soluzione FAQ zur KI-Verordnung in Zusammenarbeit mit reuschlaw

Die **EU-KI-Verordnung (AI Act)** stellt Unternehmen vor neue Herausforderungen. Viele Unternehmen fühlen sich angesichts der komplexen Anforderungen unsicher. Mit diesem Whitepaper erhalten Sie ein rechtlich geprüftes FAQ, das alle wichtigen Fragen rund um die KI-Verordnung kompakt beantwortet – von der Risikoklassifizierung über Compliance-Pflichten bis hin zu konkreten Handlungsempfehlungen.

Ein zentraler Bestandteil der Verordnung ist Artikel 4, der einen nachweisbaren Kompetenzaufbau für Mitarbeitende verlangt. Genau hier setzt der **soluzione KI-Führerschein®** an: Er unterstützt Sie dabei, Ihre Teams effizient zu schulen und auf dem aktuellsten Stand zu halten.

Übersicht

Was ist die KI-Verordnung (KI-VO)? 2
Was ist ein KI-System im Sinne der KI-VO? 3
Welche KI-Systeme sind von der KI-VO reguliert und wie erkenne ich, welche Risikoklasse vorliegt? 4
Wer ist Adressat der KI-VO? 6
Welche Pflichten gelten? 8
Wann finden welche Regelungen Anwendung? 9
Welche Risiken bestehen bei Non-Compliance? 10
Was haben Unternehmen beim Einsatz von KI-Tools wie ChatGPT oder Copilot zu beachten? 11
Welche Abteilungen im Unternehmen sollten sich wie mit der KI-VO befassen? 13
Wie müssen Mitarbeitende geschult werden, um die Anforderungen aus der KI-VO zu erfüllen? 14
Wie kann ein Unternehmen langfristig die KI-Compliance sicherstellen? 15
Kontakt und Quellen 17

SOLUZIONE | reusch law

Was ist die KI-Verordnung (KI-VO)?

Die **KI-Verordnung** (kurz: KI-VO, im Englischen: AI Act oder kurz AIA) ist eine produktbezogene Verordnung, die strenge Anforderungen für die Entwicklung und Nutzung von Künstlicher Intelligenz (KI) festlegt. Mit der KI-VO soll in der EU erstmals ein Rechtsrahmen für den sicheren und transparenten Einsatz von KI geschaffen werden. Die KI-VO ist spezifisches Produktsicherheitsrecht. Je nach Schwere des Risikos, welches ein KI-System für die Grundwerte der EU darstellt, gelten unterschiedlich strenge Pflichten. Adressaten sind Anbieter, Produkthersteller, Betreiber, Bevollmächtigte, Einführer oder Händler, für die wiederum abgestufte Pflichten gelten. Die KI-VO ist seit dem 1. August 2024 in Kraft und die neuen Anforderungen finden schrittweise bis zum 2. August 2027 Anwendung. Bei Verstößen drohen Behördenmaßnahmen und hohe Bußgelder. Neben der KI-VO können weitere Rechtsakte Anwendung finden, wie z.B. die Datenschutz-Grundverordnung, der Cyber Resilience Act, das Urheberrecht und das Verbraucherrecht. Unternehmen sollten sich daher bereits jetzt auf die neuen Anforderungen einstellen und frühzeitig mit der Überprüfung ihrer Systeme und Prozesse beginnen.

Was ist ein KI-System im Sinne der KI-VO?

Primärer Regelungsgegenstand der KI-VO sind KI-Systeme. Nach Art. 3 Nr. 1 KI-VO ist ein KI-System ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den Eingaben Ausgaben ableitet, welche die physischen oder virtuellen Umgebungen beeinflussen können. Die KI-VO verfolgt damit ein weites Begriffsverständnis. In der Praxis besteht die Herausforderung zu bestimmen, ob ein System als KI-System i.S.d. KI-VO einzustufen ist. Dies ist im Zweifelsfall zu bejahen. Als Hilfestellung hat die EU-Kommission **Leitlinien zur Definition von KI-Systemen** veröffentlicht, die Unternehmen in der Praxis heranziehen sollten.

Zudem bestehen einige wenige Ausnahmen vom Anwendungsbereich der KI-VO, insbesondere:

1. Forschungs-, Test- und Entwicklungstätigkeiten: Die KI-VO gilt nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. Für KI-Reallabore gilt diese Ausnahme jedoch nicht.
2. Freie und quelloffene KI: Die KI-VO gilt nicht für KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden. Liegt jedoch ein Hochrisiko-KI-System (Art. 6) oder als ein KI-System, das eine verbotene KI-Praktik (Art. 5) oder ein KI-System mit begrenztem Risiko darstellt (Art. 50), vor, gilt die Ausnahme nicht.

