Systeme und den bereits bestehenden bankrechtlichen Vorschriften. Während in einigen Bereichen eine Integration erreicht wird, bestehen in anderen wesentliche Lücken und Doppelregelungen, die für Finanzinstitute Herausforderungen darstellen. Diese hätten durch klarere Verweise und Abgrenzungen relativ einfach, ohne Verlust an Grundrechtsschutz, vermieden werden können. Besonders betroffen sind Kreditbewertungssysteme und Versicherungsprodukte im Bereich Leben und Gesundheit, die sich künftig weiteren und zum Teil möglicherweise strikteren Vorschriften unterwerfen müssen. Trotz einiger Ausnahmen, wie bei Betrugserkennungssystemen, wird der AI Act das regulatorische Umfeld für viele Finanzprodukte erheblich verändern.

3. Medizinprodukte

Die Finanzbranche ist nicht die einzige, die durch den Erlass des AI Act mit einer weiteren, horizontalen Regulierungsschicht konfrontiert wird. Gleiches gilt für die Nutzung von Künstlicher Intelligenz (KI) im medizinischen Bereich. Die Integration von KI in Medizinprodukte führt zu Abgrenzungsschwierigkeiten zwischen der Medizinprodukteverordnung (EU) 2017/745 (MDR) und dem AI Act.[40] Dies ist besonders relevant, da beide Verordnungen verschiedene Risikobewertungen verfolgen. Aufgrund der internationalen Reichweite des AI Act wird er praktisch alle 690 in den USA bei der Food and Drug Administration (FDA) zugelassenen Anbieter von Medizinprodukten betreffen – und damit auch praktisch alle, die in der EU aktiv sind.[41] Ein besseres Verständnis der Konflikte lässt sich anhand spezifischer Beispiele wie der Krebsdiagnose, der Erstellung von Arztbriefen und der Verwaltung des Terminkalenders einer Ärztin oder eines Arztes erzielen.

a | Allgemeine Konflikte zwischen MDR und AI Act

Die Medizinprodukteverordnung (MDR) und der AI Act verfolgen komplementäre, aber nicht deckungsgleiche Ziele: Die MDR konzentriert sich primär auf die Sicherheit und Effektivität von Medizinprodukten, während der AI Act weitergehend die Risiken von KI-Systemen minimieren soll, insbesondere auch in Bezug auf Diskriminierung, Intransparenz und IT-Sicherheit. Ein zentraler Bestandteil der MDR ist die Nutzen-Risiko-Abwägung (Art. 61 Abs. 1 und Art. 2 Abs. 24 MDR). Letztlich werden damit sowohl die Risiken als auch die möglichen positiven Effekte als Medizinprodukt in den Blick genommen und in ein Verhältnis gebracht. Nur wenn der Nutzen das Risiko überwiegt, wird das Medizinprodukt zugelassen. Eine derartige Abwägung nicht nur der Risiken, sondern auch der Chancen sieht der AI Act nicht explizit vor. Zwar mag man diese in manche unbestimmte Rechtsbegriffe hineinlesen können (z. B. „angemessenes Maß an Genauigkeit“, Art. 15 Abs. 1 AI Act; „geeignete Maßnahmen“, Art. 10 Abs. 2 AI Act), es offenbart sich jedoch eine erhebliche Differenz in der Methodik der Bewertung.

Zwar gelten auch hier die oben angesprochenen allgemeinen Verschränkungen und Lockerungen, insbesondere mit Blick auf das Risikomanagementsystem. Wie im Finanzbereich sind jedoch zahlreiche weitere Vorschriften nicht mit der sektoralen Regulierung im medizinischen Bereich verknüpft. Dies führt hier ebenso zu potenziellen Überschneidungen und Doppelregulierungen bei Produkten, die sowohl unter die MDR als auch unter den AI Act fallen. Ein zentrales Problem ist die Frage, welche Anforderungen Vorrang haben, wenn ein KI-System gleichzeitig als Medizinprodukt und als Hochrisiko-KI eingestuft wird.

40 Zusätzlich gelten noch die EU In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR) und die Clinical Trials Regulation (EU) No 536/2014 (CTR), die hier aber außen vorgelassen werden; siehe auch Onitiu, Wachter und Mittelstadt 2024.

41 Aboy, Minssen und Vayena 2024: 2.

b | Beispiel 1: Krebsdiagnose

Ein KI-System, das zur Krebsdiagnose eingesetzt wird, zeigt deutlich die Abgrenzungsschwierigkeiten zwischen beiden Verordnungen. Die Medizinprodukteverordnung (MDR) kennt drei zentrale Risikoklassen: Klasse III (potenzielle Auswirkung: Tod des Patienten); Klasse II (direkte Auswirkung auf diagnostische oder therapeutische Entscheidungen, mit Unterklassen IIb – potenziell schwerwiegende Verschlechterung des Gesundheitszustands – und IIa – nur Diagnostik/Therapie) – sowie Klasse I (Rest). Unter der MDR fällt ein solches Krebsdiagnosesystem typischerweise in die Risikoklasse IIa oder bei Verknüpfung mit Effektoren sogar IIb und höher, da es dann eine direkte Auswirkung auf diagnostische und therapeutische Entscheidungen hat und potenziell eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person hervorrufen kann (Anhang VIII Kapitel 3 Regel 11 MDR).[42]

Der AI Act behandelt solche Systeme ebenfalls als Hochrisiko-KI-Systeme nach Art. 6 Abs. 1 AI Act.[43] Dies führt zu einer gewissen Doppelregulierung, da sowohl die MDR als auch der AI Act strenge Anforderungen an Qualitätsmanagement, Risikomanagement und technische Dokumentation stellen.

Sehr punktuell wurden Vorrangregelungen eingeführt, nach denen die MDR Priorität hat. Dies betrifft etwa die Frage, ob Änderungen an einem KI-System eine erneute Konformitätsprüfung notwendig machen. In diesem Fall legt der 84. Erwägungsgrund des AI Act fest, dass die Medizinprodukteverordnung entscheidet, wie dies zu bewerten ist. Sofern danach keine neue Prüfung erforderlich ist (z. B. Art. 16 Abs. 2 MDR), verlangt auch der AI Act diese nicht. Ferner können die Qualitätsmanagementsysteme nach AI Act und MDR ineinander integriert werden (Art. 17 Abs. 3 AI Act). Anders als im Bereich der Finanzmarktregulierung fehlen hier jedoch die spezifischen, detaillierten Verschränkungen wie in Art. 17 Abs. 4 AI Act, die lediglich Finanzinstituten, nicht aber den Herstellern von Medizinprodukten zugutekommen.

Diese Doppelregulierung kann zu erheblichen bürokratischen Hürden führen, insbesondere für kleine und mittelständische Unternehmen (KMU), die mit den Anforderungen beider Verordnungen konfrontiert sind. Sie müssen nicht nur die MDR-konforme technische Dokumentation bereitstellen, MDR-konforme Sicherheitsmechanismen testen und einpflegen, sondern auch den zusätzlichen Anforderungen des AI Act, wie z. B. der erweiterten Dokumentationspflicht,[44] der automatischen Protokollierung von Ereignissen, der spezifischen Datengovernance und der Nachverfolgbarkeit, gerecht werden. Durch bessere Aufteilung und Abstimmung der Anforderungen hätte sich hier unnötige Doppelarbeit vermeiden lassen.

Die technischen Dokumentationen nach MDR und AI Act können zwar verbunden werden (Art. 11 Abs. 2 AI Act); dennoch sind deutlich mehr Informationen nach dem AI Act als nach MDR notwendig. Immerhin ist für KMU eine vereinfachte Dokumentation geplant, nach einem Formular der Kommission (Art. 11 Abs. 1 UAbs. 2 AI Act). Da jedoch Anbieter von Medizinprodukten, insbesondere KMU, bereits mit der Implementierung der MDR signifikante Probleme haben,[45] nicht zuletzt aufgrund eines Engpasses an Konformitätsbewertungsstellen,[46] wird die Operationalisierung der zusätzlichen AI-Act-Vorgaben – so sinnvoll sie auch im Einzelfall seien mögen – angesichts fehlender Abgrenzungsnormen für viele Unternehmen eine erhebliche Herausforderung darstellen. Auch hier gilt: Eine klare Abgrenzung vermindert diese, ohne den Grundrechtsschutz für Betroffene anzutasten.

