VDA | Verband der Automobilindustrie

Position

KI-Verordnung („Artificial Intelligence Act“)

Inhalt

Berlin, Juli 2023

Executive Summary

Die europäische KI-Verordnung wird auf die Unternehmen der Automobil- und Zuliefererindustrie massive Auswirkungen haben. Im bevorstehenden Trilog müssen Änderungen vorgenommen und die Perspektive der Industrie stärker berücksichtigt werden. Andernfalls droht ein Verlust der Wettbewerbsfähigkeit. In folgenden Punkten sieht der Verband der Automobilindustrie e. V. (VDA) Anpassungsbedarf:

1. Die Definition der „Sicherheitskomponente“ ist für die Einstufung eines Hochrisiko-KI-Systems noch unzureichend.

2. Die derzeitige, anwendungsfallbezogene Klassifizierung von Hochrisikosystemen könnte dazu führen, dass alle KI-Systeme im und um das Fahrzeug als hochriskant eingestuft würden.

3. Konformitätsbewertungen durch Dritte bedeuten zusätzlichen Aufwand und sollten daher nur dort Anwendung finden, wo dies unbedingt erforderlich ist.

4. Auf bestehende Normen und Standards muss aufgebaut werden.

5. General-purpose KI-Systeme (GPAI) sollten der gleichen risikobasierten Bewertung unterliegen wie andere KI-Anwendungen.

6. Die Anforderungen des AI-Acts sollten nicht für Open Source gelten.

7. Über Artikel 9 und 10 hinausgehende Anforderungen an das Risikomanagement sind nicht erforderlich.

8. Die Anforderungen an Daten/-sätze (Art. 10, Abs. 2–5) gehen teilweise zu weit und müssen praxistauglicher gestaltet werden.

9. Die Forderung nach Transparenz darf nicht mit dem Schutz von Geschäftsgeheimnissen kollidieren.

10. Eine Einrichtung von Reallaboren ist zu begrüßen, gleichwohl besteht hinsichtlich der genauen Ausgestaltung dieser Nachbesserungsbedarf.

11. Die Notwendigkeit einer kontinuierlichen menschlichen Überwachung von Hochrisiko-KI-Systemen könnte die Einführung automatisierter oder autonomer Fahrfunktionen erschweren.

12. Doppelregulierungen etwa im Bereich der Cybersicherheit müssen vermieden werden.

13. Es sollten Leitlinien für KI-Entwicklerinnen und -Entwickler eingeführt werden, damit abstrakte Formulierungen im Gesetzestext praxisnah und rechtssicher umgesetzt werden können.

1 Europäische Verordnung zur Künstlichen Intelligenz

Im April 2021 hat die EU-Kommission einen Vorschlag für das „Gesetz über die künstliche Intelligenz“ bzw. die KI-Verordnung (KI-VO) (engl. „Artificial Intelligence Act = AI-Act“) des Europäischen Parlaments und des Rates vorgelegt.[1] Die KI-VO ist weltweit der erste Regulierungsansatz für Künstliche Intelligenz und wird auch auf die Fahrzeug- und Zuliefererindustrie massive Auswirkungen haben.

Kernelement des vorliegenden Kommissionsentwurfs ist ein risikobasierter Regulierungsansatz, der KI-Systeme nach ihrem vermuteten Risikopotenzial hin differenziert. Für „Hochrisikosysteme“ gelten umfassende Anforderungen. Die Anwendung bestimmter Systeme mit „inakzeptablem Risiko“ werden verboten.

Der Verband der Automobilindustrie e.V. (VDA) begrüßt die Schaffung eines Rechtsrahmens für den rechtssicheren Einsatz von Künstlicher Intelligenz (KI) in Deutschland und Europa. Ein regulatorischer Ansatz sollte Rechtssicherheit für Anbieter, Entwicklerinnen und Entwickler sowie Nutzerinnen und Nutzer schaffen – gleichzeitig muss darauf geachtet werden, dass die Anforderungen an die Anbieter von KI-Anwendungen praktikabel und umsetzbar sind, da dem europäischen KI-Ökosystem ansonsten die Gefahr droht, an Innovationsfähigkeit zu verlieren. KI betrachtet der VDA als Schlüsseltechnologie, um den Weg zu einer effizienteren sowie sichereren Mobilität in Deutschland und Europa zu ebnen. Sie findet bereits heute in der Fahrzeug- und Zuliefererindustrie breite Anwendung. Zukünftig werden weitere Einsatzfelder hinzukommen.

Die Typgenehmigung für Fahrzeuge ist explizit vom Regelungsrahmen der KI-VO ausgenommen (Art. 2 Abs. 2). Der VDA befürwortet diesen sektorspezifischen Ansatz der Kommission, den Einsatz von KI im Fahrzeug durch den entsprechenden, fahrzeugspezifischen Rechtsrahmen zu regeln. In Erwägungsgrund 29 wird jedoch festgehalten, dass die Regelungen der KI-VO in bestehende Rechtsakte wie z. B. die EU-Verordnung 2018 / 858 über die Kraftfahrzeug-Typgenehmigung eingeführt werden sollen. Die Anforderungen der KI-VO müssen dabei sektorspezifisch mit hohem Ressourcenaufwand übertragen werden.

