Mittelstand-Digital
Zentrum
Kaiserslautern

KI-VERORDNUNG

PRAXISBEISPIELE ZUR ORIENTIERUNG FÜR KMU

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

INHALTSVERZEICHNIS

AG KI

Die Arbeitsgruppe (AG) Künstliche Intelligenz (KI) von Mittelstand-Digital tauscht sich zu Ergebnissen und Herausforderungen im Themenkomplex Künstliche Intelligenz in regelmäßigen Expertenrunden aus. Teilnehmen können alle Zentren des Mittelstand-Digital-Netzwerks. Unternehmen können so direkt von unserem Erfahrungsaustausch profitieren. Der gezielte Einsatz KI-basierter Lösungen hat eine signifikante Bedeutung für und Auswirkung auf die Wirtschaftlichkeit von Unternehmen. Durch die Arbeit in der AG Künstliche Intelligenz werden Unternehmen dazu befähigt, ein besseres Verständnis der Methoden und Hintergründe Künstlicher Intelligenz zu entwickeln sowie daraus entstehende neue Potentiale und Chancen für das eigene Unternehmen zu erkennen. Den Unternehmen wird anhand von Praxisbeispielen aus dem Mittelstand-Digital Netzwerk Orientierung gegeben sowie diese bei der Einführung KI-basierter Lösungen unterstützt.

FORUM RECHT

Das Forum Recht fungiert als zentraler Arbeitskreis mit drei wesentlichen Funktionen. Als Forum zum fachlichen Austausch dient es der Vernetzung der Zentren, um Informationen auszutauschen, Bedarfe des Mittelstands deutschlandweit zu analysieren sowie rechtliche Herausforderungen gemeinsam zu bewältigen. Der Austausch von Erfahrungen und das Erweitern des Wissens schaffen Synergien, die effektiv genutzt werden können. Als Impulsgeber greift das Forum mittelstandsrelevante Rechtsthemen auf, bereitet sie zielgruppenorientiert auf und entwickelt Transfermedien, um den Wissenstransfer sowohl in die Zentren als auch in den Mittelstand sicherzustellen. Schließlich agiert das Forum als Ansprechpartner, indem es den Dialog mit dem Mittelstand, anderen Arbeitsgruppen, der Plattform Industrie 4.0 sowie interessierten Kreisen wie Verbänden und Kammern fördert und somit eine Brücke zwischen den Akteuren schlägt. Das Forum Recht ist somit ein Schlüsselakteur für den Wissens- und Informationstransfer im Bereich mittelstandsrelevanter Rechtsthemen.

VORWORT

Die Verordnung über künstliche Intelligenz (KI-VO) der Europäischen Union definiert erstmals einen Rechtsrahmen für Systeme künstlicher Intelligenz (KI-Systeme). Insbesondere für kleinere und mittlere Unternehmen (KMU) ergeben sich aus der Verordnung vielfältige Fragestellungen, die in dieser Publikation der Mittelstand-Digital Zentren mit umfangreichen Beispielen adressiert werden.
Mehr und mehr wird KI in Geschäftsprozessen, Produkten und Dienstleistungen verwendet. Sie bietet enorme Chancen, um Innovationen voranzutreiben, birgt aber gleichzeitig viele rechtliche Fragestellungen, Risiken und Herausforderungen. Die neue KI-Verordnung setzt Rahmenbedingungen, damit Entwicklung, Inverkehrbringen, Inbetriebnahme und Verwendung von KI-Systemen mit den Werten der Europäischen Union vereinbar sind.
Konkret gelten seit dem Inkrafttreten der Verordnung am 1. August 2024 umfangreiche Vorschriften, die auf einem risikobasierten Ansatz basieren: Je höher das Risiko, dass ein KI-System die Grundrechte der Europäischen Union gefährden kann, desto strenger sind die Vorschriften. Für viele KMU können die Vorgaben zunächst überwältigend wirken. Genau hier setzt diese Handreichung an: Sie gibt Orientierung, die Anforderungen der Verordnung besser zu verstehen, bietet praktische Umsetzungstipps und hilft KMU, „KI-ready“ zu werden.
In die Handreichung ist die Expertise der Arbeitsgemeinschaften „Künstliche Intelligenz“ und „Forum Recht“ des Netzwerks der Mittelstand-Digital Zentren eingeflossen. Nach einer allgemeinen Einführung in die KI-Verordnung wird anhand fiktionaler Beispiele die praktische Umsetzung der KI-Verordnung beschrieben. Zu jedem Beispiel werden Ausgangssituation, Vorgehen, Ziel des KI-Einsatzes und Details des jeweiligen KI-Systems erläutert. Darauf aufbauend erfolgt die Beschreibung möglicher Risiken und eine Einstufung nach der KI-Verordnung, wonach Handlungsbedarfe und Verpflichtungen für das Unternehmen aufgezeigt werden. Die Beispiele sind so gewählt, dass sie leicht auf viele Anwendungsfälle bezogen werden können und KMU so eine Hilfe für die Umsetzung im eigenen Betrieb bieten.

HAFTUNGSAUSSCHLUSS

Dieser Leitfaden dient ausschließlich der allgemeinen Information und enthält Handlungsempfehlungen zur KI-Verordnung. Dabei wird darauf hingewiesen, dass die rechtliche Einschätzung und Risikoeinstufung stets vom spezifischen Einzelfall abhängen. Aus diesem Grund sollten sämtliche rechtlichen Bewertungen und daraus resultierende Handlungsanweisungen durch eine individuelle Überprüfung, beispielsweise durch einen Fachanwalt, validiert werden.

Innerhalb des Leitfadens wurden offizielle rechtliche Definitionen zur besseren Verständlichkeit verkürzt. Zur rechtlichen Eindeutigkeit ziehen Sie den Gesetzestext heran. Es wird keinerlei Haftung für mögliche Lücken in der Darstellung sowie für Änderungen der Rechtslage übernommen, die sich in der Zukunft ergeben können. Die hier dargestellten Informationen gehen nach dem Stand zum 1. Juli 2025. Wichtige Aspekte der KI-Verordnung werden weiterhin diskutiert.

Weitere Handlungsempfehlungen bezüglich anderer Rechtsvorschriften wie der Datenschutzgrundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG), dem Allgemeinen Gleichbehandlungsgesetz (AGG), dem Betriebsverfassungsgesetz (BetrVG) und anderen relevanten Gesetzen können ergänzend hinzukommen. Diese liegen jedoch außerhalb des Anwendungsbereichs dieses Leitfadens. Sollten sie dennoch erwähnt werden, erhebt die Aufzählung keinerlei Anspruch auf Vollständigkeit.

1. WAS IST DIE KI-VERORDNUNG?

Die KI-Verordnung der Europäischen Union (KI-VO) ist neben dem Digital Services Act und dem Data Act Teil der Europäischen Datenstrategie. Die KI-Verordnung (KI-VO) hat als produktsicherheitsrechtliche Rahmenverordnung zum Ziel, die Entwicklung von Künstlicher Intelligenz (KI) in der Europäischen Union (EU) in ethisch vertretbare Bahnen zu lenken. Außerdem soll die Grundlage für klare Regeln für die verantwortungsvolle Nutzung von KI geschaffen werden.

Um Effektivität dieser Ziele sicherzustellen, gilt das Marktortprinzip. Das heißt, dass die KI-VO immer auf KI-Systeme oder -Modelle sowie deren Output Anwendung findet, wenn es zur Verwendung innerhalb der EU kommt. Damit fallen auch Anbieter von KI-Systemen aus Drittstaaten wie den USA oder China, die ihre Systeme in der EU anbieten, unter die KI-VO. Hierdurch soll die Umgehung der KI-VO verhindert werden. Ein „Forum Shopping" nach dem Entwicklungsstandort mit den günstigsten Bedingungen (also den wenigsten Anforderungen) ist daher nicht möglich .

WAS IST KI NACH DER KI-VO?

Die KI-VO folgt einem technologieoffenen Ansatz und definiert den Begriff der KI weit. Hierdurch soll verhindert werden, dass die Festlegungen in der KI-VO durch den technischen Fortschritt innerhalb von kurzer Zeit überholt werden. Bei KI handelt es sich nach der KI-VO um

01	ein maschinengestütztes System,
02	das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist,
03	das nach seiner Betriebsaufnahme anpassungsfähig sein kann,
04	das für explizite oder implizite Ziele
05	aus den erhaltenen Eingaben ableitet,
06	wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die
07	physische oder virtuelle Umgebungen beeinflussen können.