42 Siehe auch Onitiu, Wachter und Mittelstadt 2024: 5 Fn. 17 und 6 Fn. 19, die ein „advanced imaging tool for prediction and diagnosis" als Produkt der Risikoklasse IIa einordnen. Diese Feinheiten (IIa oder IIb) spielen für die Abgrenzung zum AI Act jedoch keine Rolle.

43 In Verbindung mit Anhang I Abschnitt A Nr. 11.

44 Aboy, Minssen und Vayena 2024: 2.

45 Carl und Hochmann 2023.

46 Aboy, Minssen und Vayena 2024: 4.

c | Beispiel 2: Arztbriefe

Ein KI-System, das zur Erstellung von Arztbriefen verwendet wird, verdeutlicht die Problematik der Abgrenzung zwischen administrativen und medizinischen Funktionen. Unter der Medizinprodukteverordnung (MDR) würde ein solches System wohl nicht als Hochrisiko-System eingestuft, da es keine direkte Auswirkung auf Diagnose oder Therapie hat (Anhang VIII Kapitel 3 Regel 11 MDR). Es fällt daher eher in die Klasse I, die nur eine geringe regulatorische Kontrolle erfordert. In dem Fall ist eine Selbstzertifizierung möglich.[47]

Der AI Act folgt zunächst dieser Beurteilung: Wenn keine Zertifizierung durch externe Stellen nach der sektoralen Regulierung notwendig ist – z. B. weil die KI lediglich unterstützende Funktionen übernimmt, ohne in diagnostische Entscheidungen einzugreifen –, gilt sie grundsätzlich nicht als Hochrisiko-KI-System nach dem AI Act.[48] Insoweit ergeben sich weitere Anforderungen daher nur aus den Transparenzpflichten des Art. 50 AI Act und dem Erfordernis, für KI-Kompetenz aller Beteiligten nach Art. 4 AI Act zu sorgen. Dies erscheint durchaus sachgerecht.

Die Herausforderung liegt hier jedoch darin, sicherzustellen, dass der Einsatz der Arztbrief-KI nicht indirekt in medizinische Entscheidungen eingreift. Damit entsteht ein Graubereich, in dem Hersteller nachweisen müssen, dass die KI keine wesentlichen medizinischen Entscheidungsprozesse beeinflusst. Dies führt letztlich zu Unsicherheiten in der Einstufung nach MDR und AI Act, die allerdings bei möglichen diagnostisch oder therapeutisch relevanten Vorgängen auch gerechtfertigt sein dürften.

d | Beispiel 3: Terminkalender und Triage

Ein KI-gestützter Terminkalender stellt nur ein minimalinvasives Modell dar. Solche Systeme fallen weder unter die MDR als Hochrisiko-Medizinprodukte noch unter den AI Act als Hochrisiko-KI-Systeme, da sie keinen Einfluss auf medizinische Entscheidungen haben. Sie gelten daher als Systeme mit begrenztem Risiko, die nur geringfügige regulatorische Anforderungen erfüllen müssen (Transparenz und KI-Kompetenz).

Allerdings könnten weitere Anforderungen entstehen, wenn der Terminkalender beispielsweise mit einem Algorithmus ausgestattet ist, der eine automatische Priorisierung basierend auf medizinischen Daten vornimmt. In einem solchen Fall wäre denkbar, dass sowohl MDR als auch, dem folgend, der AI Act zusätzliche Anforderungen vorsehen. Sofern eine Triage bei der Notfallversorgung vorgenommen wird (nicht aber im regulären Betrieb), ordnet der AI Act die KI gar selbstständig als Hochrisiko-KI ein (Anhang III Nr. 5 lit. d AI Act) – in aller Regel wird sie aber auch ein Produkt der Klasse II nach der MDR darstellen. Dies unterstreicht, dass selbst bei auf den ersten Blick nicht diagnostischen/therapeutischen Systemen die Abgrenzung zwischen den Risikoklassen und Verordnungen komplex sein kann.

e | Zwischenergebnis für Medizinprodukte

Die Beispiele der Krebsdiagnose, der Arztbriefe und des Terminkalenders verdeutlichen die Schwierigkeiten bei der Abgrenzung der Medizinprodukteverordnung (MDR) und des AI Act. Während bei Systemen mit direkter medizinischer Relevanz, wie der Krebsdiagnose, eine klare Hochrisiko-Einstufung nach beiden Verordnungen erfolgt, sind bei administrativen Systemen wie Arztbriefen oder Terminkalendern differenzierte Betrachtungen notwendig. Die potenziellen Überschneidungen und Zusatzanforderungen nach dem AI Act führen zwar zu einem erhöhten Aufwand für Hersteller, die sicherstellen müssen, dass ihre Produkte sowohl den medizinrechtlichen als auch den KI-spezifischen Anforderungen gerecht werden; sie sind jedoch angesichts der im Medizinbereich vorherrschenden Risiken grundsätzlich sinnvoll. Dennoch wäre es wünschenswert, dass genau benannt wird, welche Kriterien nach dem AI Act effektiv noch zusätzlich erfüllt werden müssen.

47 Aboy, Minssen und Vayena 2024: 4.

48 Siehe Art. 6 Abs. 1 lit. b AI Act; anders aber Aboy, Minssen und Vayena 2024: 4.

Angesichts der bereits jetzt bestehenden Engpässe bei der Zulassung von Medizinprodukten müssen jedoch vor allem die Kapazitäten der Konformitätsbewertungsstellen dringend und schnell erhöht werden, um die erwartbare Menge an neuen Systemen zu bewältigen und verantwortungsvolle medizinische KI auch in Deutschland und Europa nach vertretbarer Prüfdauer für den Einsatz freizugeben.

4. Automotive

Der AI Act hat schließlich auch Auswirkungen auf den Automobilbereich, insbesondere auf autonome Fahrsysteme. Die Hochrisiko-Bestimmungen des AI Act gelten zwar nicht unmittelbar für den Automobilbereich, da dieser in wesentlichen Teilen ausdrücklich ausgenommen wird (Art. 2 Abs. 2 in Verbindung mit Art. 6 Abs. 1 und Anhang I Abschnitt B AI Act). Die Idee hinter dieser Ausnahme ist nicht etwa, dass autonome Fahrsysteme gar nicht reguliert werden sollen, sondern dass die bereits bestehende, spezifische Zulassungsregulierung für Fahrzeuge von der Kommission überarbeitet wird (Erwägungsgrund 49 AI Act). Bei der Neufassung müssen dann die Regelungen des AI Act für Hochrisiko-Systeme in diese sektorale Regulierung konkret eingearbeitet werden (Art. 104 und 107 AI Act).[49]

Insofern unterscheidet sich das Regime deutlich von den bisher betrachteten sektoralen Regulierungen, die unverändert bestehen bleiben, während der AI Act neben sie tritt. Im Automobilbereich sowie in allen anderen in Anhang I Abschnitt B AI Act aufgeführten Sektoren (z. B. Zivilluftfahrt, Eisenbahninteroperabilität, Schiffsausrüstung) gelten nur die sektoralen Regeln. Diese werden jedoch neu gefasst; dabei müssen auch die Anforderungen des AI Act an Hochrisiko-KI-Systeme berücksichtigt werden. Unklar ist jedoch, welche Regelungen der Automobilregulierung genau wie erfasst sind.

a | Zulassungsverfahren im Automobilbereich

Um genauer zu verstehen, welche Bereiche vom AI Act wie betroffen werden, muss man zunächst einen Überblick über die verschiedenen Regulierungssysteme und Zulassungsverfahren im Automobilbereich gewinnen.