Am 14. Juni 2023 hat das Europäische Parlament über die zahlreichen Kompromissänderungsanträge zum Kommissionsentwurf abgestimmt und die eigene Position für den anstehenden Trilog festgelegt. Es ist geplant die KI-VO noch in diesem Jahr zu verabschieden. Zwei Jahre später soll sie in Kraft treten. Am vorliegenden Kompromissentwurf sieht der VDA erheblichen Änderungsbedarf.

[1] COM (2021) 206: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union.

2 Bedeutung von KI für die Fahrzeug- und Zuliefererindustrie

In der Fahrzeug- und Zuliefererindustrie werden KI-Anwendungen im gesamten Wertschöpfungsprozess eingesetzt: Von der Forschung und Entwicklung über die Produktion und den Vertrieb sowie Nutzung des Fahrzeugs bis zum After-Sales-Bereich. Wichtig ist jedoch zu betonen, dass Produkte oder Prozesse mit ‚end-to-end KI-Anwendungen‘ in Fahrzeugen bislang noch nicht eingesetzt werden. KI-Anwendungen sind derzeit in herkömmliche Software eingebettet und dienen ausschließlich der Unterstützung und Optimierung bereits bestehender Anwendungen und Systeme.

Beispiele im Fahrzeugkontext für KI-Anwendungen:

Fahrerassistenzsysteme, bzw. autonome / automatisierte Fahrfunktionen können erst durch KI ihr volles Potenzial entfalten. Die hierfür eingesetzten Kamerasysteme kombinieren Bildverarbeitungsalgorithmen mit KI-Methoden. Darüber hinaus basieren Systeme zur Spracherkennung sowie zur kamerabasierten Müdigkeits- und Aufmerksamkeitsüberwachung auf Künstlicher Intelligenz. Zukünftig wird es auch möglich sein, das eigene Fahrzeug per Gesichtserkennung zu öffnen und zu schließen.

Auch in der Fahrzeugproduktion werden KI-Anwendungen bereits heute genutzt, sei es bei der Wartung von Anlagen und Maschinen (Predictive Maintenance) oder der Optimierung von Prüfprozessen der eingesetzten Materialien. KI-Anwendungen ermöglichen es, durch die Erkennung akustischer Anomalien festzustellen, dass Getriebeteile nicht optimal passen. Auch in der Batteriefertigung können KI-Systeme anhand von Mustererkennung feststellen, ob ein verbautes Teil fehlerhaft ist. Ein letztes Beispiel ist die Entwicklung neuer Felgendesigns, bei der die Möglichkeiten der KI genutzt werden können.

3 Änderungsbedarf

3.1 Definition eines KI-Systems und einer Sicherheitskomponente (Art. 3)

Die Definition der „Sicherheitskomponente“ ist für die Einstufung eines Hochrisiko-KI-Systems noch unzureichend.

Eine solche Definition gemäß Artikel 3 (14) würde auch rein technische Prozesse ohne Gefährdungspotenzial wie z. B. im Rahmen der Entwicklung, Fertigung oder Überwachung von Produkten und Systemen als Hochrisiko-KI-Systeme klassifizieren. Auch könnten alle zulassungsrelevanten Bauteile eines Fahrzeugs aktuell als „Sicherheitskomponente“ verstanden werden. Die in der Position des EU-Parlaments erfolgte Streichung des Begriffs „Sache“ aus der Definition begrüßen wir. Die neu eingefügte Einschränkung in Artikel 3 Absatz 14 hinsichtlich der Abgrenzung einer Sicherheitskomponente („einen Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt“) ist ebenfalls positiv zu bewerten. Da es sich um einen auslegungsbedürftigen Begriff handelt, sollte jedoch zumindest in den Erwägungsgründen erläutert werden, dass es sich um Funktionen handelt, deren Sicherheitsrelevanz daraus resultiert, dass eine hohe Verfügbarkeit gewährleistet sein muss oder, dass eine Fehlfunktion oder ein Ausfall kausal unmittelbar zu einer Gefährdung oder Verletzung von Rechtsgütern führt.

Die allgemeine Definition von KI in Artikel 3 (1) war lange Diskussionsgegenstand. **Der VDA begrüßt die erfolgte begriffliche Einengung der Definition** und die Orientierung an der internationalen KI-Definition der OECD / NIST / ISO-IEC 22989:2022.

Im Trilog muss sichergestellt werden, dass gewöhnliche Softwareanwendungen im Fahrzeug nicht unter den Regelungsrahmen des Artikel 3 (1) fallen. Ferner muss die KI-Software wie jede andere Software regulatorisch als Produkt verstanden werden (vgl. europäische Produktsicherheitsverordnung). Maschinen und Systeme, die zwar autonom im menschlichen Umfeld agieren, aber keine Methoden des maschinellen Lernens nutzen, sollten von der KI-VO klar ausgenommen werden.

