bitkom

Stellungnahme

März 2024

Stakeholderdialog zu Leitlinien der EU-Kommission (Art. 96 KI VO)

Zusammenfassung

Der Vorschlag für eine Verordnung über Künstliche Intelligenz („KI VO“) ist durch das Europäische Parlament und den Rat gebilligt worden. Der Rechtsakt wird somit in absehbarer Zeit Wirkung entfalten. Die praxistaugliche, effiziente und innovationsfreundliche Durchführung der Verordnung wird die zentrale Aufgabe der Mitgliedstaaten, aber auch der Europäischen Kommission („EU-Kommission“) sein.

Aus diesem Grund wird die EU-Kommission eine Arbeitsgruppe, bestehend aus Vertrer/innen der Mitgliedstaaten, einrichten. Die Arbeitsgruppe soll die EU-Kommission bei ihren Durchführungsaufgaben unterstützen, etwa bei der Erarbeitung von Leitlinien. Diese Leitlinien sollen den Regulierungsadressaten der KI VO die Anwendung der neuen Rechtsvorschriften erleichtern, indem sie die gesetzlichen Anforderungen sinnvoll konkretisieren.

Bitkom nimmt im Folgenden Stellung zu Leitlinien, die für die folgenden Bereiche erarbeitet werden sollen:

- 1. Das Verhältnis der KI VO zu bestehender Sektorregulierung (ehem. Art. 82a Abs. 1e KI VO, jetzt Art. 96 Abs. 1e KI VO)
- 2. Pflichten für Hochrisiko-KI-Systeme (ehem. Art. 82a Abs. 1a KI VO, jetzt Art. 96 Abs. 1a KI VO)
- 3. Die Risikoklassifizierung nach der KI VO (ehem. Art. 6 Abs. 2c KI VO, jetzt Art. 6 Abs. 5 KI VO).
- 4. Bestimmungen über wesentliche Änderungen (ehem. Art. 82a Abs. 1c KI VO, jetzt Art. 96 Abs. 1 c KI VO)
- 5. Die Definition von KI nach der KI VO (ehem. Art. 82a Abs. 1f KI VO, jetzt Art. 96 Abs. 1 f KI VO)
- 6. Weitere Themen und Fragestellungen

Es ist von grundlegender Bedeutung, dass die die EU-Kommission bei der Erarbeitung ihrer Leitlinien die Expertise und die Belange der Industrie in Betracht zieht. Nur in Zusammenarbeit mit denjenigen, die als Anbieter von KI-System die KI VO anwenden werden, ist es möglich, praxistaugliche und klare Leitlinien zu schaffen, die für alles Beteiligten einen Mehrwert darstellen. Es ist darüber hinaus unabdingbar, dass die Leitlinien der EU-Kommission in allen Mitgliedstaaten anerkannt und von den zuständigen Stellen einheitlich umgesetzt werden. Ansonsten würde ihr eigentlicher Zweck – eine reibungslose Durchführung der KI VO zu gewährleisten – fehlgehen.

Der Bitkom ist daher dankbar für die Möglichkeit, im Rahmen des Stakeholderdialogs an dieser bedeutenden Stelle des Gesetzgebungsprozesses noch einmal Stellung nehmen zu können.

Bei der konkreten Formulierung der Leitlinien sollten die Stakeholder wiederum konsultiert werden um die Praktikabilität, Anwendungsfreundlichkeit und Auslegungssicherheit für die betroffenen Unternehmen zu gewährleisten.

1. Das Verhältnis der KI VO zu bestehender Sektorregulierung

Das Verhältnis der KI VO zu bestehender sektoraler Regulierung war und ist einer der kritischsten Aspekte, wenn es um die Regulierung künstlicher Intelligenz geht. Eine funktionierende und praxistaugliche Wechselwirkung ist unabdingbar für ihren Erfolg.

Es ist zu befürchten, dass KI-Systeme, die in NLF-regulierte Produkte integriert oder selbst solche Produkte sind, durch die KI VO zusätzlich zur bestehenden Regulierung einer teilweise widersprüchlichen Doppelregulierung unterworfen werden. Folgen einer solchen Doppelregulierung können für die Beteiligten (Nutzer, Behörden, zuständigen Stellen und Unternehmen) sowohl Rechtsunsicherheit, zusätzlicher bürokratischer Aufwand, längere Wartezeiten für den Markteintritt innovativer Produkte sowie erhöhte Gesamtkosten sein, ohne dass ein Mehrwert in Bezug auf die Sicherheit und Qualität der Produkte entsteht.

