KI BUNDESVERBAND

„Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz“

Schriftliche Stellungnahme von
RA Dr. Robert Kilian, Vorstand KI-Bundesverband & CEO CertifAI

zur öffentlichen Anhörung des Ausschusses für Digitales
des Deutschen Bundestages am Mittwoch, 15. Mai 2024

Inhaltsverzeichnis

Vorbemerkung

Mit der KI-Verordnung schafft die Europäische Union erstmals einen umfassenden Regulierungsrahmen für Künstliche Intelligenz (KI). Auch wenn die endgültige Verabschiedung durch den Rat der Europäischen Union noch aussteht, ist klar, dass das Gesetz höchstwahrscheinlich noch im ersten Halbjahr des Jahres 2024 in Kraft treten wird. Der Zeitplan für die Umsetzung dieser weitreichenden Software-Regulierung sowohl auf nationaler als auch auf EU-Ebene ist eng.

Kurzfristig wird sich der nationale Gesetzgeber insbesondere mit der Ausgestaltung der nationalen Aufsichtsstrukturen, den Kriterien des Testens von KI-Systemen und vor allem der Einflußnahme der KI-Verordnung auf die sektorale Regulierung befassen müssen.

Das deutsche und auch europäische KI-Ökosystem besteht zu einem großen Teil aus KMU. Für diese Unternehmen ist es entscheidend, dass durch die KI-Verordnung keine doppelten Regulierungen und Zulassungsverfahren entstehen, die sie angesichts des rasanten technologischen Fortschritts in ihrer Innovationskraft bremsen und hohe Zusatzkosten verursachen. Es bedarf einer schlanken Umsetzung und klarer Zuständigkeiten, um insbesondere Zulassungsverfahren nicht unnötig zu verzögern.

Diese Stellungnahme bezieht sich auf den Fragenkatalog der Bundestagsfraktionen vom 26. April 2024, der 18 Fragen umfasst.[1] Aus Gründen der Kohärenz und Übersichtlichkeit wurden die zu beantwortenden Fragen thematisch gruppiert (siehe Inhaltsverzeichnis). Bei deutlichen inhaltlichen Überschneidungen wird zu mehreren Fragen eine gemeinsame Antwort gegeben.

Berlin, den 13. Mai 2024

[1] Siehe: https://www.bundestag.de/resource/blob/999958/0d7adea910b67e0c6b7a60460f645f12/Fragenkatalog-KI.pdf (Abgerufen am 12.05.2024).

I. Nationaler Umsetzungsbedarf und gesetzgeberischer Spielraum

Frage 2: ***Der AI Act eröffnet den Mitgliedstaaten in der nationalen Umsetzung im Bereich Arbeit Spielräume. Wie sollten diese Spielräume im Sinne gestärkter Arbeitnehmer:innenrechte genutzt werden?***

Die KI-Verordnung der EU[2] ist im Kern eine horizontale Produktsicherheitsverordnung und regelt die Entwicklung, den Einsatz und die Nutzung von KI anhand definierter Risikokategorien. Die Stärkung von Arbeitnehmer:innenrechten ist vielfach im Gesetz angelegt und kann durch die nationalen Gesetzgeber und Aufsichtsbehörden über die folgenden Prozesse adressiert werden. Zum einen fallen KI-Systeme, die am Arbeitsplatz in den Bereichen Recruiting (z.B. zur Einstellung oder Bewertung von Bewerber:innen) oder Personalmanagement (z.B. zur Unterstützung von Entscheidungen über Beförderungen oder Entlassungen, Aufgabenzuweisungen oder Leistungsbeurteilungen von Arbeitnehmer:innen) eingesetzt werden, in die Hochrisikokategorie nach Anhang III Nr. 4 KI-Verordnung, wodurch der Einsatz solcher KI-Anwendungen strengen regulatorischen Anforderungen unterliegt und damit nur unter Begleitung eines umfassenden Risiko- und Qualitätsmanagements sowie der Sicherstellung menschlicher Aufsicht umgesetzt werden darf. Zum anderen verpflichtet die KI-Verordnung mit Art. 26 Abs. 7 Betreiber vor dem Einsatz von KI-Anwendungen, die als Hochrisiko-Anwendungen klassifiziert werden, Arbeitnehmer:innenvertretungen und betroffene Arbeitnehmer:innen über den Einsatz zu informieren. Dabei können laut des Gesetzestextes nationale Besonderheiten und Vorschriften mit Blick auf die Information der Arbeitnehmer:innen berücksichtigt werden. Ein weiterer Schutz der Arbeitnehmer:innenrechte findet sich in der nach Art. 27 KI-Verordnung vorgeschriebenen Grundrechte-Folgeabschätzung, in der dargelegt werden muss, wie z.B. die menschliche Überwachung sichergestellt werden soll, welche potenziellen Risiken die Einführung eines entsprechenden KI-Systems für betroffene Personen, also auch Arbeitnehmer:innen, mit sich bringt bzw. welche Maßnahmen bei Eintritt eines solchen Risikos zu ergreifen sind.[3]

Darüber hinaus verpflichtet die KI-Verordnung die Europäische Kommission in Art. 6 Abs. 5, innerhalb von 18 Monaten nach Inkrafttreten über das AI Board konkrete Leitlinien zur praktischen Umsetzung von Art. 6 KI-Verordnung zur Qualifizierung von Hochrisiko-KI-Anwendungen sowie eine umfassende Liste beispielhafter Anwendungsfälle

[2] Gesetzesstellen beziehen sich in dieser Stellungnahme auf den Text des Corrigendums des Europäischen Parlaments vom 17.04.2024, abrufbar unter: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf (Abgerufen am 06.05.2024).

[3] Zu den Auswirkungen des Einsatzes von KI-Systemen auf den Arbeitsmark und der dabei zentralen menschlichen Aufsicht und Autonomie siehe auch Kilian, R. (2024). *Schriftliche Stellungnahme für die 53. Sitzung des Ausschusses für Kultur und Medien des Deutschen Bundestages vom 20. März 2024*. https://ki-verband.de/wp-content/uploads/2024/03/KIBV_Stellungnahme_BTAusschuss-Kultur-Medien_20240320.pdf (Abgerufen am 10.05.2024).

zu veröffentlichen. In diesem Gremium kann sich der nationale Gesetzgeber entsprechend einbringen und sich für eine Stärkung der angesprochenen Rechte aussprechen. Weitergehende nationale Maßnahmen, wie in Art. 2 Abs. 11 KI-Verordnung vorgesehen, sind aufgrund des Bedürfnisses einzelner Mitgliedstaaten, namentlich vor allem Spanien entstanden um bereits geltende nationale KI-Regulierung zum Schutz von Arbeitnehmer:innenrechten beibehalten zu können.

Die Bundesregierung sollte sich über das AI Board an der in Art. 6 Abs. 5 KI-Verordnung vorgesehenen Erstellung von Leitlinien zur praktischen Umsetzung von Art. 6 KI-Verordnung beteiligen. Da diese Leitlinien auch den in Anhang III aufgeführten Bereich '*Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit'* und die in diese Kategorie fallenden KI-Systeme betreffen, eröffnet sich eine entscheidende Mitgestaltungsmöglichkeit zur Stärkung der Arbeitnehmer:innenrechte. Für die Erstellung und Veröffentlichung dieser Leitlinien bleibt für die wartende KI-Praxis zu hoffen, dass dies nicht unter voller Ausnutzung der gesetzlichen Frist von 18 Monaten geschieht, sondern deutlich früher Rechtssicherheit in den Unternehmen und bei den Arbeitnehmer:innen geschafft werden kann. Insgesamt sind in den Leitlinien Maßgaben und Beispiele für den Bereich Arbeit und KI-Systeme zu wählen, die vor allem das Vertrauen der Arbeitnehmer:innen in die genutzten KI-Systeme schaffen.

Frage 4: ***Inwieweit beinhaltet der AI Act Instrumente zum Kampf gegen Desinformation, wie spielt er mit dem DSA zusammen und inwieweit ergeben sich daraus Handlungsempfehlungen für die nationale Ebene?***

Die KI-Verordnung beinhaltet keine spezifischen Instrumente gegen Desinformation. Es handelt sich bei dem Rechtsakt um ein generalisiert wirkendes Instrument der Produktsicherheit, welches sich an Anbieter und Nutzer von KI-Systemen richtet. Allerdings sind einige Vorschriften der KI-Verordnung durchaus so zu verstehen, dass sie sich auch gegen Desinformation richten können.

- So verbietet Art. 5 Abs. 1 lit. a) KI-Verordnung bestimmte Manipulationssysteme. Diese müssen allerdings einen Schaden bei Einzelpersonen oder Gruppen verursachen; viel spricht dafür, auch Schäden am Schutzgut der "unverfälschten öffentlichen Meinungsbildung" - wie es insbesondere in Art. 34 DSA anerkannt wird - hinreichen zu lassen, womit in Grenzfällen KI-Systeme gegen Desinformation auch durch die KI-Verordnung verboten sein können.

