

Stellungnahme

zur Klassifizierung von Hochrisiko-KI-Systemen

Juni 2026



1. Executive Summary

Der Verband der Automobilindustrie (VDA) begrüßt die Veröffentlichung der Entwürfe der Europäischen Kommission zu den Leitlinien für die Klassifizierung von Hochrisiko-KI-Systemen gemäß Artikel 6 der Verordnung (EU) 2024/1689 (AI Act). Die Leitlinien leisten einen wichtigen Beitrag zur praktischen Auslegung des risikobasierten Ansatzes des AI Acts und schaffen zusätzliche Orientierung für Anbieter, Betreiber und Marktüberwachungsbehörden. Insbesondere die Bemühungen der EU-Kommission, die Abgrenzung zwischen Hochrisiko- und Nicht-Hochrisiko-KI-Systemen anhand konkreter Beispiele und horizontaler Kriterien zu präzisieren, werden ausdrücklich unterstützt.

Aus Sicht des VDA ist jedoch entscheidend, dass die Leitlinien in ihrer finalen Fassung eine innovationsfreundliche, verhältnismäßige und sektorspezifisch praktikable Anwendung des AI Acts gewährleisten. Für die deutsche Automobilindustrie ist insbesondere relevant, dass moderne Fahrzeuge zunehmend KI-basierte Funktionen integrieren, die unterschiedliche Sicherheits-, Komfort-, Assistenz- und Digitalisierungszwecke erfüllen. Vor diesem Hintergrund muss verhindert werden, dass die Hochrisiko-Klassifizierung über den gesetzgeberisch intendierten Anwendungsbereich hinaus ausgeweitet wird oder erhebliche Rechtsunsicherheiten für Hersteller und Zulieferer entstehen.

Der VDA unterstützt ausdrücklich die Klarstellung der Kommission, dass nicht sämtliche KI-Systeme innerhalb regulierter Produkte automatisch als Hochrisiko-KI-Systeme einzustufen sind. Positiv hervorzuheben ist insbesondere die Betonung, dass Artikel 6 Absatz 1 AI Act nur solche KI-Systeme erfassen soll, die tatsächlich sicherheitsrelevant sind und zugleich einer Drittstellen-Konformitätsbewertung unterliegen. Ebenso begrüßt der VDA die Feststellung, dass der AI Act bestehende sektorale Regime nicht erweitert oder ersetzt.

Gleichzeitig sieht der VDA an mehreren Stellen weiteren Konkretisierungsbedarf. Dies betrifft insbesondere die Auslegung des Begriffs der „safety component“, die Bewertung komplexer und modularer KI-Systemarchitekturen sowie die Reichweite der Ausnahmeregelungen nach Artikel 6 Absatz 3 AI Act („Filtermechanismus“). Die Leitlinien sollten deutlicher sicherstellen, dass unterstützende, vorbereitende oder rein organisatorische KI-Funktionen nicht unbeabsichtigt als Hochrisiko-KI-Systeme eingestuft werden. Dies ist insbesondere für datengetriebene Entwicklungs-, Qualitäts- und Serviceprozesse der Automobilindustrie von hoher praktischer Bedeutung.

Darüber hinaus hält der VDA eine stärkere Verzahnung mit bestehenden sektorspezifischen Sicherheits- und Typgenehmigungsregimen – insbesondere im Automobilbereich – für erforderlich. Die bestehenden regulatorischen Rahmenwerke im Fahrzeugsektor, einschließlich der europäischen Typgenehmigung sowie international harmonisierter UNECE-Regelungen, enthalten bereits umfassende Anforderungen an funktionale Sicherheit, Cybersecurity und softwarebezogene Systemvalidierung. Die Leitlinien sollten daher ausdrücklich verdeutlichen, dass Doppelregulierungen und parallele Bewertungsmechanismen vermieden werden müssen.

2. Einführung

Die Europäische Kommission verfolgt mit den Entwürfen der Leitlinien zur Hochrisiko-Klassifizierung das Ziel, die Anwendung von Artikel 6 AI Act unionsweit zu harmonisieren und Marktakteuren praktische Orientierung zu bieten. Die Leitlinien erläutern sowohl die Hochrisiko-Klassifizierung nach Artikel 6 Absatz 1 in Verbindung mit Anhang I als auch die Einstufung bestimmter Anwendungsfälle nach Artikel 6 Absatz 2 in Verbindung mit Anhang III AI Act.