Verhältnis zur Medizinprodukteverordnung (MDR) und In-Vitro-Diagnostik-Verordnung (IVDR)

In Bezug auf Medizinprodukte ist die Besonderheit zu beachten, dass bisher ausschließlich im Medizinprodukte-Sektor die Möglichkeit besteht, eigenständige Software („standalone software“) nach den bestehenden EU-Rechtsvorschriften mit der CE-Kennzeichnung zu versehen. Hieraus ergibt sich das dringende Erfordernis, bestehende Qualitäts-zertifizierungs- und Konformitätsbewertungskompetenzen zu

nutzen und die Zertifizierung nach der MDR und IVDR anzuerkennen. Eine Prüfung und Zertifizierung unter der KI VO **und** MDR/IVDR würde eine unverhältnismäßige Belastung sowohl für Anbieter als auch die notifizierten Stellen mit sich bringen. Gem. Art. 28 Abs. 1 KI VO hat jeder Mitgliedstaat der EU mindestens eine notifizierende Behörde zu benennen, die die Konformitätsbewertungsstellen notifiziert. Im Auftrag der Deutschen Akkreditierungsstelle (DAkkS) notifiziert derzeit die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG) die Konformitätsbewertungsstellen im Rahmen der MDR und IVDR.

Um Mehraufwand zu vermeiden und eine reibungslose Durchführung der KI VO sowie der bestehenden Regeln zu gewährleisten, sollte die ZLG ermächtigt werden, Konformitätsbewertungsstellen für Hochrisiko-KI-Systeme zu benennen, die unter die MDR/IVDR fallen, und damit eine einzige, einheitliche benennende Behörde für intelligente Medizinprodukte und In-vitro-Diagnostika einzurichten.

Qualitätsmanagementzertifikate für EU MDR für IVDR sollten darüber hinaus für intelligente Medizinprodukte, die unter die KI VO fallen, genutzt werden können. Zusätzliche Qualitätsmanagementzertifizierungen sollten vermieden werden, und bestehende Zertifizierungen sollten so genutzt werden, dass sie auch unter der KI VO anwendbar sind.

Verhältnis zu existierenden Verordnungen nach Annex I A & B

In den Leitlinien sollte klargestellt werden, wie sich die Regelungen der KI VO zu bestehender Sektorregulierung verhalten, wenn sich die jeweiligen Anforderungen widersprechen.

Aus Erwägungsgrund49 ergibt sich, dass Änderungen der jeweiligen Produktregulierungen im Wege von delegierten Rechtsakten oder Durchführungsrechtsakten durch den Gesetzgeber zu erlassen sind. Damit will die Kommission aufbauend auf den technischen und regulatorischen Besonderheiten des jeweiligen Sektors und ohne Beeinträchtigung bestehender Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen, die in der KI-VO festgelegten verbindlichen Anforderungen an Hochrisiko-KI-Systeme auf diese Sektoren ausweiten. Somit existiert zwar keine direkte Vorrangregel der KI VO, aber eine explizite Aufforderung der Kommission die Rechtsakte zu den Produktregulierungen im Einklang mit der KI-VO zu bringen. Die Rechtsakte zu den Produktregulierungen sind daher parallel (ergänzend) zur KI-VO anzuwenden.

Verhältnis zu Typengenehmigungsvorschriften

Artikel 113 Abs. 1 c) KI VO definiert eine Umsetzungsfrist von 36 Monaten für Systeme nach Artikel 6 Abs. 1 KI VO. Für derartige KI Systeme, die “safety component of a product“ sind „or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex II” soll jedoch nach Art. 2 Abs. 2 die Verordnung gerade keine unmittelbare Anwendung finden, dafür aber die entsprechenden Typgenehmigungsvorschriften angepasst werden. Zum Zeitpunkt des Inkrafttretens der

KI VO stehen diese Vorschriften jedoch noch nicht einmal fest. Es ist rechtlich untragbar, dass eine Umsetzungsfrist bereits zu laufen beginnt, bevor überhaupt die Anforderungen final feststehen.