KI-MODELLE UND KI-SYSTEME

Im Rahmen von „KI mit allgemeinem Verwendungszweck" unterscheidet die KI-VO KI-**Systeme** mit allgemeinem Verwendungszweck von KI-**Modellen** mit allgemeinem Verwendungszweck.
KI-**Modelle** mit allgemeinem Verwendungszweck sind KI-Modelle, die einen hohen Grad an allgemeiner Anwendbarkeit aufweisen und unabhängig von der Art und Weise, wie sie in Verkehr gebracht werden, in der Lage sind, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen (ausgenommen sind KI-Modelle, die vor ihrem **Inverkehrbringen** für Forschungs- und Entwicklungszwecke oder zur Erstellung von Prototypen verwendet werden). Sie können in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden. Obwohl KI-Modelle wesentliche Bestandteile von KI-Systemen sind, stellen sie selbst keine KI-Systeme

Inverkehrbringen und Bereitstellung von KI-Systemen:
„Inverkehrbringen" meint die erstmalige Bereitstellung eines KI-Systems und KI-Modellen mit allg. Verwendungszweck auf dem Markt. (vgl. Art. 3 Nr. 9 KI-VO)

Die „Bereitstellung" umfasst dabei die entgeltliche oder unentgeltliche Abgabe zum Vertrieb oder zur Verwendung im Rahmen einer Geschäftstätigkeit. (Art. 3 Nr. 10 KI-VO)

dar. Damit aus KI-Modellen KI-Systeme werden, müssen weitere Komponenten hinzugefügt werden, z.B. eine Benutzerschnittstelle. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil von ihnen.

Große **generative KI-Modelle** sind ein typisches Beispiel für ein KI-Modell mit allgemeinem Verwendungszweck. Sie können u.a. flexibel Inhalte in Text-, Audio-, Bild- oder Videoform erzeugen. Diese eignen sich für eine breite Palette von Aufgaben.

KI-**Systeme** mit allgemeinem Verwendungszweck sind KI-Systeme, die auf einem KI-Modell mit allgemeinem Verwendungszweck basieren und für eine Vielzahl von Zwecken eingesetzt werden können, sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme.

FÜR WEN GILT DIE KI-VO?

Verpflichtet nach der KI-VO sind die **Anbieter** von KI. Anbieter sind Unternehmen, die entweder KI-Systeme, die außerhalb der EU entwickelt wurden, unter eigenem Namen oder eigener Marke in der EU in Verkehr bringen oder KI-Systeme entwickeln oder entwickeln lassen (Art. 3 Nr. 3 KI-VO).

Neben den Pflichten für Anbieter sind auch Pflichten für **Betreiber** von KI-Systemen vorgesehen. Darunter sind alle Unternehmen zu verstehen, die KI-Systeme in eigener Verantwortung einsetzen (Art. 3 Nr. 4 KI-VO). Davon abgegrenzt ist die rein private Nutzung. Auch der eigene Betrieb von KI auf fremder Infrastruktur (Infrastructure as a Service - IaaS) wird von der Nutzung umfasst.

Die KI-VO gilt neben Anbietern und Betreibern auch für **Einführer** und **Händler**. Ein Einführer ist jeder, der ein KI-System in Verkehr bringt, das den Namen oder die Marke einer außereuropäischen (natürlichen oder juristischen) Person trägt. Ein Einführer ist somit jede in der EU ansässige Person, die KI-Systeme aus dem Ausland importiert. Händler ist jeder, der KI-Systeme bereitstellt und damit jeder in der Lieferkette, der nicht Einführer oder Lieferant ist.

KI-VERORDNUNG: FÜR WEN GILT SIE?

ANBIETER ...	ANBIETER ...	BETREIBER ...	EINFÜHRER ...	HÄNDLER ...
... juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System entwickeln oder entwickeln lassen	... natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-Modell entwickeln oder entwickeln lassen	... natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen	... jede natürliche oder juristische Person mit Niederlassung in der EU	... jede natürliche oder juristische Person in der Lieferkette, die selbst nicht Anbieter oder Einführer sind
... die KI-Systeme im eigenen Namen oder unter eigener Marke in der EU in Verkehr bringen oder in Betrieb nehmen	... die KI-Modelle mit allgemeinem Verwendungszweck im eigenen Namen oder unter eigener Marke in der EU in Verkehr bringen	... eigenverantwortliche Verwender von KI-Systemen in der EU	... bringen KI-Systeme ein in den Verkehr, die den Namen oder die Marke einer nicht europäischen natürlichen oder juristischen Person tragen	... stellen KI-Systeme bereit

Abb. 1: KI-Verordnung: Für wen gilt sie?

HAT DIE KI-VO BEDEUTUNG FÜR KMU?

Es ist daher immer möglich, dass neben Unternehmen, die KI-Systeme entwickeln, auch Unternehmen, die solche Systeme vertreiben, und Unternehmen, die KI in ihren Geschäftsprozessen nutzen, von den Regelungen der KI-Verordnung betroffen sind. Auch in kleinen und mittleren Unternehmen (KMU) sind vielfältige Einsatzmöglichkeiten für KI gegeben, wie z.B. Kundenservice und -support, personalisierte Werbung, Automatisierung von Geschäftsprozessen oder **Predictive Analytics** (vorausschauende Wartung, Betrugserkennung, Optimierung der Lieferkette, Personalmanagement und -rekrutierung, etc.) Weit mehr Unternehmen als auf den ersten Blick ersichtlich sind daher von der KI-VO betroffen.

WIE REGULIERT DIE KI-VO KI (RISIKOKLASSEN)?

Die KI-VO verfolgt einen risikobasierten Ansatz, um KI zu regulieren. KI-Systeme werden vier Risikokategorien zugeordner: **minimal, begrenzt, hoch und inakzeptabel.** Zusätzlich zu den oben genannten risikobasierten Anforderungen gibt es Anforderungen für **Allzweck-KI-Modelle** (General Purpose AI - GPAI). Aufgrund der Relevanz für KMU fokussiert diese Publikation zu diesem Zeitpunkt KI-Systeme. Den Anforderungen an die KI-Systeme entspricht jeweils eine der genannten Risikokategorien. Je höher das Risiko ist, das die Systeme für den Menschen darstellen, desto höher sind die Anforderungen. Daher muss das System in eine der dargestellten Risikokategorien eingeordnet werden, um die Anforderungen an das System zu bestimmen. Die Anforderungen der KI-Verordnung können je nach System von der (freiwilligen) Einhaltung von Verhaltenskodizes über Dokumentations- und Transparenzpflichten bis hin zu einer Untersagung des Systems reichen.