Der VDA unterstützt grundsätzlich das Ziel einer unionsweit einheitlichen Auslegung des AI Acts. Insbesondere für weltweit agierende Industrien mit komplexen Wertschöpfungs- und Lieferketten ist regulatorische Kohärenz von zentraler Bedeutung. Dies gilt daher insbesondere auch für die deutsche Automobilindustrie, die zunehmend KI-basierte Systeme in Fahrzeugen, Produktionsprozessen, Qualitätsmanagement, Wartung, Logistik sowie digitalen Mobilitätsdiensten einsetzt.

Die Leitlinien stellen zutreffend klar, dass die Hochrisiko-Klassifizierung dem risikobasierten Ansatz des AI Acts folgt und nur solche Systeme erfassen soll, die erhebliche Risiken für Gesundheit, Sicherheit oder Grundrechte verursachen können. Der VDA begrüßt diese risikoorientierte und verhältnismäßige Grundausrichtung ausdrücklich.

Gleichzeitig zeigt die Vielzahl der in den Entwürfen enthaltenen Fallkonstellationen, dass weiterhin erhebliche Interpretationsspielräume bestehen. Dies betrifft insbesondere die Frage, unter welchen Voraussetzungen KI-Systeme als sicherheitsrelevante Komponenten eines Produkts einzustufen sind, wie komplexe Systemverbünde zu bewerten sind und wann Ausnahmen von der Hochrisiko-Klassifizierung Anwendung finden. Gerade in technologieintensiven Industrien mit hochintegrierten Softwaresystemen besteht andernfalls die Gefahr einer überschießenden Regulierung mit erheblichen Auswirkungen auf Innovationszyklen, Entwicklungsprozesse und internationale Wettbewerbsfähigkeit.

3. Hochrisiko-Klassifizierung nach Artikel 6 Absatz 1 AI Act und sektorale Regulierung

Der VDA begrüßt ausdrücklich die Klarstellung der Kommission, dass Artikel 6 Absatz 1 AI Act lediglich einen begrenzten Teil KI-basierter Systeme innerhalb regulierter Produkte erfasst. Positiv hervorzuheben ist insbesondere die Feststellung, dass nicht sämtliche KI-Komponenten innerhalb regulierter Produkte automatisch als Hochrisiko-KI-Systeme gelten. Vielmehr müssen kumulativ sowohl eine Sicherheitsrelevanz als auch die Pflicht zu einer Drittstellen-Konformitätsbewertung vorliegen.

Diese Auslegung wird durch die im Rahmen der AI-Omnibus-Initiative vorgesehenen Präzisierungen zu Artikel 6 AI Act zusätzlich gestützt. Danach sollen KI-Systeme, die ausschließlich für nicht sicherheitsbezogene Zwecke wie Nutzerunterstützung, Leistungsoptimierung, Serviceeffizienz, Automatisierung, Komfortfunktionen oder Qualitätskontrolle eingesetzt werden, grundsätzlich nicht als Sicherheitsbauteile („safety components“) gelten. Gleichzeitig bleibt klargestellt, dass KI-Systeme, deren Ausfall oder Fehlfunktion ein Risiko für Gesundheit und Sicherheit begründet, weiterhin als Sicherheitsbauteile einzustufen sind. Ebenso soll eine Drittstellen-Konformitätsbewertung nur dann für die Hochrisiko-Klassifizierung relevant sein, wenn sie aufgrund von Risiken für Gesundheit und Sicherheit erforderlich ist.

Der VDA hält es in diesem Zusammenhang für erforderlich, die Begriffe „Automatisierung“ und „Komfortfunktion“ in den Leitlinien weiter zu konkretisieren. Beide Begriffe sind technologisch und funktional sehr weit gefasst und können im Fahrzeugbereich ein breites Spektrum von Anwendungen umfassen, von rein unterstützenden Nutzerfunktionen bis hin zu komplexeren softwaregestützten Systemen. Die Leitlinien sollten daher klarstellen, dass weder der Automatisierungsgrad einer Funktion noch ihre Einordnung als Komfortfunktion

für sich genommen eine Sicherheitsrelevanz oder die Eigenschaft als „safety component“ begründen. Maßgeblich sollte vielmehr sein, ob die betreffende KI-Funktion tatsächlich sicherheitskritische Aufgaben erfüllt oder ob ihr Ausfall beziehungsweise ihre Fehlfunktion ein vernünftigerweise vorhersehbares und hinreichend substantielles Risiko für Gesundheit und Sicherheit verursacht. Eine solche Präzisierung würde die notwendige Rechtssicherheit schaffen und verhindern, dass nicht sicherheitsrelevante KI-Anwendungen allein aufgrund einer weiten Auslegung der Begriffe „Automatisierung“ oder „Komfortfunktion“ in den Anwendungsbereich der Hochrisiko-Klassifizierung einbezogen werden.