Zu klären bleibt also, welche Folge es für die Automobilindustrie haben soll, wenn die Typgenehmigungsvorschriften gar nicht oder nicht rechtzeitig innerhalb der 36 Monatsfrist des Artikel 113 Abs. 1 c) angepasst werden. Wird dann die KI-VO doch unmittelbar ersatzweise gelten? Oder wird es verlängerte Umsetzungsfristen in den angepassten Typgenehmigungsvorschriften geben?

Nach Art. 111 Abs. 2 Satz 1 gilt die KI VO außerdem nicht für Hochrisiko-KI-Systemen in Produkten, die bereits vor Geltungsbeginn in Verkehr gebracht oder in Betrieb genommen wurden, außer diese werden nach Geltungsbeginn signifikant verändert. Eine solche ausdrückliche Regelung wäre gerade im Fahrzeug-Kontext ebenfalls notwendig: Viele der Anforderungen für HR-KI, die sich an die Entwicklung der KI-Systeme richten, sind bei aktuell produzierten Produkten schwer umsetzbar. Die Entwicklung der in den nächsten 3 Jahren produzierte Fahrzeuge ist bereits größtenteils abgeschlossen. Realistisch umsetzen lassen sich die Anforderungen daher erst mit komplett neuen Fahrzeug-Typen. Wichtig ist daher die Klarstellung, dass sich das „Inverkehrbringen“ nicht auf einzelne Fahrzeuge, sondern auf ein gesamten neuen Fahrzeug-Typ beziehen kann.

Im Wege der Leitlinien sollte die EU-Kommission daher klarstellen, ob die in Art. 113 Abs. 1 c) genannte Frist vor dem Hintergrund von Art. 2 Abs. 2 überhaupt gilt und auf was sich der inhaltliche Geltungsbeginn bezieht. Müssen ab dem Zeitpunkt des Geltungsbeginns alle ab dann vertriebene Produkte den Anforderungen entsprechen oder nur neu in Verkehr gebrachte Produkttypen, z.B. neue Fahrzeugtypen?

Die gleichen Fragen nach dem inhaltlichen Geltungsbeginn stellen sich in Bezug auf die Frist zur Umsetzung von Transparenzpflichten gem. Art. 113 Abs. 1 b) KI VO. Die Anforderung sollte sinnvollerweise erst für alle ab dem Zeitpunkt des Geltungsbeginns neu in Verkehr gebrachten Fahrzeugtypen gelten. Da diese allerdings nicht unter Art. 2 Abs. 2 fallen, lässt sich dies auch nicht über die Umsetzungsrechtsakte gem. Art. 107, 109 lösen. Dieser Punkt scheint in der KI VO nicht bedacht worden zu sein. Hier drohen immense zusätzliche Kosten aufgrund der Umsetzung der Transparenzanforderungen in den aktuellen Produktlinien auf die Industrie zukommen.

Kohärente Durchsetzung

Die EU-Kommission sollte die Kohärenz der Durchsetzungsmaßnahmen zwischen den verschiedenen Mitgliedstaaten fördern, um die Aufgabe des AI-Boards zu unterstützen und zu berücksichtigen, dass sehr unterschiedliche Behörden mit unterschiedlichen Perspektiven und Fachkenntnissen die nationalen Durchsetzungsmaßnahmen leiten werden. Die EU-Kommission sollte Leitlinien bereitstellen, die eine Koordinierung zwischen verschiedenen Behörden innerhalb eines Mitgliedstaates vorschlagen, deren Zuständigkeiten sich überschneiden, z. B. in den Bereichen Datenschutz, Produktsicherheit und Verbraucherschutz.

Die Europäische Kommission und die Mitgliedstaaten sollten die Zuständigkeiten und Abstimmungsprozesse für den Fall klären, dass die GPAI eines Anbieters in einem risikoreichen Anwendungsfall eines anderen Akteurs verwendet wird, was die Zuständigkeiten des Amtes für künstliche Intelligenz und der zuständigen nationalen Behörden betreffen könnte. Der GPAI-Anbieter soll dem Anbieter des risikobehafteten Anwendungsfalls die Einhaltung der Vorschriften gemäß Art. 25(2) und Erwägungsgrund 85 und 86.