Daraus lässt sich ableiten, dass **für die Automobilindustrie detailliertere Beschreibungen in einem delegierten Rechtsakt oder über sektorspezifische Ausführungen erfolgen müssen.**

3.2 Definition Hochrisiko-KI-Systeme (Art. 6(1) & (2) / Anh. II & III)

Die derzeitige anwendungsfallbezogene Klassifizierung von Hochrisikosystemen könnte dazu führen, dass pauschal alle KI-Systeme im und um das Fahrzeug als hochriskant eingestuft würden. Hierzu macht der VDA konkrete Vorschläge:

Als Hochrisiko-KI-System gilt u.a. ein System, das „einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden [muss]“ (Art. 6 (1)). Diese Hochrisiko-KI-Systeme sollen „erhebliche Risiken für die Gesundheit und Sicherheit oder die Grundrechte von Personen bergen“. In Anhang III

werden konkrete Einsatzfelder genannt, in denen es sich um Hochrisiko-KI-Systeme handeln kann: So u.a. im Bereich der „kritischen Infrastruktur“ (Anh. III, 2), der „Allgemeinen und beruflichen Bildung“ (Anh. III, 3) oder bei „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“ (Anh. III, 4).

Hier ist eine weitere Präzisierung erforderlich, damit nicht pauschal alle KI-Systeme im und um das Fahrzeug als Hochrisiko eingestuft werden. Es ist unklar, ob diese Definition auch das ‚Backend‘ der Fahrzeuge einschließt oder, ob sich der Regelungsrahmen nur auf die Straßeninfrastruktur bezieht. Der VDA schlägt daher vor, den Begriff der „kritischen Infrastruktur“ mit der Definition der CER-Richtlinie (Art. 2 Nr. 4) zu harmonisieren. Es wird empfohlen, eine Präzisierung dahingehend vorzunehmen, dass sich der Regelungsrahmen ausschließlich auf KI-gestützte Infrastrukturkomponenten im Straßenverkehr außerhalb von Fahrzeugen bezieht (z. B. KI-unterstützte Lichtzeichen oder Schranken).

Artikel 6 (2) sollte dahingehend geändert werden, dass die EU-Regelungen zur Harmonisierung in Anhang II sektorspezifisch erfolgen. Mit Blick auf die Automobilindustrie wäre es denkbar, dass diese selbst festlegen könnte, wann in diesem Sektor eine Hochrisiko-Komponente vorliegt, um der Vielfalt der Rollen, die ein KI-System im Fahrzeug ausüben kann, angemessen Rechnung zu tragen.

Als Sicherheitskomponente sollte nur ein Bauteil oder System gelten, dessen Ausfall kausal unmittelbar die Gesundheit und Sicherheit von Menschen gefährdet. Wenn eine Gefährdung lediglich mittelbar entsteht, z. B. durch die Reaktion eines Nutzenden auf den Ausfall, sollte keine Klassifizierung als Sicherheitskomponente erfolgen. Eine nur mittelbare Kausalität kann beispielsweise angenommen werden, wenn es sich um ein KI-System einer Komfortfunktion (z. B. Infotainment) handelt.

Beispiel KI-basiertes Sprachsystem im Fahrzeug

Angenommen, eine Fahrerin / ein Fahrer interagiert mit einem KI-basierten Sprachsystem im Fahrzeug. Aufgrund einer Fehlfunktion gibt das Sprachsystem unsinnige Antworten. Der Fahrer führt nun einen „Dialog“ mit dem System, wird dadurch abgelenkt und steuert das Fahrzeug in den Gegenverkehr, was zu einem Unfall führt. Die Fehlfunktion des Sprachsystems führt lediglich mittelbar zum Unfall, da die Reaktion des Fahrers ein es-senzieller Bestandteil der Kausalkette war. In diesem Fall ist das Sprachsystem nicht als Sicherheitskomponente anzusehen.

Das in diesem Beispiel beschriebene Phänomen wird bereits durch die etablierten Richtlinien zur „Fahrerablenkung“ ausreichend adressiert und bedarf daher keiner KI-spezifischen Regelung.

Die Klassifizierung nach Anwendungsfällen spiegelt noch nicht die verschiedenen Funktionen wider, die ein KI-System einnehmen kann.

Mit der vorgesehenen Möglichkeit, den Anhang III fortlaufend durch die EU-Kommission anpassen zu lassen, soll der Entwicklungsdynamik von KI Rechnung getragen werden. Diese Möglichkeit zur späteren Erweiterung des Anhangs III führt zu Rechtsunsicherheit für Unternehmen. Eine mögliche turnusmäßige Neubewertung sollte daher nach klar definierten Kriterien erfolgen. Dabei ist die Dauer der Entwicklungszyklen in der Automobilindustrie zu berücksichtigen. Für die Aufnahme neuer Sektoren sollten feste Übergangsfristen von mindestens 24 Monaten gelten.

3.3 Konformitätsbewertung durch Dritte (Art. 6, 1)

Konformitätsbewertungen durch Dritte sind mit zusätzlichem Aufwand und Kosten verbunden. Sie sollten daher nur Anwendung finden, wo dies unbedingt erforderlich ist.

Für einige Hochrisiko-KI-Systeme ist vor dem Inverkehrbringen oder der Inbetriebnahme eine Konformitätsbewertung / -prüfung durch Dritte vorgesehen.