Der VDA weist darauf hin, dass die Leitlinien die zweite kumulative Voraussetzung – die Pflicht zu einer Drittstellen-Konformitätsbewertung – bislang im Wesentlichen anhand der Systematik des New Legislative Framework (Beschluss 768/2008/EG, Module A–H, notifizierte Stelle) erläutern. Für den Fahrzeugbereich, dessen Konformitätsbewertung auf der Typgenehmigung durch Genehmigungsbehörden und technische Dienste (einschließlich der im Typgenehmigungsrecht vorgesehenen Prüf- und Nachweisstrukturen) beruht, fehlt eine entsprechende Auslegung. Der VDA regt daher an, die Leitlinien, um ein konkretes Anwendungsbeispiel zu ergänzen, das darlegt, ob und unter welchen Voraussetzungen eine Typgenehmigung nach der Verordnung (EU) 2018/858 die Voraussetzung der Drittstellen-Konformitätsbewertung im Sinne des Artikels 6 Absatz 1 AI Act erfüllt. Andernfalls verbleibt für die betroffenen Marktakteure erhebliche Rechtsunsicherheit hinsichtlich der Hochrisiko-Einstufung.

Die Leitlinien sollten darüber hinaus klarstellen, wie sogenannte Kombinationsrisiken zu bewerten sind. In der Praxis können Sicherheitsrisiken erst durch das Zusammenwirken mehrerer Systeme oder Komponenten entstehen. Für Hersteller ist daher von zentraler Bedeutung, nachvollziehbar bestimmen zu können, unter welchen Voraussetzungen die Kombination mehrerer KI-Systeme oder die Interaktion eines KI-Systems mit anderen Produktkomponenten zu einer Hochrisiko-Einstufung führt.

Ebenso unterstützt der VDA die Aussage der Kommission, dass der AI Act keine Erweiterung bestehender sektoraler Regulierung bewirken soll und sich die Hochrisiko-Klassifizierung auf bestehende unionsrechtliche Harmonisierungsregelungen stützt. Dies ist für die deutsche Automobilindustrie von zentraler Bedeutung, da Fahrzeuge bereits heute umfassenden sektoralen Sicherheits-, Cybersecurity- und Typgenehmigungsanforderungen unterliegen.

Vor diesem Hintergrund sollten aus Sicht des VDA die Leitlinien die im AI Act angelegte Differenzierung zwischen Anhang I Abschnitt A und Abschnitt B ausdrücklich aufgreifen. Für Produkte, die der in Abschnitt B aufgeführten Harmonisierungsgesetzgebung unterliegen, namentlich der Verordnung (EU) 2018/858 und der Verordnung (EU) 2019/2144, finden gemäß Artikel 2 Absatz 2 AI Act ausschließlich Artikel 6 Absatz 1, die Artikel 102 bis 109 sowie Artikel 112 AI Act Anwendung. Die materiellen Anforderungen an Hochrisiko-KI-Systeme werden insoweit nicht unmittelbar, sondern über die sektoralen delegierten Rechtsakte und Durchführungsrechtsakte in das Typgenehmigungsrecht integriert. Eine ausdrückliche Bestätigung dieser Systematik in den Leitlinien würde Doppelregulierung vermeiden und parallele, KI-Konformitätspfade für die Typgenehmigung von Fahrzeugen ausschließen.

Gleichzeitig sollte deutlicher herausgearbeitet werden, wie die Hochrisiko-Klassifizierung nach dem AI Act mit bestehenden sektoralen Sicherheits- und Zulassungsregimen zusammenwirkt.

Im Fahrzeugbereich bestehen mit der europäischen Typgenehmigung, der General Safety Regulation sowie den UNECE-Regelungen zu Cybersecurity, Software Updates und funktionaler Sicherheit bereits umfassende regulatorische Anforderungen an softwarebasierte Fahrzeugsysteme. Diese sektoralen Regelwerke adressieren Sicherheitsrisiken über den gesamten Produktlebenszyklus hinweg und beinhalten umfangreiche Validierungs-, Prüf- und Überwachungsmechanismen. Die Leitlinien sollten daher klarstellen, dass bestehende sektorale Sicherheitsbewertungen grundsätzlich berücksichtigt und Doppelprüfungen vermieden werden.