2. Pflichten für Hochrisiko-KI-Systeme

Art. 9 KI VO (Risikomanagement)

Es werden Leitlinien für das Risikomanagement, z.B. mit Blick auf autonome Fahrfunktionen, benötigt. In komplexen Anwendungen sind Risiken sehr schwer zu exakt zu beschreiben. Dies verlangt eine Zusammenarbeit von Original Equipment Manufacturer (OEM) und Lieferant, die heute auch noch unklar ist. Risiken können sich sowohl aus der Funktion sowie aus der integrierten Verwendung im Gesamtfahrzeug ergeben. Hier benötigt die Industrie klare Guidelines in welcher Granularität und auf welchen Bezugspunkt hin die Risiken zu bewerten sind.

Art. 12 KI VO (Aufzeichnungspflichten):

Die Konkretisierung der Aufzeichnungspflichten durch Leitlinien der Kommission ist notwendig. Konkret stellt sich etwa im Hinblick auf Fahrzeuge die Frage, wie eine Umsetzung des Loggings im Fahrzeug konkret aussehen soll. Genügt es, wenn die Logs im Fahrzeug gespeichert und bei Bedarf z.B. in Werkstätten ausgelesen werden können?

Dieser Aspekt spielt aus dem Grund eine wichtige Rolle, weil die Übermittlung von geloggten Events an Backends Datenverbindungen erfordert, die nicht immer zu gewährleisten sind.

Art. 14 KI VO (Menschliche Aufsicht):

Im Rahmen der Leilinien sollte außerdem die konkrete Ausgestaltung der menschlichen Aufsicht über KI-Systeme konkretisiert werden.

Gerade in Bezug auf Fahrzeuge ist dies besonders relevant. Viele Funktionen im Fahrzeug entscheiden in Echtzeit und können durch den Fahrer auch nicht beeinflusst werden. Ab Level 4 nehmen auch fahrzeug-fremde Aktivitäten aus der Umwelt einen zentralen Platz für die Reaktion des Fahrzeugs ein. Wie soll eine menschliche Aufsicht hier realistisch ablaufen und welche Personen sollen sie durchführen? Der Fahrer kann diese Funktion kaum erfüllen. Für vom OEM gestellte Experten wäre eine Echtzeit-Überwachung der gesamten Feldflotten erforderlich. Dies erfordert fortlaufende Datenbanken, würde zu einem immensen Daten-aufkommen führen und ist faktisch schon nicht realisierbar. Auch ein jederzeitiges Abschalten einzelner KI-Systeme im Fahrzeug ist weder möglich noch sinnvoll. Hierdurch wären Rückeinflüsse auf die

übrigen Fahrfunktionen zu erwarten, was ggfs. das Sicherheitsrisiko noch erhöhen würde. Es müssen hier dringend praktisch umsetzbare und auch im Sinn der Kund/innen realisierbare Lösungen geschaffen werden, die auch datenschutzkonform gestaltet werden können.

Art. 25 KI VO (Pflichten entlang der Wertschöpfungskette)

Durch die Leitlinien ist zu konkretisieren, wie Art. 25 auszulegen ist.

Fraglich ist, wie die Konstellation aus Art. 25 für Fahrzeuge abgebildet wird. Wie wird sichergestellt, dass der Fahrzeug-Hersteller für die KI-Systeme im Fahrzeug, für die er als Anbieter gilt, die erforderlichen Informationen und Unterstützungen durch die Lieferanten bekommt? Die Konstellation ist für Fahrzeuge äußerst relevant, allerdings ist Art. 25 für die in Art. 2 Abs. 2 genannten Umfänge erst einmal nicht anwendbar. Praktisch muss es aber dieselbe Logik geben, da nur der Fahrzeug-Hersteller in der Lage sein wird, die inhaltlichen Anforderungen aus Titel III Kapitel 2 sinnvoll umzusetzen. Dafür benötigt er allerdings hinreichende Unterstützung des Lieferanten. Hier ist schon Art. 25 Abs. 2 keine Hilfe, da sich dieser nur auf die Konstellationen in Art. 28 Abs. 1 bezieht. Eine vergleichbare inhaltliche Regelung ist allerdings zwingend erforderlich, da die eigentliche Entwicklung oftmals ein Lieferant vornimmt, der als einziger die an die Entwicklung knüpfenden Anforderungen wie Art. 10, 11, 12, 15 umsetzen kann.

