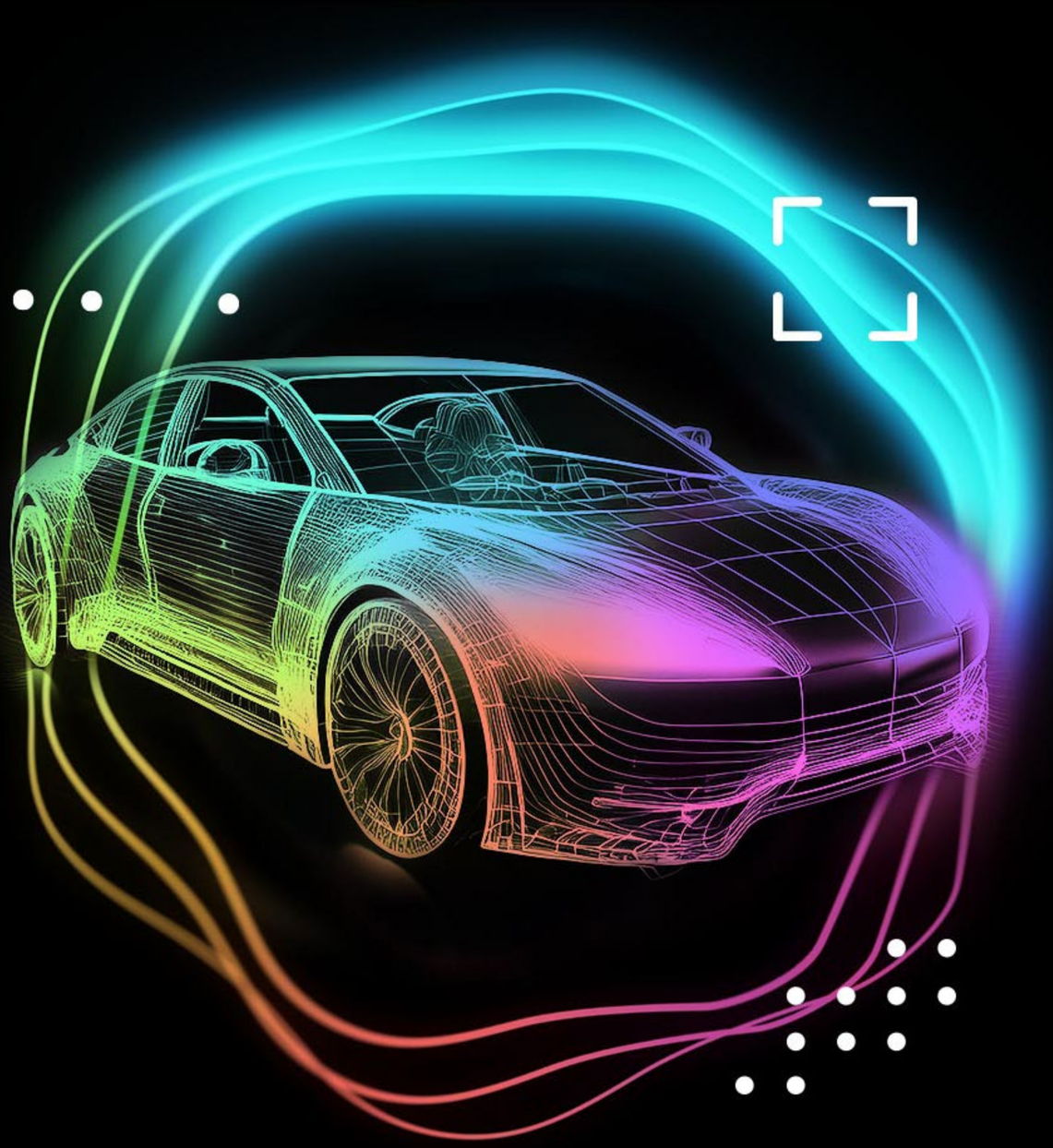
Deloitte.



Grünes Licht für KI

Wie die neue KI-Verordnung die Automobilbranche in die Zukunft lenkt.

Inhalt

Status quo: die KI-Verordnung	3
Sektorale Sicht: die KI-Verordnung und Auswirkungen auf die Automobilbranche	8
Systematische Grundlagen zur Bewältigung der KI-Verordnung schaffen: KI-Governance und Integration in bestehende Programme	11
Ausblick und Fazit	16
Ansprechpartner	17

1 **Status quo:** die KI-Verordnung

In der sich entwickelnden Landschaft der Regulierung von künstlicher Intelligenz (KI) hat die Europäische Union (EU) eine Vorreiterrolle eingenommen und sich bemüht, einen umfassenden Rahmen zu schaffen, der die Komplexität und die potenziellen Risiken von KI-Systemen berücksichtigt. Eine der wichtigsten Prioritäten der EU-Kommission für die Amtszeit 2019–2024 ist die Schaffung eines Europas, das fit ist für das digitale Zeitalter[1]. Diese ehrgeizige Agenda hat zur Vorlage von mehr als zehn wichtigen digitalen Verordnungen geführt, die sich mit Bereichen wie Datenwirtschaft, Cybersicherheit und Regulierung von Plattformen befassen. Die europäische Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (KI-Verordnung) ist ein entscheidendes Puzzlestück in diesem komplexen Rahmen der digitalen EU-Regulierung. Der folgende Artikel konzentriert sich zwar auf die KI-Verordnung, sollte aber immer im breiteren Kontext der gesamten digitalen Regulierungslandschaft der EU gesehen werden.

Die KI-Verordnung fordert von Unternehmen künftig, den Einsatz von KI im europäischen Raum vertrauenswürdig, transparent und grundrechtskonform zu gestalten. Unternehmen müssen eine angemessene Governance über ihre KI-Systeme ausüben und ein effektives KI-Risikomanagementsystem sicherstellen, um den Umsetzungsanforderungen gerecht zu werden und empfindliche Strafen von bis zu 7 Prozent des weltweiten Jahresumsatzes bzw. 35 Mio. EUR zu vermeiden.

Weiterhin stellt die KI-Verordnung einen umfassenden regulatorischen Rahmen der Europäischen Union (EU) für KI dar, der darauf abzielt, eine digitale Landschaft zu schaffen, die mit Sicherheits-, Transparenz- und ethischen Standards übereinstimmt. Als Teil der umfassenderen digitalen Regulierungsagenda der EU standardisiert die KI-Verordnung die Markteintritts- und Betriebsverfahren für Single-Purpose-AI-(SPAI-)Systeme durch einen risikobasierten Ansatz, welcher einen einheitlichen Einsatz in allen EU-Mitgliedsstaaten gewährleistet. Dieser Ansatz kategorisiert KI-Systeme nach ihren Anwendungsfällen und den damit verbundenen Risiken.