Welche KI-Systeme sind von der KI-VO reguliert und wie erkenne ich, welche Risikoklasse vorliegt?

Die KI-VO verfolgt einen risikobasierten Ansatz und unterscheidet zwischen verbotener KI, Hochrisiko-KI, KI mit beschränktem Risiko und KI mit minimalem bis keinem Risiko. Daneben werden zudem sog. KI-Modelle mit allgemeinem Verwendungszweck (sog. General Purpose AI (GPAI)) reguliert. Entscheidend ist, ob und wenn ja, mit welcher Intensität, ein Risiko für die Grundwerte der EU (wie z.B. Freiheit, Demokratie, Sicherheit, Grundrechte) vorliegt. Je nach Einstufung des KI-Systems oder -Modells gelten unterschiedlich strenge Pflichten.

1. Verbotene KI

Verboten sind gemäß Art. 5 KI-VO KI-Systeme, die ein unannehmbares Risiko bergen. Betroffen sind KI-Systeme, von denen erhebliche Gefahren für die Grundrechte, die Sicherheit und das gesellschaftliche Zusammenleben ausgehen. Dazu zählen beispielsweise manipulative KI-Systeme, Social-Scoring-Systeme, Scraping-Systeme oder biometrische Kategorisierungssysteme. Als Hilfestellung hat die EU-Kommission **Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz** veröffentlicht.

2. Hochrisiko-KI-Systeme

Schwerpunkt der KI-VO ist die Regulierung von Hochrisiko-KI-Systemen. Diese bergen zwar kein unannehmbares Risiko, die Risiken sind jedoch so hoch, dass ihre Entwicklung, ihr Betrieb und ihre Nutzung besonders strengen Regeln unterliegen. Ob ein Hochrisiko-KI-System vorliegt, wird nach Art. 6 KI-VO auf zwei unterschiedliche Arten ermittelt:

a) Regulierte Produkte (Anhang I)

Gemäß Art. 6 KI-VO gilt ein KI-System als Hochrisiko-KI-System, wenn es als Sicherheitsbauteil in einem Produkt verwendet werden soll, das von einer in Anhang I der KI-VO aufgeführten Harmonisierungsrechtsvorschrift der EU erfasst ist, oder wenn das KI-System selbst ein solches Produkt darstellt. Zusätzlich muss das Produkt nach der Harmonisierungsvorschrift einer Konformitätsbewertung durch Dritte unterzogen werden.

Relevante Produkte, die von den Harmonisierungsvorschriften in Anhang I KI-VO erfasst werden, sind z.B.:

- Maschinen i.S.d. Richtlinie 2006/42/EG
- Funkanlagen i.S.d. Richtlinie 2014/53/EU
- Medizinprodukte i.S.d. Verordnung (EU) 2017/745
- In-vitro-Diagnostika i.S.d. Verordnung (EU) 2017/746

b) Hochrisiko-Kategorien nach Anhang III

Darüber hinaus kann ein Hochrisiko-KI-System vorliegen, wenn das KI-System in einen der in Anhang III KI-VO genannten Bereiche fällt. Dazu gehören insbesondere folgende Systeme:

- KI-Systeme zur biometrischen Identifizierung
- KI-Systeme, die als Sicherheitsbauteil in kritischer Infrastruktur verwendet werden
- KI-Systeme im Rahmen der allgemeinen und beruflichen Bildung
- KI-Systeme zur Personalverwaltung
- KI-Systeme zur Vergabe öffentlicher Leistungen, Strafverfolgung, Migration und Rechtspflege