- Art. 9 KI-Verordnung verpflichtet Anbieter von Hochrisiko-KI-Systemen zudem zum permanenten Risikomanagement. Auch Desinformation lässt sich ohne weiteres unter den sehr weiten Risikobegriff fassen.

- Art. 10 Abs. 2 lit. f) KI-Verordnung verpflichtet Anbieter von Hochrisiko-KI-Systemen dazu, die Trainingsdaten und -modelle auf Schädlichkeit gegenüber Grundrechten und auf Diskriminierungen zu prüfen. Art. 10 KI-Verordnung soll insgesamt diskriminierungsfreie KI-Anwendungen sicherstellen, was tendenziöse Desinformation ausschließt.

- Darüber hinaus verpflichtet Art. 15 Abs. 4 KI-Verordnung Anbieter von Hochrisiko-KI-Systemen dazu, die Systeme resilient auszugestalten, insbesondere auch in der Interaktion mit natürlichen Personen, welche die Ergebnisse gezielt verfälschen könnten. Anlassgebend für diese Vorschrift war die Reaktion von Chatbots auf rechtsradikales Gedankengut von Nutzern mit der Verbreitung desselben.

Insgesamt können die genannten Vorschriften der KI-Verordnung als Ergänzung zum Programm des DSA verstanden werden. Sie können insbesondere andere Adressaten haben als die Anbieter von Digitalen Diensten, was dann relevant wird, wenn der Anbieter Digitaler Dienste nicht zugleich Anbieter eines KI-Systems ist. Dies kann etwa der Fall sein, wenn der Anbieter eines Digitalen Dienstes kein KI-System entwickelt oder entwickeln lässt (vgl. Art. 4 Abs. 3 KI-Verordnung), sondern über eine Schnittstelle einen Drittanbieter einschaltet (in diesen Fällen wäre der Anbieter des Digitalen Dienstes allenfalls Nutzer des KI-Systems iSd. Art. 4 Abs. 4 KI-Verordnung). Neuer Rechtsvorschriften im Rahmen der KI-Verordnung bedarf es auf dieser Basis nicht. Sowohl DSA als auch KI-Verordnung sehen eine ganze Reihe an Regelungsinstrumenten vor. An dieser Stelle kann als Handlungsempfehlung auf nationaler Ebene aber die umfassende und zeitnahe Umsetzung der behördlichen Strukturen empfohlen werden (vgl. dazu II. Aufsichtsstruktur und Marktüberwachung), welche DSA und KI-Verordnung vorsehen, um KI-Anwendungen insbesondere auf Medienplattformen zu identifizieren und die Pflichten von DSA und KI-Verordnung mit besonderer Rücksicht auf das hohe Gut unverzerrter Informationsräume durchzusetzen.

> **Frage 10:** ***Wie sollte die nationale Gesetzgebung zur Umsetzung des AI Acts strukturiert werden, um einerseits detaillierte und spezifische Anforderungen zu adressieren und andererseits genügend Flexibilität für zukünftige Anpassungen und die Berücksichtigung sektorspezifischer Bedürfnisse zu gewährleisten? Welche Vor- und Nachteile würden sich aus den verschiedenen regulatorischen Ansätzen ergeben?***

Im engen EU-Verordnungsrahmen liegt der Spielraum der nationalen Gesetzgeber vor allem in der Aufsicht über die KI-Systeme im Hochrisikobereich und in der Einflussnahme der KI-Verordnung auf einzelne, bislang nicht direkt von dem Gesetz erfassten Industriesektoren.

- Es gilt zeitnah mit einem entsprechenden Durchführungsgesetz die nationale Marktüberwachungsbehörde sowie die notifizierende Behörde zu bestimmen.[4] Dabei ist darauf hinzuweisen, dass dringend die Kohärenz mit bestehenden europäischen und deutschen Aufsichts- und Marktbeobachtungsmechanismen sichergestellt werden muss. Dies erfordert eine eingehende Prüfung und Identifizierung der Schnittmengen zwischen dem bestehenden Recht und der KI-Verordnung.[5] Doppelregulierungen und parallele Aufsichtszuständigkeiten sind zu vermeiden. So sollten für die Beaufsichtigung der nach Anhang III Nr. 5b KI-Verordnung einbezogenen KI-Systeme zur Kreditwürdigkeitsprüfung stets die nationalen Finanzmarktaufsichtsbehörden im Rahmen ihrer jeweiligen Zuständigkeiten auch als zuständige Behörden für die Beaufsichtigung der Durchführung der KI-Verordnung benannt werden. Für Deutschland sollte die BaFin für die Beaufsichtigung derartiger KI-Systeme benannt werden. Nach AT 4.3.5 der Mindestanforderungen an das Risikomanagement bei Banken (MaRisk) sind Institute ohnehin gezwungen, auch die KI-Komponenten ihrer Kreditrisikomodelle zu validieren. Die bestehende MaRisk Validierungspraxis dürfte aufgrund der neuen Kriterien zur Hochrisikosystemprüfung aus der KI-Verordnung anzupassen sein. Es bestehen zudem langjährige Aufsichtsbeziehungen zwischen der BaFin und den deutschen Finanzinstituten. Von der in Erwägungsgrund 158 am Ende vorgesehenen anderweitigen Verantwortungszuweisung an eine andere nationale Behörde sollte kein Gebrauch gemacht werden.

- Ein bislang zumindest in der Unternehmenspraxis kaum beachteter Punkt ist die Einflussnahme der KI-Verordnung auf die sektorale Regulierung der nicht dem NLF-Verfahren folgenden harmonisierten Vorschriften aus Anhang I Abschnitt B KI-Verordnung. So muss zum Beispiel nach Art. 104, 107 sektorale Automotiveregulierung, insbesondere die EU-Typengenehmigung, die in Kapitel III Abschnitt 2 KI-Verordnung festgelegten Anforderungen berücksichtigen. Damit werden die Voraussetzungen an Hochrisikosysteme aus der KI-Verordnung auch auf die zentralen europäischen und deutschen Homologationsvorschriften der Automotive-Industrie übertragen. Gleiches gilt nach Art. 103 KI-Verordnung auch für die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen

[4] Die „notifizierende Behörde“ ist gemäß Art. 3 Ziff. 19 KI-Verordnung “eine nationale Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist”.

[5] Siehe Abschnitt VIII.1 in Hacker, P. (2024). *Comments on the Final Trilogue Version of the AI Act*. https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf (Abgerufen am 10.05.2024).

Fahrzeugen.[6] Konkret wird so zum Beispiel erreicht, dass die KI-Komponenten bei den bereits aktuell vielfältig in Fahrzeugen eingesetzten KI-Systemen ebenfalls Teil des Testingkatalogs vor Typenzulassung von Fahrzeugen werden. Bei der jetzt erforderlichen Anpassung der europäischen Gesetze wie auch bei der Änderung der entsprechenden nationalen Durchführungsverordnungen sollten weitgehend die bestehenden Genehmigungsprozesse beibehalten werden. Produktbasierte KI-System Prüfung kann in die Homologationsverfahren des deutschen Produktsicherheitsrechts integriert werden. Mit Blick auf die Zulassungsverfahren in anderen Mitgliedsstaaten der EU ist durch Deutschland eine einheitliche Auslegung der entsprechenden Prüfungsvorschriften und Leitlinien anzustreben, um ein echtes Level playing field zu gewährleisten. Ausreichend Flexibilität kann durch die Ergänzung und Änderung technischer Normen im Rahmen der sektoralen Regulierung erreicht werden. Die Einbringung der Hochrisiko-Grundsätze der KI-Verordnung in die sektorale Regulierung wird die nationalen Gesetzgeber, die Aufsichtsbehörden und vor allem die Anwender der KI-Verordnung in den nächsten Jahren noch umfassend beschäftigen.

- Darüber hinaus ist der nationale Gesetzgeber bei der Ausgestaltung der Reallabore gefordert, jetzt spezifische Anforderungen zu setzen, um aus diesem auch in der Vergangenheit nicht immer funktionierenden Konstrukt ein echtes Instrument der Innovationsförderung entstehen zu lassen. Darüber hinaus ist der Gesetzgeber nach Art. 57 Abs. 10 KI-Verordnung verpflichtet, die Datenschutzbehörden angemessen in den Betrieb der Reallabore einzubeziehen, was die Aufgabe bedingt, eine differenzierte Auslegung der KI-Verordnung aufgrund der föderalen Kompetenzverteilung der deutschen Datenschutzbehörden zu vermeiden. Weiter ist es Aufgabe des nationalen Gesetzgebers, Anreize zur Teilnahme an KI-Reallaboren zu berücksichtigen und entsprechend zu adressieren sowie mögliche negative Folgen für die teilnehmenden Unternehmen, z. B. im Bereich des Haftungsschutzes oder der Marktaufsicht, frühzeitig abzumildern.
  Weitergehende konkrete Empfehlungen zur Ausgestaltung von KI-Reallaboren finden sich in der Antwort zu Frage 9.