Zentral ist die Typgenehmigung, auch Homologation genannt. Darunter versteht man einen Prozess, der sicherstellt, dass ein Fahrzeug oder eine Fahrzeugkomponente die EU-weiten Sicherheits- und Umweltstandards erfüllt. Dieser Prozess umfasst eine Überprüfung durch die Behörden und schließt die Ausstellung eines Zertifikats ein, das die Konformität des Fahrzeugs bestätigt. Die Typgenehmigung deckt verschiedene Aspekte ab, darunter Emissionen, Sicherheit, Energieeffizienz und die allgemeine Verkehrstauglichkeit. Im August 2022 veröffentlichte die Kommission bereits eine Durchführungsverordnung, welche die wesentlichen Aspekte für die Prüfung von automatisierten Fahrsystemen für vollkommen automatisierte Fahrzeuge für die Typzulassung umfasst.[50] In Zukunft werden weitere Durchführungsverordnungen erwartet, welche die Typzulassung auch für andere KI-Systeme genauer regeln.[51] Auch die nationalen Gesetzgeber werden gefordert sein, entsprechende Zulassungsgesetzgebungen anzupassen (z. B. die Straßenverkehrs-Zulassungs-Ordnung, StVZO) und dabei die Vorgaben für Hochrisiko-Systeme des AI Act spezifisch zu berücksichtigen (Art. 107 AI Act).

b | Mögliche Konflikte zwischen dem AI Act und bestehenden Automobilregulierungen

Industrieseitig gab es während des Gesetzgebungsprozesses Bedenken, dass der AI Act zu einer Dop-

49 Siehe etwa Kilian 2024a: 130, 132; 2024b: 5 f.

50 Durchführungsverordnung (EU) 2022/1426 der Kommission vom 5. August 2022 mit detaillierten Regelungen zur Durchführung der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates im Hinblick auf die einheitlichen Verfahren und technischen Spezifikationen für die Typgenehmigung des automatisierten Fahrsystems (Automated Driving System, ADS) vollautomatisierter Fahrzeuge, siehe auch https://ai-regulation.com/the-eu-commission-regulatory-stance-on-autonomous-vehicles/.

51 Köllner 2024.

pelregulierung führen könnte.[52] Die Befürchtung war insbesondere, dass bestimmte Systeme, die keine hohen Risiken bergen, unnötig streng reguliert werden, was – so der Industrietenor – Innovationen in der Automobilbranche behindern könnte.[53] Andererseits ist zu berücksichtigen, dass auch bei Systemen, die nicht von Natur aus ein hohes Risiko aufweisen (z. B. Infotainment, Sprachsteuerung), dafür Sorge getragen werden muss, dass diese nicht zu einer unnötigen Aufmerksamkeitsreduzierung der Fahrer führen.

Die Gefahr einer Doppelregulierung scheint jedoch im Bereich der Produkte, die von Anhang I Abschnitt B AI Act erfasst werden (z. B. Kraftfahrzeuge), weitgehend gebannt. Denn Art. 2 Abs. 2 AI Act enthält eine weitreichende Freistellung. Konkret ausgenommen von der Anwendbarkeit der Hochrisiko-Vorschriften des AI Act sind Systeme, die unter Anhang I Abschnitt B AI Act fallen; im Automobilbereich umfasst dies besonders:

- die Typgenehmigungsverordnung: Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge

- Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen

- Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmer:innen

- Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen

Diese Freistellung reicht nach Art. 2 Abs. 2 AI Act weit: Es genügt, dass es sich um Hochrisiko-Systeme nach Art. 6 Abs. 1 AI Act handelt, die „im Zusammenhang mit Produkten stehen", die unter Anhang I Abschnitt B fallen. Damit sind also wohl auch Systeme erfasst, die nicht unmittelbar in einem solchen Produkt selbst verbaut, für dessen Betrieb aber essenziell sind.

Eine auf den ersten Blick paradoxe Folge aus der Freistellung ist jedoch auch, dass solche Systeme, die nicht nach Art. 6 Abs. 1 AI Act als Hochrisiko-Systeme eingestuft sind, den Anforderungen des AI Act vollkommen unterliegen – etwa den Anforderungen an die KI-Kompetenz der mit dem System befassten Mitarbeiter:innen nach Art. 4 AI Act und den Transparenzbestimmungen nach Art. 50.

Relevant werden kann dies bei nicht unmittelbar den Sicherheitssystemen zugeordneten Elementen wie dem Infotainment oder Steuerungssystemen wie einem Sprachassistenten: Sofern diese wegen der Integration in sonstige relevante Hardware als Hochrisiko-Systeme nach Art. 6 Abs. 1 AI Act eingeordnet werden, sind sie vom AI Act ausgenommen und unterliegen nur der jeweiligen sektoralen Regulierung. Sind sie jedoch nicht als Hochrisiko-Systeme zu qualifizieren, gilt auch die Ausnahme nach Art. 2 Abs. 2 AI Act nicht. Dann müssen etwa die Transparenzanforderungen nach Art. 50 AI Act, wegen Interaktion mit Menschen, sowie die Vorgaben über die KI-Kompetenz bei den entwickelnden und betreibenden Unternehmen nach Art. 4 AI Act erfüllt werden.

Auch wenn die Einordnung letztlich eine Frage des Einzelfalls ist, ist die Sicherheitsrelevanz dieser Systeme (Infotainment; Sprachassistent) nicht gänz-

52 VDA 2023: 13.

53 Siehe a. a. O.: 6.

lich in Abrede zu stellen. Auch diese Systeme können bei Fehlfunktionen zu einem Unfall führen, da Fahrer durch die dann erschwerte Bedienung abgelenkt sein können.[54] Ablenkung ist zwar kein KI-spezifisches Risiko, da dieses genauso bei der Interaktion mit dem Radio oder anderen Insassen auftreten kann. Nichtsdestoweniger sollte sichergestellt werden, dass Infowtainmentprodukte so entwickelt werden, dass eine längerfristige Bedienung oder Interaktion mit ihnen während der Fahrt durch den Fahrer möglichst technisch ausgeschlossen wird.

c | Zwischenergebnis für den Automotive-Bereich

Die Typgenehmigung ist das zentrale Verfahren für die Zulassung von Fahrzeugen, bei dem die Einhaltung technischer und sicherheitsrelevanter Normen geprüft wird. Der AI Act bringt zusätzliche Anforderungen nur für nicht nach seiner Terminologie hochriskante KI-Systeme in Fahrzeugen. Hochrisiko-Systeme im engeren Sinne werden hingegen von den Anforderungen des AI Act freigestellt. Für sie gelten vielmehr die EU-Typgenehmigungsverordnung sowie andere europäische und nationale Vorschriften, die künftig allerdings jeweils unter Berücksichtigung der Hochrisiko-Prinzipien des AI Act umgestaltet werden müssen.

54 Siehe VDA 2023: 6.

IV. Empfehlungen

Diese Studie untersucht die Friktionen und Synergien zwischen dem AI Act und bestehenden EU-Regulierungen. Die vergangenen Abschnitte haben gezeigt, dass der AI Act als horizontaler Rechtsrahmen die sektoralen Regelungen, etwa im Finanz-, Medizin- und Automobilsektor, ergänzt, jedoch nur unzureichend auf sie abgestimmt ist. Daraus leiten sich verschiedene Handlungsempfehlungen ab, die im Folgenden untergliedert werden in kurzfristige, mittelfristige und langfristige Maßnahmen. Innerhalb dieser sind die jeweiligen Vorschläge nach Adressaten aufgeteilt, die vom europäischen Gesetzgeber über verschiedene Regulierungsbehörden bis hin zum nationalen Gesetzgeber, zu Standardisierungsorganisationen, Unternehmen und nicht zuletzt der Rechtswissenschaft selbst reichen. Die Tabelle 1 bietet eine Übersicht über die Vorschläge.