Der VDA begrüßt in diesem Zusammenhang die im AI Act bereits angelegten Mechanismen zur Vermeidung von Mehrfachaufwand: Artikel 8 Absatz 2, Artikel 9 Absatz 10 und Artikel 17

Absatz 3 AI Act ermöglichen es, die Bewertung KI-spezifischer Risiken in bestehende Risiko- und Qualitätsmanagementsysteme zu integrieren; Artikel 40 AI Act verlangt die Kohärenz der harmonisierten KI-Normen mit den unter der sektoralen Harmonisierungsgesetzgebung entwickelten Normen. Die Leitlinien sollten ausdrücklich klarstellen, dass diese Mechanismen so auszugestaltet sind, dass etablierte Verfahren der funktionalen Sicherheit (etwa nach ISO 26262 und ISO 21448/SOTIF sowie der entstehenden ISO/PAS 8800 für KI), der Cybersicherheit und der Typgenehmigung als Nachweisgrundlage genutzt werden können und nicht durch eigenständige KI-spezifische Verfahren dupliziert werden.

Dementsprechend kritisch ist die Ziffer 46 der Draft Commission Guidelines on High Risk classification zu bewerten. Das Risiko für Health and Safety wird bei der Typzulassung eingehend bewertet, unterschieden nach Einsatzszenario. In der Automobilindustrie wird zwischen Assistenzfunktionen (Level 2) und Automatisierungsfunktionen (Level 3) unterschieden. Für Level 2 Funktionen wird die Kontrollierbarkeit durch den Menschen als Risikoreduzierungsfaktor berücksichtigt. Darüber hinaus werden konventionell entwickelte Sicherheitsfunktionen zur Performancelimitierung herangezogen, um die Kontrollierbarkeit sicherzustellen.

Aus Sicht des VDA bedarf insbesondere der Begriff der „safety component“ weiterer Präzisierung. Die Entwürfe lassen bislang offen, wie weit der Sicherheitsbezug bei softwarebasierten KI-Funktionen reicht. Dabei ergibt sich die Sicherheitsbauteil-Eigenschaft nach Artikel 3 Nummer 14 AI Act nicht nur aus der Zweckbestimmung einer Funktion, sondern auch daraus, dass ihr Ausfall oder ihre Fehlfunktion Gesundheit, Sicherheit oder Eigentum gefährden kann. Eine Einordnung allein anhand des erklärten Komfort- oder Effizienzszwecks greift daher zu kurz. Der VDA empfiehlt, die Leitlinien an dieser Stelle zu präzisieren: Die Fehlfunktionsalternative sollte ein vernünftigerweise vorhersehbares und hinreichend substantielles Risiko voraussetzen; rein hypothetische, fernliegende oder nur abstrakt konstruierbare Gefährdungsszenarien dürfen für sich genommen keine Sicherheitsbauteil-Eigenschaft begründen. Insbesondere sollten rein informierende Überwachungs-, Diagnose- und Prognosefunktionen, die eine nachgelagerte menschliche Entscheidung lediglich anreichern und nicht selbst steuernd auf das Produkt einwirken, klar von Funktionen abgegrenzt werden, die für den sicheren Betrieb essenziell sind oder unmittelbar in sicherheitsrelevante Abläufe eingreifen.

Mit der zunehmenden Verbreitung softwaredefinierter Fahrzeuge, drahtloser Software-Updates und vernetzter digitaler Dienste gewinnt die Abgrenzung zwischen einem in das typgenehmigte Fahrzeug integrierten Sicherheitsbauteil einerseits und einem eigenständig erbrachten, dem Fahrzeug nachgelagerten digitalen Dienst andererseits erheblich an Bedeutung. Ein und dieselbe KI-gestützte Funktion kann je nach Integrationsarchitektur regulatorisch grundlegend unterschiedlich einzuordnen sein. Der VDA empfiehlt, hierfür einen vorhersehbaren, funktionsbezogenen Maßstab für diese Abgrenzung zu entwickeln, der insbesondere die Konstellationen der Nachrüstung, der nachträglichen Software-Aktualisierung und datenbasierter Dienste erfasst. Nur so lassen sich Produkt- und Architekturentscheidungen mit hinreichender Rechtssicherheit treffen und sachlich nicht gerechtfertigte Klassifizierungsunterschiede für funktional gleichartige Anwendungen vermeiden.