Anbieterpflichten und technische Norm- und Standardsetzung

Die EU-Kommission sollte zunächst eine Übersicht über die Anforderungen erstellen, die noch nicht durch bestehende oder künftige technische Normen festgelegt sind. Sie sollte dann in Absprache mit den betroffenen Interessengruppen und technischen Experten eine Liste der Anforderungen erstellen, die nicht ausreichend klar sind und einer Spezifizierung bedürfen.

3. Die Risikoklassifizierung nach der KI VO

Aus Sicht der Industrie ist in Bezug auf die Risikoklassifizierung besonders wichtig, Leitlinien zu entwerfen und eine Liste mit Beispielen bereitzustellen, welche Systeme als hochriskant einzustufen sind und welche nicht. Die Liste sollte unbedingt gemeinsam mit Vertreter/innen aus der Industrie erarbeitet werden.

Die Risikoklassifizierung erfolgt nach Art. 6 iVm den Anhängen II und III der KI VO. Die Klassifizierung als Hochrisiko-KI-System richtet sich gemäß Art. 6 i.V.m. Annex II und III KI VO maßgeblich nach der **Zweckbestimmung** des jeweiligen Systems. „Zweckbestimmung“ meint die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den

Gebrauchsanweisungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation (Art. 3 Nr. 12 KI-VO).

Die Richtlinie der EU-Kommission sollte im Hinblick auf die Risikoklassifizierung klarstellen, ob die Kenntnis des Anbieters über den möglichen Einsatz seines KI-Systems (mit allgemeinem Verwendungszweck) für bestimmte Hochrisikozwecke bereits ausreicht, um eine solche Zweckbestimmung anzunehmen. Drüber hinaus ist zu klären, der Anbieter die Nutzung seines KI-Systems für Hochrisikozwecke ausdrücklich (z.B. in der Gebrauchsanweisung) verbieten muss, um nicht unter die Hochrisikoklassifizierung zu fallen. Außerdem sollten die Leitlinien die Frage beantworten, ob die Integration einer Hochrisiko-KI in ein nachgelagertes KI-System (keine Hochrisiko-KI) automatisch eine Klassifizierung des nachgelagerten KI-Systems als Hochrisiko-KI auslöst.

Zwar ist für Fragen hinsichtlich der Vorschriften über Allzweck-KI das „AI Office" zuständig. Dennoch hängen Fragen nach der Risikoklassifizierung untrennbar mit Fragen nach Verantwortlichkeiten in der Wertschöpfungskette von Allzweck- zu zweckspezifischer KI zusammen. Aus diesem Grund werden in der vorliegenden Stellungnahme auch Forderungen vorgetragen, die das Thema Allzweck-KI (am Rande) betreffen.

Eine weitere Frage, die es im Wege der Leitlinie der EU-Kommission zu klären gilt, ist die nach der Auslegung des Begriffs „**Sicherheitskomponente**" in Art. 6 KI VO. In der KI VO ist der Begriff der Sicherheitskomponente in Art. 3 Ziff. 14 definiert als „Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Sachen gefährdet". Es gibt beispielsweise in Fahrzeugen mehr als 50.000 Bauteile mit einer hohen Bandbreite an Funktionen, für die bereits durch die EU 2028/858 und die EU 2019/2144 einschl. diverser nachgelagerter UN-Regelungen zahlreiche Anforderungen gelten. Die „Sicherheitskomponente" ist dementgegen eine neue Definition. Es muss sichergestellt werden, dass klar ist, was genau unter eine solchen Sicherheitskomponente (z.B. in Fahrzeugen) zu verstehen ist, damit auch die Dokumentation für die Konformitätsbewertung (Typgenehmigung) nicht aufgrund des abweichenden Bezugspunkts mehrfach erstellt werden muss.

Auch im Bereich der kritischen Infrastruktur sollte noch präziser definiert werden, was unter „Sicherheitskomponente" zu verstehen ist. Das gleich gilt für Medizinprodukte.