1. Kurzfristige Maßnahmen

Um kurzfristig Friktionen zu vermindern und Synergien zu stärken, bietet sich eine Reihe von Maßnahmen an.

a | Europäischer Gesetzgeber

Ausweisung eines „Lead Act“: Ein Vorschlag zur Konfliktminimierung ist die Einführung eines „Lead Act“, der als primärer Rechtsrahmen für KI-Anwendungen dient. Eine solche Verhältnisbestimmung müsste auf gesetzlicher Ebene vorgenommen werden. Lead Act könnten je nach Sektor der AI Act, aber auch ein Akt oder mehrere besonders wichtige Akte der sektoralen Regulierung sein. Die Idee wäre dann: Wird der „Lead Act“ erfüllt, besteht die Vermutung, dass die Anforderungen der jeweils anderen Regelwerke ebenfalls erfüllt sind, es sei denn, spezifische Normen aus anderen Verordnungen oder Richtlinien müssen laut gesetzlicher Regelung unabhängig vom Lead Act ausdrücklich eingehalten werden. So wäre beispielsweise denkbar, die Medizinprodukteverordnung (MDR) als Lead Act auszuweisen und dann nur noch einzelne Vorgaben des AI Act, die signifikant über die MDR hinausgehen, explizit als zusätzlich zu erfüllende Anforderungen festzulegen.

b | Europäische Kommission (insb. AI Office)

Stärkere Verzahnung von Regulierungen: Es wird grundsätzlich empfohlen, bestehende sektorspezifische Vorschriften stärker mit dem AI Act zu verbinden, um Doppelregulierungen zu vermeiden. Zum Beispiel in den Bereichen Finanzdienstleistungen, Medizinprodukte und Automobilindustrie gibt es erhebliche Überschneidungen, die durch klarere Abgrenzungen und präzise Angaben, welche Vorschriften des AI Act jeweils durch Erfüllung sektorspezifischer Vorgaben umgesetzt wurden und welche nicht, minimiert werden sollten. Dies könnte primär, soweit möglich, im Wege von Durchführungsverordnungen erreicht werden, für die keine Änderung des AI Act selbst notwendig ist.

Wichtig ist: So lassen sich regulatorische Last reduzieren, KI-Entwicklung und -Einsatz fördern, ohne dass der Grundrechtsschutz auch nur einen Deut abgesenkt würde. Denn es werden die bestehenden

Regelungen nur vorteilhafter geordnet und in ein klar umsetzbares Verhältnis gebracht, nicht aber abgebaut oder eingeschränkt.

Praxisleitlinien und Content Moderation auf Modellebene: Nach dem AI Act ist eine Moderation von KI-Ausgaben nicht ausdrücklich vorgeschrieben. Sie kann sich jedoch aus Art. 55 ergeben, wenn anders systemische Risiken, z. B. für Nichtdiskriminierung und demokratische (Wahl-)Prozesse, nicht effektiv verringert werden können. Dies sollte auch in den Praxisleitlinien nach Art. 56 AI Act festgehalten werden.

Gleichzeitig muss darauf geachtet werden, dass übermäßige Moderation keine negativen Folgen für die Freiheit der Meinungsäußerung und die Vielfalt der Ausgaben hat. Allerdings ist zu beachten, dass legale, jedoch fälschlicherweise vom Modell geblockte KI-Inhalte selbstverständlich auch ohne Zuhilfenahme von generativer KI niedergeschrieben und gepostet werden können.

Wechselseitige Risikoanalysen (AI Office und Kommissionsaufsicht über VLOPs/VLOSEs): Insbesondere bei großen Plattformen (VLOPs/VLOSEs), die generative KI integrieren, könnte eine ganzheitliche Risikoanalyse durchgeführt werden, die sowohl die plattform- als auch die KI-spezifischen Risiken bewertet. Die Aufsichtsbehörden (nach DSA und AI Act) sollten aktiv dazu anhalten. Denn eine verstärkte Verzahnung der Risikoanalysen aus dem AI Act und dem Digital Services Act (DSA) ist zentral.

c | Europäischer Datenschutzausschuss

Harmonisierung mit der DS-GVO: Es wird empfohlen, kurzfristig spezifische Leitlinien durch den Europäischen Datenschutzausschuss entwickeln zu lassen (Art. 70 Abs. 1 lit. e DS-GVO), möglichst gar gemeinsam oder zumindest in Abstimmung mit dem europäischen AI Office, um die rechtliche Unsicherheit im Umgang mit Trainingsdaten für KI-Modelle zu reduzieren. Diese Leitlinien sollten klare Vorgaben zur Wiederverwendung von personenbezogenen Daten zu Trainingszwecken unter Berücksichtigung der DS-GVO enthalten.

d | Nationaler Gesetzgeber

Verschränkte Aufsicht: Die Koordinierung zwischen der nationalen Marktaufsichtsbehörde (z. B. Bundesnetzagentur (BNetzA) in Deutschland) und sektorspezifischen Regulierungsbehörden (z. B. im Gesundheits- oder Verkehrssektor) könnte durch eine engere, institutionell abgesicherte Verzahnung der Aufsicht verbessert werden. Zum Beispiel könnten einzelne Beamt:innen aus der sektoralen an die zentrale Behörde abgeordnet werden; diese könnten dann eine Scharnierfunktion einnehmen und in Fällen herangezogen werden, die sektorspezifischer Expertise bedürfen. Ferner sollten regelmäßige Austauschformate (Jour fixes etc.) zwischen den jeweils betroffenen Behörden eingerichtet werden. Dies könnte zu kohärenteren und effizienteren Regulierungsprozessen führen und Doppelprüfungen reduzieren.

Einführung eines zentralen Datenzugangsportals für KI: Um den Anforderungen des Digital Services Act (DSA) und den Herausforderungen des AI Act gerecht zu werden, könnte ein zentrales Portal entwickelt werden, das Forscher:innen und Regulierungsbehörden den Zugang zu KI-Daten erleichtert. Dies würde Transparenz schaffen und die Überwachung von Hochrisiko-KI-Systemen verbessern. Ein solches Portal könnte auch in nationalen Umsetzungsgesetzen zum AI Act jeweils eingerichtet werden. Zudem sollte für GPAI- und Hochrisiko-Systeme ein Zugangsrecht für zugelassene Forscher:innen im AI Act verankert werden, wie in Art. 40 Abs. 8 DSA, wofür allerdings der europäische Gesetzgeber zuständig wäre.

Verstärkung sektoraler Ausbildung und Schulung: Für Unternehmen in regulierten Sektoren könnten staatliche Stipendienprogramme aufgesetzt werden, mit denen die Teilnahme an spezifischen, marktüblichen Schulungsprogrammen (co-)finanziert wird. Im verwandten Bereich der Cybersicherheit werden ganze Aufklärungskampagnen sowie Trainingspro-

gramme durch die Agentur der Europäischen Union für Cybersicherheit (European Network and Information Security Agency, ENISA) zur Verfügung gestellt (Art. 10 Cybersecurity Act). Insbesondere kleine und mittlere Unternehmen (KMU), inklusive Start-ups, sollten dadurch zu reduzierten Kosten auf die Anforderungen des AI Act und sektorspezifischer Regelungen vorbereitet werden. Dies könnte sicherstellen, dass Unternehmen nicht nur die technischen, sondern auch die rechtlichen Anforderungen besser verstehen und umsetzen können. Mittelständische Unternehmen können dadurch frühzeitig explorieren, welche KI-Anwendungen für sie sinnvoll sein können und welche nicht. Ziel wäre es, zu verhindern, dass KMU aus Sorge vor Kosten und Compliance gesellschaftlich sinnvolle KI-Anwendungen unterlassen.

e | Nationale Aufsichtsbehörden

Guidelines (nationale KI-Aufsicht, ggf. AI Office): Nationale Aufsichtsbehörden, ggf. auch das bei der Europäischen Kommission nunmehr eingerichtete AI Office, sollten detaillierte Leitlinien erarbeiten, um Klarheit darüber zu schaffen, wie der AI Act in spezifischen Fällen anzuwenden ist, bei denen auch sektorale Regulierung zum Tragen kommt. Diese nicht bindenden Guidelines könnten auch sektorspezifische Unterschiede berücksichtigen und so die Entwicklung und den Einsatz von KI passgenau steuern sowie erleichtern. Voraussetzung ist jedoch, dass die Behörden auch mit entsprechenden Ressourcen ausgestattet werden, um derartige Guidelines – neben dem Alltagsgeschäft – zu entwickeln.