c) KI-Systeme mit begrenztem Risiko

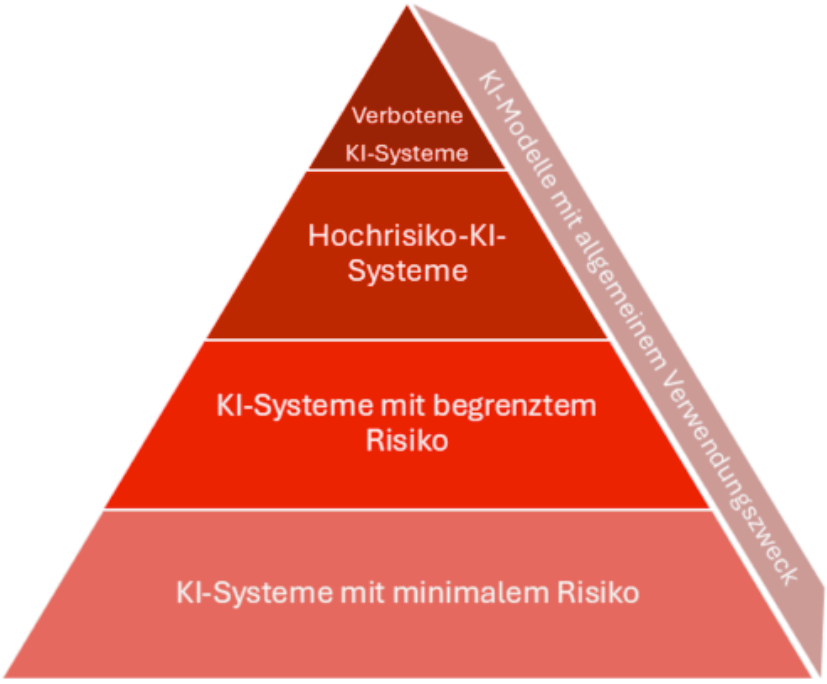
Spezielle Transparenzpflichten gelten gem. Art. 50 KI-VO für Anbieter von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind. Besonderes adressiert werden hierbei KI-Systeme, welche Text-, Bild-, Ton oder Videoinhalte erzeugen oder manipulieren. Die KI-Systeme, die den Pflichten aus Art. 50 KI-VO unterfallen, sind KI-Systeme mit begrenztem Risiko.

d) KI-Systeme mit minimalem oder keinem Risiko

KI-Systeme mit geringem oder keinem Risiko werden negativ abgegrenzt. Fallen KI-Systeme weder unter die verbotenen KI-Praktiken des Art. 5 KI-VO, den Hochrisiko-KI-Systemen aus Art. 6 KI-VO oder gelten als KI-Systeme mit begrenztem Risiko im Sinne des Art. 50 KI-VO, unterliegen sie nur den allgemeinen Pflichten des Art. 4 KI-VO.

Sonderfall: KI-Modelle mit allgemeinem Verwendungszweck (GPAI)

Als GPAI gelten KI-Modelle, welche eine erhebliche allgemeine Verwendbarkeit aufweisen und in der Lage sind, unabhängig von der Art und Weise ihres Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert zu werden. Für GPAI sieht die KI-VO besondere (Transparenz-)Pflichten vor. Darüber hinaus sind GPAI in die oben genannten Risikoklassen einzuordnen, sodass je nach Risikoklasse weitere Pflichten gelten.



Wer ist Adressat der KI-VO?

Die KI-VO regelt die Pflichten und Verantwortlichkeiten entlang der gesamten KI-Wertschöpfungskette. Je nach Adressateneigenschaft gelten unterschiedlich strenge Pflichten. Die KI-VO unterscheidet zwischen den folgenden Adressaten:

1. Anbieter

Die Anbieterpflichten bilden den Kern des Anforderungskatalogs der KI-VO. Als Anbieter gilt nach Art. 3 Nr. 3 KI-VO, wer das KI-System oder KI-Modell entwickelt oder entwickeln lässt und es unter dem eigenen Nehmen in Verkehr bringt oder in Betrieb nimmt. Aus den für Anbieter geltenden Verpflichtungen leiten sich abgestuft die Pflichten der weiteren Wirtschaftsakteure ab.

2. Betreiber

Als Betreiber gilt, wer ein KI-System in eigener Verantwortung verwendet. Die Pflichten, die die KI-VO den Betreibern eines KI-Systems auferlegt, sind im Vergleich zu denen der Anbieter reduziert.

3. Einführer

Als Einführer gelten in der Union ansässige natürliche oder juristische Personen, die ein KI-System, das den Namen einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringen. Sie treffen im Wesentlichen Kontrollpflichten in Bezug auf das importierte KI-System.

4. Händler

Als Händler gilt, wer ein KI-System auf dem Unionsmarkt bereitstellt. Ein KI-System gilt als bereitgestellt, wenn es im Rahmen einer Geschäftstätigkeit zum Vertrieb oder zur Verwendung auf dem Unionsmarkt abgegeben wird. Auch die Händler treffen im Wesentlichen Kontrollpflichten.