KI-Systeme werden umfassend definiert und umfassen Technologien, die Vorhersagen treffen, Inhalte vorschlagen oder Entscheidungen treffen, die physische oder virtuelle Umgebungen beeinflussen. Das Gesetz gilt für KI-Anbieter und -Nutzer innerhalb der EU sowie für diejenigen außerhalb der EU, deren Systeme EU-Nutzer betreffen. Ausnahmen vom Gesetz umfassen militärische Nutzung, wissenschaftliche Forschung und persönliche nicht-professionelle Aktivitäten.

[1] Europäische Kommission (Abrufdatum: 8.8.2024)

Status quo: die KI-Verordnung

Das KI-Gesetz kategorisiert KI-Systeme in vier Risikostufen (s. Abb. 1):

Unannehmbares Risiko
Verbotene Praktiken wie KI, die menschliches Verhalten manipuliert oder soziale Bewertungen vornimmt. Aufgrund des kritischen Schadenspotenzials dürfen solche KI-Systeme nicht betrieben werden.

Hochrisiko-KI-Systeme
Systeme, die Sicherheit oder Grundrechte betreffen. Aufgrund des erhöhten Schadenspotenzials sind vor einer Inbetriebnahme eines solchen KI-Systems strenge Compliance-Auflagen zu erfüllen und die Einhaltung durch Konformitätsbewertungen nachzuweisen.

Systeme mit Transparenzanforderung
KI-Systeme, die direkt mit natürlichen Personen interagieren. Bei solchen KI-Systemen muss die betreffende Person informieren werden, dass sie mit einem KI-System interagiert.

Geringes/kein Risiko
KI-Systeme ohne hohes Risiko. Für solche KI-Systeme können auf freiwilliger Basis Verhaltenskodizes und Governance-Mechanismen aufgestellt werden.

Risikoklassen Einordnung von KI-Systemen in Risikoklassen	**Rechtliche Auflagen**	**Mögliche Beispiele**	**Bußgelder**
Unannehmbares Risiko Anwendbar: + 6 Mon. ≙ Feb '25	**Verbotene Praktiken** Kapitel II, Art. 5	Sozialbewertung, Gesichtserkennung, Dark-Pattern, Identifikation von Emotionen am Arbeitsplatz	**Bis zu 35 Mio. €** oder 7% des GAT[2]
Hochrisiko + 24–36 Mon. ≙ Aug '26	**Konformitäts-bewertung** Kapitel III, Art. 6	Sicherheitskomponenten von Produkten[1], Kritische Infrastruktur, Biometrische Erkennung, Kreditprüfung, Recruiting, Personalmanagement	**Bis zu 15 Mio. €** oder 3% des GAT
Begrenztes Risiko + 24 Mon. ≙ Aug '26	**Transparenz-pflichten** Kapitel IV, Art. 50	Chatbots, Deepfakes, Emotions-erkennungssysteme, biometrische Kategorisierungssysteme	**Bis zu 15 Mio. €** oder 3% des GAT
Minimales Risiko	**Freiwillig: Verhaltenskodizes** Kapitel X, Art. 95	Spamfilter	N/A
KI-Modelle mit allgemeinem Verwendungszweck, zzgl. systematischem Risiko	**KI-Modelle mit all-gemeinem Verwen-dungszweck** Kapitel V	Basismodelle, LLMs, Multimodale Modelle	**Bis zu 15 Mio. €** oder 3% des GAT

Für Hochrisiko-KI-Systeme müssen erweiterte gesetzliche Anforderungen zur Konformität umgesetzt werden

[1] Siehe Anhang I des AI Acts für eine vollständige Liste der Harmonisierungsrechtsvorschriften der Union bzgl. der als hochriskant eingestuften Sicherheitskomponenten in Produkten
[2] GAT = Gesamter weltweiter Jahresumsatz des vorangegangenen Geschäftsjahres

Abbildung 1 *Risikoklassen und rechtliche Auflagen zur Risikosteuerung durch die KI-Verordnung*

Status quo: die KI-Verordnung

Die Verordnung legt spezifische Verantwortlichkeiten für verschiedene Akteure einschließlich Anbieter, Nutzer, Vertriebshändler und Importeure fest. Der Schwerpunkt liegt auf dem Aufbau von Risiko- und Qualitätsmanagementsystemen, der Durchführung von Konformitätsbewertungen und der Sicherstellung von Transparenz.

Der Schwerpunkt der KI-Verordnung liegt auf Hochrisiko-KI-Systemen, da die meisten Verpflichtungen und Schutzmaßnahmen dieses Gesetzes auf KI-Anwendungen mit hohem Risiko abzielen. Hochrisiko-KI-Systeme sind solche, die potenziell die Sicherheit oder Grundrechte von EU-Bürgern negativ beeinflussen können und daher vor dem Inverkehrbringen und während ihres gesamten Lebenszyklus bewertet werden müssen. KI-Systeme können auf zwei Wegen als hochriskant eingestuft werden: durch Einbeziehung in die spezifischen Anwendungen in Anhang III oder durch Bezugnahme auf die in Anhang I genannten Sicherheitsprodukte. Akteure in Sektoren, die in Anlage I genannt sind, müssen feststellen, ob eine durch das Gesetz geregelte KI in ein Produkt integriert ist, also ein Sicherheitsbauteil darstellt, und einer Konformitätsbewertung durch Dritte unterliegt. Die Regeln für Hochrisiko-KI-Systeme nach Anhang I gelten 36 Monate nach Inkrafttreten.