Artikel 43 (1) sieht eine Konformitätsbewertung durch Dritte für Hochrisiko-KI-Systeme vor, bei denen „die harmonisierten Normen gemäß Artikel 40 nicht oder nur teilweise angewandt (werden) oder es solche harmonisierten Normen nicht [gibt] und […] keine gemeinsamen Spezifikationen gemäß Artikel 41 [vorliegen]“. Hinweise zum Konformitätsbewertungsverfahren in diesem Fall finden sich in Anhang VII. Artikel 43 (2) sieht für Hochrisiko-KI-Systeme gemäß Anhang III eine „interne Kontrolle“ durch die Anbieter der Systeme vor. Regelungen zur „internen Kontrolle“ finden sich in Anhang VI. Im Trilog muss geklärt werden, wann eine Bewertung der KI-Anwendungen durch eine interne Kontrolle oder durch Dritte erfolgen soll. Eine Überprüfung aller Hochrisiko-Systeme durch Dritte ist aus Praktikabilitätsgründen abzulehnen. Bereits heute ist absehbar, dass es die derzeitigen Prüforganisationen vor Herausforderungen stellen wird, die erforderlichen Ressourcen bereitzustellen, um KI-Anwendungen in Kraftfahrzeugen ausreichend zu überprüfen. Aus diesem Grund regt der VDA an, unabhängige interne Inspektions- und Bewertungsstellen (sog. Typ C-Stellen gemäß DIN EN ISO / IEV 17020) einzuführen. Dies ist in anderen europäischen Industrien bereits etablierte Praxis.

3.4 Standardisierung (Art. 40)

Es sollte auf bestehende Normen und Standards bei der KI-Verordnung aufgebaut werden.

Die EU-Kommission zielt auf die Einführung eines delegierten Rechtsakts ab. Dieser Rechtsakt soll die EU-Verordnung 2018 / 858 über die Typgenehmigung und Marktüberwachung von Kraftfahrzeugen ergänzen. Hierdurch könnte sichergestellt werden, dass KI-Anwendungen im Fahrzeug weiterhin sektoriell reguliert bleiben. Der VDA appelliert an das EU-Parlament und den Rat, diesem Ansatz der Kommission zuzustimmen. Insbesondere sollte gewährleistet bleiben, dass die Kompetenz zum Erlass solcher sektorspezifische Regulierungen genug Flexibilität beinhaltet, dass sachgerechte Anpassungen an den Vorgaben der KI-Verordnung möglich bleiben.

Der VDA begrüßt die Einführung eines spezifischen delegierten Rechtsaktes, der auf bereits bestehende Normen und Standards für KI verweist und diese für anwendbar erklärt. Die technische Expertise liegt bei den Teilnehmerinnen und Teilnehmern dieser Standardisierungsorganisationen und dort kann auch auf neue Entwicklungen oder Marktanforderungen schnell reagiert werden.

Eine komplett neue technische europäische Normung im Bereich der KI ist nicht erforderlich. Verschiedene technische Normen existieren bereits seit Jahren und haben sich in der Industrie etabliert. Um das Kosten-Nutzen-Verhältnis für die Industrie möglichst effizient zu halten, sollten solche Standardisierungsaktivitäten auf ISO / IEC-Ebene stattfinden. Dies geschieht bereits u.a. in der ISO / IEC JTC1 TC42 AI.

Der VDA spricht sich explizit für die Beibehaltung der fahrzeugspezifischen Zulassungsverfahren aus (Art. 80). In der Fahrzeugtypgenehmigung wird geprüft, ob alle EU-Vorschriften – insbesondere auch zur Fahrzeugsicherheit – bei neuen Fahrzeugmodellen eingehalten werden. Folgerichtig schließt der Entwurf der KI-Verordnung fahrzeugspezifische Anforderungen aus. Unklar ist bislang, wann konkret ein Hochrisiko-KI-System vorliegt. Davon hängt ab, welche Vorschriften für die jeweilige KI-Anwendung gelten. Die Fahrzeugtypengenehmigung sollte daher regeln, wie die Definition von KI für den Fahrzeugsektor konkretisiert wird und wann ein Hochrisiko-System vorliegt. Ebenso können spezifische Anforderungen für den Fahrzeugsektor festgelegt werden.

3.5 General-purpose KI-Systeme (GPAI) (Art. 3(1b), Art. 4, Art. 52) und Generative KI-Systeme (Art. 3(1b), Art. 4, Art. 28b, Art. 52)

GPAI und speziell Generative KI-Systeme sollten derselben risikobasierten Einschätzung unterliegen wie andere KI-Anwendungen.

Neue Bestimmungen des EU-Parlaments sollen die Verwendung von General purpose-KI-Anwendungen („Allzweck-KI-Systeme“) (GPAI) regeln. In einem delegierten Rechtsakt soll sichergestellt werden, dass General purpose-Systeme die gleichen Anforderungen erfüllen wie Hochrisiko-KI-Systeme.

Der Begriff „General Purpose AI“ ist außerhalb des AI-Acts noch nicht klar definiert. Unter GPAI sind nach dem AI-Act KI-Systeme zu verstehen, die keinen spezifischen Zweck verfolgen, sondern in der Lage sind allgemeine Funktionen wie z. B. Bild- oder Spracherkennung, Generierung von Videos, oder die Beantwortung von Fragen zu gewährleisten und darüber hinaus auch in andere, (Hochrisiko-)KI-Systeme integriert werden können.