Frage 11: ***Welche Ideen und Herangehensweisen zur Umsetzung des AI-Act sind Ihnen aus den anderen EU-Mitgliedstaaten bislang bekannt und welche dieser***

[6] Ebenso auf **Schifffahrtsindustrie** mit Änderung der Richtlinie 2014/90/EU vom 23.07.2014 über Schiffsausrüstung, **Eisenbahn-Industrie** mit Änderung der Richtlinie (EU) 2016/797 vom 11.05.2016 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union, **Luftfahrt-Industrie** mit Änderung der Verordnung (EU) 2018/1139 vom 04.07.2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit.

sollten in Deutschland für die Umsetzung genauer betrachtet bzw. einbezogen werden?

Für das offizielle Inkrafttreten ist noch die endgültige Abstimmung im Rat der Europäischen Union und die anschließende Veröffentlichung im Amtsblatt erforderlich. Dementsprechend befinden sich nach meinem Kenntnisstand viele Prozesse zur nationalen Umsetzung der KI-Verordnung in den einzelnen Mitgliedstaaten noch im Anfangsstadium. Die nachfolgenden Ausführungen berücksichtigen die zum Zeitpunkt dieser Anhörung am 15. Mai 2024 bekannten Prozesse.

So wurde im Juni 2022 ein Pilotprojekt Spaniens zur Einrichtung einer ersten Regulatory Sandbox angekündigt, die im November letzten Jahres per königlichem Dekret offiziell gestartet wurde.[7] Dieses erste europäische KI-Reallabor nach den Gestaltungsvorgaben der KI-Verordnung befindet sich derzeit im Aufbau und soll als Pilotprojekt auch den anderen EU-Mitgliedstaaten als Unterstützung und Vorbild dienen. Es ist zunächst offen für KI-Systeme, die sich bereits auf dem Markt befinden, für solche, die sich in einer substanziellen Änderungsphase befinden und die sich bereits in einem ausreichenden Entwicklungsstadium befinden, so dass davon ausgegangen werden kann, dass sie innerhalb des definierten Zeitrahmens des Reallabors auf den Markt gebracht werden können.[8] Das Reallabor zielt dabei darauf ab, dass in der kontrollierten Testumgebung des KI-Reallabors KI-Anwendungen aus dem Hochrisikobereich gemäß Art. 6 in Verbindung mit den Anhängen I und III der KI-Verordnung sowie General Purpose AI-Modelle gemäß Kapitel V bzw. Art. 51ff. KI-Verordnung unter direkter Aufsicht gemäß den regulatorischen Anforderungen der KI-Verordnung getestet werden können. Das KI-Reallabor steht sowohl privatwirtschaftlichen als auch öffentlichen Organisationen offen.[9] Zu weiteren Einzelheiten des spanischen Vorstoßes bei der Etablierung von Reallaboren für KI-Systeme verweise ich auf meine Antwort zu Frage 6.

Als bislang einziger EU-Mitgliedstaat hat Spanien zudem bereits im August 2023 die *Agencia Española de Supervisión de la Inteligencia Artificial* (AESIA) gegründet und ist damit der erste EU-Mitgliedstaat mit einer eigenen Behörde zur Umsetzung der KI-Verordnung.[10] Insbesondere im Hinblick auf die nationale Überwachung und die entsprechenden Marktüberwachungsbehörden ist jedoch in den anderen Mitgliedstaaten noch keine klare

[7] Siehe: https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented (Abgerufen am 10.05.2024).
[8] Rivaya, J. F., & Vidal, A. (29.09.2023). *Spain: The artificial intelligence regulatory "sandbox" has arrived*. Lexology. https://www.lexology.com/library/detail.aspx?g=99939c25-d7bb-4d06-b154-4a972eb71e9b (Abgerufen am 10.05.2024).
[9] Bru, P. & Vidal, L. (17.11.2023). *Spain legislates for first EU AI Act regulatory sandbox*. Pinsent Masons. https://www.pinsentmasons.com/out-law/news/spain-legislates-for-first-eu-ai-act-regulatory-sandbox (Abgerufen am 10.05.2024).
[10] Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2023). Real Decreto 729/2023. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-18911 (Abgerufen 10.05.2024).

Richtung erkennbar.[11] In einigen Mitgliedstaaten wird die Einrichtung einer eigenen, ausschließlich zuständigen Behörde favorisiert.[12] In anderen Mitgliedstaaten wird hingegen die Übertragung der Aufsichtskompetenz auf bestehende Behörden diskutiert. Dabei stehen unterschiedliche Behörden im Vordergrund. In Frankreich, aber auch in den Niederlanden wird die nationale Aufsicht voraussichtlich den nationalen Datenschutzbehörden übertragen.[13] Dabei wird die Angliederung an Datenschutzbehörden gerade bei kleineren Staaten auch aus Kostengründen erfolgen. Eine weitere weit diskutierte Option ist die Angliederung der Aufsichtskompetenz an nationale Cybersicherheitsbehörden in einigen Mitgliedstaaten.

Für die Aufstellung einer komplett eigenständigen KI-Aufsichtsbehörde dürfte - wie in II. dargelegt - die Zeit fehlen. Auch besteht das Risiko, dass eine solche Behörde zu viele Kompetenzen an sich zieht, was dann zu einer Zersplitterung der Zuständigkeiten im Rahmen der Marktaufsicht führen kann.

II. Aufsichtsstruktur und Marktüberwachung

Frage 1: ***Wie muss die nationale Aufsicht aufgestellt sein, um eine möglichst kohärente, schlanke Governance zu gewährleisten? Wie gelingt uns trotz sektoraler Zuständigkeiten und föderaler Aufteilung der vielzitierte One-Stop-Shop? Welche genauen Aufgaben sollte die Aufsicht übernehmen?***

Frage 12: ***Wie kann bei der Marktüberwachung mit Blick auf die hohe Zahl in Deutschland existieren der Stellen und die aktuell sehr unterschiedliche Verteilung von bundesweiten bis hin zu regionalen Zuständigkeiten eine geographische und sektorale Zersplitterung verhindert werden, im Sinne einer effizienten, möglichst auf Bundesebene koordinierten Aufsicht und welche gesetzlichen Änderungen könnten aus Ihrer Sicht notwendig werden, um dieses Ziel zu erreichen?***

Hinsichtlich der Bestimmung und Ausgestaltung der nationalen Aufsicht, bestehend aus der in Art. 70 Abs. 1 KI-Verordnung genannten Marktüberwachungsbehörde und der notifizierenden Stelle ist festzuhalten, dass die nach Art. 70 Abs. 2 KI-Verordnung gesetzte Frist von zwölf

[11] Eine informelle Umfrage unter den Mitgliedern des European AI Forum, dem europäischen Dachverband von neun nationalen KI-Verbänden, dem auch der KI Bundesverband als Gründungsmitglied angehört, hat ergeben, dass in einem Großteil der Mitgliedsstaaten die Diskussionen über die nationale Aufsicht und die zuständigen Behörden ebenfalls erst begonnen haben und Ergebnisse erst in den nächsten Monaten zu erwarten sind.

[12] Für detaillierte Ausführungen siehe z.B.: Borruey, M. V., Latasa Vassallo, L. M., & Ñíguez Olalla, M. (22.11.2023). *Spain: Agency for the supervision of AI - overview*. DataGuidance. https://www.dataguidance.com/opinion/spain-agency-supervision-ai-overview (Abgerufen am 10.05.2024).

[13] Niederlande: Grazette, M. (22.02.2023). *AI regulation around the world: the Netherlands*. https://www.holisticai.com/blog/the-netherlands-ai-regulation (Abgerufen am 10.05.2024).
Frankreich: Hartmann, T., & Hartmann, T. (16.05.2023). *French data protection authority lays out action plan on AI, ChatGPT*. Euractiv. https://www.euractiv.com/section/artificial-intelligence/news/french-data-protection-authority-lays-out-action-plan-on-ai/ (Abgerufen am 10.05.2024).

Monaten nach Inkrafttreten des Gesetzes für die Auswahl, Benennung und den Aufbau der entsprechenden Aufsichtsbehörde sehr knapp bemessen ist. Die für Deutschland zuständige Aufsichtsbehörde ist zeitnah zu benennen. Eine originär zu diesem Zweck geschaffene KI-Aufsichtsbehörde dürfte zum jetzigen Zeitpunkt nicht als Option in Betracht kommen.[14] Vielmehr bietet sich zur Verkürzung der Aufbauzeit eine Eingliederung in eine bestehende Bundesoberbehörde an. Trotzdem bleibt eine gebündelte Umsetzung von Digitalregulierungen langfristig sinnvoll.[15] Vorzugswürdig erscheint mir daher jetzt eine existierende Bundesbehörde zu benennen, diese schnell mit einem schlagkräftigen Kompetenzmix aus Behördenmitarbeitern und extern einzustellenden KI-Fachleuten auszustatten und ggfls. nach einiger Zeit eine Abspaltung zu einer eigenständigen KI-Aufsichtsbehörde zu evaluieren.