KI-VERORDNUNG: DIE RISIKOSTUFEN IM ÜBERBLICK

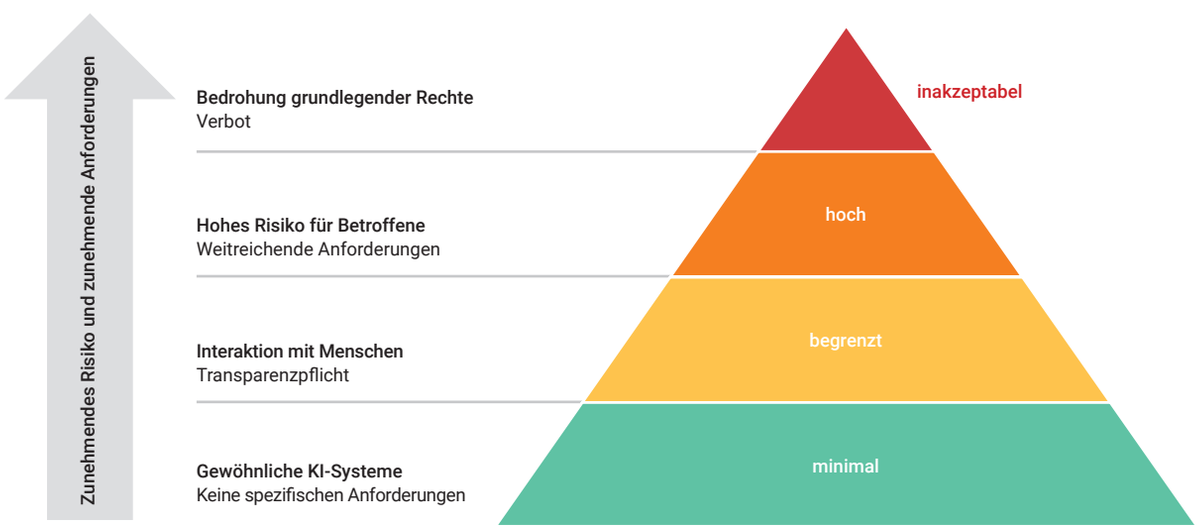


Abb. 2: KI-Verordnung: Die Risikostufen im Überblick

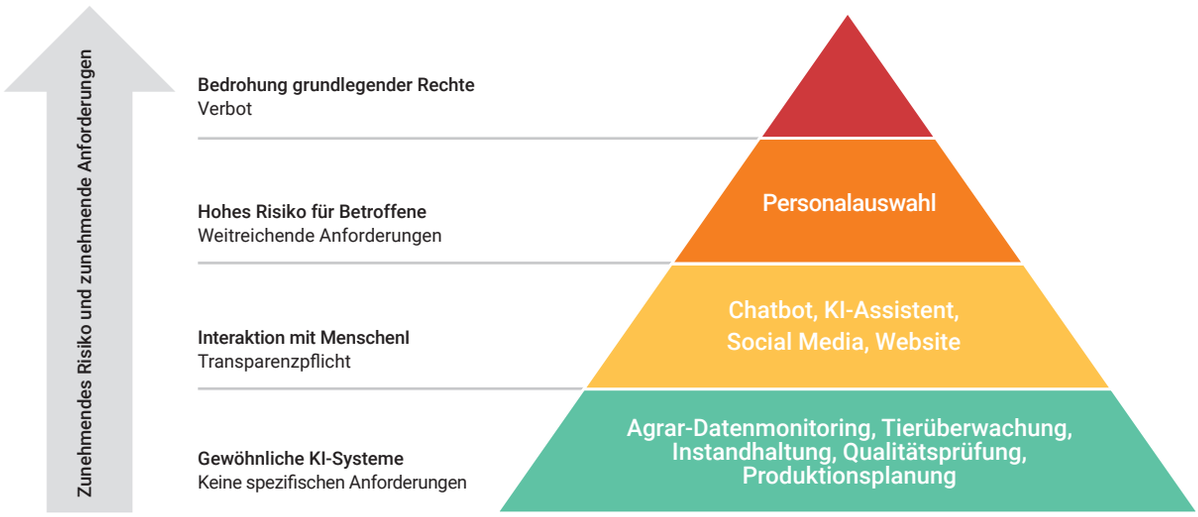
RISIKOKLASSE	BESCHREIBUNG	REGULIERUNG	BEISPIEL
inakzeptabel	Bedrohung grundlegender Rechte	Verbot	Social Scoring
hoch	Potenziell hohes Risiko für Betroffene	Weitreichende Anforderungen (menschliche Aufsicht, hochwertige Datensätze, etc.)	Kreditwürdigkeitsprüfung, KI im Personalbereich
begrenzt	Interaktion mit Menschen & Allzweck-KI	Transparenzpflicht (praxisleitfaden Art.56 AIA)	Chatbots
minimal	Alle anderen Systeme	Keine rechtlichen Anforderungen (freiwillig Verhaltenskodizes)	Spamfilter

Abb. 3: KI-Verordnung: Die Risikostufen und ihre Anforderungen

AB WANN GILT WAS?

Die KI-VO ist seit August 2024 in Kraft. Für die verschiedenen Regelungen sind allerdings unterschiedliche Übergangsfristen festgelegt, bis sie tatsächlich angewendet werden müssen. Ab dem Februar 2025 gelten die Regelungen, die verbotene KI-Systeme und KI-Kompetenz betreffen. Ab August 2025 gelten die Sanktionen und die Regelungen über Allzweck-KI-Modelle. Ab August 2026 gelten die Anforderungen an Hochrisiko-KI-Systeme nach Art. 6 und Anhang III VO (Use Cases). Außerdem gelten die Regelungen zur Kennzeichnung von KI-generierten Bildern und Texten und bezüglich der Transparenzpflichten für KI-Systeme, die mit Menschen interagieren (z. B . Kunden-Support-Chatbots) ab August 2026. Die Anforderungen für Hochrisiko-KI-Systeme nach Art. 6 und Anhang I KI-VO gelten erst ab August 2027.
Als Verordnung gilt die KI-VO zwar in jedem Mitgliedsstaat der EU unmittelbar, jedoch bedarf sie als Rahmengesetz der Konkretisierung. Viele dieser Konkretisierungen stehen zum aktuellen Zeitpunkt (Juli 2025) noch aus.

2. ANWENDUNGSFÄLLE



In diesem Kapitel werden nun elf Anwendungsfälle/ **Use Cases** aus deutschen Unternehmen im Bereich der Landwirtschaft, des Handwerks, der industriellen Fertigung und der Bauindustrie behandelt. Diese sind zwar fiktiv, dennoch repräsentativ für die individuellen Bedarfe und Standpunkte zu KI von KMU.

Die Anwendungsfälle behandeln die Nutzung und Planung verschiedener KI-Systeme, je nach Ausgangslage des KMU, und untersuchen die rechtlichen Konsequenzen der Einführung für die Unternehmen im Sinne der KI-Verordnung. Diese Konsequenzen und Anforderungen richten sich nach der jeweiligen Risikoeinstufung (minimal, begrenzt, hoch, inakzeptabel). Um ein solches Risiko zu ermitteln, wurden die wichtigsten Kriterien gesammelt, die bei der Einführung und Verwendung eines KI-Systems eine Rolle spielen.

Konkret werden zuerst die Ausgangslagen und Ziele der Unternehmen dargelegt, für die passende KI-Systeme ausgesucht werden. Anhand von Kriterien wie den Inputdaten, der Interaktion mit Menschen, den Risiken und schließlich den technischen Eigenschaften des Systems selbst, wird eine Risikoeinstufung vorgenommen und eine Handlungsempfehlung bezüglich der KI-Verordnung ausgesprochen.
Die präsentierten Kriterien können ebenfalls als Leitfaden für die Bewertung Ihres KI-Systems verstanden werden und Ihnen eine rechtlich sichere Anwendung erleichtern. Bereits in den Ergebnissen der elf Anwendungsfälle werden Sie jedoch schnell feststellen, dass die KI-Verordnung für die meisten KMU bzw. geläufigen KI-Systeme keine nennenswerte Relevanz besitzen wird. So kann meistens lediglich ein minimales oder begrenztes Risiko zugeordnet werden. Das erfordert in der Regel eine ohnehin sinnvolle Dokumentation der Nutzung des Systems sowie eine Aufklärung und Schulung des Personals nach Bedarf.

KI-GESTÜTZTE BODENSENSOREN UND WETTERDATENANALYSE

Biohof Landleben | Branche: Landwirtschaft

Ausgangssituation:

Das Unternehmen sucht eine effiziente Lösung zur Erkennung und Vorbeugung von Bodendegradation, Nährstoffungleichgewichten und Schädlingsbefall.

Ziel:

Ziel ist die Überwachung der Bodengesundheit, um frühzeitig Probleme zu erkennen und gezielte Maßnahmen zu ergreifen, die Erträge zu sichern und nachhaltige Landwirtschaft zu fördern.

Input:

Echtzeitdaten zu
- Bodenfeuchtigkeit
- Nährstoffgehalt
- pH-Wert
- Wetterbedingungen
- sowie historische Ernte- und Bodendaten

KI-Themenfelder:

- Sensordatenanalyse
- **Anomalieerkennung**
- Predictive Analytics

Vorgehen:

Durch den Einsatz KI-gestützter Bodensensoren und Datenanalyse werden Echtzeitinformationen über Feuchtigkeit, Nährstoffgehalt und pH-Wert des Bodens überwacht. Dadurch können frühzeitig Probleme wie Nährstoffungleichgewichte, Bodenerosion oder Schädlingsbefall erkannt und gezielte Maßnahmen zur Bodenpflege eingeleitet werden, zur langfristigen Sicherung der Fruchtbarkeit und Nachhaltigkeit der landwirtschaftlichen Produktion.

Zielgruppe:

Landwirt*innen

Interaktion mit Menschen:

Nein

Output:

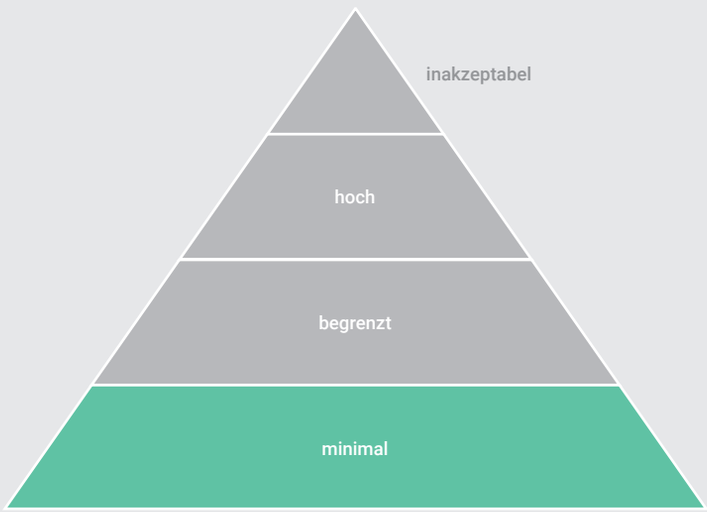
- numerische Vorhersagen zu Bodenfeuchtigkeit, Nährstoffleveln und Ernteerträgen
- grafische Visualisierungen von Bodenzustandsmustern und
- Handlungsempfehlungen

KI-Methoden und -Technologien:

- Machine Learning-Modelle wie **Random Forests** oder **LSTMs**

Entwicklung:

- Externer Dienstleister
- Sitz: Deutschland
- Branche: Agrartechnologie



Risiken:

- Falsche Vorhersagen

Fachliche Beschreibung:

Das System sammelt Echtzeitdaten zu Bodenfeuchtigkeit, Nährstoffgehalt und Wetter mithilfe von Sensoren und Satelliten. Diese Daten werden durch Machine-Learning-Modelle auf Muster und Bodengesundheitstrends analysiert. Die Befunde und Ergebnisse werden über ein zentrales Dashboard übersichtlich dargestellt. Auf das Dashboard kann über eine mobile App zugegriffen werden. Zusätzlich beinhaltet das System die Möglichkeit automatisiert und datenbasiert Empfehlungen zur Düngung, Bewässerung, etc. auszusprechen.

Technische Umsetzung:

Es gibt eine **cloudbasierte** Plattform, die Echtzeitdaten von Sensoren sammelt, die durch Machine Learning -Modelle (Random Forests und LSTM) analysiert werden. Präsentiert werden die Ergebnisse in einem Dashboard mit Vorhersagen und Empfehlungen für Landwirte, zugänglich über eine mobile App.