Eine prinzipielle Klassifizierung aller GPAI als Hochrisiko-KI-Systeme ist inhaltlich nicht plausibel und weder wirtschaftlich noch politisch sinnvoll, da hierdurch Innovationshemmnisse erzeugt würden. Die Anforderungen des Artikels 52 zielen für Generative KI-Systeme in die richtige Richtung, jedoch befürwortet der VDA eine Aufnahme von GPAI in Anhang III oder Artikel 52 des AI-Acts nicht, da dies dem risikobasierten Ansatz widerspricht. Das Risiko von GPAI folgt aus den jeweiligen Anwendungsfällen. Aus diesem Grund ist es für Hersteller von GPAI unmöglich, ein umfassendes Risikomanagementsystem einzuführen, wie es für Hochrisiko-KI-Systeme erforderlich wäre.

Zudem bedarf es einer Klarstellung, ob und wann Arbeitsanteile einer KI bei der Entwicklung einer eigentlich konventionellen Software zur Anwendbarkeit des AI-Acts über die Definition des Artikel 3 (1b) führen (z. B. ChatGPT schreibt einen konventionellen Programmteil ohne maschinelles Lernen und dieser wird in ein Produkt übernommen).

Das Europäische Parlament hat in Artikel 28b Pflichten für die Anbieter von Foundation Models („KI-Basismodellen“) und generativer KI neu eingebracht. Im weiteren Gesetzgebungsverfahren ist auf eine inhaltliche Schärfung dieser Begriffe hinzuwirken.

Mit Blick auf die gesamte Wertschöpfungskette setzt sich der VDA dafür ein, dass Downstream-Providern („nachgelagerten Anbietern von KI-Anwendungen“) keine überbordenden Verpflichtungen auferlegt werden, wie z. B. die in Artikel 28b (4) genannte Pflicht zur Offenlegung von Trainingsmaterial. Im Hinblick auf die Zusammenarbeit in der Wertschöpfungskette ist unklar, wie der ursprüngliche Provider den Downstream-Provider unterstützen muss. Diese Unklarheit entsteht aufgrund der Ausführungen in Artikel 28 und 28b, in denen variierende Begrifflichkeiten (Deployer / Provider) verwendet werden. Der VDA forciert hier, dass im Gesetzgebungsprozess eine klare Abtrennung zwischen Deployer und Provider erfolgt.

Das EU-Parlament hat in Artikel 28a Bestimmungen zur Unangemessenheit von Vertragsklauseln eingeführt, die für Hochrisiko-KI-Systeme gelten. Der VDA fordert hier, dass die Regelungen des Artikels 28a nicht nur – wie aktuell vorgesehen – auf KMUs und Start-Ups beschränkt bleiben, sondern generell für alle Unternehmen gelten. Diese Ausweitung würde dazu beitragen, einer unfairen Vertragsgestaltung entgegenzuwirken.

3.6 Open Source

Die Anforderungen im AI-Act sollen bei Open Source keine Anwendung finden.

Die hohen Anforderungen an die Entwicklerinnen und Entwickler von KI-Systemen würden aktuell auch für Open Source KI gelten, z. B. hinsichtlich der Datenqualität. Aus dem AI-Act ließen sich auch rechtliche Haftungsansprüche für quelloffene GPAI-Modelle begründen und dadurch deren Entwicklung untergraben.

Open Source KI ist jedoch positiv zu bewerten. Es kann zu mehr Transparenz beitragen und dabei helfen, mögliche negative Auswirkungen von KI, z. B. durch Verzerrungen im zugrundeliegenden Datensatz, zu erkennen und abzumildern.

In einer früheren Entwurfsfassung hatte der Europäische Rat Open Source KI aus dem Regelungsrahmen des AI-Acts ausgeschlossen. Open Source sollte nur dann unter den Rechtsrahmen fallen, wenn es in einem Hochrisiko-KI-System verwendet wird. Dieser Passus muss wieder aufgenommen werden. Andernfalls wird dies erhebliche negative Auswirkungen auf die europäische KI-Forschung und -Entwicklung haben.

3.7 Risikomanagementsysteme (Art. 9 und 10)

Die Regelungen in Artikel 9 und 10 schützen die Grundrechte effektiv. Weitere Regulierungen sind nicht notwendig.

Sofern ein Unternehmen ein Hochrisiko-KI-System einsetzt, muss es ein Risikomanagementsystem einrichten, anwenden, dokumentieren und aufrechterhalten. Dies gilt für den gesamten Lebenszyklus des KI-Systems. Artikel 9 und 10 schützen Grundrechte und minimieren Risiken beim KI-Einsatz. Die Definition des von einigen EU-Parlamentariern diskutierten „Fundamental rights impact“ ist unklar und entsprechende Mechanismen sind bereits durch andere Gesetze klar geregelt.

Fahrzeuganwendungen mit und ohne KI werden bereits heute z. B. aus Haftungsgründen mit Risikomanagementsystemen entwickelt. Die Erfahrungen zeigen, dass es während und nach einem Produktanlauf zu keinen Unzulänglichkeiten gekommen ist.

3.8 Anforderungen an die Datenverarbeitung (Art. 10)

Einige Anforderungen an Daten/-sätze gehen teilweise zu weit. Diese Anforderungen müssen praxistauglicher gestaltet werden.