Ebenfalls reguliert werden KI-Modelle mit allgemeinem Verwendungszweck. Definiert werden sie als umfassendes selbstüberwachtes, vielseitiges KI-Modell, das unabhängig vom Einsatzbereich viele Aufgaben kompetent bewältigen und in verschiedene Systeme oder Anwendungen integriert werden kann. Für solche KI-Modelle fallen unter anderem technische Dokumentationspflichten und Offenlegung der Inhalte, die für das Training des KI-Modells verwendet wurden, an. Ausgenommen sind KI-Modelle für Forschungs- und Entwicklungsprototypen. Der Gesetzgeber stuft darüber hinaus zusätzlich jene KI-Modelle mit allgemeinem Verwendungszweck strenger ein, die ein systemisches Risiko bergen. Das sind solche mit leistungsstarken Fähigkeiten, die durch technische Instrumente bewertet werden, oder wenn es vom Gesetzgeber aufgrund bestimmter Kriterien so entschieden wird. Modelle mit Trainingsberechnungen über 10^25 Gleitkommaoperationen gelten ebenfalls als risikoreich. Zu den bestehenden Anforderungen additiv hinzukommende Pflichten für solche KI-Modelle sind im Wesentlichen eine zweiwöchige Meldefrist gegenüber der Kommission, Durchführung von Modellbewertungen und Angriffstests, Bewertung und Minimierung systemischer Risiken auf Unionsebene, Meldung schwerwiegende Vorfälle sowie robuste Cybersicherheitsmaßnahmen.

Um Innovation zu fördern und gleichzeitig die Einhaltung der Vorgaben sicherzustellen, fördert das KI-Gesetz die Nutzung von regulatorischen KI-Reallaboren – kontrollierten Umgebungen, in denen KI-Systeme vor der Markteinführung getestet und validiert werden können.

Status quo: die KI-Verordnung

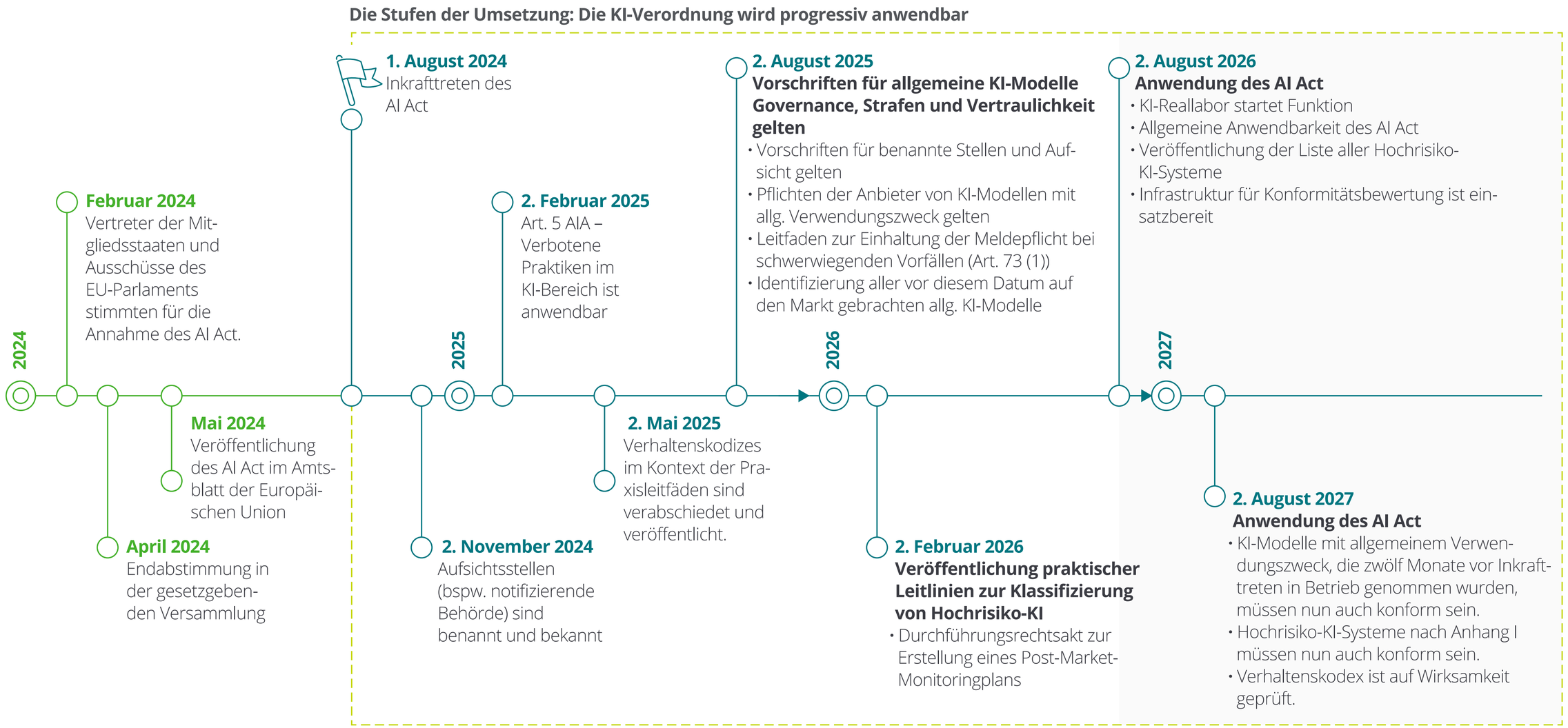


Abbildung 2 *Zeitleiste für das Inkrafttreten und die progressive Anwendbarkeit der KI-Verordnung*

Status quo: die KI-Verordnung

Der AI Act tritt zum 1. August 2024 in Kraft und wird progressiv anwendbar. Während der Transitionsphase haben Unternehmen Zeit, sich auf die Einhaltung vorzubereiten, um einen reibungslosen Übergang zu gewährleisten. Diese Gesetzgebung stellt einen bedeutenden Schritt zur Regulierung von KI innerhalb der EU dar und zielt darauf ab, Innovation mit Sicherheits- und Ethikstandards in Einklang zu bringen. Unternehmen müssen sich an diese Vorschriften anpassen, um die Einhaltung sicherzustellen und die Entwicklung vertrauenswürdiger KI zu fördern.

Bis 2035 wird voraussichtlich jede dritte Fahrt in deutschen Städten durch ein autonomes Fahrzeug erfolgen. Das Umsatzvolumen autonomer Fahrdienste wird dabei schätzungsweise €16,7 Mrd. erreichen.[2,3]

[2] Deloitte. (2019). Datenland Deutschland. Urbane Mobilität und autonomes Fahren im Jahr 2035: Welche Veränderungen durch Robotaxis auf Automobilhersteller, Städte und Politik zurollen. Abgerufen am 29.08.2024

[3] Statista. (2023). Künstliche Intelligenz - Statista Dossier. Abgerufen am 29.08.2024

2 **Sektorale Sicht:** die KI-Verordnung und Auswirkungen auf die Automobilbranche

KI-Technologie ist in unserem Alltag längst angekommen. Ob Sprachassistenten, Bild- und Gesichtserkennung, smarte IoT-Geräte oder personalisierte Empfehlungssysteme – die Liste der beispielhaften KI-Anwendungen ist lang. Spätestens seit dem Aufschwung generativer KI-Technologie (GenAI) zur Erzeugung neuer Inhalte, bspw. via Chatbots, hat das Thema KI zudem eine breite öffentliche Aufmerksamkeit erfahren.