Harmonisierung mit der DS-GVO (nationale KI-Aufsicht und Datenschutzaufsicht): Um die Konflikte zwischen dem AI Act und der DS-GVO zu mindern, sollten zudem verstärkte Kooperationsmechanismen zwischen den zuständigen Behörden eingerichtet werden (siehe auch soeben, unter Abschnitt IV.1.d). Nationale KI-Aufsichtsbehörden müssen eng mit Datenschutzbehörden zusammenarbeiten, um sicherzustellen, dass beide Regulierungen kohärent umgesetzt und Friktionen durch Richtlinien und Beratung entschärft werden. Diese Kooperationspflichten sind jedoch bislang nicht ausreichend konkretisiert, was in der Praxis zu Unsicherheiten führen könnte. Sinnvoll erscheint z. B. eine interne Richtlinie, die eine Konsultation der Datenschutzbehörden durch die Marktaufsichtsbehörde zumindest immer dann vorsieht, wenn die DS-GVO für die Beurteilung der AI Act Compliance von Bedeutung ist. Dies ist regelmäßig in den unter Abschnitt II.2. diskutierten Fällen gegeben (z. B. KI-Training; Biasreduzierung).

Insgesamt bleibt die Harmonisierung zwischen dem AI Act und der DS-GVO eine Herausforderung, die sowohl auf rechtlicher als auch auf technischer Ebene angegangen werden muss, um die Interessen der betroffenen Personen zu wahren und gleichzeitig sozial wünschenswerte Innovationen im Bereich der Künstlichen Intelligenz gerade auch in der EU und in Deutschland zu ermöglichen.

Kooperation der Aufsichtsbehörden: Zudem müssen Regulierungsbehörden eng zusammenarbeiten, um die Umsetzung beider Regelwerke zu erleichtern. Hierfür sollte eine agile Struktur innerhalb der nationalen AI-Act-Marktüberwachungsbehörde eingeführt werden, die dort fest tätige Personen und solche, die von sektoralen Behörden abgeordnet werden, vereint. Je nach Fall können und müssen dann Teams gebildet werden, welche die KI-Kompetenzen der Marktüberwachungsbehörde mit der fachlichen Expertise der abgeordneten Personen jeweils sachverhaltsspezifisch zusammenführen. Zugleich ist der Austausch mit dem AI Office wichtig, damit ein dauerhafter, neuer und übergreifender AI Enforcement Hub mit entsprechender Expertise, Feedback und strukturierten Lernprozessen entstehen kann.[55]

Stärkung sektoraler Expertengremien: Innerhalb der Marktüberwachungsbehörde sollten ferner sektorspezifische Expertengremien eingerichtet werden, die die Implementierung des AI Act in Verbindung mit sektorspezifischen Regelungen koordinieren. Deren Mitglieder sollten sich primär aus Wissen-

55 Siehe auch Novelli et al. 2024: 4.

schaft und Zivilgesellschaft, aber auch der Industrie rekrutieren. Diese Gremien könnten sicherstellen, dass spezifische Risiken und Besonderheiten einzelner Sektoren im Rahmen des AI Act und seiner Durchsetzung angemessen berücksichtigt werden.

f | Standardisierungsorganisationen

Entwicklung übergreifender technischer Standards: Der AI Act wird durch Standards ergänzt, die aktuell entwickelt werden, um die praktische Umsetzung zu unterstützen. Um rechtliche Unsicherheiten zu reduzieren, können übergreifende technische Normen als Safe-Harbor-Mechanismen für den AI Act und sektorale Regulierungen, aber auch weitere Digitalgesetze wie der DS-GVO etabliert werden. Diese Normen könnten Unternehmen helfen, die Anforderungen mehrerer Regelwerke gleichzeitig zu erfüllen. Soweit kein Lead Act oder delegierter Rechtsakt vorliegt, der eine trennscharfe Abgrenzung gewährleistet (siehe Empfehlung IV.1.a und b), können über diese Standards konkrete Querverbindungen zwischen AI Act und sektoraler Regulierung hergestellt werden. Dann gilt bei Erfüllung der Standards eine Vermutung der Konformität mit den entsprechenden Anforderungen des AI Act (Art. 40 Abs. 1 AI Act).

g | Unternehmen

Nutzung und Update bestehender Compliance-Systeme: Unternehmen, die bereits etablierte Compliance-Systeme für andere Regulierungen (z. B. DS-GVO, Produktsicherheitsrecht) betreiben, können diese für den AI Act adaptieren. Dafür müssen jedoch die spezifischen Neuerungen, die der AI Act bringt, genau untersucht und die Differenzen zu den bestehenden Anforderungen und Praktiken geklärt werden. Diese Neuerungen müssen dann in entsprechende Compliance-Routinen übersetzt werden. Eine solche Integration kann den Aufwand für zusätzliche Compliance-Verfahren verringern und die Einführung des AI Act in bestehende operative Strukturen erleichtern.

Codes of Practice: Die Entwicklung von Praxisleitfäden (Codes of Practice) gemäß Art. 56 AI Act bietet eine flexible Methode zur regulierten Selbstregulierung und könnte die harmonisierte Umsetzung in verschiedenen Branchen fördern. Insbesondere sektorale Codes könnten branchenspezifische Anforderungen operationalisieren und eine effektive Zusammenarbeit zwischen Regulierern und Unternehmen gewährleisten.

h | Rechtswissenschaft

Lex specialis: In Fällen, in denen kein Lead Act ausgewiesen wird, muss die allgemeine Rechtsmethodik zur Anwendung kommen, z. B. auch das Prinzip des Vorrangs der Spezialregelung („lex specialis derogat legi generali“[56]). Das bedeutet, dass speziellere Regelungen, wie sie in sektorspezifischen Vorschriften bestehen, grundsätzlich Vorrang vor allgemeinen Regeln des AI Act haben. Konkret könnte dies bedeuten: Wenn die Vorschriften über die notwendige Performanz eines Medizinprodukts nach der Medizinprodukteverordnung (MDR) erfüllt sind, lassen sich aus dem allgemeineren Art. 15 Abs. 1 AI Act keine weiteren Vorgaben zur „Genauigkeit“ mehr ableiten. Allerdings muss jeweils geklärt werden, ob denn die sektorale Regulierung (sachliche Nähe) oder der AI Act (technische Nähe) die tatsächlich speziellere Norm ist. Dies kann nur im Einzelfall entschieden werden. Die Rechtswissenschaft kann hier erheblich zur Systematisierung beitragen;[57] aufgegriffen werden sollten diese Regeln dann in Guidelines der Behörden oder in konkreten Gerichtsurteilen.

56 Ein spezielles Gesetz (lex specialis) geht dem allgemeinen Gesetz (lex generalis) vor und hat damit Anwendungsvorrang.

57 Siehe nur Hacker 2020: § 5 A.II. mit weiteren Nachweisen.

2. Mittel- und langfristige Maßnahmen

Während sich kurzfristige Maßnahmen primär an Regulierungsbehörden, nationale Gesetzgeber, Standardsetzungsorganisationen und Unternehmen selbst richten, wird mittel- und langfristig ein Feintuning des AI Act selbst sowie angrenzender Digitalgesetze notwendig sein. Dies obliegt primär dem europäischen Gesetzgeber; aber auch der nationale Gesetzgeber ist hinsichtlich der Umsetzungsgesetze gefordert.

a | Europäischer Gesetzgeber

Stärkere Nutzung von spezifischen Verweisen im Rechtstext: In den AI Act sind Pflichten zu regelmäßigen Evaluationen eingebaut (Art. 112 AI Act). Diese sollten auch die sektoralen Schnittstellen beleuchten. Bei einer allfälligen Revision müssten dann weitere explizite Verweise auf andere einschlägige Regulierungen aufgenommen werden, um Überschneidungen und Mehrdeutigkeiten zu vermeiden. Diese Verweise sollten den rechtlichen Rahmen klarer gestalten und die Anwendung der betroffenen Rechtsakte harmonisieren. Art. 17 Abs. 4 AI Act hat hier Vorbildcharakter.