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Minimales" Risiko
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

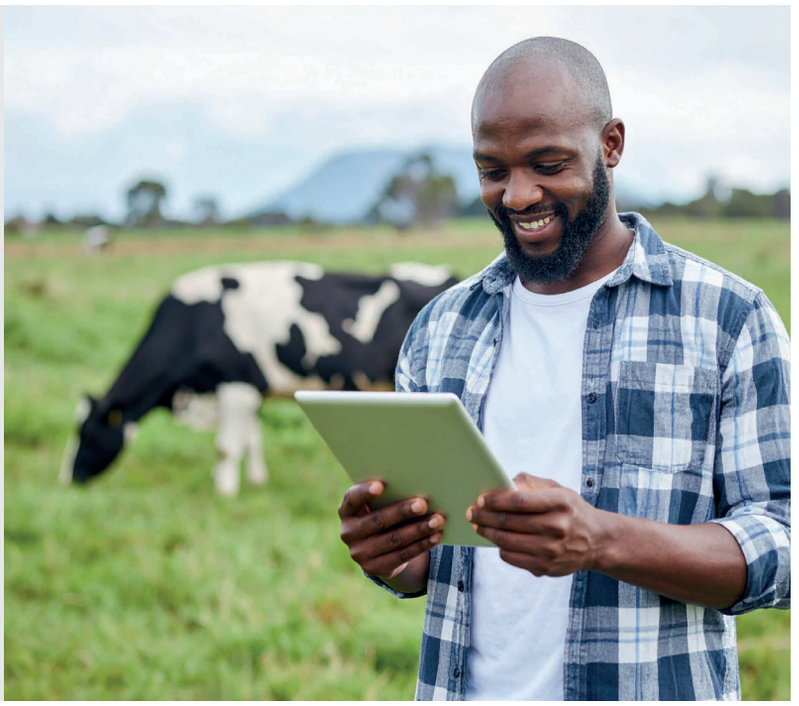
Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Der Arbeitgeber hat die Arbeitnehmenden, die mit dem System arbeiten, nach Bedarf über das System zu schulen. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

KI IN DER TIERÜBERWACHUNG

Milchhof Steinberger | Branche: Landwirtschaft



Ausgangssituation:

Das Unternehmen möchte den Gesundheitszustand und das Verhalten seiner Rinder überwachen.

Interaktion mit Menschen:

Nein

Input:

Daten zu
- Atmung
- Temperatur
- Herzfrequenz

der Rinder

KI-Themenfelder:

- **Computer Vision**
- Sensordatenanalyse
- Anomalie-Erkennung
- Predictive Analytics

Vorgehen:

Mittels automatisierter, sensorischer Erfassung der Atemfrequenz der Rinder in Form von Infrarot-Videoüberwachung, **Wearables** mit Sensoren und akustischen Sensoren können Aussagen über den Gesundheitszustand der einzelnen Tiere getroffen werden. Auf Basis der Daten kann eine Stressbelastung oder eine beginnende Erkrankung durch Einschränkungen im Wohlbefinden der Tiere frühzeitig erkannt werden.

Ziel:

Ziel ist die frühzeitige Erkennung von gesundheitlichen Problemen, um rechtzeitig reagieren zu können, das Senken der Tierarztkosten und des Einsatzes von Antibiotika und die langfristige Verbesserung des Gesundheitszustandes der Herde.

Zielgruppe:

Landwirt*innen und Tierbetreuungspersonal

Output:

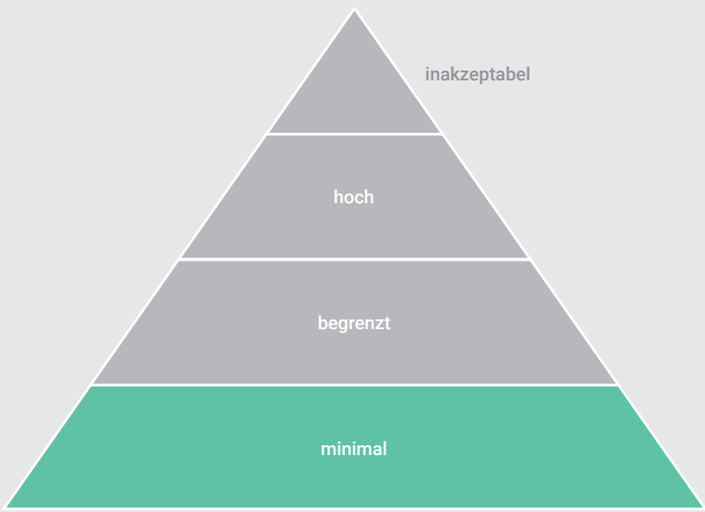
- Vorhersage zum Gesundheitszustand der Rinder

KI-Methoden und -Technologien:

- Bildgebende Verfahren (Infrarot-Thermografie Tiefenkamera)
- maschinelles Lernen (ML)
- Mustererkennung, Musteranalyse, Mustervorhersage
- **Neuronale Netze**

Entwicklung:

- Externer Dienstleister
- Sitz: Deutschland
- Branche: Agrartechnologie



Fachliche Beschreibung:

Das System sammelt kontinuierlich Gesundheitsdaten der Tiere durch den Einsatz von Sensoren und Computer Vision. Anschließend werden die Daten lokal durch Machine-Learning-Modelle auf bestimmte Verhaltensklassifikationen und potenzielle Anomalien analysiert. Bei auffälligen Befunden erhalten die Nutzer*innen eine Echtzeit-Benachrichtigung. Außerdem werden regelmäßig Berichte über Tierverhalten und -gesundheit erstellt.

Technische Umsetzung:

Das System erhebt die Bilddaten, analysiert sie und verarbeitet sie zu einer Gesundheitsvorhersage.

Risiken:

- Falsche Aussagen über die Gesundheit der Tiere
- Erhebung sensibler Gesundheitsdaten (z.B. Vitalzeichen) des Personals, durch z.B. Infrarot-Videoüberwachung

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Minimales" Risiko
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Alle Mitarbeitenden, die mit dem KI-System arbeiten, werden nach Bedarf geschult, damit sie wissen, wie sie das System richtig nutzen. Nutzer*innen (z.B. das Betreuungspersonal der Tiere) sollten u.a. informiert werden, dass die Benachrichtigungen und die Berichterstattung unter Beteiligung einer KI generiert sind. Dies ermöglicht u.a. die Zuverlässigkeit der Informationen einzuschätzen. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

PRÄDIKTIVE INSTANDHALTUNG MIT KI

Müller Maschinenteile GmbH | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte überraschende Ausfälle der wichtigsten Maschinen in der Fertigungslinie vorbeugen und minimieren.

Ziel:

Ziel ist die Einleitung von Instandhaltungsaktivitäten vor dem Ausfall der Maschine.

Zielgruppe:

Produktionsabteilung

Input:

- Maschinendaten wie Vibration, Geschwindigkeit, etc.

KI-Themenfelder:

- Predictive Analytics

Entwicklung:

- Selbstentwickelt mit **Open Source**-Algorithmen

Vorgehen:

Für die wichtigsten Maschinen in der Fertigung werden **Machine-Learning-Algorithmen** entwickelt, die mit maschinenbezogenen Daten gefüttert werden, die durch an den Maschinen angebracht Sensoren und Schnittstellen gesammelt werden. Mithilfe der Algorithmen können Anomalien und Handlungsbedarf frühzeitig erkannt und die Restlebensdauer der Maschine prognostiziert werden. Damit können unvorhergesehene Ausfälle vermieden werden.

Interaktion mit Menschen:

Nein

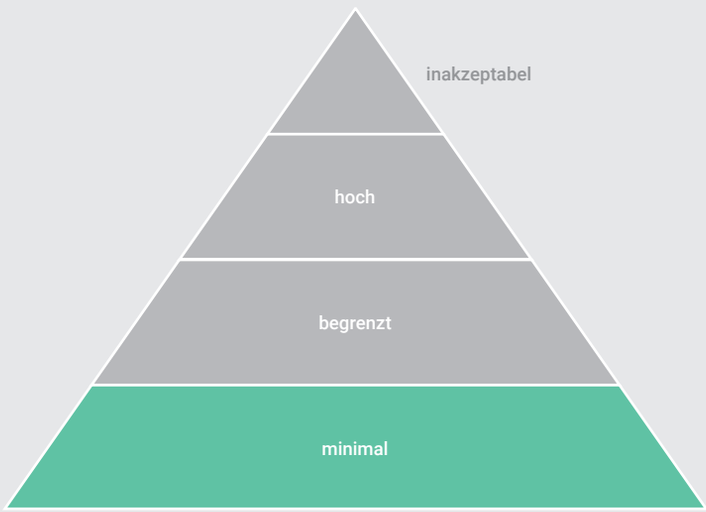
Interaktion mit Menschen gemäß der KI-Verordnung:
Entgegen mancher Erwartungen liegt hier nach der KI-Verordnung keine nennenswerte menschliche Interaktion vor. Zweck des Artikels 50 ist es, menschliche Interaktionen mit KI-Systemen hervorzuheben, bei denen Verwechslungs- oder Täuschungsrisiken bestehen. Das tritt beispielsweise ein, wenn die nutzende Person nicht erkennen kann, dass es sich um eine KI handelt. In einem solchen Fall sind verschiedene Aufklärungspflichten notwendig. Hier sind solche Aufklärungspflichten nicht nötig, da es für die Nutzer*innen der Maschinen offensichtlich ist, dass es sich um eine KI handelt (und nicht etwa um eine Kollegin).