Bei der Wahl der KI-Aufsichtsbehörde und der Frage der Marktüberwachung sind die Besonderheiten der föderalen Strukturen in Deutschland zu berücksichtigen. Die Bundesländer sind grds. für den Vollzug der Marktüberwachung zuständig. Die KI-Marktüberwachung sollte aber - um ein einheitliches Aufsichtsregime zu fördern - mindestens auf Bundesebene koordiniert werden, was aufgrund der tlw. grundgesetzlich festgelegten Zuständigkeit durch einen KI-Staatsvertrag der Bundesländer unter Beteiligung des Bundes, etwa nach dem Vorbild des Rundfunkstaatsvertrags, abgesichert werden könnte. Denkbar ist, dass die Bundesländer auch einzelne Marktüberwachungskompetenzen an den Bund übertragen könnten; auch die Mischverwaltung stellt eine Option dar. Im Ergebnis braucht es auf Bundesebene eine schlagkräftige Koordinierungsstelle, die selbst bei vereinzelter Zuständigkeit der Bundesländer mit einer agilen Taskforce beratend zur Seite steht.

Mit Blick auf die Auswahl und die Ausgestaltung der nationalen Aufsicht in anderen Mitgliedstaaten der Europäischen Union verweise ich auf die Antwort zu Frage 11.

An dieser Stelle wird auch appelliert, dass nicht nur auf nationaler Ebene eine Abstimmung zwischen den zuständigen Marktüberwachungsbehörden sichergestellt wird, sondern dass sich der nationale Gesetzgeber auch auf EU-Ebene für eine europaweit harmonisierte Durchsetzung und Überwachung einsetzt. Deutsche und europäische KI-Unternehmen vermarkten ihre Anwendungen überwiegend mit gesamteuropäischen oder gar globalen Strategien und beschränken sich nicht auf einzelne nationale Märkte. Sie benötigen daher vor allem innerhalb des europäischen Binnenmarktes eine einheitliche Auslegung der

[14] Siehe auch: Novelli, C., Hacker, P., Morley, J., Trondal, J. & Floridi, L. (2024). *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*. https://dx.doi.org/10.2139/ssrn.4817755 (Abgerufen am 14.05.2024).

[15] Neben der KI-Verordnung zum Beispiel auch die Aufsicht im Rahmen des Cyber Resilience Act, Data Act, Digital Services Act. Ebenso Seite 6 in Verbraucherzentrale Bundesverband (2024). *AI-Act Verbraucher:innen bei der Umsetzung berücksichtigen*. https://www.vzbv.de/sites/default/files/2024-04/24-04-18_Positionspapier_vzbv_AI-Act_Umsetzung.pdf (Abgerufen am 10.05.2024).

KI-Verordnung sowie harmonisierte Prozesse und Mechanismen zwischen den EU-Mitgliedstaaten und europaweit einheitliche rechtliche Vorgaben.

> **Frage 5:** ***Bitte beschreiben Sie die rechtlichen Anforderungen des AI Act an die zuständigen nationalen Behörden: Wie ist insbesondere die Vorgabe auszulegen, dass die Behörden ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen ausüben müssen, und welche Regelungsoptionen zur Aufsichtsstruktur sind im nationalen Umsetzungsgesetz vor dem Hintergrund der bestehenden rechtlichen und organisatorischen Strukturen der Marktüberwachung (MÜ-VO, MÜ-G, RAPEX Informationssystem, Deutsches Forum für Marktüberwachung) denkbar, zulässig und mit Blick auf den Regelungsgegenstand KI-Systeme sachgerecht?***

Siehe Antworten zu den Fragen 1 und 12.

> **Frage 8:** ***Welche gesetzlichen und politischen Maßnahmen sind notwendig, um die Zusammenarbeit zwischen den zuständigen Behörden in Deutschland und den Einrichtungen auf EU-Ebene (insbesondere AI Office, AI Board, Advisory Forum und Scientific Panel) schlagkräftig und effizient aufzustellen und wie lässt sich gewährleisten, dass zivilgesellschaftliche und interdisziplinäre wissenschaftliche Expertise bei der Auslegung, Konkretisierung, Umsetzung und Weiterentwicklung des AI Acts substantiell Berücksichtigung finden?***

Um eine adäquate und signifikante Beteiligung Deutschlands und aller seiner Stakeholder aus Wissenschaft, Wirtschaft und Zivilgesellschaft in diesen Gremien sicherzustellen, ist in erster Linie ein politisches Signal erforderlich, welches das Engagement langfristig sichert und incentiviert. Die Verantwortung liegt bei den federführenden Bundesministerien, entsprechend kompetentes Fachpersonal aus den Ministerien in das AI Board und in die nationalen KI-Behörden zu entsenden. Zudem sollten Fachkräfte aus der Wissenschaft, Wirtschaft und der Zivilgesellschaft entsprechend motiviert werden, sich bei diesem Thema einzubringen.

Die zweite Seite dieser Frage betrifft die interbehördliche Zusammenarbeit zwischen den aufzubauenden EU-Gremien (AI Office, AI Board, Advisory Forum und Scientific Panel) sowie den in Deutschland zu bestimmenden Aufsichtsbehörden. Um die Zusammenarbeit zwischen den für Deutschland zuständigen nationalen Aufsichtsbehörden und primär dem AI Office sicherzustellen, wird empfohlen, zügig standardisierte und permanente interbehördliche Kommunikations- und Kollaborationsprozesse aufzubauen. Diese könnten jeweils mit einem sektorspezifischen Fokus und einer divers besetzten Taskforce ausgestaltet werden. Die Etablierung solcher Gremien würde zudem gewährleisten, dass alle Stakeholder über potenzielle Entwicklungen auf nationaler wie auch europäischer Ebene informiert sind,

beispielsweise im Falle einer nachträglichen Änderung der KI-Verordnung durch delegierte Rechtsakte der Europäischen Kommission.

Darüber hinaus sollte ein nationales KI-Beratungsforum - entsprechend dem europäischen Pendant des Advisory Forums nach Art. 67 KI-Verordnung - etabliert werden. Das Forum hat nicht nur die Aufgabe, sich mit dem europäischen Advisory Forum abzustimmen, sondern berät primär die nationale Aufsichtsbehörde bei der Einbringung wissenschaftlicher und industriespezifischer Belange. Mitglieder sollten neben der Industrie, Start-up-Unternehmen, KMU, Vertreter aus der Zivilgesellschaft und die Wissenschaft sein.

Frage 16: ***Das neu einzurichtende Europäische AI-Büro soll „eine Schlüsselrolle bei der Umsetzung des KI-Gesetzes spielen, indem sie die Leitungsorgane in den Mitgliedstaaten bei ihren Aufgaben unterstützt". Sollte mit dieser „Unterstützung" eine Kontrolle und eine Weisungsbefugnis verbunden sein? Wo sollte das AI-Büro angesiedelt und wie sollte es personell, finanziell und organisatorisch ausgestattet sein, damit man es „politisch unabhängig" nennen könnte?***

Selbstverständlich muss das AI Office personell mit entsprechender Fachexpertise besetzt und finanziell so ausgestattet werden, dass es seinen Aufgabenkatalog effizient und kompetent erfüllen kann. Die nach meinem Kenntnisstand bereits im Aufbau befindliche Angliederung des AI Office an die Europäische Kommission, insbesondere an die Generaldirektion für Kommunikationsnetze, Inhalte und Technologien (GD Connect), ist insofern zu begrüßen, als dass der unmittelbar anstehende Aufbau des AI Office nicht durch einen eigenständigen Behördenaufbau unnötig in die Länge gezogen wird, was sich maßgeblich negativ auf das europäische KI-Ökosystem auswirken würde. Auch wird der Rückgriff auf vorhandene Fachexpertise einfacher möglich sein.

III. Testing von KI-Systemen und Konformitätsbewertung

Frage 7: ***Welche politischen und gesetzlichen Maßnahmen sind notwendig, um die im AI Act vorgesehenen harmonisierten Standards, gemeinsamen Spezifikationen und Zertifizierungsmechanismen für KI-Systeme voranzutreiben und das Konformitätsbewertungsverfahren insgesamt so auszugestalten, dass es für Unternehmen effizient umsetzbar ist, für Verbraucher*innen aber zugleich ein hinreichendes Schutzniveau gewährleistet?***

Frage 13: Inwiefern lässt der AI Act, was die Prüfungen von KI-Systemen angeht, Ihrer Ansicht nach genügend Raum für eine fortwährende Anpassung der Prüfschemata- und Kriterien an die sich schnell vollziehende weitere technologische Entwicklung bei KI, an welchen Stellen könnten hier mittelfristig

Probleme entstehen und welche Maßnahmen sind bei der Umsetzung des AI-Act von Anfang an mitzudenken, um ausreichenden Spielraum für innovationsorientierte Anpassungen sicherzustellen?