Harmonisierung mit der DS-GVO: Da der AI Act in einigen Bereichen die Verarbeitung sensibler Daten erforderlich macht, sollten Ausnahmen von und Verknüpfungen zur DS-GVO klarer und umfassender formuliert werden. Besonders für GPAI-Modelle und -Systeme, die diskriminierungssensible Daten verarbeiten, sollten die Anforderungen der DS-GVO und des AI Act besser abgestimmt werden.

Art. 10 Abs. 5 AI Act enthält eine Ausnahme vom Verbot der Verarbeitung sensitiver personenbezogener Daten, das Art. 9 DS-GVO aufstellt. Diese dürfen nun verarbeitet werden, wenn die Verarbeitung der Reduzierung von diskriminierenden Verzerrungen von Hochrisiko-KI-Systemen dient und eine Reihe von Vorkehrungen zum Schutz der Grundrechte eingehalten werden. Diese sinnvolle Ausnahme sollte gesetzlich auf alle KI-Systeme ausgeweitet werden, um leistungsfähige und zugleich diskriminierungssensitive Modelle zu ermöglichen. Andernfalls blockieren sich DS-GVO und AI Act unnötig gegenseitig, und dies gerade auf dem besonders bedeutsamen Gebiet der generativen KI. Auch ökonomisch erscheint es viel effizienter, einmal an der Quelle (dem Basismodell) Diskriminierung zu reduzieren als separat in jeder einzelnen (Hochrisiko-)Anwendung.

Zudem sollte klargestellt werden, dass die Ausnahme für sensitive Daten auch für nicht sensitive personenbezogene Daten gilt: Sonst dürfen sensitive Daten für Diskriminierungsreduzierung verarbeitet werden, „normale“ personenbezogene Daten aber womöglich nicht, was widersprüchlich wäre. Momentan wird man diese Regel zu den personenbezogenen Daten in den Abwägungstest nach Art. 6 Abs. 1 lit. f DS-GVO hineinlesen müssen.

Ferner sind neue Ausnahmeregelungen wie in Art. 10 Abs. 5 des AI Act notwendig, um eine ausgewogene Datennutzung zu ermöglichen, die sowohl den Schutz der betroffenen Personen durch besondere verfahrensrechtliche Absicherungen sicherstellt als auch innovative Lösungen in zentralen Gebieten von gesellschaftlicher Bedeutung, etwa der Medizin, ermöglicht. Sonst gerät Art. 9 DS-GVO unter Umständen in Konflikt mit den Leistungskriterien aus Art. 15 AI Act. Das Gesundheitsdatennutzungsgesetz (GDNG) geht erste Schritte in diese Richtung (s. oben, Abschnitt II.2.d).

Rechtsrahmen für KI-Training: Mittelfristig ist ein kohärenter Rechtsrahmen erforderlich, der sowohl AI Act als auch die DS-GVO in Bezug auf Trainingsdaten integriert, um die Entwicklung verantwortungsvoller und datenschutzkonformer KI in Europa zu fördern. Dabei ist darauf zu achten, dass dieser Rahmen Innovationen gerade auch in Bereichen ermöglicht und fördert, in denen die Compliance aufgrund von Überschneidungen mit sektoraler Regulierung komplex ist. Zugleich muss Grundrechten gebührlich Rechnung getragen werden, durch prozedurale Vorschriften, wo nötig aber auch harte Schranken der Datennutzung.

Daher sollte bei einer Revision des AI Act angestrebt werden, eine explizite Ausnahme für die Nutzung von Daten zu Trainingszwecken zu schaffen. Dazu ist allerdings nur der europäische Gesetzgeber berufen. Während es im Urheberrecht bereits eine Ausnahme für Text- und Data Mining gibt, fehlt eine solche Regelung im Datenschutzrecht. Diese Lücke könnte mit einer Revision des AI Act geschlossen werden, wie es für spezifische Zwecke (z. B. Diskriminierungsreduzierung in medizinischer KI) bereits in dessen Art. 10 Abs. 5 vorgesehen ist.

Eine etwaige, neue Ausnahme vom Schutz sensitiver Daten nach Art. 9 DS-GVO für KI-Training sollte sektorspezifisch angelegt, mit strengen prozeduralen Schutzvorschriften (vgl. Art. 10 Abs. 5 AI Act und Art. 22 Abs. 3 DS-GVO) und ggf. einer Opt-out-Möglichkeit (vgl. Art. 21 DS-GVO) versehen sein.[58] Dabei könnte Art. 10 Abs. 5 AI Act als Vorlage dienen, um spezifische Anwendungsbereiche wie medizinische KI zu regeln. Erforderlich ist dann wie in Art. 10 Abs. 5 AI Act eine Begrenzung auf spezifische Zwecke (z. B. Training für medizinische KI oder für spezifische Robotik) mit stringenten, prozeduralen Schutzgarantien für Betroffene. Gerade der Gesundheitsdatenschutz ist in Deutschland durch kleinteilige Regelungen auf Länderebene zu einem nur schwer durchdringlichen Dschungel geworden, der für anspruchsvolle Forschung keine adäquate Grundlage mehr bietet (siehe auch oben zum GDNG, Abschnitt II.2.d).

Content Moderation auf Modellebene: Eine sinnvolle Erweiterung wäre es ferner, wenn vertrauenswürdige Hinweisgeber gemäß Art. 22 DSA auch schädliche Eingabeaufforderungen (Prompts) und illegale Ausgaben von generativen KI-Systemen, z. B. auf hybriden Plattformen, aber auch in sonstigen generativen KI-Systemen, melden könnten. Dies würde eine umfassende Integration der Plattform- und KI-Risiken ermöglichen und sicherstellen, dass Risiken sowohl auf Plattform- als auch auf KI-Ebene abgedeckt sind.

58 Vgl. auch die Text- und Data-Mining-Ausnahme im Urheberrecht, dazu etwa Raue 2021: 793.

b | Nationaler Gesetzgeber

Verknüpfung von Durchführungsgesetzen: Der nationale Gesetzgeber sollte mittelfristig darauf achten, dass die verschiedenen Durchführungsgesetze und Ergänzungsregelungen für die einzelnen Digitalgesetze, etwa für die DS-GVO, den Digital Services Act (DSA) und den AI Act, zusammenhängend überarbeitet und verknüpft werden. So können bestimmte Synergien, etwa im Bereich des Datenzugangs oder des Risikomanagements, noch besser auf gesetzlicher Ebene unterstützt werden.

3. Langfristige Maßnahmen

Schließlich bedarf es auch auf längere Sicht hin Maßnahmen des europäischen und nationalen Gesetzgebers sowie der Aufsichtsbehörden, um die Feinabstimmung zwischen KI-, Digital- und sektoraler Regulierung auf solider Datengrundlage stetig zu verbessern. So können auch die kurz- und mittelfristigen Maßnahmen aufgegriffen und weiterentwickelt werden.

a | Europäischer Gesetzgeber

Grundlegende Evaluation AI Act: Der AI Act sollte nach einer angemessenen Anwendungszeit grundlegend, und über Art. 112 AI Act hinausgehend, extern empirisch und theoretisch überprüft und hinsichtlich seiner Auswirkungen auf den Grundrechtsschutz sowie die Entwicklung und Anwendung von KI evaluiert werden. Dabei könnte auch untersucht werden, ob Haftungsregelungen in Verbindung mit Verboten für sozial besonders unerwünschte Praktiken, Regeln für GPAI und Transparenzanforderungen ausreichen könnten, ggf. ohne die spezifischen prozeduralen und substanziellen Regelungen für Hochrisiko-KI (z. B. Art. 8 bis 27 AI Act) beizubehalten. Dies könnte schlankere Compliance ermöglichen bei gleichzeitiger Beibehaltung von Anreizen zur Entwicklung und Anwendung verantwortungsvoller KI auch in den bisherigen Hochrisiko-Gebieten – auf Grundlage des

durch die Neufassung der Produkthaftungsrichtlinie sowie möglicherweise die KI-Haftungsrichtlinie verschärften und ggf. nochmal nachjustierten Haftungsrechts. Zudem würde die sektorale Regulierung in diesen Bereichen weiter gelten und könnte ebenfalls angepasst werden. Betroffenenrechte, die sich bewährt haben, könnten dann im AI Act beibehalten werden; sie treten jedoch neben das ohnehin häufig schärfere Schwert der Betroffenenrechte nach der DS-GVO.