Trainingsmodelle für Daten in Hochrisiko-KI-Systemen müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, welche den genannten Qualitätskriterien entsprechen (Art. 10, Abs. 2–5). Artikel 10 Abs. 3 formuliert hohe Anforderungen an die Qualität der Daten, die Hochrisiko-KI-Systemen zugrunde liegen. In Abs. 2 f) wird eine „Untersuchung im Hinblick auf mögliche Verzerrungen (Bias)“ genannt, ohne jedoch Bias zu definieren. Artikel 10 (2) e) & g) (3) und (4) gehen in ihrer Regelungstiefe zu weit und sind in der Praxis nur für wenige KI-Systeme erfüllbar.

Werden die hohen Anforderungen an die Datenqualität nicht erfüllt, drohen den beteiligten Unternehmen hohe Strafen. Die Systeme werden oftmals von nicht in der EU ansässigen Anbietern trainiert oder entwickelt, sodass entsprechende Systeme in der EU entweder nicht verwendet werden können, was einem Wettbewerbsnachteil gleichkäme, oder das Risiko auf den OEM bzw. Tier 1 verlagert wird.

Ferner erfordert die Umsetzung der Bestimmungen des Artikels 10 spezielle KI- und Datenanalysekenntnisse, über die nicht jedes Unternehmen verfügt. Unternehmen, die „KI-Dienstleister“ (z. B. „KI-as-a-Service“) mit der Entwicklung von KI-Systemen beauftragen, müssten sich bescheinigen lassen, dass diese Dienstleister die Regelungen des Artikels 10 befolgt haben. Die Pflichten sollten daher nur die entsprechenden Dienstleister oder Provider der trainierten Systeme treffen.

Die Methoden und Regeln sind für den zu erbringenden Nachweis regulatorisch nicht klar geregelt: Da es keine Standards für die in Artikel 10 (2), (3) und (4) genannten Kriterien gibt, ist die Einschätzung rein subjektiv, ob die Daten diese Kriterien erfüllen oder nicht. Auch könnte sich die öffentliche Meinung über „Datenlücken“, „Mängel, „Verfügbarkeit“, „geeignete Merkmale“, „Verzerrung“ etc. im Laufe der Zeit allgemein oder für ein bestimmtes Produkt ändern, da neue Erkenntnisse, neue Sensoren oder andere Datenquellen verfügbar werden. Dies bedeutet, dass Entwicklerinnen und Entwickler von KI-Systemen ein hohes juristisches Risiko eingehen müssen, um solche KI-Systeme zu entwickeln, auf den Markt zu bringen und dort langfristig zu halten. Dies könnte die Innovationsfähigkeit Europas und das gesamtwirtschaftliche Wachstum erheblich schwächen. Die Absätze sollten in Empfehlungen umgewandelt werden. Alle anderen Risiken, die sich aus einer schlechten Datenlage ergeben, werden durch das allgemeine Risikomanagement abgebildet.

Die Anforderung, Trainings- und Testdatensätze so zu wählen, dass Bias / Diskriminierung / unfaire Behandlung vermieden bzw. minimiert werden, ist grundsätzlich nachvollziehbar und berechtigt. Die Automobilindustrie unterstützt sowohl entsprechende Untersuchungen vor Inbetriebnahme als auch deren Überprüfung im laufenden Betrieb. Dabei handelt es sich nicht nur um eine rechtlich und ethisch begründete Anforderung, sondern um ein wesentliches Qualitätsmerkmal von KI-Systemen, insbesondere im Hochrisikobereich.

Allerdings müssen die Adressatinnen und Adressaten der Anforderung auch rechtlich in die Lage versetzt werden, entsprechende Datensätze zu erstellen und zu verwenden, nämlich in Form einer hinreichenden Erlaubnis zur entsprechenden Datenerhebung. Folglich ist die Anforderung nur in Verbindung mit entsprechend liberalen Datenschutzvorschriften umsetzbar. Aktuell droht die Regelung in Artikel 10 mit dem europäischen Datenschutzrecht zu kollidieren.

Ferner ist zu prüfen, ob und in welchem Umfang Anbieter von KI-Systemen Trainings- und Testdaten nutzen können, ohne gegen die Grundsätze der Europäischen Datenschutz-Grundverordnung (DSGVO) zu verstoßen.

3.9 Transparenzanforderungen (Art. 52)

Die Forderung nach Transparenz darf nicht mit dem Schutz von Geschäftsgeheimnissen kollidieren.

Nachvollziehbarkeit und Transparenz sind wichtige Voraussetzungen für die Akzeptanz von KI-Systemen. Daher werden in Artikel 52 Transparenzpflichten für Anbieter sowie Nutzerinnen und Nutzer bestimmter KI-Systeme eingeführt. Allerdings bedarf es einer Konkretisierung, was unter der formulierten Ausnahme für die Mitteilung an natürliche Personen bei der Interaktion zu verstehen ist: Die Formulierung „aufgrund der Umstände und des Kontexts der Nutzung offensichtlich“ (Art. 52 (1)) ist unspezifisch.

Transparenzanforderungen sollten risikoadäquat formuliert und entsprechend ausgestaltbar sein. Eine adressatengerechte Beschreibung eines KI-Systems könnte unter Berücksichtigung des zuvor genannten Grundsatzes der Risiko-Adäquanz die Zweckbestimmung und Anwendungshinweise des Systems umfassen, um keine überzogenen Transparenzanforderungen an Low-Risk-Systeme zu stellen. Eine Offenlegung der verwendeten Datensätze hält der VDA für zu weitgehend und im Hinblick auf die DSGVO-Anforderungen für problematisch. Die Trainingsdaten, sowie deren Auswahl und Verwendung, könnten Geschäftsgeheimnisse betreffen.