Der zeitnahe Erlass der harmonisierten Standards ist eine der wichtigsten Voraussetzungen für eine innovationsfreundliche Umsetzung der KI-Verordnung. Insbesondere KMU müssen mit massiven Compliance-Kosten rechnen, wenn die Möglichkeit der Konformitätsvermutung im Rahmen der erforderlichen Konformitätsbewertungsverfahren nicht mit ausreichendem Implementierungsvorlauf geschaffen wird.[16] Eine anderweitige Herstellung der Compliance mit der KI-Verordnung ist gerade bei einem technisch komplexen Gesetz in vielen Fällen nur mit massivem Zeit- und externem Beratungseinsatz möglich. Die folgenden Maßnahmen würden dazu beitragen, die für die Umsetzung der KI-Verordnung so wichtigen Standards für KI-Systeme voranzutreiben:

- Deutschland sollte sich dafür einsetzen, dass international anwendbare ISO/IEC-Normung, insbesondere ISO/IEC 42001 und ISO/IEC 42006, zur Grundlage der harmonisierten Standards nach Art. 40 KI-Verordnung wird. Europäische Besonderheiten können bei Bedarf in den regulativen Anhängen (Anhänge Z) abgebildet werden. Nur so kann eine Fragmentierung des Weltmarktes und gleichzeitig gravierende Nachteile für europäische und deutsche Anbieter, insbesondere bei Exporten in die USA und China, vermieden werden.

- Eine Reihe nationaler Initiativen leistet bereits entscheidende Vorarbeiten für die technische Normierung unter der KI-Verordnung. So entwickelt beispielsweise CertifAI mit Mission KI[17] im Auftrag des Bundesministeriums für Digitales und Verkehr zusammen mit Fraunhofer IAIS, PwC Deutschland, VDE, TÜV AI Lab und dem AI Quality & Testing Hub bereits heute KI-Verordnungskonforme Prüfansätze, also Kriterien und Werkzeuge, um eine breite und skalierbare Anwendung von KI zu gewährleisten. Konkrete Use Cases von KI-Systemherstellern werden bei dem Projekt einbezogen. Weitere Initiativen sind der für den sicheren Einsatz von KI-Systemen in der Cloud geschaffene BSI AIC4 Standard[18], der in Zusammenarbeit von u.a. Bosch,

[16] Allgemein zur Durchführung und zu den Arten der Konformitätsbewertung unter der KI-Verordnung Denga, M. (2023). *Konformitätsbewertung von KI-Systemen*. ZfPC 2023, 154.; Ders. (2023). *Unternehmenshaftung für KI – zur Konformitätsbewertung in Permanenz*. CR 2023, 277ff.

[17] Pressemitteilung zu Mission KI - Säule 2: Mission KI (2023). *Mission KI – Nationale Initiative entwickelt KI-Prüfansätze und zwei KI-Zentren*. Presseinformation, 24.11.2023. https://mission-ki.de/wp-content/uploads/2023/11/2023-11-24-Mission-KI-Presseinformation.pdf. (Abgerufen am 11.05.2024).

[18] BSI. *Kriterienkatalog für KI-Cloud-Dienste – AIC4*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/AIC4/aic4.html (Abgerufen am 11.05.2024).
Insbesondere im Umfeld digitaler Dienste hat die deutsche Verwaltung mit dem BSI C5 für Cloud einen weltweiten Standard gesetzt. Die Chance, Erfahrungswerte in der KI-Prüfung zu sammeln und diese in praktikable Normierungsarbeit einfließen zu lassen, bestünde auch, wenn der BSI AIC4, der den BSI C5 um KI ergänzt, ebenfalls zum Mindeststandard würde.

Siemens und VDE herausgegebene Spec 90012[19] oder der von Wissenschaftlern der Universität Oxford erarbeitete capAI-Katalog für Konformitätsbewertungen[20]. Für die jetzt anstehende finale Phase der Normungsarbeit sollte noch stärker auf diese frühen europäischen Forschungsarbeiten zurückgegriffen werden, um schneller Rechtssicherheit für die Unternehmen zu erreichen, aber auch um die Belange und Besonderheiten gerade der deutschen und europäischen Industrie angemessen in die technische Normgebung zu übertragen.

- Deutschland ist im Bereich der KI-Absicherung und der zugrundeliegenden regulatorischen und technischen Forschung eine der weltweit führenden Nationen. Die hier bereits vorliegenden Erkenntnisse, insbesondere aus der Qualitätssicherung, sollten noch breiter Eingang in die technische Normierung finden. Derzeit werden nach unserer Beratungserfahrung Forschungsergebnisse oft direkt in die Compliance-Anwendung überführt. Für die aktuellen Fragestellungen bedarf es jedoch deutlich mehr Kapazitäten im wissenschaftlichen Bereich, va. Lehrstühle für KI-Regulierung und Qualitätssicherung von KI-Systemen. Trotz der Initiativen aus der freien Wirtschaft (siehe oben) sind entscheidende wissenschaftliche Grundlagen für die Konformitätsbewertung von KI-Systemen noch nicht erarbeitet. So fehlen beispielsweise Referenzwerte für "qualitativ hochwertige Daten", Methoden zur Messung der Vertrauenswürdigkeit von KI-Systemen und der Robustheit bestimmter Modelltypen. Um diese Lücken zu schließen, sind Forschungsprojekte notwendig, an denen Wissenschaftler aus dem Bereich der KI-Absicherung, Konformitätsbewertungsstellen, nationale Akkreditierungsstellen und Bundesforschungseinrichtungen wie die Physikalisch-Technische Bundesanstalt (PTB) und die Bundesanstalt für Materialforschung und -prüfung (BAM) beteiligt sein sollten.

- Die Europäische Kommission sollte zeitnah eine weitere Leitlinie nach Art. 96 KI-Verordnung auch für die Durchführung der Konformitätsbewertung herausgeben. Die Praxis benötigt pragmatische Hilfestellungen auch bei der Auslegung der Anhänge. So ist zum Beispiel nicht abschließend geklärt, inwieweit die Konformitätsbewertung (richtigerweise) auch evidenzbasiertes Software-Testing erfordert oder ob eine rein Risikomanagement-basierte Prüfung rglm. ausreicht.

- Bislang ist nicht geklärt, wie genau Konformitätsbewertungsstellen akkreditiert werden können. Art. 28-31 KI-Verordnung beschreiben lediglich die grundlegenden Sicherheitsanforderungen an die notifizierten Stellen. Insbesondere für die komplexen

[19] VDE (2022). *Kann Künstliche Intelligenz wertekonform sein? VDE SPEC als Grundlage künftiger Entwicklungen*. https://www.vde.com/de/presse/pressemitteilungen/ai-trust-label (Abgerufen am 11.05.2024).
[20] Floridi, L. et al. (2022). *capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act*. https://dx.doi.org/10.2139/ssrn.4064091 (Abgerufen am 11.05.2024).

deutschen föderalen Strukturen könnte es sinnvoll sein, auf das etablierte System des AkkStelleG mit dem zweistufigen System aus Akkreditierung und nachfolgender Notifizierung durch die Behörde zurückzugreifen. So kann der Aufbau unnötiger, doppelter Verwaltungsstrukturen und insbesondere eine doppelte Prüfung für die Hersteller von KI-Systemen verhindert werden. Die Erteilung der Notifizierung erfolgt dann auf der Grundlage einer Akkreditierung im Sinne der Verordnung (EG) 765/2008 durch die nationale Akkreditierungsstelle. Dies hätte den Vorteil, dass auf bestehende Strukturen zurückgegriffen werden kann. Akkreditierungs- und Konformitätsbewertungsstellen arbeiten auch in anderen hochtechnisierten Prüfverfahren seit Jahren zusammen. Für KMU ist es erforderlich, dass sie durch Förderprogramme in die Lage versetzt werden, die Anlauf- und Entwicklungskosten der KI-System-Zertifizierungsprogramme mit der Konformitätsbewertungsstelle möglichst kostensparend zu gestalten.

Die Konformitätsbewertungsverfahren sind für deutsche Unternehmen nur dann effizient umsetzbar, wenn auch die zugrundeliegende technische Normierung auf ihre spezifischen Bedürfnisse ausgerichtet ist. In den entsprechenden Gremien der deutschen und europäischen Standardisierungsorganisationen sind KMU jedoch kaum vertreten. Dabei sind es gerade kleinere Unternehmen und Mittelständler aus der Fertigungsindustrie, die bereits heute Effizienzsteigerungen durch den breiten Einsatz von KI erzielen und auf schnell umsetzbare und kostengünstige Time-to-Market-Prozesse angewiesen sind. Die technische Normierung selbst bleibt Aufgabe der Industrie. Hier gilt es jedoch, die deutschen Unternehmen durch gezielte Informationskampagnen weiter zu sensibilisieren und eine breite Beteiligung sicherzustellen. Zudem sollten zumindest für kleinere Unternehmen Anreize für eine direkte Beteiligung gesetzt werden, zum Beispiel durch eine umfassende Beitragsförderung bei den Standardisierungsorganisationen.