b | Nationaler Gesetzgeber

Aufsichtsarchitektur: Die im Laufe der Zeit etablierte Zusammenarbeit zwischen den verschiedenen sektoralen und KI-spezifischen Aufsichtsbehörden sollte institutionalisiert werden. Dazu bedarf es eines klaren gesetzlichen Rahmens, der Zuständigkeiten, Kommunikationskanäle und Entscheidungsprozesse definiert.

c | Aufsichtsbehörden

Framework für Kooperation und Evaluation: Um die Effektivität dieser Kooperation sicherzustellen und kontinuierlich zu verbessern, sind evidenzgestützte Mechanismen zur Evaluation erforderlich. Diese sollten regelmäßig die Zusammenarbeit anhand definierter Kriterien wie Schnelligkeit, Konsistenz und Vollständigkeit des Informationsaustauschs sowie der Fähigkeit, gemeinsame Positionen und Maßnahmen zu entwickeln, bewerten. Die Ergebnisse dieser Evaluationen sollten ggf. veröffentlicht und jedenfalls genutzt werden, um die Kooperationsstrukturen und -prozesse fortlaufend anzupassen und zu optimieren.

Tabelle 1 **Übersicht über die Handlungsempfehlungen**

Zeitrahmen	Akteur	Maßnahme	Beschreibung
Kurzfristig	Europäischer Gesetzgeber	Ausweisung eines „Lead Act“	Ein „Lead Act“ als primärer Rechtsrahmen zur Konfliktminimierung bei KI-Anwendungen
Kurzfristig	Europäische Kommission (insb. AI Office)	Stärkere Verzahnung von Regulierungen	Klarere Abgrenzungen und präzise Angaben in Durchführungsverordnungen
Kurzfristig	Europäische Kommission	Durchführung ganzheitlicher Risikoanalysen	Bei VLOPs/VLOSEs mit generativer KI durch AI Office und VLOP-/VLOSE-Aufsicht
Kurzfristig	Europäische Kommission (insb. AI Office)	Festlegung von Praxisleitlinien zu Content Moderation	In Leitlinien nach Art. 56 AI Act, unter Beachtung möglicher negativer Folgen für die Meinungsfreiheit
Kurzfristig	Europäischer Datenschutz-ausschuss	Entwicklung spezifischer Leitlinien	Zum Umgang mit Trainingsdaten zur Reduzierung rechtlicher Unsicherheiten bei der Harmonisierung mit der DS-GVO
Kurzfristig	Nationaler Gesetzgeber	Institutionelle Verzahnung der Aufsicht	Zwischen nationaler KI-Aufsichtsbehörde und sektorspezifischen Regulierungsbehörden
Kurzfristig	Nationaler Gesetzgeber	Einrichtung eines zentralen Datenzugangsportals	Für den Zugang zu KI-Daten für Forscher:innen und Regulierungsbehörden
Kurzfristig	Nationaler Gesetzgeber	Unterstützung für Schulungen	Stipendien für KMU in regulierten Sektoren zur Vorbereitung auf AI Act und sektorspezifische Regelungen
Kurzfristig	Nationale Aufsichtsbehörden	Erarbeitung detaillierter Leitlinien	Zur Anwendung des AI Act bei sektoraler Regulierung durch nationale KI-Aufsicht und ggf. AI Office
Kurzfristig	Nationale Aufsichtsbehörden	Einrichtung verstärkter Kooperationsmechanismen	Zwischen nationaler KI-Aufsicht und Datenschutzaufsicht zur Harmonisierung mit der DS-GVO
Kurzfristig	Nationale Aufsichtsbehörden	Etablierung einer agilen Struktur	Innerhalb der nationalen KI-Aufsichtsbehörde mit Abordnungen aus sektoralen Behörden für sachverhaltsspezifische Teams
Kurzfristig	Nationale Aufsichtsbehörden	Einrichtung sektorspezifischer Expertengremien	Innerhalb der nationalen KI-Aufsichtsbehörde zur Koordinierung der Implementierung des AI Act
Kurzfristig	Standardisierungs-organisationen	Etablierung übergreifender technischer Normen	Als Safe-Harbor-Mechanismen für AI Act, sektorale Regulierungen und weitere Digitalgesetze
Kurzfristig	Standardisierungs-organisationen	Entwicklung technischer Standards	Als Safe-Harbor-Mechanismen für AI Act und DS-GVO zur Schaffung von Rechtssicherheit
Kurzfristig	Unternehmen	Adaption etablierter Compliance-Systeme	Für den AI Act durch Untersuchung spezifischer Neuerungen und Übersetzung in entsprechende Compliance-Routinen
Kurzfristig	Unternehmen	Entwicklung von Praxis-leitfäden (Codes of Practice)	Gemäß Art. 56 AI Act zur flexiblen regulierten Selbstregulierung und harmonisierten Umsetzung in verschiedenen Branchen
Kurzfristig	Rechtswissenschaft	Systematisierung der Normen und ihres Verhältnisses	Zur Klärung des Vorrangs speziellerer sektoraler Regelungen vor allgemeinen Regeln des AI Act im Einzelfall

Zeitrahmen	Akteur	Maßnahme	Beschreibung
Kurzfristig	Europäischer Gesetzgeber	Stärkere Nutzung von spezifischen Verweisen im Rechtstext	Explizite Verweise auf andere einschlägige Regulierungen im AI Act zur Vermeidung von Überschneidungen und Mehrdeutigkeiten
Mittelfristig	Europäischer Gesetzgeber	Harmonisierung mit der DS-GVO	Klarere und umfassendere Formulierung von Ausnahmen und Verknüpfungen zur DS-GVO, insbesondere für GPAI-Modelle und -Systeme
Mittelfristig	Europäischer Gesetzgeber	Rechtsrahmen für KI-Training	Revision des AI Act zur Schaffung einer expliziten Ausnahme für die Nutzung von Daten zu Trainings-zwecken
Mittelfristig	Europäischer Gesetzgeber	Content Moderation auf Modellebene	Erweiterung des DSA, um vertrauenswürdigen Hinweisgebern die Meldung schädlicher Prompts und illegaler Ausgaben von generativen KI-Systemen zu ermöglichen
Mittelfristig	Nationaler Gesetzgeber	Verknüpfung von Durchführungsgesetzen	Zusammenhängende Überarbeitung und Verknüpfung der verschiedenen Durchführungs-gesetze und Ergänzungsregelungen für Digital-gesetze
Langfristig	Europäischer Gesetzgeber	Evaluation AI Act und neue Architektur der KI-Regulierung	Grundlegende Überprüfung des AI Act und Prüfung einer neuen Architektur für die KI-Regulierung basierend auf Haftungsregelungen, Regeln für GPAI und Transparenzanforderungen
Langfristig	Nationaler Gesetzgeber	Aufsichtsarchitektur	Institutionalisierung der Zusammenarbeit zwischen sektoralen und KI-spezifischen Aufsichtsbehörden durch einen klaren gesetzlichen Rahmen
Langfristig	Aufsichtsbehörden	Framework für Kooperation und Evaluation	Entwicklung evidenzgestützter Mechanismen zur regelmäßigen Evaluation der Zusammenarbeit und fortlaufenden Anpassung der Kooperations-strukturen und -prozesse

Quelle: eigene Darstellung

Quellenverzeichnis

Aboy, Mateo, Timo Minssen und Effy Vayena (2024). „Navigating the EU AI Act: implications for regulated digital medical products". npj Digital Medicine 7 Art.-Nr. 237. https://doi.org/10.1038/s41746-024-01232-3.

Braegelmann, Tom (2024). „KI-VO und Compliance – aktuelle Brennpunkte". Künstliche Intelligenz und Recht (KIR) 2. 39–42.

Carl, Ann-Kathrin, und David Hochmann (2023). „Impact of the new European medical device regulation: a two-year comparison". Biomedical Engineering / Biomedizinische Technik (69) 3. 317–326. https://doi.org/10.1515/bmt-2023-0325.