Die Forderung nach einer deutlichen Kennzeichnung einer KI-Anwendung kann insbesondere dann unterstützt werden, wenn das System die Illusion eines menschlichen Akteurs erzeugt (z. B. ein Chatbot mit natürlicher Sprachausgabe und ggf. auch einem menschlichen Erscheinungsbild im Display). Bereits heute werden entsprechende Kennzeichnungslösungen von VDA-Mitgliedsunternehmen praktiziert: So sind im Produktionsbereich entsprechende Label an den Maschinen angebracht, um die Mitarbeitenden auf den Einsatz von KI hinzuweisen.

Im Fahrzeug selbst sollte aufgrund der zukünftig zu erwartenden Zunahme der KI-Nutzung auf weitere spezielle Labels verzichtet werden. Stattdessen empfiehlt der VDA einfache Kennzeichnungen z. B. in Handbüchern anstelle von KI-Hinweisen im Human-Machine-Interface (HMI), da sonst die Benutzerfreundlichkeit stark leidet.

3.10 Nutzung von Reallaboren (Art. 53 / 54)

Die Einrichtung von Reallaboren ist zu begrüßen. Hinsichtlich der genauen Ausgestaltung besteht jedoch noch Nachbesserungsbedarf.

Die Einrichtung von Reallaboren sollte in Artikel 53 und 54 eindeutig geregelt werden. Ziel sollte es sein, dass Unternehmen unterschiedlicher Größe ohne große bürokratische Prozesse Zugang zu den Reallaboren erhalten.

Aktuell ist unklar, was die Reallabore genau ermöglichen würden – zudem ist die Einrichtung von Reallaboren für die Mitgliedsstaaten nicht verpflichtend. Es ist außerdem unklar, ob sich Reallabore auf ein „echtes Labor“ oder auch auf die Möglichkeit beziehen, KI-Technologien (auch Hochrisiko-KI-Systeme) ohne vollständiges Assessment zu testen. Das Testen von KI, z. B. im Straßenverkehr, auch ohne vollständige Freigabe, aber mit entsprechender Anmeldung, wäre für Automobilunternehmen sehr hilfreich, sinnvoll und begrüßenswert. In Reallaboren können neue autonome KI-Fahrfunktionen mit Prototypenfahrzeugen unter realen Straßenbedingungen getestet werden. Ihre Einrichtung sollte automatisch auf Antrag erfolgen. Die Innovationskraft Europas wird durch fehlende Reallabore gehemmt.

Begrüßenswert wäre es zudem, wenn nach Nutzung eines solchen Reallabors den Unternehmen von einer Aufsichtsbehörde bescheinigt würde, dass sie die Auflagen des AI-Acts erfüllen. Dies könnte zu zusätzlichen globalen Wettbewerbsvorteilen führen.

3.11 Menschliche Überwachung von Hochrisiko-KI-Systemen (Art. 14)

Eine menschliche Überwachung von Hochrisiko-KI-Systemen gem. Artikel 14 (1) könnte die Einführung automatisierter oder autonomer Fahrfunktionen erschweren.

Gem. Artikel 14 (1) sind Hochrisiko-KI-Systeme so zu konzipieren, dass diese „von natürlichen Personen wirksam beaufsichtigt werden können“. Hierdurch sollen Risiken für „die Gesundheit, die Sicherheit oder die Grundrechte“ (Art. 14 (2)) verhindert oder minimiert werden. Bei automatisierten Fahrerassistenzsystemen ist eine menschliche Aufsicht bereits heute gesetzlich vorgesehen.

Eine menschliche Überwachung von KI-Systemen ist jedoch nicht in allen Fällen möglich, da die Entscheidungslogik nicht immer für den Menschen nachvollziehbar ist. Bei technischen Systemen wird es dem Menschen bereits aus tatsächlichen Gründen nicht immer möglich sein, diese zu überwachen. Müsste die Überwachung stets ohne technische Hilfsmittel eingehalten werden, wäre dies das Aus für eine ganze Reihe derartiger Produkte und Systeme! Artikel 14 sollte sich daher auf die grundlegenden Anforderungen an die menschliche Aufsicht beschränken. Praktisch nicht umsetzbare Regelungen sind zu vermeiden. Zudem bleibt unklar, ob sich der Terminus „Überwachung“ auf eine reale Überwachung durch einen Menschen bezieht oder auch auf technische Möglichkeiten im Sinne einer Warnlampe, die dann eine Person benachrichtigt. Die Formulierung „wirksam beaufsichtigen kann“ könnte dazu führen, dass durch die menschliche Beaufsichtigung, sicherheitsrelevante KI-Funktionen wie z. B. eine Notbremsfunktion, in ihrer vorgesehenen Funktionsweise behindert werden könnten. Dies könnte zu schweren Unfällen führen.

Darüber hinaus ist zu vermeiden, dass KI-Anwendungen, die eine kontinuierliche menschliche Überwachung gerade obsolet machen sollen (bspw. Level-3- oder insbesondere Level-4-Fahrzeugsysteme), mit dieser Anforderung konfrontiert werden. Dementsprechend ist eine Konkretisierung vorzunehmen oder alternativ eine sektor- oder anwendungsbezogene Öffnungsklausel vorzusehen.