5. Quasi-Anbieter

Es besteht die Möglichkeit, einen bereits vorhandenen Anbieter in seiner Anbietereigenschaft abzulösen. Die Möglichkeiten eines solchen Adressatenwechsels sind konkret in Art. 25 KI-VO geregelt. Weiterentwicklungen durch Betreiber können eine wesentliche Änderung im Sinne des Art. 3 Nr. 23 KI-VO i.V.m. Art. 25 I lit. b KI-VO darstellen, wodurch der Wirtschaftsakteur selbst zum Anbieter wird.
In bestimmten Situationen können Akteure mehr als eine Rolle gleichzeitig einnehmen und müssen daher alle relevanten Pflichten kumulativ erfüllen. Ein mögliches Szenario ist beispielsweise, dass ein Konzernunternehmen eine KI von einem externen Anbieter erwirbt, diese KI aber einige Zeit später auch anderen Konzernunternehmen als eigene Lösung im eigenen Namen zur Verfügung stellt.
In räumlicher Hinsicht orientiert sich der Anwendungsbereich der KI-VO am sog. Marktortprinzip. Der Sitz oder die Niederlassung eines Unternehmens innerhalb der EU ist daher grundsätzlich keine Voraussetzung. Die KI-VO gilt für KI-Systeme, die auf dem EU-Markt bereitgestellt oder deren Output im EU-Binnenmarkt verwendet werden. Generative KI-Anwendungen, die zur Interaktion mit natürlichen Personen konzipiert wurden, unterfallen dem Anwendungsbereich der KI-VO, wenn sich die betroffenen Personen in der Union befinden.

Welche Pflichten gelten?

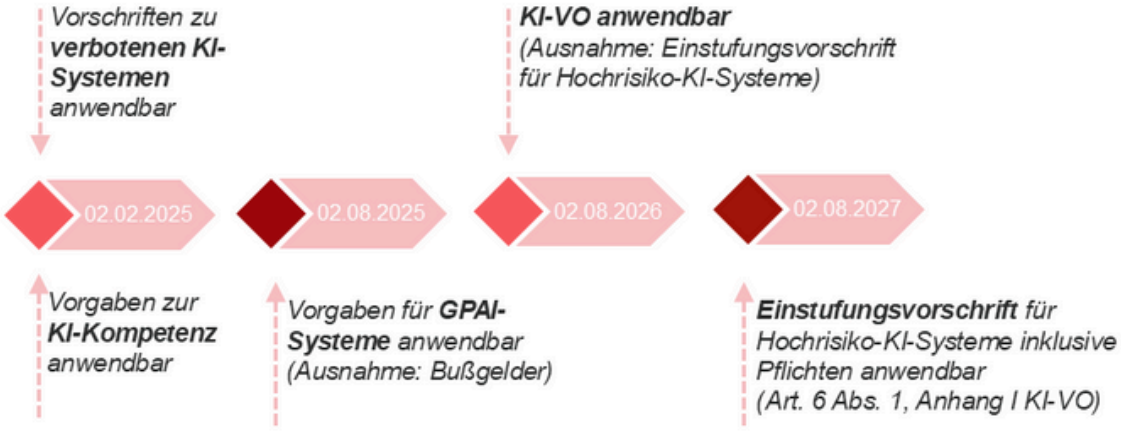
Die von den Wirtschaftsakteuren einzuhaltenden Pflichten richten sich nach der Risikoklassifizierung des KI-Systems und nach der Adressateneigenschaft. Grundsätzlich gilt: Je höher das Risiko, desto strenger sind die regulatorischen Anforderungen. Ergänzend sieht die KI-VO besondere Pflichten für GPAI vor. Diese gelten zusätzlich zu den Anforderungen der jeweiligen Risikoklasse.