Zur Rolle der Doppelregulierung insbesondere für KMU im Rahmen effizienter Compliance-Prozesse siehe die Antwort zu Frage 10.

Die KI-Verordnung lässt ausreichend Spielraum für eine fortwährende Anpassung der Prüfschemata und -kriterien. Die KI-Verordnung sieht keine starren Regelungen im Rahmen der Durchführung der Konformitätsbewertung vor, sondern stellt klar auf den dynamischen „Stand der Technik“ ab (etwa in ErwG 42 und 42a). Dies muss auch im Konformitätsbewertungsverfahren als Anforderung reflektiert werden. Die Harmonisierten Normen sind lediglich eine Hilfestellung des Gesetzgebers, denn ihre Einhaltung begründet eine Konformitätsvermutung in ihrem sachlichen Anwendungsbereich, womit pragmatisch und skalierbar Compliance erleichtert wird.[21] So kann es in Einzelfällen sogar notwendig sein,

[21] Vgl. auch die umfassende Betrachtung zur Konformitätsbewertung unter der KI-Verordnung bei Denga, M. (2023). *Konformitätsbewertung von KI-Systemen*. ZfPC 2023, 154.

von den standardisierten Normen abzuweichen, insbesondere wenn es sich um innovative KI-Anwendungen oder um Applikationen mit starken sektoralen Besonderheiten handelt. In solchen Fällen kann der System-Hersteller begründete Ausnahmen vorlegen, die von den zuständigen Stellen geprüft werden. Zudem kann der Hersteller eigens für diese Sonderfälle Konformitätsbewertungsprogramme mit der KI-Zertifizierungsstelle entwickeln.

IV. Innovationsförderung

Frage 6: ***Bitte bewerten Sie die im AI Act vorgesehenen Maßnahmen zur Innovationsförderung (Kapitel VI): Wie sollten insbesondere KI-Reallabore und Tests unter realen Bedingungen national geregelt, angeschoben und durch politische Maßnahmen flankiert werden – und welchen Anforderungen muss die nationale und unionsweite Aufsichtsstruktur erfüllen, um zu einer kohärenten Nutzung dieser Instrumente beizutragen?***

KI-Reallabore können angesichts rasanter technologischer Entwicklung einen wertvollen Beitrag zu einer zukunftsorientierten und innovationsfreundlichen KI-Regulierung leisten, indem sie Start-ups und KMU bei der Markteinführung innovativer KI-Lösungen unterstützen, Innovation fördern und die Erprobung von KI-Systemen in spezifischen Anwendungsbereichen ermöglichen. Um einen Beitrag zur Erreichung der in Art. 57 Abs. 9 KI-Verordnung genannten Ziele zu leisten, sind bei der Einrichtung der vorgesehenen KI-Reallabore insbesondere folgende Aspekte von Bedeutung[22]:

- Bisherige Erfahrungen mit Reallaboren, z.B. im Fintech-Bereich, zeigen deutliche nationale Unterschiede in der Akzeptanz und Nutzung dieses Instruments durch Gründer:innen und Unternehmen. Die Teilnehmenden an Reallaboren unterliegen weniger Regelungen, gleichzeitig schaut die jeweilige Aufsicht genauer hin. Einer Teilnahme steht daher zum Teil die Befürchtung der Unternehmen entgegen, dadurch unnötig früh in den Fokus der Marktüberwachung zu geraten und Wettbewerbsnachteile zu erleiden. Marktüberwachung und Betrieb von KI-Reallaboren sollten daher organisatorisch getrennt werden. Denkbar wäre der Betrieb der Sandbox mit ihren unterschiedlichen Geschäftsmodellen durch ein Innovationsteam der Aufsichtsbehörde, das organisatorisch von der laufenden Aufsicht getrennt ist und an der Anzahl der Unternehmen, die die Sandbox erfolgreich abschließen, gemessen wird.

[22] Vgl. zu den rechtlichen Hindernissen für den Einsatz von Reallaboren auch das vom BMWK bei der Kanzlei Noerr in Auftrag gegebene Gutachten *Analyse der Potentiale und rechtlichen Umsetzungsmöglichkeiten von KI-Reallaboren auf europäischer und nationaler Ebene unter besonderer Berücksichtigung des Entwurfs der Europäischen Kommission für einen KI-Rechtsrahmen*, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/gutachten-noerr-reallabore.pdf?__blob=publicationFile&v=1 (Abgerufen am 11.05.2024).

- Weiterhin ist die Frage des Haftungsschutzes von Bedeutung. Nach Art. 57 Abs. 2 KI-Verordnung bleiben (potenzielle) Anbieter im KI-Reallabor für Schäden haftbar, die Dritten durch die dort durchgeführten Tests entstehen. Fehlende Vorteile beim Haftungsschutz bzw. die haftungsrechtliche Gleichbehandlung von KI-Systemen im Reallabor und auf dem Markt könnten sich negativ auf die Teilnahmebereitschaft innovativer KI-Unternehmen auswirken.[23]

- Die KI-Verordnung schreibt in Art. 57 Abs. 1 und 2 die Einrichtung mindestens eines KI-Reallabors auf nationaler Ebene vor, betont aber gleichzeitig die Möglichkeit einer gemeinsamen Einrichtung durch mehrere Mitgliedstaaten und die parallele Einrichtung weiterer KI-Reallabore auf verschiedenen Ebenen (lokal, regional, mitgliedstaatenübergreifend). Ziel muss es sein, Fragmentierung zu minimieren und von Anfang an Klarheit über das Verhältnis von Reallaboren zu schaffen, die auf verschiedenen Ebenen koexistieren, und eine einheitliche Auslegung der Vorschriften zu gewährleisten. Ressourcen und Erkenntnisse sollten zwischen den zuständigen Behörden pragmatisch gebündelt und geteilt werden.

- In die Sandbox sollten nicht einzelne Use Cases, sondern insbesondere im Fall von KMU ganze Unternehmen aufgenommen werden. Nur die wenigsten Unternehmen, die sich mit KI beschäftigen, werden sich auf die Erprobung einer einzelnen KI-Technologie oder gar eines einzelnen Anwendungsfalls beschränken wollen.

- Das Harmonisierungserfordernis gilt insbesondere auch für die Einbeziehung der Datenschutzbehörden. Nach Art. 57 Abs. 10 KI-Verordnung sind die nationalen Datenschutzbehörden entsprechend ihrer Zuständigkeit am Betrieb der Reallabore zu beteiligen und in die Aufsicht einzubeziehen. Angesichts der föderalen Kompetenzverteilung bei der Datenschutzaufsicht in Deutschland sollte dies nicht zu Auslegungsunterschieden führen.

Unter den EU-Mitgliedstaaten gilt Spanien als Vorreiter, seit die spanische Regierung bereits im Juni 2022 ein Pilotprojekt für ein erstes KI-Reallabor präsentierte.[24] Nachdem Spanien bereits im August 2023 als erster EU-Mitgliedstaat eine nationale KI-Aufsichtsbehörde (AESIA) eingerichtet hatte,[25] wurde Anfang November das Gesetz zur Einrichtung des

[23] Truby, J. et al. (2021). *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*. European Journal of Risk Regulation, 2022;13(2):270-294. https://doi.org/10.1017/err.2021.52 (Abgerufen am 08.05.2024).
[24] Europäische Kommission (2022). *First regulatory sandbox on Artificial Intelligence presented*. https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented (Abgerufen 10.05.2024).
[25] Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2023). *Real Decreto 729/2023*. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-18911 (Abgerufen am 10.05.2024).