Der VDA gibt zu bedenken, dass die Einstufung einer funktional gleichartigen KI-Anwendung maßgeblich davon abhängen kann, auf welchem Wege sie in den Verkehr gebracht wird, etwa als integrierter Bestandteil eines typgenehmigten Produkts oder als eigenständig erbrachter, nachgelagerter Dienst. Aus Sicht eines kohärenten und wettbewerbsneutralen Ordnungsrahmens sollte die regulatorische Behandlung solcher Anwendungen so weit wie möglich an ihrem tatsächlichen Risiko und ihrer Funktion ausgerichtet sein und nicht an inzidentellen Merkmalen der Integrationsarchitektur. Der VDA regt an, dass die Leitlinien diesen Gesichtspunkt aufgreifen und, soweit künftige Anpassungen des Anwendungsbereichs erwogen werden, auf die im AI Act vorgesehene risikobasierte Methodik (insbesondere Artikel 7 AI Act) verweisen, damit etwaige Fortentwicklungen vorhersehbar, verhältnismäßig und einheitlich erfolgen. Auf diese Weise lassen sich sowohl ungerechtfertigte Wettbewerbsunterschiede als auch sprunghafte, schwer planbare Reklassifizierungen vermeiden.

Darüber hinaus begrüßt der VDA die Feststellung der EU-Kommission, dass auch Verbraucherprodukte nicht automatisch als Hochrisiko-KI-Systeme einzustufen sind und viele KI-basierte Alltagsanwendungen die kumulativen Voraussetzungen des Artikels 6 Absatz 1 gerade nicht erfüllen. Dieser Ansatz sollte auch im Automobilbereich konsequent angewendet werden, um eine unverhältnismäßige Ausweitung regulatorischer Anforderungen zu vermeiden.

4. Verantwortlichkeiten entlang der KI-Wertschöpfungskette (Artikel 25 AI Act)

Die Hochrisiko-Klassifizierung entfaltet ihre praktische Wirkung erst über die Zuordnung der jeweiligen Pflichten zu den Akteuren entlang der KI-Wertschöpfungskette. Gerade in der arbeitsteilig organisierten Automobilindustrie, in der KI-gestützte Komponenten und Software von einer Vielzahl von Akteuren entwickelt, integriert, aktualisiert und betrieben werden, ist eine vorhersehbare und kohärente Zuordnung der Verantwortlichkeiten von hoher Bedeutung; für Hersteller wie für Zulieferer gleichermaßen.

Der VDA regt an, dass die Leitlinien das Zusammenspiel der Klassifizierung mit den Verantwortlichkeiten entlang der Wertschöpfungskette nach Artikel 25 AI Act adressieren und insbesondere klarstellen, unter welchen Voraussetzungen die Rolle des Anbieters wechselt (Artikel 25 Absatz 1). Dabei sollte die im AI Act ausdrücklich vorgesehene Möglichkeit, die Verteilung der Pflichten durch vertragliche Vereinbarungen abweichend auszugestalten, anerkannt und praktikabel gehalten werden. Der VDA verweist auf die angekündigten gesonderten Leitlinien zu Artikel 25 AI Act und spricht sich dafür aus, beide Leitlinienwerke aufeinander abzustimmen, um konsistente und rechtssichere Ergebnisse für die gesamte Wertschöpfungskette zu gewährleisten.

5. Bewertung der Hochrisiko-Klassifizierung nach Artikel 6 Absatz 2 und Anhang III AI Act

Der VDA begrüßt die Klarstellung der EU-Kommission, dass die in Anhang III genannten Hochrisiko-Anwendungsfälle abschließend geregelt sind und nur gezielt bestimmte risikobehaftete Einsatzszenarien erfassen sollen. Dies trägt zur Rechtssicherheit bei und unterstützt den risikobasierten Ansatz des AI Acts.

Positiv hervorzuheben ist ferner die ausdrückliche Feststellung, dass die bloße menschliche Beteiligung an Entscheidungen die Hochrisiko-Einstufung weder automatisch ausschließt noch ersetzt. Gleichzeitig verdeutlichen die Leitlinien zutreffend, dass menschliche Aufsicht ein wesentliches Element der Compliance-Anforderungen für Hochrisiko-KI-Systeme bleibt.