Verbotene KI **Art. 5 KI-VO**	**Hochrisiko-KI** **Art. 6-49 KI-VO**	**KI-Systeme mit begrenztem Risiko** **Art. 50 KI-VO**	**Sonstige KI** **Art. 4, Art. 95 KI-VO**	**GPAI** **Art. 51-54 KI-VO**
= unannehmbares Risiko	= hohes Risiko	= konkrete Anwendungsfälle, z.B. direkte Interaktion mit natürlichen Personen	= geringes bis minimales Risiko	= weiter Einsatzbereich, allgemeine Zwecke
• Verbot der Herstellung, des Inverkehrbringens und der Nutzung der KI-Systeme	• KI-Kompetenz, Art. 4 KI-VO • Risikomanagement • Datenqualität und Datenverwaltung • Schulung • Technische Dokumentation und Protokollierung • Transparenz und Information • Menschliche Überwachung • Genauigkeit, Robustheit und Cybersicherheit • Konformitätsbewertung	• KI-Kompetenz, Art. 4 KI-VO • Kennzeichnungspflicht für KI-Systeme, welche zur menschlichen Interaktion bestimmt sind • Kennzeichnung von KI-generierten Texten über Angelegenheiten im öffentlichen Interesse • Kennzeichnung von synthetisch erzeugten Bild-, Audio-, Videoinhalten • Ausnahmen vorhanden (Geeignete Schutzmaßnahmen für die Rechte und Freiheiten Dritter)	• KI-Kompetenz, Art. 4 KI-VO • Freiwillige Verhaltenskodizes	• KI-Kompetenz, Art. 4 KI-VO • Technische Dokumentation • Informations- und Kooperationspflichten ggü. Downstream-Anbietern und der EU-Kommission • Strategie zur Einhaltung des Urheberrechts • Liste über urheberrechtlich geschützte Trainingsdaten • Zusätzliche Pflichten für GPAI mit systemischem Risiko → Nachweis über „codes of practice“
Anbieter, Betreiber, Einführer, Händler, Produkthersteller, Bevollmächtigte	Anbieter, Betreiber, Einführer, Händler, Produkthersteller, Bevollmächtigte	Anbieter, Betreiber	Anbieter, Betreiber	Anbieter, Bevollmächtigte

Wann finden welche Regelungen Anwendung?

Die KI-VO wurde am 12. Juli 2024 im Amtsblatt der EU veröffentlicht und trat am 1. August 2024 in Kraft.

Die neuen Pflichten finden schrittweise Anwendung:



Welche Risiken bestehen bei Non-Compliance?

Verstößt ein Unternehmen gegen die Vorschriften der KI-VO können unterschiedliche Folgen eintreten:

Behördenmaßnahmen

Die zuständigen Aufsichtsbehörden erhalten mit der KI-VO weitreichende Untersuchungs-, Abhilfe- und Sanktionsbefugnisse. Dazu gehören beispielsweise Verwarnungen, Anordnungen oder Verbote. Darüber hinaus können die zuständigen Behörden nach der **EU-Marktüberwachungsverordnung** Zugang zu Daten und Dokumentationen verlangen, KI-Systeme überprüfen und Korrekturmaßnahmen anordnen.

Sanktionen (Bußgelder)

Je nach Art des Verstoßes können unterschiedlich hohe Bußgelder verhängt werden:

- Bei Verstößen im Zusammenhang mit verbotener KI drohen Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.
- Verstöße im Bereich von Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck (GPAI) können mit bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes sanktioniert werden.
- Bei falschen oder irreführenden Angaben gegenüber Behörden sind Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes vorgesehen.
- Darüber hinaus ist es den EU-Mitgliedstaaten überlassen im Rahmen von nationalen Durchführungsgesetzen weitere Verstöße zu sanktionieren.

Zivilrechtliche Klagen & Reputationsschäden

Neben den behördlichen Maßnahmen können zudem Klagen von Betroffenen oder Wettbewerbern auf Schadensersatz sowie damit einhergehende Reputationsschäden drohen. Die KI-VO ist spezielles Produktsicherheitsrecht, sodass bei Produktfehlern u.a. auch die Vorschriften zur allgemeinen Produkthaftung Anwendung finden.

Was haben Unternehmen beim Einsatz von KI-Tools wie ChatGPT oder Copilot zu beachten?

Zunächst ist eine **Prüfung nach der KI-VO** durchzuführen. Mit dieser Prüfung sollte begutachtet werden, ob ein KI-System i.S.d. der KI-VO vorliegt, in welche Risikoklasse das KI-System im konkreten Nutzungsszenario fällt und in welcher Rolle das Unternehmen tätig wird. Je nach Ergebnis der KI-Prüfung gelten unterschiedlich strenge Pflichten.