Es ist wichtig, dass KI-Systeme, die für die Cybersicherheit in kritischen digitalen Infrastrukturen eingesetzt werden, nicht als "Hochrisiko" eingestuft werden. Zur Absicherung der kritischen Infrastruktur setzen die Unternehmend zunehmend KI-basierte Tools ein. Solche Tools verhindern Hackerangriffe und Betrugsversuche oder analysieren Angriffsversuche, um zukünftige Gefahren abzuwenden. Diese KI-Systeme beinhalten keinerlei zusätzliche Risiken, sondern sind im Gegenteil ausschließlich dafür entwickelt, Risiken für die Infrastruktur und Nutzer zu minimieren. In einer sich immer schneller verändernden Welt der Bedrohung durch Cyberangriffe ist es äußerst wichtig, dass die Unternehmen schnell reagieren und die Abwehrtools entsprechend entwickeln oder anpassen können, ohne vorab die für Hochrisiko-KI-Systeme vorgesehenen

erhöhten technischen und organisatorischen Maßnahmen implementieren zu müssen. Es gibt hierzu im aktuellen Verordnungstext bereits eine Aussage im Erwägungsgrund 55 (vorher 34). Die Formulierung "Components intended to be used solely for cybersecurity purposes should not qualify as safety components" weist zwar in die richtige Richtung, der Begriff „cybersecurity purposes" ist aber nicht legaldefiniert. Es bleibt deshalb eine Auslegungsfrage und damit unsicher, ob alle Security-Anwendungen unter diese Ausnahme fallen werden. Gerade wenn sich die KI technisch weiterentwickelt und breiter, also neben Cybersecurity auch in anderen Bereichen eingesetzt werden kann und soll, stellen sich unter Umständen schwierige Abgrenzungsfragen. Die Herausnahme von Cybersecurity-Lösungen aus dem Hochrisiko-Bereich sollte deshalb auch in den Leitlinien eindeutig und zukunftssicher klargestellt werden.

Die KI VO definiert ferner **Biometrik** Hockrisiko-KI als KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensitiven oder geschützten Attributen oder Merkmalen oder auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen. Aus einer praktischen Perspektive ist es notwendig, dass die Kommission im Rahmen der Leitlinien eine abschließende Auflistung jener Merkmale und Attribute aufnehmen könnte, welche als „sensitiv oder geschützt" zu qualifizieren sind.

In Bezug auf sämtliche Filtervoraussetzungen des Art. 6 Abs. 3 KI VO sind ebenfalls Konkretisierungen im Wege der Leitlinien der EU-Kommission notwendig**. Art. 6 Abs. 3** KI VO ist ein **Ausnahmetatbestand** , der KI-systeme, die grundsätzlich nach Art. 6 Abs. 2 iVm Annex III als hochriskant eingestuft sind, aus der Hochrisikokategorie ausnimmt. Voraussetzung hierfür ist etwa, dass das KI-System die in Rede stehende Entscheidung nicht wesentlich beeinflusst. Dies ist wiederum der Fall, wenn das KI-system lediglich eine enge Verfahrensaufgabe erfüllt, das Ergebnis einer menschlichen Entscheidung verbessert, es dazu dient, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen und nicht dazu gedacht, die die zuvor von Menschen vorgenommene Bewertung zu ersetzen oder zu beeinflussen oder wenn das KI-system lediglich eine vorbereitende Aufgabe übernimmt.

Diese Voraussetzungen sind durch die Leitlinien aus Gründen der Rechtssicherheit und der Praktikabilität zu konkretisieren. Es ist zum einen notwendig, dass die EU-Kommission im Rahmen der Leitlinien Abgrenzungskriterien entwickelt, ab wann eine Verfahrensaufgabe nicht mehr als „eng gefasst" zu qualifizieren wäre und darüber hinaus Beispiele aufnimmt von eng gefassten Verfahrensaufgabe im Rahmen einer Produktion. Die Definition von KI in Art. 3 lit. 1 KI VO verlangt unter anderem eine gewisse Autonomie. Zu klären ist also, wie sich das Element der Autonomie in der Definition für KI zu der eng gefassten Verfahrensaufgabe verhält, die ja gerade auf das Gegenteil von Autonomie abzielt.Darüber hinaus ist klärungsbedürftig, wann eine Aufgabe nicht mehr „vorbereitend" iSd. Art. 3 Abs. 3 gilt. Auch hier sind Abgrenzungskriterien und Beispielsfälle für die Praxis von großer Bedeutung.