In der Automobilbranche werden KI-basierte Systeme seit geraumer Zeit in verschiedenen gesicherten und getesteten Bereichen entlang der gesamten Wertschöpfungskette eingesetzt: von der Rohstoffverarbeitung über das fertige Fahrzeug bis hin zum After-Sales-Bereich. Diese KI-Systeme sind häufig in bestehende Software integriert und dienen der Unterstützung oder Optimierung vorhandener Systeme. Mit Blick auf die rasante Entwicklung der vergangenen Jahre kommt dem Einsatz von KI für beispielsweise autonomes Fahren, Konnektivität, intelligente Produktion, innovative Forschung und Entwicklung, Design oder Infotainment in verschiedenen Aspekten der Mobilität von heute und morgen eine immer bedeutendere Rolle zu. Stets mit dem Ziel, das Produkt Fahrzeug effizienter, nutzerfreundlicher und sicherer für die Insassen zu machen und andererseits auch Produktionsabläufe zu optimieren. In Zukunft ist zu erwarten, dass weitere Anwendungsgebiete hinzukommen werden, da KI eine zentrale Rolle in der fortschreitenden Automatisierung und der Entwicklung der Industrie 4.0 spielt.

Der steile Anstieg des Leistungsvermögens von KI und die damit verbundenen vielfältigen Anwendungsgebiete eröffnen enorme Chancen für die Automobilbranche. Allerdings bringt dieser Boom auch wichtige und berechtigte Fragestellungen mit sich. Ungeklärte regulatorische Gesichtspunkte wie der Umgang mit Gefahrensituationen sind besonders relevant für die Fahrzeug- und Zulieferindustrie im Kontext autonom fahrender Fahrzeuge oder fortschreitender Produktionstechnologien. Der dringende Bedarf nach einem verbindlichen gesetzlichen Rahmen ist gerechtfertigt – und dem kommt der europäische Gesetzgeber mit der KI-Verordnung dahingehend jetzt nach.

Mit Blick auf die eingangs beschrieben Risikoklassen der KI-Verordnung und den Schwerpunkt auf Hochrisiko-KI-Systeme lassen sich in der Automobilbranche angeregte Diskussionen feststellen. So lösen zum Beispiel insbesondere die Begriffsbestimmung eines „Sicherheitsbauteils“ gemäß Art. 3 (14) sowie die „Einstufungsvorschriften für Hochrisiko-KI-Systeme“ gemäß Art. 6 der KI-Verordnung gesteigerten Diskussionsbedarf aus. Als Sicherheitsbauteil wird ein Bestandteil eines Produkts oder KI-Systems beschrieben, welches eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder wenn dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet. Demnach wäre vorstellbar, dass eine Vielzahl von KI-Systemen im Fahrzeug grundsätzlich als hochriskant eingestuft werden könnten. Denn wird beispielsweise ein KI-System als Sicherheitsbauteil im Rahmen eines bereits heute zulassungsrelevanten Fahrzeugbauteils eingesetzt (übereinstimmend mit den EU-Harmonisierungsrechtsvorschriften im Anhang I), gilt dieses automatisch als Hochrisiko-KI-System und müsste strenge rechtliche Auflagen erfüllen. Diese noch breitflächige Definition in der KI-Verordnung könnte zu Handlungsunsicherheiten und Innovationshindernissen in der Automobilbranche führen. Inwiefern der beschriebene Fall über einen delegierten Rechtsakt und sektoral gerichtete Ausführungen zur bestehenden EU-Typgenehmigung für Kfz-Zulassung (Verordnung 2018/858 über die Genehmigung von Fahrzeugtypen) künftig näher spezifiziert und eingegrenzt wird, bleibt es intensiv zu beobachten.

Zwei exemplarische und simplifizierte KI-bezogene Anwendungsfälle sollen aufzeigen, welche regulierende Auswirkung der KI-Verordnung auf den KI-Einsatz im Automobilumfeld zu erwarten ist.

Beispiel 1: autonomes Fahren und Fahrassistenzsysteme.

Die fünf Stufen des autonomen Fahrens bezeichnen die Fortbewegung bzw. Steuerung eines Fahrzeugs mit immer geringerem Mitwirken des Fahrers bis hin zum Fahren ohne jegliches Eingreifen auf Stufe 5. Dabei arbeitet nicht ein System für sich allein. Das Fahrzeug greift auf verschiedene Informationen zurück, um so das aktuelle Fahrverhalten entsprechend zu adaptieren. Mögliche Fahrassistenz- und Fahrsicherheitssysteme sind dabei Spurhalte-, Abstandshalte- oder Notbremsassistent. Diese Informationen werden mit weiteren angereichert, die über die Umgebung generiert werden können. So erhält die Fahrzeugsteuerung einen 360°-Blickwinkel, analysiert das Fahrverhalten benachbarter bzw. beteiligter Verkehrsteilnehmer, leitet daraus ein ideales Fahrverhalten ab und steuert das Fahrzeug entsprechend. Erst durch den Einsatz von KI-Technologie können diese Funktionen ihr Potenzial vollumfänglich entfalten. So werden beispielsweise bei Kamerasensoren klassische Bildverarbeitungsalgorithmen mit KI-Methoden verknüpft.

Entlang der zuvor erwähnten Harmonisierungsvorschriften könnten Fahrassistenzsysteme, sofern sie analog Art. 3 (14) der KI-Verordnung als Sicherheitsbauteil definiert werden, automatisch in den Anwendungsbereich von Hochrisiko-KI-Systemen fallen. Als ein Beispiel kann der Abstandshalteassistent angeführt werden. Da dessen Ausfall oder eine schwerwiegende Fehlfunktion gesundheitliche Konsequenzen zur Folge haben kann, ist aktuell davon auszugehen, dass dieses KI-gestützte System als Hochrisiko-KI-System eingestuft werden könnte. Infolgedessen müssen sämtliche Fahrassistenzsysteme, die für das autonome Fahren verwendet werden und damit bei Ausfall oder Störung eine ähnlich geartete Implikation verursachen, ebenso als Hochrisiko-KI-System eingestuft werden.