Tools wie ChatGPT oder Microsoft Copilot sind – abhängig vom konkreten Einsatzszenario – in der Regel als KI-Systeme mit begrenztem Risiko einzustufen. Beim Einsatz von KI-Tools wie ChatGPT oder Copilot ist in jedem Fall die allgemeine Pflicht zur **KI-Kompetenz** nach Art. 4 KI-VO zu beachten. Danach sind Maßnahmen zu treffen, die sicherstellen, dass die Beschäftigten über ausreichende Kenntnisse bezüglich der Funktionsweise, der Risiken, der Grenzen sowie der rechtlichen und ethischen Implikationen von KI-Systemen verfügen. Die Maßnahmen beziehen sich jedoch nicht nur auf technische Kompetenzen. Auch Kompetenzen in Bereichen wie Datenschutz und Cybersicherheit müssen gezielt geschult werden. Die Entwicklung interner Aus- und Weiterbildungsmaßnahmen sowie der Aufbau organisationsinterner KI-Governance-Strukturen sind daher wesentliche Schritte, um diesen Anforderungen gerecht zu werden. Diese Verpflichtung gilt für alle, die KI-Systeme entwickeln oder betreiben, unabhängig von der Risikoklassifizierung des KI-Systems. Dabei ist es unerheblich, ob die Nutzung des Hochrisiko-KI-Systems lokal auf dem eigenen Server oder Rechner erfolgt, ob auf das KI-System über eine Programmierschnittstelle (API) zugegriffen wird oder ob das KI-System in einer Webanwendung (wie bei ChatGPT) genutzt wird.

Zusätzlich enthält Art. 50 KI-VO spezifische **Transparenzpflichten** für synthetisch erzeugte Inhalte. Betreiber müssen klar und deutlich offenlegen, wenn es sich bei den erzeugten Inhalten um sogenannte Deepfakes handelt – das betrifft insbesondere Bild-, Ton- oder Videomaterial, das künstlich erzeugt oder verändert wurde. Ebenso müssen Betreiber offenlegen, wenn Texte mithilfe von KI generiert oder verändert wurden und diese Texte mit dem Ziel veröffentlicht werden, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren. Unternehmen sollten daher entsprechende technische und organisatorische Maßnahmen treffen, um eine transparente Kennzeichnung sicherzustellen.

Ganzheitliche Compliance: Unternehmen sind verpflichtet, die Einhaltung der Vorgaben nachvollziehbar zu dokumentieren und fortlaufend zu überprüfen. Das gilt nicht nur für die Compliance nach der KI-VO. Daneben sind die weiteren Regelwerke zu beachten. Nach Art. 2 Abs. 7 KI-VO bleibt z.B. die Datenschutz-Grundverordnung (DSGVO) von der KI-VO unberührt. Darüber hinaus dürfen auch urheberrechtliche Fragestellungen sowie der Schutz von Geschäftsgeheimnissen nicht außer Acht gelassen werden. Auch die Cybersicherheits-Compliance ist sicherzustellen. Schließlich kann die Integration von KI-Tools in betriebliche Abläufe Mitbestimmungsrechte des Betriebsrats auslösen.

Welche Abteilungen im Unternehmen sollten sich wie mit der KI-VO befassen?

Die KI-VO hat weitreichende Auswirkungen auf die Geschäftsprozesse. Für die Entwicklung einer unternehmensweiten KI-Strategie ist ein interdisziplinärer Ansatz unerlässlich. Dies erfordert eine enge Zusammenarbeit – in der Regel – von Geschäftsführung, Rechtsabteilung, IT/OT, Einkauf, ggf. externen Experten sowie ggf. dem Betriebsrat.

Neben den neuen Anforderungen der KI-VO finden regelmäßig weitere Regelwerke Anwendung. Beim Einsatz von KI im Unternehmen stellen sich grundsätzlich auch Fragen im Bereich Datenschutz & Geschäftsgeheimnisschutz, Cybersicherheit, Arbeitsrecht und geistiges Eigentum. Letzteres betrifft u.a. Fragen zum geistigen Eigentum an Trainingsdaten sowie an Input- und Output-Daten. Auch der Schutz von Geschäftsgeheimnissen spielt beim Einsatz von KI im Unternehmen eine bedeutende Rolle. Darüber hinaus kann die Nutzung von KI Mitbestimmungsrechte des Betriebsrats auslösen.

Es bedarf daher eines ganzheitlichen und interdisziplinären Ansatzes zur Gewährleistung der KI-Compliance im Unternehmen. Die bereichsübergreifende Zusammenarbeit muss durch klare Verantwortlichkeiten, transparente Entscheidungswege und ein effektives Projektmanagement unterstützt werden, um die Anforderungen der KI-VO effizient, konsistent und revisionssicher umzusetzen.

Wie müssen Mitarbeitende geschult werden, um die Anforderungen aus der KI-VO zu erfüllen?