Zuletzt sollte im Rahmen der Leitlinien geklärt werden, welche weiteren Tatbestände neben dem in Art. 6 Abs. 3 ausdrücklich genannten (keine wesentliche Beeinflussung

der Entscheidung) KI-Systeme aus der Hochrisikokategorie ausnehmen sollen. Dass das KI-System die in Rede stehende Entscheidung nicht wesentlich beeinflusst, ist nur **ein** Beispiel für eine Ausnahme aus der Hochrisikokategorie (sie Formulierung „unter anderem“).

4. Wesentliche Änderungen iSd KI VO

Gem. Art. 96 Abs. 1 c) erarbeitet die EU-Kommission Leitlinien für die praktische Durchführung der Bestimmungen über „wesentliche Änderungen“. Gem. Art. 3 Abs. 23 ist eine „wesentliche Änderung“ eine Änderung des KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen an Hochrisiko-KI-Systeme beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System geprüft wurde. Aus EG 128 ergibt sich, dass hiervon grundsätzlich jede Änderung erfasst sein sollte, die die Einhaltung der KI-VO durch das Hochrisiko-KI-System beeinträchtigen könnte (z. B. Änderung des Betriebssystems oder der Softwarearchitektur). Ebenfalls erfasst sind Änderungen der Zweckbestimmung des Systems.

Viele Anbieter von KI-Systemen bieten autonome Updates an, um ihren Kunden schnelle und effektive Aktualisierungen des Produkts zu ermöglichen. Durch eine zu weit gefasste Definition des Begriffs "wesentliche Änderung" besteht die Gefahr, dass Anbieter von KI-Systemen de facto verpflichtet werden, sich während der Lebensdauer eines Produkts mehreren Konformitätsbewertungen zu unterziehen, wodurch der Anbieter/Entwickler überlastet wird und dringend benötigte Aktualisierungen für den Kunden verzögert werden. Der weit gefasste Begriff der "wesentlichen Änderung" wird auch Vertreibern, Anwendern, Importeuren und anderen juristischen Personen Verpflichtungen auferlegen, wenn eine Änderung nur geringfügig ist und die Risikobewertung in Wirklichkeit nicht verändert, da die Hauptfunktion eines Produkts nach wie vor dieselbe ist.

Eine mögliche Lösung besteht darin, sich auf Änderungen zu konzentrieren, die die Hauptfunktion des KI-Systems wesentlich verändern, und so sicherzustellen, dass die in Artikel 96 Abs. 1 c) Leitlinien der EU-Kommission Konformitätsbewertungen nicht für jede Änderung vorschreiben, sondern nur dann, wenn eine Änderung im Wesentlichen ein neues KI-System mit hohem Risiko schafft. Eine weitere Möglichkeit bestünde darin, von einer wesentlichen Veränderung nur dann auszugehen, wenn die Gewichtung des Modells angepasst wird.

Konkretisiert werden sollte im Rahmen der Leilinien deshalb, ab wann genau eine Änderung des Hochrisiko-KI-Systems (z. B. Änderung des Betriebssystems oder der Softwarearchitektur) die Einhaltung der KI-VO durch das System beeinträchtigt und ab wann die Einhaltung der KI VO durch eine Änderung beeinträchtigt wird. Ist hierfür ein klarer Widerspruch mit den Ergebnissen der ursprünglichen Konformitätsbewertung erforderlich oder ist ein niedrigschwelliger Ansatz anzunehmen? Gilt die nachträgliche

Verbesserung des Hochrisiko-KI-Systems (z.B. durch Fine-Tuning) auch als „wesentliche Änderung“, wenn diese nicht vorab schon in der Konformitätsbewertung berücksichtigt worden sind?

Zu klären ist außerdem für NLF-regulierte Produkte, wie sich eine nicht-wesentliche Änderung im Sinne der KI-VO auf die Konformität des Produktes mit der entsprechenden NLF-Rechtsvorschrift auswirkt. Denn die KI-VO ermöglicht das "Weiterlernen" eines KI-Systems nach Inverkehrbringen bzw. nach Inbetriebnahme, während die sektoralen Bestimmungen für NLF-regulierte Produkte (z. B. Medizinprodukte) diese Möglichkeit nicht vorsehen.