Zur Erfüllung der regulatorischen Auflagen für diese als hochriskant eingestuften KI-Systeme wäre mit einem erheblichen Verwaltungsaufwand zu rechnen.

Beispiel 2: Spracherkennung und intelligente Infotainmentsysteme.

Einen weiteren bedeutenden Anwendungsberiech von KI stellen Sprachassistenten und intelligente Infotainmentsysteme dar. Diese ermöglichen eine nahtlose Interaktion zwischen Fahrer und Fahrzeug, verbessern die Benutzererfahrung und erhöhen die Sicherheit im Straßenverkehr. Sprachassistenten im Auto nutzen fortschrittliche Spracherkennung und natürliche Sprachverarbeitung, um Befehle und Anfragen des Fahrers zu verstehen und auszuführen. Dies reduziert die Ablenkung, da Fahrer ihre Hände am Lenkrad und ihre Augen auf der Straße lassen können, während sie verschiedene Funktionen des Fahrzeugs steuern. Durch die Integration von KI können diese Systeme zudem aus den Vorlieben und Gewohnheiten der Nutzer lernen und personalisierte Empfehlungen geben, beispielsweise für Routenplanung, Musik oder Nachrichten. Intelligente Infotainmentsysteme wiederum gehen über einfache Sprachbefehle hinaus und bieten eine Vielzahl von Diensten, die durch KI unterstützt werden. Dazu gehören Echtzeit-Verkehrsinformationen, Wettervorhersagen, Integration von Drittanbieter-Apps und sogar vorausschauende Wartungsinformationen. Diese Systeme sammeln und analysieren kontinuierlich Daten, um den Fahrkomfort zu erhöhen und die Effizienz des Fahrzeugs zu verbessern.

Wir nehmen für dieses Fallbeispiel an, dass der Fahrzeugfahrer mit dem KI-gestützten Sprachassistenten im Auto interagiert und Letzterer aufgrund einer Fehlfunktion irreführende Aussagen gegenüber dem Fahrer macht. Dadurch entsteht eine Ablenkung in der Verkehrsführung des Fahrzeugs, was zu einem Unfall im Straßenverkehr mit gesundheitlichen Folgen führt. In diesem Fall wäre die Fehlfunktion des Sprachsystems nur indirekt für den Unfall verantwortlich, da die Reaktion des Fahrers ein wesentlicher Teil der Kausalkette bleibt.

In diesem Beispiel könnte das Sprachsystem als nicht-sicherheitsrelevante Komponente berücksichtigt werden.

3 Systematische Grundlagen zur Bewältigung der KI-Verordnung schaffen:
KI-Governance und Integration in bestehende Programme

Die Einhaltung der KI-Verordnung ist keine Einmalangelegenheit, sondern ein kontinuierlicher Prozess. Darüber hinaus ist anzumerken, dass die KI-Verordnung nicht nur in Bezug auf das Fahrzeug selbst Anwendung findet, sondern grundsätzlich immer dann betrachtet werden muss, wenn der Schutz vor schädlichen Auswirkungen von KI-Systemen gegenüber Personen zu gewährleisten und ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und Grundrechte der EU sicherzustellen ist.

Das heißt, dass neben vorausschauenden Wartungsmaßnahmen (Predictive Maintenance) für das Fahrzeug im After-Sales beispielsweise auch die KI-gestützte Kundenanalyse und Kundenansprache unter die KI-Verordnung fallen. Als weiteres Beispiel ist das Personalwesen anzuführen, welches durch KI-gestützte Personalbeschaffung sowie Mitarbeiterbewertung und -führung die Vorgaben des KI-Verordnung zu berücksichtigen hat. Sofern KI-Systeme hier unterstützend zum Einsatz kommen und Personen beurteilen, gelten diese KI-Systeme als hochriskant. Auch das Finanzdienstleistungsgeschäft eines Automobilherstellers muss beim Einsatz von KI-Systemen, die zur Bewertung der Bonität oder Kreditwürdigkeit von Personen verwendet werden, die Vorgaben für ein Hochrisiko-KI-System erfüllen, da sie den Zugang zu Finanzmitteln für Personen bestimmen.

Daher ist ein systematisches Vorgehen erforderlich, um als Unternehmen die Umsetzungsanforderungen der KI-Verordnung nachhaltig bewältigen und auf etwaige Veränderungen angemessen reagieren zu können.

(Weiter-)Entwicklung der KI-Governance.
Bildet die notwendige Grundlage, um einen unternehmensweit geregelten Umgang mit KI zu ermöglichen. Dafür stellt die KI-Governance den strukturierten Rahmen auf, der dabei hilft, einen ganzheitlichen Überblick über KI im Unternehmen zu gewinnen und zu gewährleisten, dass KI-Systeme transparent und gesetzeskonform betrieben werden können. Die Kernbausteine umfassen unter anderem die Schaffung eines klaren Organisationsmodells inkl. Steuergremien zur Steuerung von KI-Technologie; die Definition von Rollen und Verantwortlichkeiten; die Entwicklung einschlägiger Richtlinien und Verfahrensanweisungen sowie harmonisierte Prozesse und Technologieabstimmung mit dem Ziel, den KI-Lebenszyklus zu regeln und zu standardisieren – vom Designvorhaben über Datenaufbereitung, Modellentwicklung und Produktionssetzung bis zur kontinuierlichen Überwachung. Die KI-Governance begünstig die gewinnbringende Nutzung von KI-Systemen im regulatorisch zulässigen Rahmen und ermöglicht die flexible Reaktion auf weitere regulatorische Entwicklungen im Umfeld der KI. Die einzelnen Geschäftsbereiche profitieren von zentralen Regelungen und werden befähigt, mit mehr Handlungssicherheit innovationsgetrieben KI für ihre individuellen Geschäftsanforderungen zu entwickeln und einzusetzen.

Verzahnung mit der Daten-Governance.

Data Governance ist die strategische Handhabung und Kontrolle von Datenressourcen in einer Organisation, um auf Basis von belastbaren Daten den Geschäftsnutzen risikogesteuert zu maximieren. Im Kontext der KI-Governance spielt die Daten-Governance eine wesentliche Rolle. Sie stellt sicher, dass die Datenversorgung für die Entwicklung und den Betrieb von KI-Modellen und KI-Systemen den Vorgaben der KI-Verordnung entsprechen kann. Besonders hervorzuheben sind hierbei die regulatorischen Anforderungen an „Daten und Daten-Governance“ für Hochrisiko-KI-Systeme gemäß Art. 10 KI-Verordnung. Demnach sind KI-Systeme mit qualitativ hochwertigen, repräsentativen und fehlerfreien Daten zu entwickeln. Bestimmte Daten-Governance-Verfahren sind hierbei festgelegt, einschließlich der Datenerhebung, -aufbereitung, -bewertung und -überwachung, um eine mögliche Voreingenommenheit (Bias) beim KI-Einsatz zu identifizieren und korrigierend einzugreifen.