3.12 Doppelregulierungen vermeiden

Es besteht die Gefahr, dass es bei Hochrisiko-KI-Systemen zu regulatorischen Überschneidungen oder Widersprüchen kommt, z. B. bei Cybersicherheit (Art. 15) oder beim Datenschutz.

Statt der Einführung neuer Vorschriften wäre eine Ergänzung der bestehenden Vorschriften im Automobilsektor zu begrüßen. Die fahrzeugspezifische UN-R155 fordert bereits umfassende Maßnahmen für die Cybersicherheit. Diese UN-Regulierung wird durch die EU-Regulierung 2019/2144 im Europäischen Rechtsraum implementiert. Artikel 15 des AI-Acts ist in diesem Fall irrelevant.

Außerdem sollte es keine doppelten Auflagen z. B. für die Marktüberwachung der Systeme geben. Auch eine Doppelregulierung durch die Regeln der DSGVO muss vermieden werden. Hieraus würden zusätzliche administrative Kosten und Rechtsunsicherheiten entstehen. Es fehlt aktuell an technischen Normen und Standards, die eine Hilfestellung für Wirtschaftsakteure darstellen. Dies würde – bei gleichzeitiger Verschärfung der Haftungsregularien – dazu führen, dass digitale Produkte ohne entsprechende Leitplanken entwickelt würden.

3.13 Einführung von Leitlinien für KI-Entwicklerinnen und -Entwickler

Konkrete Leitlinien sind notwendig, damit abstrakte Formulierungen im Gesetzestext praxisnah und rechtssicher umgesetzt werden können.

Neben dem Gesetzestext muss ein anwendungsorientierter Leitfaden erstellt werden. In diesem sollten die Regelungen praxisnah und verständlich für KI-Entwicklerinnen und -Entwickler „übersetzt“ werden, z. B. mit entsprechenden Checklisten und Step-by-Step-Anleitungen. Leitlinien können Entwicklerinnen und Entwickler beispielsweise bei der Beantwortung der Frage unterstützen, wann von einem KI-System ein hohes Risiko ausgeht oder wie sichergestellt werden kann, dass Datensätze keine Bias enthalten.

Ein interessanter Ansatz stellt das „AI Risk Management Framework 1.0“ der NIST[2] dar. Dieser Leitfaden bietet KI-Entwicklerinnen und -Entwicklern einfache Schritte für den Entwicklungsprozess und das Betreiben von KI-Systemen. Die EU könnte sich daran orientieren, um zu große Unterschiede in der Risikomanagement-Praxis zu vermeiden. Dies könnte die Transaktionskosten im transatlantischen Handel senken.

[2] NIST = US National Institute of Standards and Technology

4 Zusammenfassung

Zusammenfassend ist festzuhalten, dass der AI-Act sowohl Anwenderinnen und Anwender, Nutzerinnen und Nutzer als auch Entwicklerinnen und Entwickler von KI-Systemen betreffen wird. Die Verordnung wird große Auswirkungen für den europäischen, aber auch für den außereuropäischen Markt, haben.

Der VDA befürwortet den Ansatz der EU zur Regulierung von KI und erkennt an, dass im Laufe des Verhandlungsprozesses Fortschritte in Richtung einer praxistauglicheren Regulierung erzielt wurden. Zudem wurde der Regelungsumfang angesichts aktueller Entwicklungen wie General Purpose AI (GPAI) kontinuierlich erweitert. Nach nunmehr zwei Jahren Verhandlungen fordert der VDA die an den Gesetzgebungsverfahren beteiligten Akteure dazu auf, den Verhandlungsprozess zügig zu einem erfolgreichen Abschluss zu bringen, um Rechtssicherheit für den Einsatz und die Entwicklung von KI in Deutschland und Europa zu schaffen. Die KI-Verordnung wird aus der Sicht der VDA-Mitgliedsunternehmen noch immer zu sehr von einer Perspektive bestimmt, die die Risiken von KI überbetont und die Chancen dieser Technologie für die europäische Wirtschaft unterminiert.

Die Anforderungen der KI-Verordnung an Fahrzeuge müssen in das bestehende Typgenehmigungsverfahren integriert werden, um Überschneidungen zu vermeiden. Die Harmonisierung von UNECE-Regelungen und europäischem Recht muss kontinuierlich sichergestellt werden.

Wenn die in dieser Stellungnahme dargestellten Änderungsbedarfe im Trilog beachtet werden, sieht der VDA Chancen, dass Europa auch in Zukunft ein weltweit bedeutender KI-Innovationstandort für die Automobilbranche bleibt.

Ansprechpartnerinnen und Ansprechpartner

Dr. Marcus Bollig
Geschäftsführer Bereich Produkt & Wertschöpfung
marcus.bollig@vda.de

Anja Misselbeck
Leiterin Fachgebiet Technologiestrategie
anja.misselbeck@vda.de

Sebastian Witte
Referent Digitalisierung
sebastian.witte@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 650 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovations-standort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e.V. Behrenstraße 35, 10117 Berlin www.vda.de Registrierter Interessenvertreter R001243 EU-Transparenzregister-Nr. 95574664768-90

Version	Version 1.0, Juli 2023

@VDA_online
Verband der Automobilindustrie