Aus Sicht des VDA ist jedoch entscheidend, dass die in Anhang III vorgesehenen Anwendungsfälle eng und verhältnismäßig ausgelegt werden. Viele KI-Anwendungen innerhalb industrieller Prozesse dienen ausschließlich unterstützenden, organisatorischen oder vorbereitenden Zwecken und treffen keine eigenständigen Entscheidungen mit erheblichen Auswirkungen auf natürliche Personen. Die Leitlinien sollten daher noch klarer hervorheben, dass rein unterstützende Systeme nicht unbeabsichtigt in den Hochrisiko-Bereich fallen dürfen.

Zur Erhöhung der praktischen Anwendbarkeit und Rechtssicherheit sollten die Leitlinien zusätzliche sektorspezifische Beispiele für KI-Systeme enthalten, die zwar einem der in Anhang III genannten Anwendungsbereiche zugeordnet werden können, aufgrund ihres rein unterstützenden oder vorbereitenden Charakters jedoch nicht als Hochrisiko-KI-Systeme einzustufen sind. Dies betrifft beispielsweise KI-gestützte Systeme zur Unterstützung der Personalauswahl, die Bewerbungsunterlagen lediglich strukturieren, kategorisieren oder auf Vollständigkeit prüfen, ohne eine Auswahlentscheidung vorzuschlagen oder zu treffen, KI-Anwendungen zur individuellen Aufbereitung betrieblicher Weiterbildungsangebote ohne Auswirkungen auf den Zugang zu Beschäftigung oder formaler Bildung sowie KI-gestützte Qualitäts- und Analysewerkzeuge, die Produktions- oder Prozessdaten auswerten und ausschließlich technische Handlungsempfehlungen für menschliche Entscheidungen bereitstellen.

Darüber hinaus besteht weiterer Klarstellungsbedarf hinsichtlich der Abgrenzung einzelner Anwendungsbereiche des Anhangs III. So scheint insbesondere der Begriff des Zugangs zu beruflicher Bildung teilweise sehr weit gefasst. Die Leitlinien sollten klarstellen, dass betriebliche Aus- und Weiterbildungsangebote privater Unternehmen nicht allein aufgrund ihres Bildungsbezugs automatisch in den Anwendungsbereich von Anhang III fallen, sofern keine mit formalen Bildungsentscheidungen vergleichbaren Auswirkungen auf die betroffenen Personen bestehen.

Besonders relevant für die Automobilindustrie ist die Bewertung komplexer und modularer KI-Systemarchitekturen. Die Leitlinien führen aus, dass mehrere KI-Systeme gemeinsam als ein Hochrisiko-System angesehen werden können, wenn ihre kombinierten Funktionen wesentlichen Einfluss auf individuelle Entscheidungen haben. Der VDA erkennt das Ziel an, Umgehungen regulatorischer Anforderungen zu verhindern. Gleichzeitig besteht jedoch das Risiko, dass hochgradig modulare Entwicklungs- und Softwaresysteme übermäßig weitgehend als einheitliche Hochrisiko-Systeme interpretiert werden.

Die finale Fassung der Leitlinien sollte deshalb stärker differenzieren zwischen funktional unabhängigen Modulen und tatsächlich integrierten Entscheidungsarchitekturen. Gerade im Fahrzeugbereich bestehen komplexe Softwarelandschaften mit zahlreichen voneinander getrennten Funktionen, deren regulatorische Behandlung klar und vorhersehbar bleiben muss.

Zur Bestimmung der Grenzen eines KI-Systems und zur Bewertung funktionaler Zusammenhänge sollte die finale Fassung der Leitlinien stärker auf etablierte Grundsätze der funktionalen Sicherheit Bezug nehmen. Eine solche Betrachtung würde eine nachvollziehbare Abgrenzung von Systemgrenzen und Wirkzusammenhängen ermöglichen und zugleich die Konsistenz mit bestehenden sektoralen Sicherheitsmethodiken fördern.

6. Ausnahmeregelungen nach Artikel 6 Absatz 3 AI Act („Filtermechanismus“)

Der VDA begrüßt ausdrücklich, dass die Kommission den sogenannten Filtermechanismus nach Artikel 6 Absatz 3 AI Act ausführlich erläutert und damit die Verhältnismäßigkeit des AI Acts stärken möchte. Die Möglichkeit, bestimmte Systeme trotz grundsätzlicher Zuordnung zu Anhang III von der Hochrisiko-Klassifizierung auszunehmen, ist für innovationsfreundliche und praktikable Regulierung von zentraler Bedeutung.