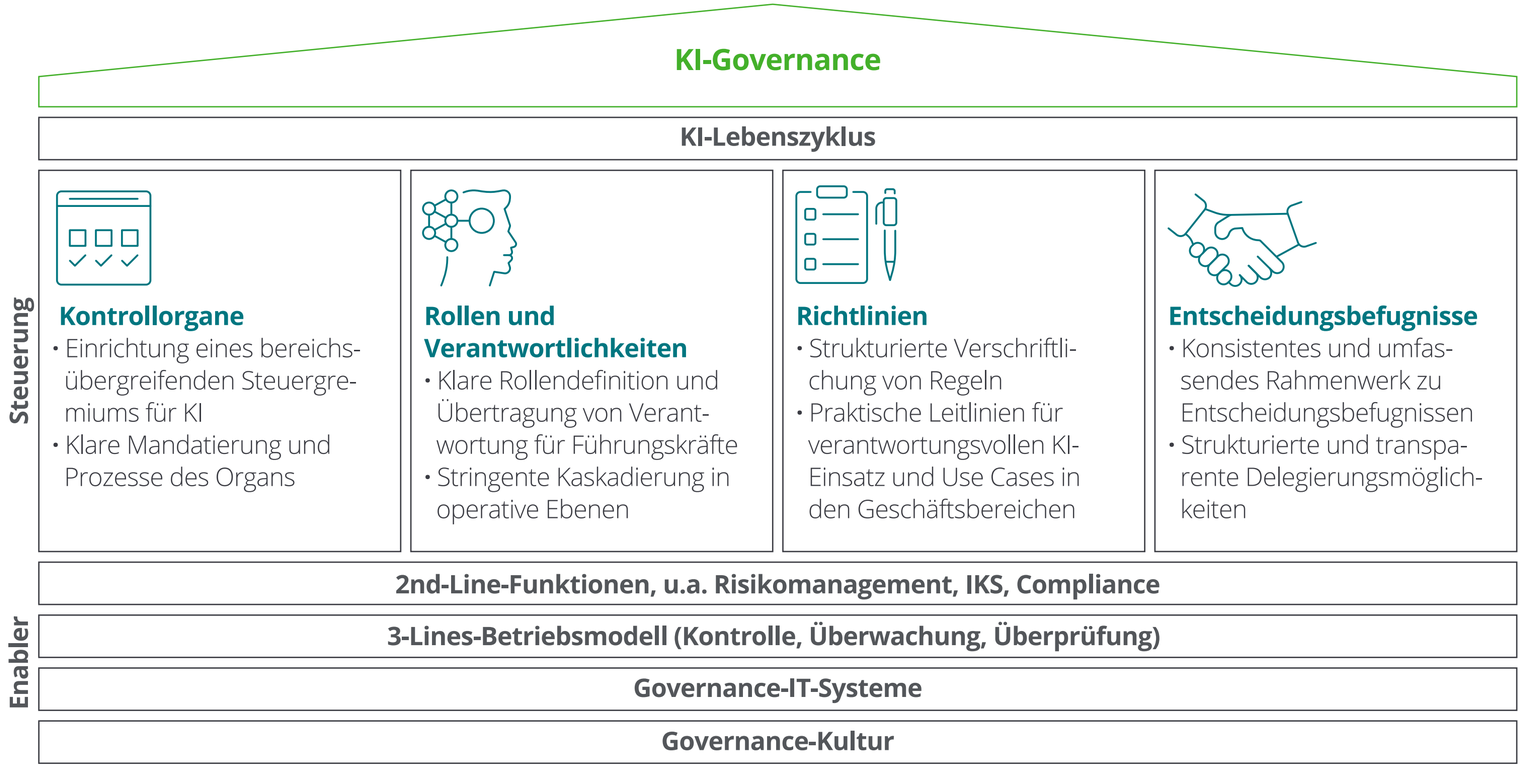


Abbildung 3 *Strukturen einer KI-Governance*

Datenbezogene Compliance-Pflichten für KI-Modelle mit allgemeinem Verwendungszweck inkl. jene mit systemischem Risiko können ebenfalls mithilfe der Daten-Governance geregelter abgeliefert werden. So ist zum Beispiel eine hinreichend detaillierte Zusammenfassung der für das Training des KI-Modells verwendete Daten zu erstellen und offenzulegen, wenn proprietäre Software eingesetzt wird. Für KI-Modelle mit systemischem Risiko sind zudem noch Modellbewertungen, ein dediziertes Risikomanagement sowie Cybersicherheitsmaßnahmen für die Modelle und die Infrastruktur zu leisten. Weitere interdisziplinäre Facetten der Daten-Governance verhelfen unter anderem auch dabei, den Datenschutz auszurichten, wenn es um die Bereitstellung von personenbezogenen Daten für KI-Modelle und KI-Systeme geht.