Output:

- Vorhersage des Ausfallzeitpunkts und der geschätzten Restlebensdauer der Maschine

KI-Methoden und -Technologien:

- **Überwachtes** und **Unüberwachtes Lernen (Supervised und Unsupervised Learning)**



Technische Umsetzung:

Das System erhebt und analysiert mit Hilfe von Sensoren Daten aus dem Maschinenbetrieb.

Fachliche Beschreibung:

Bei der Umsetzung werden zunächst die zu überwachenden Komponenten ausgewählt und relevante Fehlerarten identifiziert. Anschließend erfolgt die Auswahl passender Sensordaten, um den Zustand der Maschinen präzise zu erfassen. Basierend auf historischen Daten und vergangenen Ausfällen wird ein Vorhersagemodell entwickelt, das mögliche Störungen frühzeitig erkennt und Prognosen über mögliche Ausfallzeitpunkte macht. Dieses Modell wird in den Betriebsablauf integriert, sodass automatische Benachrichtigungen und eine optimierte Wartungsplanung eine reibungslose und effiziente Instandhaltung ermöglichen.

Risiken:

- Fehlerhafte Vorhersagen
- Maschinenausfälle ohne Vorwarnung

Einstufung nach KI-Verordnung:

- Rolle: Anbieter
- Risikoklasse: „Minimales" Risiko
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Alle Mitarbeitenden, die mit dem KI-System arbeiten, werden nach Bedarf geschult, damit sie wissen, wie sie das System richtig nutzen. Nutzer*innen sollten u.a. informiert werden, dass die Vorhersagen unter Beteiligung einer KI generiert sind. Dies ermöglicht u.a. die Zuverlässigkeit der Informationen einzuschätzen. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

KI-GESTÜTZTE QUALITÄTSPRÜFUNG IN DER AUTOMATISCHEN LINIE

Schneider Präzisionstechnik GmbH | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte effizienter fehlerhafte Teile bei einer vollautomatisierten Fertigung identifizieren.

Ziel:

Ziel ist es, fehlerhafte Teile zu vermeiden und vor dem Versand abzufangen.

Input:

- Bilddaten der gefertigten Teile

KI-Themenfelder:

- Computer Vision

Vorgehen:

Das Unternehmen investiert in eine vollautomatische Linie zur Fertigung der Endprodukte, die Stationen zur automatischen Fertigung und zur optischen Qualitätsprüfung der gefertigten Endprodukte beinhaltet. Im Rahmen dieser optischen Qualitätsprüfung werden Teile mittels Fotos durch Machine-Learning-Algorithmen analysiert. Damit kann die Fehlerhaftigkeit von Teilen zuverlässig erkannt werden.

Zielgruppe:

Produktionsabteilung

Interaktion mit Menschen:

Nein

Output:

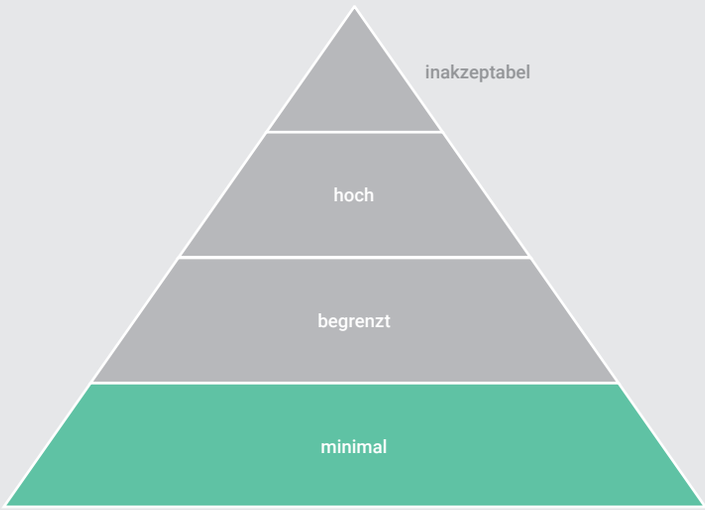
- Klassifikation der gefertigten Teile in „fehlerfrei“ und „fehlerhaft“ und entsprechende Steuerung der Förderanlage

KI-Methoden und -Technologien:

- **Convolutional Neural Networks (CNNs)**
- Maschinelles Lernen (ML)

Entwicklung:

- Externer Dienstleister
- Sitz: USA
- Branche: Anlagenhersteller



Fachliche Beschreibung:

Die optische Qualitätsprüfung erfolgt durch eine Kamera, die Bilder der gefertigten Teile aufnimmt. Diese Bilder werden dann durch vortrainierte CNNs analysiert, um die Teile als fehlerfrei oder fehlerhaft zu klassifizieren. Die Klassifikationsergebnisse steuern die Förderanlage, sodass fehlerfreie Teile zum Versand weitergeleitet und fehlerhafte Teile in den Ausschussbehälter befördert werden.

Technische Umsetzung:

Das System nutzt vortrainierte CNNs zur Klassifikation der Teile.

Risiken:

- Fehlklassifikation von Teilen und in der Folge Beeinträchtigung der Kundenzufriedenheit und Verursachung zusätzlicher Kosten

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Minimales Risiko“
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Alle Mitarbeitenden, die mit dem KI-System arbeiten, werden nach Bedarf geschult, damit sie wissen, wie sie das System richtig nutzen. Nutzer*innen sollten u.a. informiert werden, dass die Vorhersagen unter Beteiligung einer KI generiert sind. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

KI-GESTÜTZTE QUALITÄTSPRÜFUNG IN DER MANUELLEN MONTAGE

Mayer Feinmechanik GmbH & Co. KG | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte effizienter fehlerhafte Teile bei der manuellen Montage erkennen und die signifikant zunehmenden Retouren durch die Erstellung falscher Varianten reduzieren.

Ziel:

Ziel ist es, fehlerhafte Teile zu vermeiden und vor dem Versand auszusortieren.

Zielgruppe:

Produktionsabteilung

Interaktion mit Menschen:

Nein

Input:

- Bilddaten
- Auftragsdaten aus dem MES-System

KI-Themenfelder:

- Computer Vision

Technische Umsetzung:

Das System nutzt vortrainierte CNNs zur Klassifikation der Teile und gleicht diese mit den Auftragsdaten aus dem MES-System ab.

Vorgehen:

Eine optische, automatisierte Qualitätskontrolle, die mit den Auftragsdaten aus dem **MES-System** gekoppelt ist, wird in die manuelle Montage integriert. Im Rahmen dieser optischen Qualitätsprüfung werden Teile mittels Fotos durch Machine-Learning-Algorithmen analysiert.
Aufgrund der Kopplung mit dem MES-System ist möglich, Fehler in den Teilen und deren Anzahl und Zeitpunkt, teilweise sogar Rückschlüsse auf fehlerhafte Fertigung durch Mitarbeitenden festzustellen.
Damit kann die Fehlerhaftigkeit von Teilen frühzeitig erkannt werden und Retouren reduziert werden.

Open Source im Sinne der KI-Verordnung:
Open Source nach der KI-Verordnung bezeichnet kostenlose Software und Daten – einschließlich KI-Modelle –, die unter einer freien und quelloffenen Lizenz bereitgestellt werden, welche die Nutzung, Weitergabe, Veränderung und Untersuchung erlaubt, einschließlich der Offenlegung von Modellparametern, -Architektur und -Nutzung. Voraussetzung ist, dass der ursprüngliche Anbieter genannt wird und identische oder vergleichbare Lizenzbedingungen eingehalten werden.

Output:

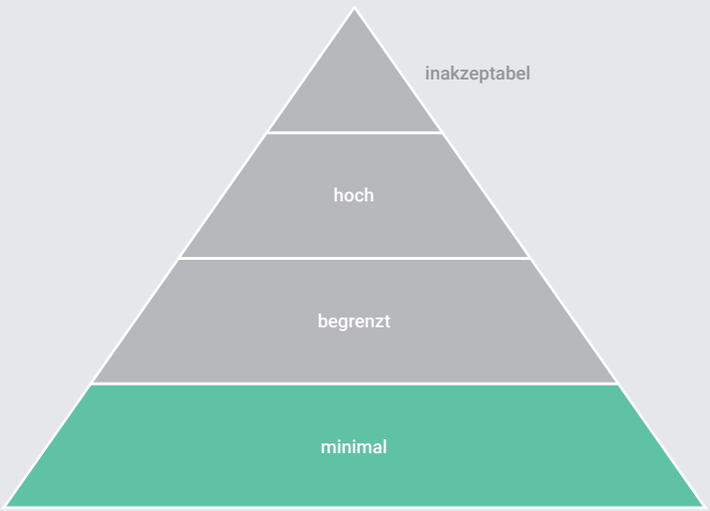
- Klassifikation der gefertigten Teile in „fehlerfrei" und „fehlerhaft" und Abgleich mit dem Auftrag

KI-Methoden und -Technologien:

- Convolutional Neural Networks (CNNs)
- Maschinelles Lernen (ML)

Entwicklung:

- Selbst entwickelt mit **Open Source-Algorithmen**



Fachliche Beschreibung:

Die optische Qualitätsprüfung erfolgt durch eine Kamera, die Bilder der gefertigten Teile aufnimmt. Diese Bilder werden dann durch vortrainierte CNNs analysiert, um die Teile als fehlerfrei oder fehlerhaft zu klassifizieren. Die Klassifikationsergebnisse steuern die Förderanlage, sodass fehlerfreie Teile zum Versand weitergeleitet und fehlerhafte Teile in den Ausschussbehälter befördert werden.