Insbesondere die Beispiele zu „narrow procedural tasks“, vorbereitenden Tätigkeiten sowie unterstützenden Qualitätssicherungsfunktionen sind aus Sicht des VDA hilfreich und praxisrelevant. Die Leitlinien verdeutlichen zutreffend, dass Systeme zur Strukturierung, Sortierung, Indexierung oder Qualitätskontrolle grundsätzlich nicht automatisch als Hochrisiko-KI-Systeme angesehen werden sollen.

Gerade für die deutsche Automobilindustrie ist diese Klarstellung essenziell. Zahlreiche KI-basierte Anwendungen in Entwicklung, Produktion, Qualitätsmanagement, Compliance oder Dokumentationsprozessen dienen ausschließlich vorbereitenden, unterstützenden oder organisatorischen Zwecken. Sie treffen keine eigenständigen Entscheidungen über natürliche Personen und entfalten keinen unmittelbaren Einfluss auf sicherheitskritische oder grundrechtsrelevante Entscheidungen.

Darüber hinaus sollte die finale Fassung der Leitlinien stärker zwischen KI-Systemen, die als Entwicklungswerkzeuge eingesetzt werden, und KI-Systemen, die tatsächlich im Fahrzeug oder in einem regulierten Produkt verwendet werden, differenzieren. Insbesondere KI-gestützte Werkzeuge zum Training und zur Optimierung von Algorithmen, zur Generierung oder Analyse von Source Code sowie zur Unterstützung von Entwicklungs-, Test- und Validierungsprozessen sollten nicht allein deshalb als Hochrisiko-KI-Systeme eingestuft werden, weil die Ergebnisse ihrer Verarbeitung später in Fahrzeugfunktionen einfließen. Maßgeblich für die Hochrisiko-Klassifizierung sollte vielmehr die Funktion, Zweckbestimmung und Risikorelevanz des jeweils konkret eingesetzten KI-Systems sein. Die Leitlinien sollten daher klarstellen, dass die Verwendung von KI-generierten Modellen, Algorithmen oder Softwareartefakten in Fahrzeugen nicht automatisch zu einer Hochrisiko-Einstufung des vorgelagerten Entwicklungswerkzeugs führt. Gleichzeitig sollte verdeutlicht werden, dass die regulatorische Bewertung des im Fahrzeug eingesetzten KI-Systems hiervon unberührt bleibt und eigenständig anhand der Kriterien des Artikels 6 AI Act vorzunehmen ist.

Gleichzeitig sieht der VDA weiteren Präzisierungsbedarf hinsichtlich der Abgrenzung zwischen vorbereitenden Tätigkeiten und tatsächlich entscheidungsrelevanten Bewertungen. Die derzeitigen Formulierungen lassen weiterhin erhebliche Interpretationsspielräume offen. Dies könnte insbesondere bei datenanalytischen oder KI-gestützten Qualitätssicherungsprozessen zu Unsicherheiten führen.

Darüber hinaus sollte die finale Fassung der Leitlinien klarstellen, dass technische Hilfs- und Assistenzfunktionen innerhalb komplexer industrieller Systeme grundsätzlich eigenständig bewertet werden können und nicht automatisch aufgrund ihrer Einbettung in größere Softwarearchitekturen ihre Ausnahmefähigkeit verlieren. Andernfalls besteht das Risiko einer unverhältnismäßigen Ausweitung der Hochrisiko-Klassifizierung auf große Teile industrieller KI-Anwendungen.

7. Profiling und Grundrechtsbezug

Der VDA erkennt an, dass der AI-Act besonderen Schutzanforderungen für Systeme mit erheblichem Einfluss auf natürliche Personen Rechnung trägt. Die Leitlinien stellen zutreffend klar, dass Systeme, die Profiling im Sinne der Datenschutzgesetzgebung durchführen, grundsätzlich nicht von den Ausnahmeregelungen des Artikels 6 Absatz 3 profitieren können.

Gleichzeitig ist aus Sicht des VDA wichtig, dass der Profiling-Begriff nicht übermäßig weit ausgelegt wird. Viele datenanalytische Systeme in industriellen Kontexten verarbeiten Informationen rein technisch, statistisch oder organisatorisch, ohne individuelle

Bewertungen natürlicher Personen vorzunehmen. Die Leitlinien sollten deshalb noch deutlicher zwischen personenbezogener Bewertung und rein technischer Datenanalyse differenzieren.