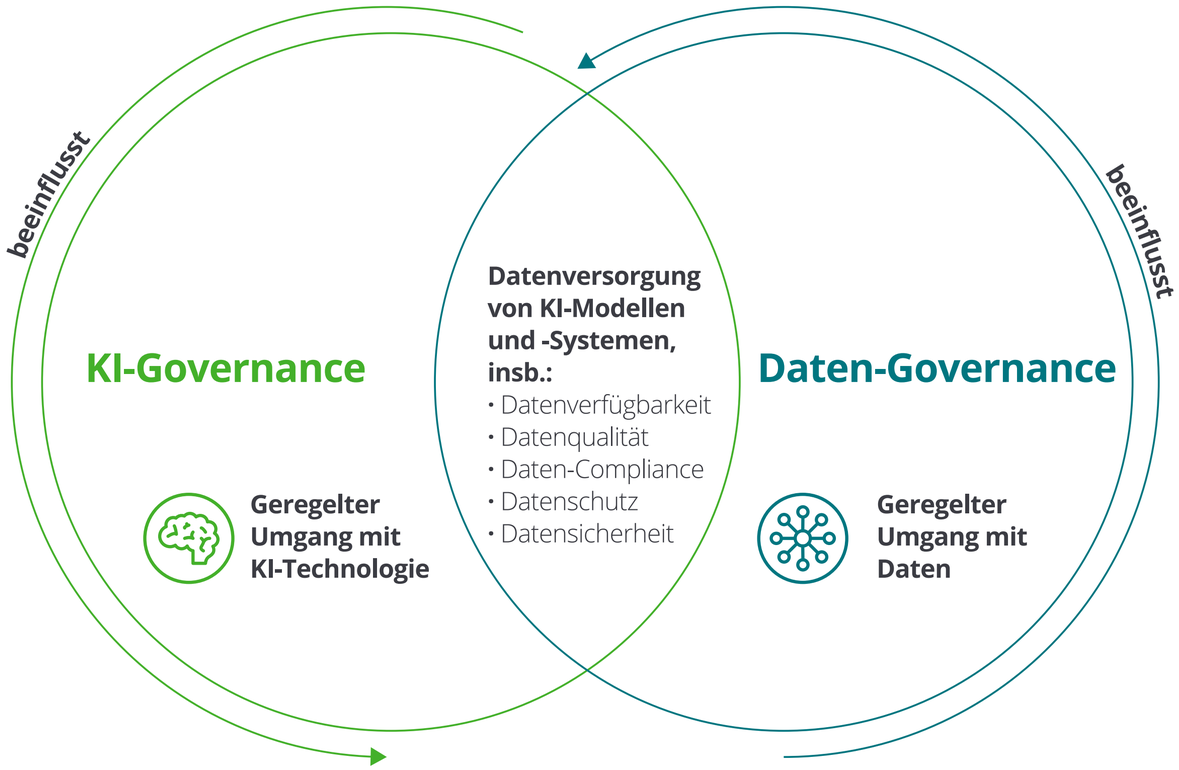


Abbildung 4 *Wechselwirkung zwischen KI-Governance und Daten-Governance*

Integration von KI in die Governance-, Risiko- und Compliance-Managementsysteme (GRC).

Die Integration der KI-Praktiken in den unternehmensweiten GRC-Rahmen spielt eine entscheidende Rolle, wenn es darum geht, die regulatorischen Anforderungen der KI-Verordnung flächendeckend, konsistent und effektiv zu erfüllen. Zudem können durch einen zentralisierten Überblick über die GRC-Funktionen Ressourcen effizienter genutzt werden.

Governance.

Setzt die internen Rahmenbedingungen für unter anderem Risikomanagement, internes Kontrollsystem (IKS) und Compliance fest. Durch die Integration der KI-Governance werden Richtlinien und Kontrollziele weiterentwickelt, die den gesamten KI-Lebenszyklus abdecken. Des Weiteren sind etablierte Standards und übergreifende Prozesse um KI-relevante Aspekte zu ergänzen und zu harmonisieren mit dem Ziel, künftig auch gezielt KI-Risiken abzudecken und Compliance-Verstöße gegen die KI-Verordnung zu vermeiden. Auch durch die KI-Governance ins Leben gerufene Rollen und Verantwortlichkeiten müssen in die erweiterten GRC-Strukturen hineinharmonisiert und verankert werden. Dazu ist eine enge Zusammenarbeit zwischen den Key-Stakeholdern der GRC-Funktionen und der KI-Governance notwendig, um eine kohärente und ganzheitliche Herangehensweise im Umgang mit KI zu gewährleisten.

Risikomanagement.
Befähigt die Organisation zur systematischen Identifikation, Analyse und Bewertung von Risiken. Durch gezielte Risikobewältigungsmaßnahmen und systematische Kontrolltätigkeiten können Schadenspotenziale gemindert werden. Angemessenheit und Wirksamkeit der Maßnahmen werden überwacht.

Bei der Integration von KI-Aspekten in das Risikomanagement ist zu beachten, dass es verschiedene Risikokategorien für KI zu steuern gilt. Hier steht zunächst hauptsächlich die Bewältigung von Compliance-Risiken für KI im Mittelpunkt, um die Konformität mit der KI-Verordnung im Grundsatz zu gewährleisten. Im erweiterten verbundenen Wirkungskreis zählen dazu auch Risiken von Datenschutzverstößen durch unzulässige Verarbeitung personenbezogener Daten und Urheberrechtsverletzungen bei der Verwendung geschützter Daten. Ebenso risikorelevant sind unzuverlässige KI-Ergebnisse durch Halluzinationen und Voreingenommenheit (Bias), die zu falschen Schlussfolgerungen und Diskriminierung führen können. Ein weiterer Risikofaktor ist die unzureichende Datenqualität, die die Genauigkeit, Vollständigkeit und Aktualität der für KI-Modelle verwendeten Daten beeinträchtigt. Ebenso das Risiko von Sicherheitslücken, die Angriffsfläche für die gezielte Vergiftung (Poisoning) oder den Diebstahl von Daten und Modellen bieten, was unter anderem Betriebsunterbrechungen verursachen kann und die Integrität und Vertraulichkeit sensibler Informationen gefährdet.

Die Integration von KI in das unternehmensweite Risikomanagement und das interne Kontrollsystem erfordert eine sorgfältige Planung und Umsetzung. Ein erster Schritt dazu ist die Beurteilung, in welchem Umfang das aktuelle Risiko- und Kontrollrahmenwerk die Nutzung von KI-Technologie berücksichtigt und an welcher Stelle noch konzeptionelle Erweiterungen notwendig sind. Die einzelnen KI-Risikokategorien stehen in Wechselwirkung zueinander und müssen übergreifend gesteuert werden, um die Risikotragfähigkeit angemessen zu bewerten und eine widerspruchsfreie Aussage zur Risikosituation bezüglich KI im Unternehmen treffen zu können.

Compliance.
Unterstützt die Einhaltung von externen, gesetzlichen Vorschriften sowie internen Vorgaben. In der Regel können Unternehmen durch die Etablierung eines standardisierten Compliance-Managementsystems (CMS) ein strukturiertes Rahmenwerk zum nachhaltigen und verantwortungsvollen Handeln vorweisen. Auch wenn die KI-Verordnung als neue Regulierung anwendbar wird, deckt ein CMS üblicherweise bereits eine Vielzahl von Einzelthemen heute schon erfolgreich ab.