KI-Reallabors verabschiedet.[26] Das befristete Pilotprojekt zielt explizit darauf ab, Unternehmen die Möglichkeit zu geben, ihre KI-Systeme bis zum Geltungsbeginn der KI-Verordnung im Hinblick auf die regulatorischen Anforderungen zu testen. Außerdem soll die Entwicklung von Leitlinien unterstützt werden, um Unternehmen bei der Vorbereitung und Anpassung an die bevorstehenden Anforderungen zu helfen.[27]

Festzuhalten bleibt, dass KI-Reallabore als Instrument der Innovationsförderung für die derzeit erfolgreichen KI-Start-ups nicht entscheidend sein werden – jedenfalls ohne zeitnahe Adressierung der oben genannten Punkte. Viel wichtiger ist, gerade in einem Venture Capital-finanzierten Umfeld, die Rechtssicherheit und insbesondere die Vereinbarkeit der KI-Verordnung mit bestehenden sektoralen Rechtsvorschriften..[28]

> **Frage 9:** ***Wie muss die Umsetzung des AI Acts in Deutschland gestaltet werden, um einerseits die Sicherheit und Bürgerrechte zu wahren und andererseits ein innovationsfreundliches Umfeld zu schaffen, das Innovationskraft und privatwirtschaftlichen Wettbewerb auf dem deutschen Markt ideal unterstützt?***

Hinsichtlich der Umsetzung der KI-Verordnung wird auf die vorstehenden Antworten verwiesen. Mit ihrem risikobasierten Ansatz ist die KI-Verordnung im Kern kein Innovationsförderungsgesetz, sondern eine Produktsicherheitsverordnung, die darauf abzielt, die Risiken für Unionsbürger:innen durch den Einsatz von KI-Systemen zu reduzieren. Insofern sollte im Sinne der übergeordneten Prioritäten der Stärkung des EU-Binnenmarktes, der Förderung von Kohäsion und der Vermeidung von Fragmentierung soweit möglich auf nationales “Gold Plating” verzichtet werden.

Aus Sicht des Wirtschafts- und Innovationsstandorts EU ist die Frage, mit welchen öffentlichen Investitionen die KI-Verordnung flankiert wird, von weitaus größerer Bedeutung.[29] Um im globalen Wettbewerb bestehen zu können und geostrategische Abhängigkeiten bei dieser Schlüsseltechnologie des 21. Jahrhunderts zu vermeiden, müssen die EU und die Mitgliedstaaten ihre öffentlichen Investitionen in die KI-Forschung und -Anwendung deutlich erhöhen. Dazu gehören Investitionen in die Chip-Produktion, KI-Recheninfrastruktur und in die Anwerbung und Bindung von Fachkräften. Staatliche

[26] Ministerio de Asuntos Económicos y Transformación Digital (2023). Real Decreto 817/2023. https://www.boe.es/buscar/doc.php?id=BOE-A-2023-22767 (Abgerufen am 10.05.2023).
[27] Pehlivan, C. et al. (2023). *Spanish AI sandbox law passed – registrations starting soon!*. Linklaters Tech Insights. https://techinsights.linklaters.com/post/102is4w/spanish-ai-sandbox-law-passed-registrations-starting-soon (Abgerufen am 10.05.2024).
[28] Hacker, P. (2024). *Comments on the Final Trilogue Version of the AI Act*. https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf (Abgerufen am 08.05.2024).
[29] Hacker, P. (2023). *What's Missing from the EU AI Act*. Verfassungsblog. https://verfassungsblog.de/whats-missing-from-the-eu-ai-act/ (Abgerufen am 08.05.2024).

Investitionen in bzw. Beteiligungen an KI-Unternehmen sind nicht nur Anreiz für die Privatwirtschaft, sondern auch für den Staat selbst von strategischer Bedeutung, sei es im Hinblick auf Wertschöpfung, Schutz kritischer Infrastrukturen oder internationale Wettbewerbsfähigkeit.

V. Biometrische Fernidentifizierung

Frage 3: ***Bei der biometrischen Fernidentifizierung im öffentlichen Raum eröffnet der AI Act die Möglichkeit des Nachschärfens der EU-weiten Mindeststandards. Sowohl für Echtzeit-Fernidentifizierungssysteme als auch für nachträgliche biometrische Fernidentifizierung im öffentlichen Raum können die Mitgliedstaaten in nationalen Rechtsgrundlagen auch strengere Regeln erlassen. Wie lässt sich diese Möglichkeit für einen umfassenderen Grundrechtsschutz nutzen, wo könnten entsprechende Vorschriften im nationalen Recht verankert werden und wie sollten diese – etwa im Hinblick auf ein ausnahmsloses Verbot – inhaltlich ausgestaltet sein?***

Frage 17:
Welche konkrete Regelung empfehlen Sie für die nationale Umsetzung des AI-Acts, um die im Koalitionsvertrag enthaltene Position eines Verbots biometrischer Fernidentifikationssysteme im öffentlichen Raum umzusetzen für die Sicherung der Grundrechte auf Privatsphäre sowie Datenschutz, auf Nichtdiskriminierung, Meinungs- und Informationsfreiheit, auf Versammlungs- und Vereinigungsfreiheit sowie auf Rechtsstaatlichkeit und inwiefern ergibt es mit Blick auf die genannten Grundrechte Sinn, dabei hinsichtlich Echtzeit und retrograder Fernidentifikation zu unterscheiden, insbesondere da die Unterscheidung zwischen Echtzeit und retrograd unklar ist?

Mit dem AI Act wurden erstmals EU-weite Mindeststandards für den Einsatz von KI-Systemen zur biometrischen Fernidentifizierung im öffentlichen Raum vereinbart. So wurde der Einsatz von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung zu Strafverfolgungszwecken gemäß Art. 5 Abs. 1h KI-Verordnung grundsätzlich in die Kategorie der in der EU verbotenen Anwendungen eingestuft, Ausnahmen sind an detaillierte Voraussetzungen geknüpft sowie zeitlich und räumlich begrenzt.

Grundsätzlich ist festzuhalten, dass die Überwachung des öffentlichen Raums und die Abwägung nationaler Sicherheitsinteressen mit dem Grundrechtsschutz und dem Recht auf Anonymität im öffentlichen Raum nicht primär ein KI-technisches, sondern ein gesellschafts- und sicherheitspolitisches Thema ist. Übergeordnetes Ziel sollte eine harmonisierte Anwendung und einheitliche Auslegung bleiben, um Rechtsunsicherheiten durch nationale Sonderwege zu vermeiden.

VI. Militärische Nutzung von KI-Systemen

Frage 15: ***Ausdrücklich ausgenommen aus dem AI Act sind die Bereiche des Militärs und der Geheimdienste, da sie unter das nationale Recht der Mitgliedstaaten fallen. Wie kann und soll bei der Umsetzung des AI Act gewährleistet werden, dass in diesen Bereichen die mächtigen KI-Modelle etwa zur Gesichtserkennung oder zur Sprachanalyse gesetzeskonform eingesetzt werden?***

Art. 2 Abs. 3 KI-Verordnung nimmt KI-Systeme, die ausschließlich für Zwecke des Militärs, der Verteidigung oder der nationalen Sicherheit bestimmt sind, vom Anwendungsbereich der KI-Verordnung aus und betont ausdrücklich, dass die Zuständigkeit der Mitgliedstaaten für die nationale Sicherheit unberührt bleibt. Die Bandbreite von KI-Anwendungen im Militärbereich ist enorm – neben Gesichtserkennungs- und Sprachanalysesystemen sind vor allem computervisionsbasierte Systeme zur Zielerfassung, vorausschauende Systeme in Wartung und Logistik sowie Simulationssysteme im Bereich der Luftverteidigung zu nennen. Gerade bei computervisionsbasierten KI-Systemen wird es häufig entscheidend sein, dass das jeweilige KI-System auch bei veränderter Bildgebung sicher funktioniert.

Es ist daher davon auszugehen, dass die KI-Verordnung jedenfalls im Hinblick auf marktübliche Tests von KI-Systemen auch Auswirkungen auf die militärische Nutzung von KI-Systemen in Europa haben wird. Entsprechende Auswirkungen werden darüber hinaus auch insofern festzustellen sein, als das fortgeschrittene KI-Technologien vielfach nicht ausschließlich für militärische Zwecke entwickelt und eingesetzt werden, sondern einen sogenannten Dual-Use-Charakter aufweisen, d.h. sowohl für zivile als auch für militärische Zwecke eingesetzt werden können. In diesen Fällen beginnt die Entwicklung häufig bei kommerziellen Anbietern und findet über Kooperationen und Aufträge den Weg in militärische KI-Systeme. Anbieter solcher Dual-Use-Systeme würden durchaus in den Anwendungsbereich der KI-Verordnung fallen bzw. müssten die Bestimmungen für Hochrisiko-Systeme einhalten.[30]

Wichtig ist festzuhalten, dass die Rüstungsindustrie bereits zu den am stärksten regulierten Branchen gehört. Herstellung, Inverkehrbringen und Export von Kriegswaffen unterliegen in Deutschland bereits einem komplexen Regelwerk. Daher sollte zunächst ein genauer Abgleich der bestehenden Regelungen mit den Zielen und Kriterien der KI-Verordnung erfolgen. Besonderes Augenmerk ist dabei auf eine produktbezogene Prüfung von KI-Komponenten (in Abgrenzung zur Abnahme des Gesamtsystems) zu legen.

[30] Fanni, R. (2023). *Why the EU must now tackle the risks posed by military AI*. Centre for European Policy Studies expert commentaries. https://www.ceps.eu/why-the-eu-must-now-tackle-the-risks-posed-by-military-ai/ (Abgerufen am 07.05.2024).