Insbesondere industrielle Analyse-, Monitoring- und Qualitätssicherungssysteme dürfen nicht allein aufgrund automatisierter Datenverarbeitung als Profiling-Systeme eingeordnet werden, sofern keine Bewertung persönlicher Eigenschaften natürlicher Personen erfolgt.

Eine zu weite Auslegung könnte andernfalls erhebliche Rechtsunsicherheit für datengetriebene Industrieprozesse verursachen.

8. Fazit

Der Verband der Automobilindustrie unterstützt die Zielsetzung der Europäischen Kommission, durch die Leitlinien zur Hochrisiko-Klassifizierung eine einheitliche und praktikable Anwendung des AI Acts sicherzustellen. Die Entwürfe enthalten bereits zahlreiche hilfreiche Klarstellungen und verfolgen grundsätzlich einen risikobasierten und verhältnismäßigen Ansatz.

Für die finale Fassung der Leitlinien ist jedoch entscheidend, dass sektorale Besonderheiten und bestehende regulatorische Strukturen ausreichend berücksichtigt werden. Insbesondere im Automobilbereich bestehen bereits umfassende Sicherheits-, Cybersecurity- und Typgenehmigungsregime, die in ihrer Wechselwirkung mit dem AI Act kohärent geregelt werden müssen.

Der VDA spricht sich daher insbesondere für:

- eine rechtssichere, an beiden Alternativen des Artikels 3 Nummer 14 AI Act ausgerichtete Auslegung des Begriffs der ‚safety component‘, die rein informierende Funktionen klar von sicherheitssensitiven Funktionen abgrenzt,
- eine klare Abgrenzung unterstützender und vorbereitender KI-Funktionen von Hochrisiko-Systemen,
- eine praxisnahe Anwendung des Filtermechanismus nach Artikel 6 Absatz 3 AI Act,
- eine Klarstellung zum Verhältnis verschiedener Hochrisiko-Kategorien, insbesondere im Hinblick auf Artikel 2 Absatz 2 AI Act, sowie zu deren möglicher Kumulation innerhalb desselben KI-Systems,
- eine differenzierte Bewertung modularer und komplexer KI-Systemarchitekturen aus,
- sowie eine vorhersehbare und kohärente Zuordnung der Verantwortlichkeiten entlang der KI-Wertschöpfungskette und eine an Funktion und Risiko ausgerichtete, wettbewerbsneutrale Einordnung funktional gleichartiger Anwendungen.

Darüber hinaus sollte die finale Fassung der Leitlinien ausdrücklich anerkennen, dass bestehende sektorale Sicherheits- und Zulassungsverfahren bereits eine differenzierte Bewertung von Risiken KI-gestützter Fahrzeugfunktionen ermöglichen. Insbesondere bei

Fahrerassistenzsystemen der Automatisierungsstufe Level 2 wird die fortbestehende menschliche Kontrolle als wesentlicher Risikominderungsfaktor berücksichtigt. Ergänzende konventionelle Sicherheitsmechanismen stellen zudem sicher, dass die Systemleistung jederzeit begrenzt und kontrollierbar bleibt.

Vor diesem Hintergrund sollte klargestellt werden, dass KI-Funktionen, deren Risiken bereits wirksam durch bestehende sektorale Sicherheitsanforderungen adressiert werden, nicht zusätzlich als Hochrisiko-KI-Systeme eingestuft werden, sofern die Voraussetzungen des Artikels 6 AI Act nicht eindeutig erfüllt sind.

Nur durch eine klare, kohärente und innovationsfreundliche Anwendung der Hochrisiko-Regeln kann der AI Act sowohl hohe Sicherheits- und Grundrechtsstandards als auch die internationale Wettbewerbsfähigkeit europäischer Industrieunternehmen gewährleisten.

Ansprechpartner

Dr. Marcus Bollig

Geschäftsführer
marcus.bollig@vda.de

Martin Lorenz

Abteilungsleiter
Security, Daten & Digitalisierung
martin.lorenz@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 620 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 Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 730.000 Menschen (2025) 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. (VDA)
Behrenstraße 35, 10117 Berlin
www.vda.de

Deutscher Bundestag Lobbyregister-Nr.: R001243
EU-Transparenz-Register-Nr.: 9557 4664 768-90

Copyright Verband der Automobilindustrie e. V. (VDA)

Nachdruck und jede sonstige Form der Vervielfältigung
ist nur mit Angabe der Quelle gestattet

Version Juni 2026