De Bruyne, Jan, Orian Dheu und Charlotte Ducuing (2023). „The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive". Computer Law & Security Review (51) Article 105894. https://www.sciencedirect.com/science/article/abs/pii/S0267364923001048 (Download 19.11.2024)

Eber, Maximilian, und Philipp Hacker (i. E.). „Policy Brief on the Future of Credit Underwriting under the EU AI Act: Implications for Europe and beyond".

Engeler, Malte, und Louis Rolfes (2024). „Datenschutzrechtliche Korrekturansprüche bei Erzeugung von Falschinformationen durch LLMs". Zeitschrift für Datenschutz (ZD) 8. 423–428.

Feldkamp, Jakob, Quirin Kappler, Maximilian Poretschkin, Anna Schmitz und Erik Weiss (2024). „Rechtliche Fairnessanforderungen an KI-Systeme und ihre technische Evaluation – Eine Analyse anhand ausgewählter Kreditscoring-Systeme unter besonderer Berücksichtigung der zukünftigen europäischen KI-Verordnung". Zeitschrift für Digitalisierung und Recht (ZfDR) 60.

Gierschmann, Sibylle (2020). „Gemeinsame Verantwortlichkeit in der Praxis". Zeitschrift für Datenschutz (ZD) 2. 69–72.

Gkritsi, Eliza (2024). „X suspends processing of some personal data for AI training". EURACTIV 9.8. https://www.euractiv.com/section/data-privacy/news/x-suspends-processing-of-some-personal-data-for-ai-training/ (Download 10.11.2024).

Hacker Philipp (2024). Proposal for adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment. Study written at the request of the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, requested in turn by the JURI Committee of the European Parliament, September 19. Strasbourg: European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)762861 (Download 10.11.2024).

Hacker, Philipp (2023). „The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future“: Computer Law & Security Review (51) Article 105871. https://www.sciencedirect.com/science/article/pii/S026736492300081X?via%3Dihub (Download 19.11.2024).

Hacker, Philipp (2021). „A legal framework for AI training data – from first principles to the Artificial Intelligence Act“. Law, Innovation and Technology (13). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598 (Download 19.11.2024).

Hacker, Philipp (2020). Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB. Tübingen.

Harrington, Esme, und Mathias Vermeulen (2024). External researcher access to closed foundation models. State of the field and options for improvement. Report. https://blog.mozilla.org/wp-content/blogs.dir/278/files/2024/10/External-researcher-access-to-closed-foundation-models.pdf (Download 19.11.2024).

Hense, Peter (2024). „Overfitting“. Multimedia und Recht (MMR) 6. 449–450.

Hermstrüwer, Yoan (2016). Informationelle Selbstgefährdung. Tübingen.

Hüger, Jakob (2024). „Die Rechtmäßigkeit von Datenverarbeitungen im Lebenszyklus von KI-Systemen“. Zeitschrift für Digitalisierung und Recht (ZfDR) 3. 263–292.

Kilian, Robert (2024a). „Nationale Spielräume bei der Umsetzung des Europäischen AI Act“. Zeitschrift für Rechtspolitik (ZRP) 5. 129–160.

Kilian, Robert (2024b). „Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz“. Schriftliche Stellungnahme für die 63. Sitzung des Ausschusses für Digitales des Deutschen Bundestages am 15.5.2024. www.bundestag.de/resource/blob/1002540/2c7af0e644c2d1b19d20896994727736/Kilian.pdf (Download 19.11.2024).

Köllner, Christiane (2024). „Was bedeutet das KI-Gesetz für die Autoindustrie?“. Springer Professional 1.8. https://www.springerprofessional.de/kuenstliche-intelligenz/automatisiertes-fahren/was-bedeutet-das-ki-gesetz-fuer-die-autoindustrie-/26700940 (Download 10.11.2024).

Marano, Pierpaolo, und Shu Li (2023). „Regulating robo-advisors in insurance distribution: Lessons from the Insurance Distribution Directive and the AI Act“. Risks (11) 12. https://www.mdpi.com/2227-9091/11/1/12 (Download 19.11.2024).

Novelli, Claudio, Frederico Casolari, Philipp Hacker, Giorgio Spedicato und Luciano Floridi (2024). „Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity“. Computer Law & Security Review (forthcoming), Article 106066. https://www.sciencedirect.com/science/article/pii/S0267364924001328?via%3Dihub (Download 19.11.2024).

Onitiu, Daria, Sandra Wachter and Brent Mittelstadt (2024). „How AI challenges the medical device regulation: patient safety, benefits, and intended uses“. Journal of Law and the Biosciences lsae007. https://doi.org/10.1093/jlb/lsae007.

Radtke, Tristan (2024). „Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke“. Recht Digital (RDi). 353–360.

Rauch, Pauline, Carina Richters und Christoph Naucke (2024). „Gesundheitsdatennutzungsgesetz: Der Zielkonflikt zwischen Datenschutz und Datennutzung“. GesundheitsRecht 218. https://www.degruyter.com/document/doi/10.9785/gesr-2024-230404/html (Download 19.11.2024).

Raue, Benjamin (2021). „Die Freistellung von Datenanalysen durch die neuen Text und Data Mining-Schranken (§§ 44b, 60d UrhG)". Zeitschrift für Urheber- und Medienrecht (ZUM) 2021. 793–802. https://irdt.uni-trier.de/wp-content/uploads/2022/02/formatiert_Raue_ZUM-2021-793.pdf (Download 19.11.2024).

Reichert, Florian, Kristina Radtke und Hermann Eske (2024). „KI-Verordnung, Rechtsgrundlagen für die Bereitstellung und Nutzung von KI". Zeitschrift für Datenschutz (ZD) 9. 483–489.

Schemmel, Frank (2024). „Grundrechte- und Datenschutz-Folgenabschätzung – zwei Seiten einer Medaille des Daten-Risikomanagements". Compliance Berater (CB) 9. 321–325.

Schneider, Uwe K., und Till Katzenstein (2024). „Weiterverarbeitung von Versorgungsdaten nach § 6 GDNG". Gesundheit und Pflege (GuP) Heft 5. 196–202).

Theisen, Susanne (2024). „Eine neue Form der Übergriffigkeit". Zahnärztliche Mitteilungen (ZM) 3. 54–55.

van Bekkum, Marvin, und Frederik Zuiderveen Borgesius (2023). „Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?". Computer Law & Security Review 48 Article 105770. https://www.sciencedirect.com/science/article/pii/S0267364922001133?via%3Dihub (Download 19.11.2024).

VDA – Verband der deutschen Automobilindustrie (2023). „Position Artificial Intelligence Act". Berkin. https://www.vda.de/de/aktuelles/publikationen/publication/ki-verordnung---artificial-intelligence-act-- (Download 21.11.2024).

Wachter Sandra (2024). „Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond". Yale Journal of Law & Technology (26) 3.

Wagner, Gerhard (2023). „Liability Rules for the Digital Age – Aiming for the Brussels Effect". European Journal of Tort Law 191. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4320285 (Download 19.11.2024).

Weatherbed, Jess (2024). „Meta fed its AI on almost everything you've posted publicly since 2007". The Verge 12.9. https://www.theverge.com/2024/9/12/24242789/meta-training-ai-models-facebook-instagram-photo-post-data (Download 10.11.2024).

Weichert, Thilo (2023). „Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit. Eine Kritik am Referentenentwurf für ein Gesundheitsdatennutzungsgesetz". Netzwerk Datenschutzexpertise (Stand 9.8.2023). https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023_08_gdng.pdf (Download 10.11.2024).

Werry, Susanne, und Elena Ntanas (2024). „Sekundärnutzung von Gesundheitsdaten – Quid deinde?". Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 641.

Woesch, Philippe, und Melanie Vogt (2024). „Die KI-Verordnung – Die digitale Zukunft im Finanzsektor". Bank- und Kapitalmarktrecht (BKR) 16. 689–736.

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0
bertelsmann-stiftung.de

Asena Soydaş
Project Manager
Digitalisierung und Gemeinwohl
Telefon: +49 5241 81-81247
asena.soydas@bertelsmann-stiftung.de