Risiken:

- Fehlklassifikation von Teilen und Beeinträchtigung der Kundenzufriedenheit und Verursachung zusätzlicher Kosten
- ungewollte Überwachung von Personalperformance führt zu Datenschutz- & Arbeitsrechtproblemen

Einstufung nach KI-Verordnung:

- Rolle: Anbieter
- Risikoklasse: „Minimales" Risiko
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

Rechenleistung und Finetuning:

In den meisten Fällen ist Rechenleistung kein limitierender Faktor. Sollte ein konkreter Bedarf bestehen, kann dies im Einzelfall mit dem jeweiligen Anbieter oder Dienstleister geklärt werden. Die Wahrscheinlichkeit, dass systemseitige Rechenleistungsschwellen überschritten werden, ist sehr gering und daher vernachlässigbar. Bei sehr umfangreichem Fine-Tuning kann es jedoch dazu kommen, dass bestimmte Rechenleistungsschwellen überschritten werden. In der Praxis wird Fine-Tuning allerdings häufig von spezialisierten Dienstleistern übernommen. Diese sollten im Vorfeld prüfen, ob besondere Anforderungen an die Rechenleistung bestehen. Beim Planen eines Fine-Tuning-Vorhabens sollte also die potenzielle Rechenlast mitbedacht und im Zweifel mit dem Anbieter abgestimmt werden.

Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein. Sollten Mitarbeitende überwacht werden können durch das System, führt dies sowohl zu datenschutzrechtlichen als auch zu arbeitsrechtlichen Verpflichtungen. Insb. kommt es bezüglich der arbeitsrechtlichen Verpflichtungen im Gegensatz zu der Bewertung nach der KI-VO nicht darauf an, dass das System nicht zur Überwachung bestimmt ist.

Handelt es sich bei YOLO um ein Allzweck-KI Modell, können hieraus Pflichten erwachsen. Handelt es sich um ein Allzweck-KI-Modell ohne systemisches Risiko, müssen Transparenzpflichten sowie Anforderungen an das Urheberrecht eingehalten werden.

Transparenz

02 Die Pflichten bezüglich der Transparenz sind in den Leitlinien zu Allzweck-KI-Modellen genauer konkretisiert. Transparenz bezieht sich auf Vortrainingsdaten und das Training von KI-Modellen mit allgemeinem Verwendungszweck . Es wurde ein "Model Documentation Form" entwickelt, das die Erfüllung der Pflichten ermöglicht. Anbieter des "Grundmodells" ist nicht Mayer Feinmechanik. Die Pflichten des Unternehmens beziehen sich daher (soweit die Informationen nicht schon **„Open Source"** sind) maximal auf **„Fine-Tuning"** des Modells.

Urheberrecht

Urheberrechtlich müssen beim Training des Modells vor allem die Anforderungen an das Text- and Datamining eingehalten werden. Insbesondere bedeutet dies, dass wirksam eingetragene Verwendungsvorbehalte Beachtung finden müssen. Für das Training werden in diesem Fall lediglich Bilder aus dem Unternehmen verwendet, also gemeinfreie Bilder und Bilder, an welchen die Mayer Feinmechanik GmbH & Co. KG ein Urheberrecht hat. Es kommt also nicht zum Text- und Data-mining nach § 44b UrhG.

03 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Alle Mitarbeitenden werden nach Bedarf geschult. Das Unternehmen erstellt klare Leitlinien zum Umgang mit dem KI-System, um die Sicherheit und den korrekten Einsatz zu gewährleisten.

KI IN DER PRODUKTIONSPLANUNG

AlpenTech Industrial Solutions GmbH | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte seine aufwendige und komplexe Produktionsplanung optimieren.

Ziel:

Ziel ist die Reduzierung der Fertigungszeiten und Kosten.

Input:

- Auftragsdaten aus dem MES-System

KI-Themenfelder:

- **Empfehlungssystem**

Vorgehen:

Die eigenen Mitarbeitenden des Unternehmens entwickeln mit der Unterstützung von Studierenden ein **On Premise**-Planungstool, welches auf **Metaheuristiken** oder **verstärkendem Lernen** basiert.
Das Tool wird innerhalb der unternehmenseigenen Infrastruktur betrieben, analysiert die Auftragsdaten und schlägt auf Basis derer automatisiert die optimale Fertigungsreihenfolge vor, um eine fristgerechte Auftragsvollendung sicherzustellen.
Dadurch kann eine effiziente Produktion zuverlässig geplant und sichergestellt werden.

Zielgruppe:

Produktionsabteilung bzw. Produktionsplaner*in

Interaktion mit Menschen:

Ja

Output:

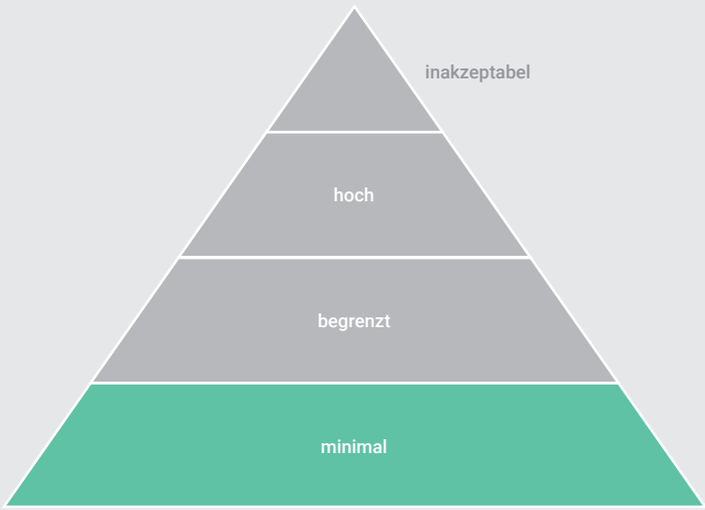
- Optimierter Fertigungsplan

KI-Methoden und -Technologien:

- Metaheuristik / verstärkendes Lernen

Entwicklung:

- Selbstentwickelt mit Open Source-Algorithmen



Fachliche Beschreibung:

Das Planungstool analysiert die Auftragsdaten aus dem MES-System und nutzt Metaheuristiken oder Reinforcement Learning, um die optimale Fertigungsreihenfolge zu bestimmen. Die Produktionsplaner*innen können das Tool über eine Benutzeroberfläche starten und die vorgeschlagenen Pläne einsehen und anpassen.

Technische Umsetzung:

Fertigungsaufträge werden im MES-System gesammelt und an das Planungstool übergeben, das Planungstool bestimmt die Reihenfolge der Abarbeitung.

Risiken:

- Gefahr einer schlechten, unzuverlässigen Planung, sodass Engpässe und zusätzliche Kosten entstehen
- Nichtbeachtung realer Einschränkungen und/oder Anforderungen

Einstufung nach KI-Verordnung:

- Rolle: Anbieter
- Risikoklasse: „Minimales" Risiko
- Ausschlaggebender Faktor: Es liegt kein inakzeptables, hohes oder begrenztes Risiko vor.