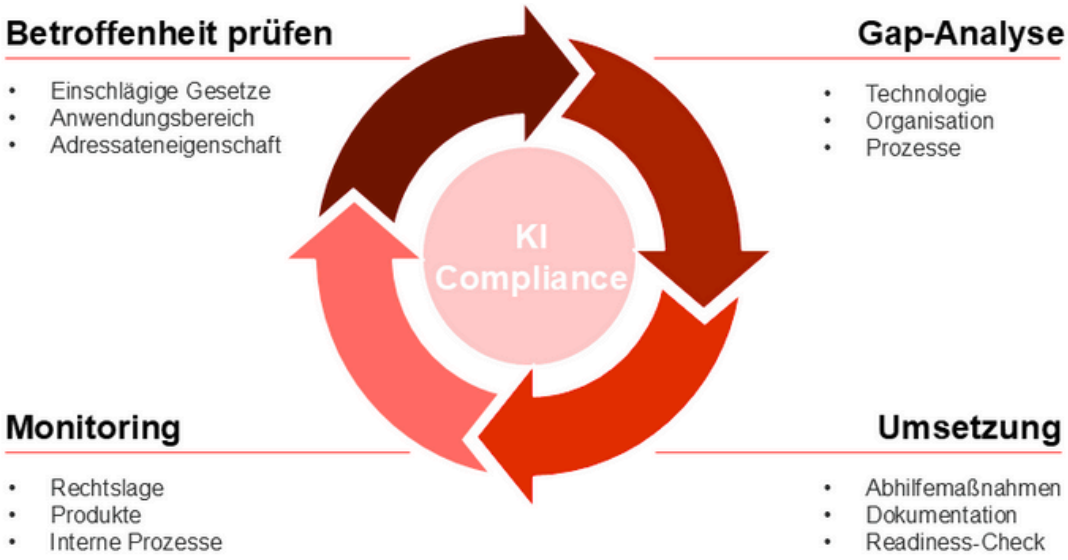
Seit dem 2. Februar 2025 sind Betreiber und Anbieter von KI-Systemen dazu verpflichtet, eine ausreichende KI-Kompetenz in ihrer Organisation sicherzustellen. Gemäß Art. 4 KI-VO sind geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass die Beschäftigten und Personen, die im Auftrag einer Organisation handeln, über ausreichende Kenntnisse bezüglich der Funktionsweise, Risiken, Grenzen sowie der rechtlichen und ethischen Implikationen von KI verfügen. Die Pflicht zur KI-Kompetenz gilt für alle KI-Systeme, unabhängig von deren Risikoklasse. Die KI-VO enthält für die konkrete Umsetzung keinen Maßnahmenkatalog. Gemäß dem risikobasierten Ansatz der KI müssen Unternehmen die Maßnahmen an dem konkreten Einsatz des spezifischen KI-Systems und der Nutzergruppen ausrichten. Als mögliche Maßnahmen sind die gängigen Compliance-Maßnahmen wie Schulungen, Richtlinien und Handreichungen oder Zertifizierungen zu nennen. Auch die Ernennung eines KI-Beauftragten kann eine solche Maßnahme sein. Zu beachten ist, dass KI-Kompetenz nach dem Stand der Technik und den aktuellen Entwicklungen gewährleistet sein muss. Es besteht somit eine Fortbildungspflicht, und die ergriffenen Maßnahmen sind fortlaufend zu überprüfen und bei Bedarf anzupassen.

Bezüglich der Schulungen sind die Umstände des Einzelfalls zu berücksichtigen. Grundsätzlich sind die Mitarbeitenden über die technischen Grundlagen und Besonderheiten, die Chancen und Risiken sowie die sozial-ethischen und rechtlichen Anforderungen im Zusammenhang mit KI zu schulen. Entsprechend dem risikobasierten Ansatz der KI-VO sind die Schulungsmaßnahmen an den Kontext und das vorhandene Wissen der Nutzenden anzupassen. In der Praxis sind die Maßnahmen daher je nach Nutzenden, Art der KI und deren Einsatzzweck unterschiedlich auszugestalten.

Wie kann ein Unternehmen langfristig die KI-Compliance sicherstellen?