Durch die Erfahrung mit der grundsätzlichen Bewältigung von externen Vorgaben und durch die Hilfe von systematischen Mechanismen zur Überwachung und Sicherstellung der Regelkonformität ist der Compliance-Bereich mit Grundlagen ausgestattet, die bei der Analyse und unternehmensindividuellen Ableitung der Anforderungen der KI-Verordnung, bei erforderlichen Anpassungen oder Erweiterungen des CMS und der Bestimmung von Kontrollhandlungen aus Compliance-Sicht helfen. Auch die vorausschauende Überwachung von künftigen Entwicklungen bezüglich der KI-Verordnung findet hier statt. Über das CMS sind typischerweise bereits Anbindungen an andere Unternehmensfunktionen hergestellt. Diese lassen sich nutzen, um die KI-Verordnung als neues Einzelthema effizient in die Geschäftsbereiche einzuspeisen und bei der Compliance vorschriftskonform zu beraten.

Im Lichte der rasanten technologischen Fortschritte durch KI kommt dem Themenkomplex Schulungs- und Sensibilisierungsmaßnahmen eine wichtige Bedeutung zu. Die Durchführung von Compliance-Schulungen vermittelt der Mitarbeiterschaft des Unternehmens Kenntnisse und Fähigkeiten, die sich an den Vorgaben der KI-Verordnung praktisch orientieren und dabei unterstützen, diese einzuhalten.

Wir empfehlen, den Einsatz von KI kohärent in den GRC-Rahmen einzubetten, um Vorteile und Synergiemöglichkeiten durch die integrierte Betrachtung der einzelnen GRC-Komponenten bestmöglich zu nutzen. Die systemische Integration steigert die Erfolgsaussichten, die Compliance mit der KI-Verordnung nicht nur effektiv, sondern vor allem langfristig und effizient zu erreichen.

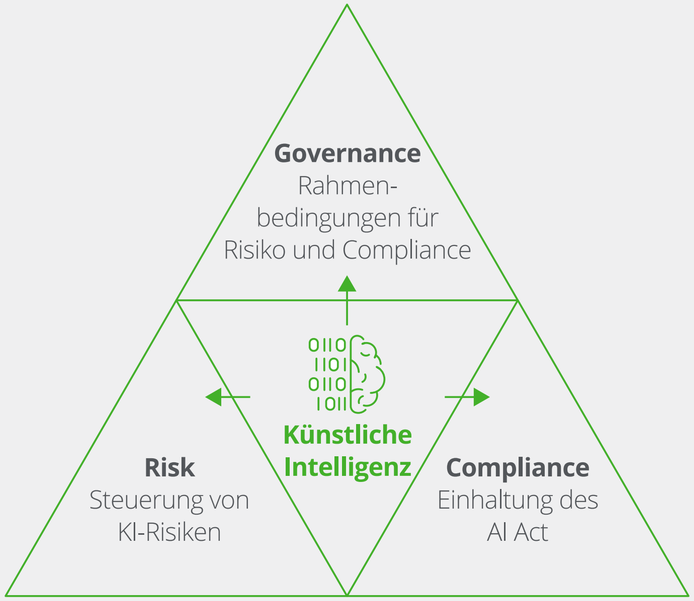


Abbildung 5 *Integration von KI in den unternehmensweiten GRC-Rahmen*

4 Fazit und Ausblick

Die KI-Verordnung stellt einen einheitlichen und verbindlichen Regulierungsrahmen für KI im europäischen Raum dar. Angesichts der zunehmenden Relevanz von KI-Anwendungen soll sie sowohl den Schutz fundamentaler Rechte und Sicherheitsbelange der Europäer gewährleisten als auch die Förderung von Innovation und Wettbewerbsfähigkeit für Unternehmen unterstützen.

Die Kernanforderungen der KI-Verordnung für Hochrisiko-KI-Systeme umfassen deren systematisches Risikomanagement – gebündelt unter einem ganzheitlichen KI-Governance-Rahmenwerk. Für die Automobilbranche wird die KI-Verordnung die zukünftige Mobilität maßgeblich mitgestalten, da diese Technologie entlang der gesamten automobilen Wertschöpfungskette vom Rohstoff über das fertige Fahrzeug bis hin zum After-Sales-Bereich eingesetzt wird.

Besonders einschlägig sind die Definition eines KI-Systems als Sicherheitsbauteil sowie die anwendungsfallbezogene Klassifizierung von Hochrisiko-KI-Systemen, die dazu führen könnte, dass eine Vielzahl von Lösungen, die bereits heute innerhalb des Fahrzeugs und um dieses herum eingesetzt werden, als hochriskant eingestuft werden. Das bedeutet nicht, dass der Betrieb solcher KI-Systeme grundsätzlich untersagt ist, jedoch werden mit der Konformitätsbewertung teilweise umfangreiche Compliance-Auflagen anfallen, die vor Inbetriebnahme zu erfüllen sind. Dazu kommen noch jene KI-Praktiken, die mit einem unannehmbaren Risiko als verboten gelten und grundsätzlich nicht betrieben werden dürfen, sowie KI-Systeme mit begrenztem Risiko, welche Transparenzpflichten gegenüber Personen erfüllen müssen.

Im Hinblick auf die empfindlichen finanziellen Sanktionen sowie Reputationsverluste bei Compliance-Verstößen sollten Unternehmen der Einhaltung der KI-Verordnung eine entsprechend hohe Priorität zuweisen.

Mit dem Inkrafttreten der KI-Verordnung zum 1. August 2024 werden die Umsetzungsanforderungen progressiv über verschiedene Zeiträume von sechs bis 36 Monaten anwendbar. Stellen Sie Ihre KI-Governance, Data Governance und GRC-Funktionen auf den Prüfstand, um angemessene Maßnahmen zur Compliance-Einhaltung zu treffen.

Deloitte unterstützt Sie, die Komplexität der Umsetzungsanforderungen der KI-Verordnung erfolgreich zu bewältigen, Wettbewerbsvorteile abzusichern sowie Ihre Innovationsführerschaft in einer sich schnell entwickelnden KI-Landschaft weiter voranzutreiben. Kommen Sie bei Fragen gerne jederzeit auf uns zu.

Ansprechpartner



Andreas Herzig
Partner | Global Head of
Automotive Risk Advisory
Tel: +49 711 16554 7160
aherzig@deloitte.de



Atrak Yadegari
Director | Data & AI Governance
Tel: +49 151 18293044
ayadegari@deloitte.de



Mosche Orth
Manager | EU Policy Center Brüssel
Tel: +49 511 3023 4167
moorth@deloitte.de

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 457.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 10/2024