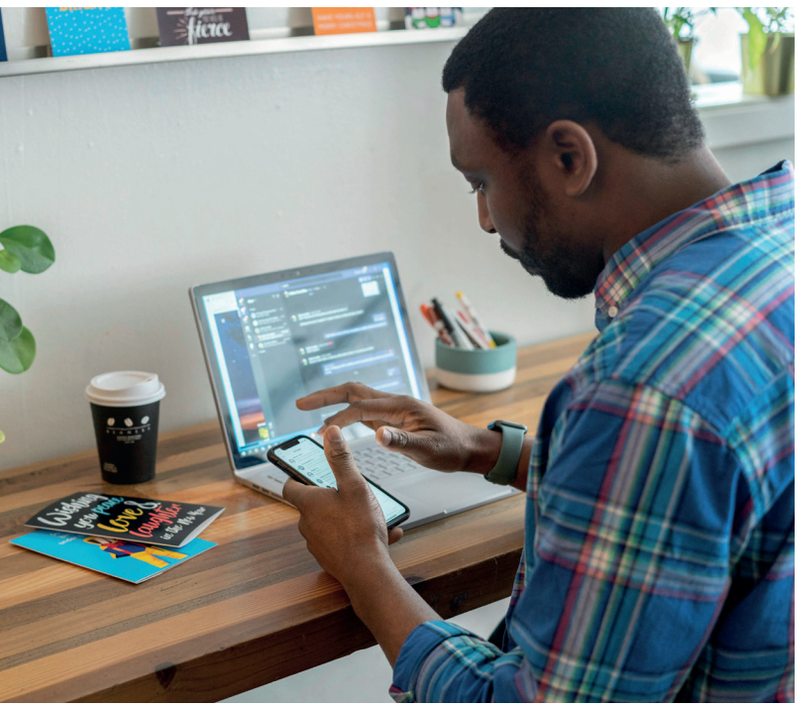
Handlungsbedarf und Verpflichtungen:

01 An KI-Systeme mit minimalem Risiko bestehen keine besonderen Anforderungen aus der KI-VO. Allerdings sind Vorgaben weiterer Gesetze zu beachten, sollten sie berührt sein.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Alle Mitarbeitenden, die mit dem KI-System arbeiten, werden nach Bedarf geschult, damit sie wissen, wie sie das System richtig nutzen. Nutzer*innen sollten u.a. informiert werden, dass die Vorhersagen unter Beteiligung einer KI generiert sind. Die Nutzer*innen sollten weiterhin aufgeklärt werden, welche Aspekte bei der Planung durch die KI Beachtung finden. Dies ist u.a. wichtig, damit die Entscheidungsfindung durch die Mitarbeitenden bewertet und gegebenenfalls korrigiert bzw. um weitere für das Unternehmen in dem konkreten Einzelfall relevante Merkmale ergänzt werden kann.

INTERNES WISSENSMANAGEMENT MIT KI-CHATBOT

Dachdeckerei First | Branche: Handwerk



Ausgangssituation:

Das Unternehmen möchte firmeninternes Wissen seinen Beschäftigten zentral verfügbar machen.

Ziel:

Ziel ist eine frei verfügbare Bereitstellung von Informationen zu Kund*innen sowie Produktdaten und relevanten Regelwerken für die Beschäftigten.

Zielgruppe:

Beschäftigte des Unternehmens

Interaktion mit Menschen:

Ja

Input:

- Fachliche Produktdatenblätter
- technisches Regelwerk
- Zugriff auf die Angebote und die Kundendaten

KI-Themenfelder:

- **Natürliche Sprachverarbeitung** mit **Large Language Models**
- **Dialogorientierte KI**

Vorgehen:

Es soll ein Chatbot entwickelt werden, der firmeninternes Wissen für die Beschäftigten verfügbar macht, indem er mit Hilfe von **Retrieval Augmented Generation** (RAG) auf eine strukturierte Wissensdatenbank zugreift, Informationen in Echtzeit abruft und verständlich aufbereitet.

Allzweck-KI-Modelle

Nach der KI-VO ist ein „KI-Modell mit allgemeinem Verwendungszweck" ein Modell mit erheblicher allgemeiner Verwendbarkeit, das unabhängig von der Art des Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen und in viele nachgelagerte Systeme integriert werden kann. Diese Allgemeinheit kann auch innerhalb einer einzelnen Modalität (z. B. Bild oder Video) bestehen. Auch Modelle, die durch Entwicklung oder Fine-Tuning in einem bestimmten Bereich besonders leistungsfähig sind, können als solche gelten. Daher lässt sich der Status als „Modell mit allgemeinem Verwendungszweck" derzeit (Stand: Juli 2025) nicht sicher ausschließen.

Output:

- Aggregation von Antwort-Daten auf Nutzeranfrage

KI-Methoden und -Technologien:

- KI ChatBot mit RAG (Retrieval Augmented Generation) als Wissensdatenbank

Entwicklung:

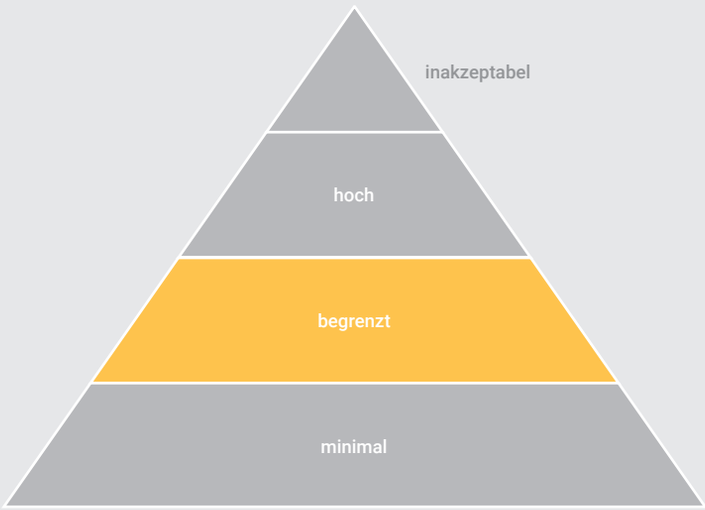
- Externer Dienstleister
- Sitz: Deutschland
- Branche: IT & Software

Risiken:

- Schäden durch Falschinformationen
- Falsche Nutzung und Verbreitung sensibler Daten der Mitarbeitenden und Unternehmensinformationen

Technische Umsetzung:

Es wird ein lokales Large Language Model (LLM) mit RAG über eine WebApp für mobile Geräte genutzt, um unternehmensspezifisches Wissen bereitzustellen.



Fachliche Beschreibung:

Das System gibt dem Personal die Möglichkeit nach bestimmten Informationen wie verbauten Teilen, Inhaltsstoffen oder technische Daten zu suchen und diese abzurufen.

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Begrenztes" Risiko/Transparenzrisiko
- Ausschlaggebender Faktor: Das KI-System interagiert mit dem Menschen.

Handlungsbedarf und Verpflichtungen:

01 Transparenzanforderungen des Art. 50 Abs. 1 KI-VO zur Information natürlicher Personen über die Interaktion mit KI treffen den Anbieter und damit nicht die Dachdeckerei First.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Der Arbeitgeber hat die Arbeitnehmenden, die mit dem System arbeiten, nach Bedarf über das System zu schulen. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

03 Da das System Informationen zu Kund*innen und Mitarbeiter*innen enthält, liegt ein Schwerpunkt der Compliance auf der Erfüllung datenschutzrechtlicher Vorgaben.

KI ALS STRATEGISCHE ASSISTENZ

Breuer & Sohn Maschinenbau KG | Branche: Industrielle Fertigung

Ausgangssituation:

Strategische Entscheider*innen der Firma haben Probleme, neue Ideen zu formulieren.

Ziel:

Ziel ist eine strategisch wertvolle Ideengenerierung und -bewertung.

Input:

- Inputdaten der Nutzer*innen

KI-Themenfelder:

- Natürliche Sprachverarbeitung und Large Language Models
- Computer Vision
- Generative Modelle

Vorgehen:

Das Unternehmen nutzt verschiedene generative KI-Anwendungen wie ChatGPT, Rationale KI, u. ä., um neue Ideen zu generieren und strategische Entscheidungen des Unternehmens zu unterstützen.

Zielgruppe:

Management

Interaktion mit Menschen:

Ja

Output:

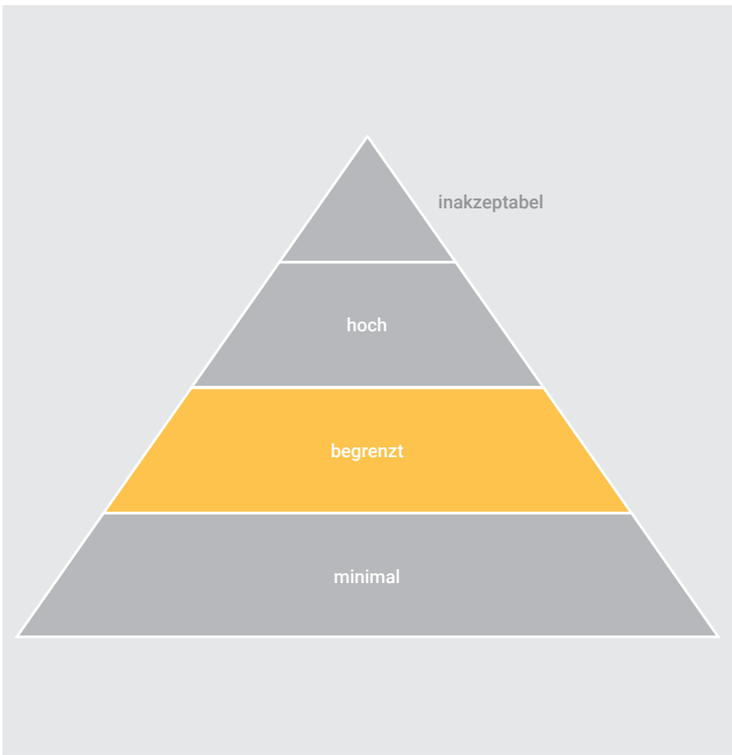
- Neue Ideen
- Vorschläge
- Bewertungen

KI-Methoden und -Technologien:

- Transformer-basierte Modelle für Textgenerierung
- **Generative Adversarial Networks** (GANs) für visuelle Inhalte
- Convolutional Neural Networks (CNNs) für Bildanalyse

Entwicklung:

- Externer Dienstleister (**SaaS**)
- Sitz: USA
- Branche: Softwareentwicklung



Fachliche Beschreibung:

Die strategischen Entscheider nutzen verschiedene GenAI-Tools, um neue Ideen zu generieren und zu bewerten. Diese Tools basieren auf fortschrittlichen KI-Modellen wie Transformer-basierten Modellen für die Textgenerierung, GANs für die Erstellung visueller Inhalte und CNNs für die Bildanalyse. Die Nutzer interagieren mit den Tools über Laptops oder Smartphones, geben ihre Anforderungen ein und erhalten Vorschläge und Bewertungen in Echtzeit.