KI-Compliance ist ein Prozess, der einer fortlaufenden Überprüfung und Anpassung bedarf. Grundsätzlich sind die folgende 4 Schritte zur KI-Compliance zu empfehlen:

1. Prüfung der Betroffenheit
2. Ermittlung der konkreten Anforderungen
3. Gap-Analyse und Umsetzung
4. Monitoring der internen Prozesse, der KI-Systeme und der Rechtslage



Um die KI-Compliance im Unternehmen zu gewährleisten, ist in der Regel ein Maßnahmenbündel erforderlich. Welche Maßnahmen in welchem Umfang zu ergreifen sind, richtet sich nach den konkreten Umständen des Einzelfalls, beispielsweise nach dem KI-System, der konkreten Nutzung und den Nutzergruppen. Als Maßnahmen zur KI-Compliance kommen unter anderem die folgenden in Betracht:

Strategie & Governance

- Bestandsaufnahme aller eingesetzten KI-Systeme inkl. Risikobewertung
- Entwicklung einer unternehmensweiten KI-Strategie
- Festlegung interner Richtlinien zur Einhaltung gesetzlicher Pflichten
- Definition von Verantwortlichkeiten
- Einrichtung eines KI-Review-Boards zur Bewertung und Freigabe von KI-Einsätzen

Regelungs- & Rechtsrahmen

- Ermittlung relevanter Vorschriften (z.B. KI-VO, DSGVO, Cybersicherheit)
- Vertragsmanagement: Prüfung und Bewertung von Verträgen und Nutzungsbedingungen (insbesondere in der Lieferkette)

Technischer & organisatorischer Umgang mit KI

- Etablierung eines Prozesses zur Einführung neuer KI-Systeme
- Ergreifen von erforderlichen technischen und organisatorischen Maßnahmen
- Monitoring der eigenen Prozesse, der genutzten KI-Anwendungen sowie der Rechtslage

Mensch im System

- Schulung und Sensibilisierung der Beschäftigten zur sicheren und verantwortungsvollen Nutzung von KI

Ein weiterer wesentlicher Baustein der KI-Compliance ist neben der Etablierung einer KI-Strategie ein vorausschauendes Risikomanagement. Dessen Notwendigkeit ergibt sich nicht nur aus den gesetzlichen Anforderungen, sondern auch aus der unternehmerischen Verantwortung, sichere und zuverlässige KI-Systeme bereitzustellen. Dementsprechend bietet sich die Einrichtung eines Risikomanagementsystems auch für KI-Systeme an, die zwar nicht als Hochrisikosysteme im Sinne des KI-Gesetzes eingestuft werden, aber dennoch erhebliche Risiken bergen können oder besonders geschäftskritisch sind. Oftmals sind bestehende Risikomanagementprozesse nicht ausreichend und müssen gezielt erweitert sowie an technologische, betriebliche, rechtliche, regulatorische und ethische Risiken angepasst werden. Aufgrund der zunehmenden Komplexität technischer und rechtlicher Anforderungen empfiehlt sich eine möglichst frühzeitige Integration einer zentralen KI-Governance. Diese fungiert sowohl als Kontrollinstanz als auch als internes Kompetenzzentrum. Nach der Implementierung von KI-Prozessen sind klare interne Richtlinien entscheidend, um die Compliance langfristig sicherzustellen. Ohne diese besteht die Gefahr, unbewusst gegen gesetzliche Vorgaben zu verstoßen, was erhebliche rechtliche, finanzielle und Reputationsschäden nach sich ziehen kann.

Ihr soluzione Kontakt:

Tim Ziegler - Director of Sales & Business Development

Mail: tim.ziegler@soluzione.de

Tel.: +49 (0) 8938997051

Verfasser / Autoren:

- Rechtsanwältin Christina Kiefer, LL.M. (Oslo), ist Senior Associate im Bereich Digital Business bei reuschlaw in Saarbrücken. Sie berät Unternehmen und öffentliche Einrichtungen zu komplexen Fragestellungen in den Bereichen Datenschutz und Cybersicherheit sowie IT- und Vertragsrecht. Ein Schwerpunkt ihrer Tätigkeit liegt in der Begleitung von Mandanten bei der Einführung digitaler Produkte. Sie ist zudem Lehrbeauftragte an der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau sowie Autorin diverser Fachpublikationen. Die Beratung zur KI-Compliance ist eines ihrer Kernthemen.
- reuschlaw gehört zu den führenden wirtschaftsberatenden Kanzleien im Produktrecht und berät seit 2004 national und international tätige Unternehmen und öffentliche Stellen mit Schwerpunkt Produktsicherheitsrecht, Produkthaftungsrecht, Data Protection. IT-Recht, Cybersecurity, Rückrufmanagement, Versicherungsrecht, Compliance Management und Vertragsrecht. Neben den beiden Niederlassungen in Deutschland bietet die Kanzlei ihre Leistungen über ihr Netzwerk mittlerweile in weiteren 30 Ländern an. info@reuschlaw.de / reuschlaw.de