Art. 25 Abs. 1 lit. b bezieht sich ausschließlich auf Hochrisiko-KI-Systeme. Für KI-Modelle mit allgemeinem Verwendungszweck ist eine entsprechende Regelung nicht vorgesehen. Gleichwohl deutet EG 97 an, dass solche Modelle „weiter geändert oder zu neuen Modellen verfeinert werden“ können. Im Rahmen der Leitlinien ist zu konkretisieren, was s die Kriterien für eine „wesentliche Änderung“ eines KI-Modells mit allgemeinem Verwendungszweck, sodass dieses ein „neues“ Modell i.S.d. der KI-VO darstellt, sein sollen. Kann es auch hier (z.B. durch Fine-Tuning eines fremden KI-Modells) zum Wechsel der Anbietereigenschaft kommen?

Zwar ist für Fragen hinsichtlich der Vorschriften über Allzweck-KI das „AI Office“ zuständig. Dennoch hängen Fragen nach wesentlichen Veränderungen untrennbar mit Fragen nach Verantwortlichkeiten in der Wertschöpfungskette von Allzweck- zu zweckspezifischer KI zusammen. Aus diesem Grund werden in der vorliegenden Stellungnahme auch Forderungen vorgetragen, die das Thema Allzweck-KI (am Rande) betreffen.

Im Falle von Allzweck-KI (GPAI) wird in EG 109 klargestellt, dass die Änderung oder Feinabstimmung („fine tuning“) eines Modells durch einen Akteur dazu führt, dass dieser Akteur nur für die geänderten oder feinabgestimmten Elemente haftet. Es ist zu klären, ob derselbe Grundsatz auch für die Änderung eines KI-Systems gilt, das in andere Risikokategorien fällt.

5. KI-Definition iSd KI VO

Die Definition von KI ist gem. Art. 96 Abs. 1f) KI VO Gegenstand von Leitlinien, die die EU-Kommission zu erlassen hat. Im Wege der Leitlinien sollte mithilfe von Beispielen unbedingt konkretisiert werden, welche (regelbasierten) Systeme nicht unter die Definition von KI fallen. Der Begriff „KI-System“ sollte eindeutig auf Systeme beschränkt werden, die auf Daten und maschinellem Lernen beruhen.

6. Weitere Themen

Hinsichtlich des Konzepts des ‚Finetunings‘ bei Allzweck-KI benötigt die Digitalwirtschaft Orientierungshilfe, was als Finetuning gewertet wird und was nicht. Die KI VO sieht Transparenzverpflichtungen für Anbieter von Allzweck-KI-Modellen vor.

Diese Verpflichtungen können zumindest teilweise auch auf andere Unternehmen anwendbar sein, wenn diese das Modell anpassen (‚finetuning'). Es stellt sich daher die Frage, was ‚Finetuning' im Sinne des Gesetzes bedeutet, insbesondere im Hinblick auf die Unterscheidung zwischen modellinhärentem Finetuning (zB prompting, Dateneingabe) und der Veränderung der Gewichtung eines Modells (zB durch Training mit neuem Datensatz). Nach dem Wortlaut des Gesetzes ist davon auszugehen, dass Finetuning eine grundlegende Veränderung des Modells als solches voraussetzt (als Beispiel werden im Gesetz die Nutzung neuer Trainingsdaten genannt). Ein bestimmungsgemäßer Gebrauch des Modells bzw. modellinhärenter Funktionen (zB durch Prompting oder Zugabe von Vektordaten), sowie vom Anbieter vorgesehen, sollte hingegen nicht als Finetuning gewertet werden und auch nicht zu einer Verlagerung der GPAI-Anforderungen führen. Allerdings wird der Gesetzgeber hier nicht eindeutig. Hier ist es wichtig, dass die Kommission im Rahmen von Leitlinien für mehr Rechtssicherheit sorgt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Lukas Klingholz | Leiter Cloud und Künstliche Intelligenz
T 030 27576-101 | l.klingholz@bitkom.org

Verantwortliches Bitkom-Gremium

AK Artificial Intelligence