VII. Verbraucherschutz und Transparenzregister

Frage 18: ***Wie sollte und könnte ein nationales KI-Transparenzregister über den Bereich der Hochrisiko-Systeme hinausgehen, um wirksame Transparenz im Sinne des Verbraucherschutzes (Nachvollziehbarkeit, Beschwerdebasis etc.) herzustellen und insbesondere beim Einsatz von KI-Systemen durch die öffentliche Hand dem erhöhten Anspruch an Grundrechtsschutz und bestehende Abhängigkeiten gerecht zu werden und wie sollte generell ein solches Transparenzregister organisiert sein, hinsichtlich: wer sollte es aufbauen und wen dabei einbeziehen; wie sollte es aufgebaut werden; wer sollte es verwalten; welche Informationen sollte es enthalten?***

Ein mögliches Vorbild für ein solches weitergehendes nationales KI-Transparenzregister könnte das Ende 2022 veröffentlichte niederländische Algorithmenregister[31] sein, das zum Ziel hat, bis Ende 2025 die von der niederländischen Regierung genutzten Algorithmen verpflichtend zu erfassen und rechtlich auf Diskriminierung und Bias zu überprüfen.

Die Verantwortung für ein solches Register wäre sinnvollerweise beim Bund anzusiedeln, der Betrieb wäre aber auch bei einer ausgelagerten Organisation (z.B. ITZBund, Bundesdruckerei) denkbar. Für die Einrichtung und die Verwaltung eines solchen Registers wären insbesondere folgende Punkte zu beachten:

- In der verwaltenden Organisation sollte Personal mit entsprechender fachlicher und technischer KI-Kompetenz vorhanden sein, um z.B. eine erste Einschätzung vornehmen zu können, ob ein Vorhaben dem Thema KI zuzuordnen ist oder nicht.

- Das nationale Register sollte unbedingt die Strukturen auf EU-Ebene berücksichtigen und an diese anknüpfen, um doppelten Registrierungsaufwand zu vermeiden, insbesondere an die EU-Datenbank für Hochrisiko-KI-Systeme, die gemäß Art. 71 KI-Verordnung von der Europäischen Kommission eingerichtet und in Zusammenarbeit mit den Mitgliedstaaten verwaltet wird.

[31] The Algorithm Register of the Dutch government. https://algoritmes.overheid.nl/en (Abgerufen am 07.05.2024).

VIII. Fachpersonal und nationale KI-Strategie

Frage 14: ***Steht für die Umsetzung des AI-Act in Deutschland Ihrer Ansicht nach genügend Fachpersonal zur Verfügung und wenn nein, in welchen konkreten Feldern deuten sich aktuell die größten Lücken an, welches sind die wichtigsten Maßnahmen, die von der Politik hier zu ergreifen sind, und wie wichtig wäre aus Ihrer Sicht das zeitnahe Vorliegen einer aktualisierten ressortübergreifenden KI-Strategie, um eine reibungslose und effiziente Umsetzung des AI-Act in Deutschland sicherstellen zu können?***

In Deutschland und Europa zeichnet sich der Aufbau ausreichender KI-Expertise in den zuständigen Aufsichtsbehörden als zentraler Engpass bei der Durchsetzung der KI-Verordnung ab. Diese Herausforderung ist keineswegs auf die neue Governance-Architektur auf EU-Aufsichtsebene beschränkt. Ein rechtzeitiger und sektorspezifischer Aufbau von technischer und regulatorischer KI-Kompetenz ist auch bei den folgenden Stellen und Stakeholdern unerlässlich:

- in den Marktüberwachungsbehörden, die sich mit der Anwendung und Durchsetzung der KI-Verordnung in spezifischen Hochrisiko-Anwendungsbereichen nach Anhang III befassen (z.B. die BaFin als Bank- und Versicherungsaufsicht oder das BfArM im Bereich der Medizinprodukte)

- in den Bundesbehörden für die in Anhang I Abschnitt B KI-Verordnung genannten Sektoren, die aufgrund der in Art. 102 ff. KI-Verordnung mandatierten Anpassungen sektoraler Verordnungen unmittelbar mit der Umsetzung der Anforderungen der KI-Verordnung an Hochrisiko-KI-Systeme konfrontiert werden (zum Beispiel Kraftfahrt-Bundesamt, Luftfahrt-Bundesamt, Eisenbahn-Bundesamt).

Der Erfolg der Umsetzung der KI-Verordnung wird auch entscheidend davon abhängen, ob es gelingt, möglichst rasch externe KI-Expertise auf verschiedenen Behördenebenen anzuwerben. Bei der Personalrekrutierung sind der Zeitdruck und die hohe Nachfrage nur eine von vielen Herausforderungen. Vor allem bieten viele der ausgeschriebenen Stellen in Aufsicht und Verwaltung Gehälter, die deutlich unter den Standards der Privatwirtschaft liegen; das Festhalten am Besserstellungsverbot erweist sich hier als erhebliches Hindernis. Hinzu kommen zum Teil langwierige und unflexible Einstellungsverfahren.

Vor allem muss die personelle Durchlässigkeit zwischen Wirtschaft, Wissenschaft und Aufsicht deutlich erhöht werden. Wie im angelsächsischen Raum längst üblich, muss auch in Deutschland die Bereitschaft von Talenten steigen, für einige Jahre in der Aufsicht zu arbeiten und umgekehrt. Gerade bei der KI-Aufsicht mit einer sich sehr schnell entwickelnden Technologie als Aufsichtsgegenstand ist dies von besonderer Bedeutung.

Ein einheitliches Vorgehen der Bundesregierung ist die Grundvoraussetzung nicht nur für eine schlanke und innovationsfreundliche nationale Durchführung der KI-Verordnung, sondern auch für ihr selbst gestecktes Ziel, KI Made in Germany an die Weltspitze zu führen. Eine Aktualisierung und Weiterentwicklung der KI-Strategie, die noch aus dem Jahr 2018 und damit aus Zeiten der Vorgängerregierung stammt, ist dringend erforderlich, um eine ressortübergreifende Antwort auf die aktuell rasante Entwicklung im Bereich KI zu geben und dem Querschnittscharakter von KI als Schlüsseltechnologie und gesamtgesellschaftlicher Aufgabe gerecht zu werden. Einzelinitiativen der Ressorts, wie zuletzt der am 7. November 2023 vorgestellte "KI-Aktionsplan" des BMBF, sind in ihren ambitionierten Zielen zu unterstützen. Gleichwohl bedarf es für das wichtigste Technologiethema dieser Legislaturperiode einer einheitlichen Strategie, klarer Verantwortlichkeiten sowie der Koordinierung und Bündelung von Maßnahmen und Ressourcen innerhalb der Bundesregierung.

Mit Blick auf das im Koalitionsvertrag vereinbarte und mittlerweile wohl gestrichene Digitalbudget und die Kürzungen im aktuellen Bundeshaushalt wird aber auch deutlich, dass jede noch so ambitionierte, aktualisierte und umfassend abgestimmte KI-Strategie nur mit konkreten Finanzierungszusagen und belastbaren Zahlen Wirkung entfalten kann. Insbesondere die dringend notwendige Förderung der Entwicklung und des Aufbaus eigener Kapazitäten für KI-spezifische Hardware und KI-Recheninfrastruktur in Deutschland wird ohne eine deutlich höhere Investitionsbereitschaft der Bundesregierung nicht gelingen. Die Bündelung und Zusammenführung kleinteiliger ressortspezifischer Einzelmaßnahmen im Rahmen einer einheitlichen KI-Gesamtstrategie ist hierfür die Mindestvoraussetzung.

—

Kontakt

Dr. Robert Kilian
CEO CertifAI
Vorstand KI-Bundesverband
[redacted]

Vielen Dank an alle Expert:innen, die zu dieser Stellungnahme beigetragen haben, insbesondere Alessandro Blank und Phillip Handy, den Mitgliedern aus der Arbeitsgruppe und dem Lenkungskreis Politik & Regulierung des KI Bundesverbandes sowie den beteiligten Mitglieds- und Partnerunternehmen.

—

Über den KI Bundesverband

Der Bundesverband der Unternehmen der Künstlichen Intelligenz e.V. vernetzt innovative KI- und Deep-Tech-Unternehmen mit der etablierten Wirtschaft und Politik und ist mit über 400 KI-Unternehmen das größte KI-Netzwerk in Deutschland. Die Mitglieder des Bundesverbandes Künstliche Intelligenz setzen sich dafür ein, dass diese Technologie im Sinne europäischer und demokratischer Werte eingesetzt wird und Europa digitale Souveränität erlangt. Dazu müssen Deutschland und die EU ein attraktiver KI-Standort für Unternehmerinnen und Unternehmer werden, an dem sich Risikobereitschaft lohnt und Innovationsgeist auf beste Bedingungen trifft.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V., im Haus der Bundespressekonferenz, Schiffbauerdamm 40, 10117 Berlin.

***