Technische Umsetzung:

Der Benutzer greift auf die Tools via Laptop, Smartphone zu.

Risiken:

- Fehlentscheidungen durch unpassende/ unrealistische Ideen
- Gefahr der Weitergabe von vertraulichen und sensiblen Informationen des Unternehmens

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Begrenztes" Risiko/Transparenzrisiko
- Ausschlaggebender Faktor: Das KI-System interagiert mit dem Menschen.

Handlungsbedarf und Verpflichtungen:

01 Transparenzanforderungen des Art. 50 Abs. 1 KI-VO zur Information natürlicher Personen über die Interaktion mit KI treffen den Anbieter und damit nicht die Breuer & Sohn Maschinenbau KG.

02 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Der Arbeitgeber hat die Arbeitnehmenden, die mit dem System arbeiten über das System nach Bedarf zu schulen. Bei der Verwendung generativer KI spielen sowohl datenschutzrechtliche als auch urheberrechtliche Vorgaben stets eine Rolle und sind einzuhalten. Da das System bei strategischen Entscheidungen wie bspw. der Geschäftsmodell(weiter)entwicklung unterstützen soll, liegt ein Schwerpunkt der Compliance auch auf Know-How und Geheimnisschutz. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen, deren Kommunikation und Schulungen hierzu können sinnvoll sein und helfen, die Anforderungen aus der KI-VO zu erfüllen.

KI ALS SOCIAL MEDIA ASSISTENZ

Trinova Engineering GmbH | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte die Erstellung von Social Media Content effizienter und kostengünstiger gestalten und automatisieren.

Ziel:

Ziel ist die Effizienzsteigerung durch Automatisierung und Beschleunigung der Erstellung von Social Media Inhalten, eine kreative Unterstützung der Social Media Manager und zielgruppengerechte Generierung von kreativen Texten und Bildern. Zudem sollen die Kosten reduziert werden.

Zielgruppe:

Öffentlichkeitsarbeit (ÖA) Abteilungen und Social Media Manager

Input:

- Interne Marketingdaten
- Öffentliche Bilddatenbanken
- Social Media Trendanalysen
- Styleguides

KI-Themenfelder:

- Natürliche Sprachverarbeitung - Large Language Models
- Computer Vision
- Generative Modelle

Vorgehen:

Das Unternehmen setzt KI-Anwendungen zur kreativen Unterstützung bei der Generierung zielgruppengerechter Social-Media-Inhalte ein. Die Tools ermöglichen die automatisierte Erstellung von Texten und Bildern für Social Media Posts, Vorschläge für Post-Zeitpunkte, Hashtag-Generierung, Tonalitätsanpassung, Übersetzungen, und **A/B-Testing** von Inhalten.
Durch den Einsatz wird die Abhängigkeit von externen Agenturen oder internen Ressourcen reduziert und ein kostengünstigerer, aber wirkungsvoller Social-Media-Auftritt ermöglicht.

Interaktion mit Menschen:

Ja

Output:

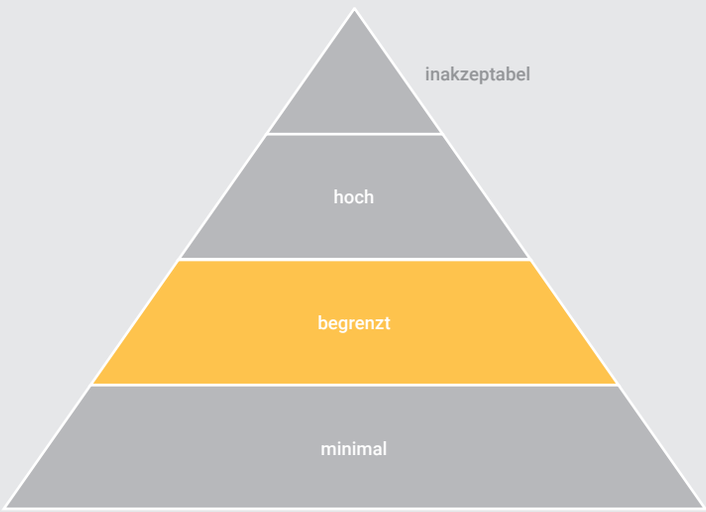
- Automatisch generierte Social Media Posts, Texte, Bilder und Vorschläge

KI-Methoden und -Technologien:

- Transformer-basierte Modelle: Textgenerierung (z.B. GPT-3)
- Generative Adversarial Networks (GANs): Generierung von Bildern/Videos,
- **Recurrent Neural Networks** (RNNs)/ Convolutional Neural Networks (CNNs): Analyse und Vorhersage von Trends/ Nutzerverhalten

Entwicklung:

- Externer Dienstleister (SaaS)
- Sitz: USA
- Branche: Softwareentwicklung



Fachliche Beschreibung:

Die Tools dienen der Erstellung und Planung von Social Media Posts, führen A/B-Tests durch. Dabei beachten sie die Einhaltung von Branding-Richtlinien und bauen Iterationen und Feedbackschleifen ein.

Technische Umsetzung:

Ein externer SaaS-Dienst mit KI-Modellen generiert Social Media Inhalte.

Risiken:

- Hohe Abhängigkeit vom Anbieter
- Generierte Inhalte könnten nicht den Markenrichtlinien entsprechen
- Monotone Inhalte
- Halluzinationen der KI
- Verletzung von Bildrechten

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Begrenztes" Risiko/Transparenzrisiko
- Ausschlaggebender Faktor: Das KI-System interagiert mit dem Menschen. Das KI-System erzeugt oder manipuliert Bild-, Ton-, oder Videoinhalte, die ein Deepfake sein können.

Handlungsbedarf und Verpflichtungen:

01 Transparenzanforderungen des Art. 50 Abs. 1 KI-VO zur Information natürlicher Personen über die Interaktion mit KI treffen den Anbieter und damit nicht die Trinova Engineering GmbH.

02 Transparenzanforderungen bestehen auch für Betreiber bei der Verwendung von Output von generativer KI. Künstlich erzeugte Bilder, bei denen es sich um Deepfakes i.S.d Art. 3 Nr. 60 KI-VO handelt, müssen nach Art. 50 KI-VO als künstlich erzeugt gekennzeichnet werden. Gleiches gilt auch für Audio- und Video-Dateien, sowie für Texte, welche über Angelegenheiten von öffentlichem Interesse informieren.

03 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Der Arbeitgeber hat die Arbeitnehmenden, die mit dem System arbeiten nach Bedarf über das System zu schulen.

Bei der Verwendung generativer KI spielen sowohl datenschutzrechtliche als auch urheberrechtliche Vorgaben stets eine Rolle und sind einzuhalten. Aus Urheberecht können sich Kennzeichnungspflichten bzw. das Unterlassen der Kennzeichnung eines Textes mit einem Autorenhinweis ergeben, wenn es sich bei dem Text um KI-generierten Inhalt handelt. Auch Unternehmensleitlinien zum Umgang mit KI-Systemen helfen, die Anforderungen aus der KI-VO zu erfüllen und die Compliance mit weiteren Regelungen und Anforderungen sicherzustellen z.B. wie und in welchem Umfang Inhalte vor Veröffentlichung zu überprüfen sind. Die Eingabe personenbezogener Daten in das SaaS-System soll verhindert werden.

WEBSITE-ENTWICKLUNG MIT KI

Hagemann Dreh- und Frästechnik GmbH | Branche: Industrielle Fertigung

Ausgangssituation:

Das Unternehmen möchte die Erstellung von Websites und Online-Shops effizienter gestalten und automatisieren.

Ziel:

Ziel ist die automatisierte Generierung von Webdesigns und Inhalten, die an individuelle Anforderungen angepasst werden können.

Input:

- Interne Datenbanken
- Produktkataloge
- Stockbilder
- Styleguides
- Designvorlagen
- Kontaktdaten von Ansprechpersonen

KI-Themenfelder:

- Natürliche Sprachverarbeitung - Large Language Models
- Computer Vision
- Generative Modelle

Vorgehen:

Das Unternehmen setzt KI-Anwendungen zur automatisierten Erstellung von HTML/CSS/JavaScript-Code, Layout-Vorschlägen, Content-Generierung (Texte, Bilder), **SEO-Optimierung** und Erweiterung der Website um Online-Shops ein. Damit kann die manuelle Entwicklungszeit von Websites reduziert werden und die Effizienz der Online-Shop-Vorgänge gesteigert werden.

Zielgruppe:

Öffentlichkeitsarbeit (ÖA) Abteilungen und Social Media Manager

Interaktion mit Menschen:

Ja

Output:

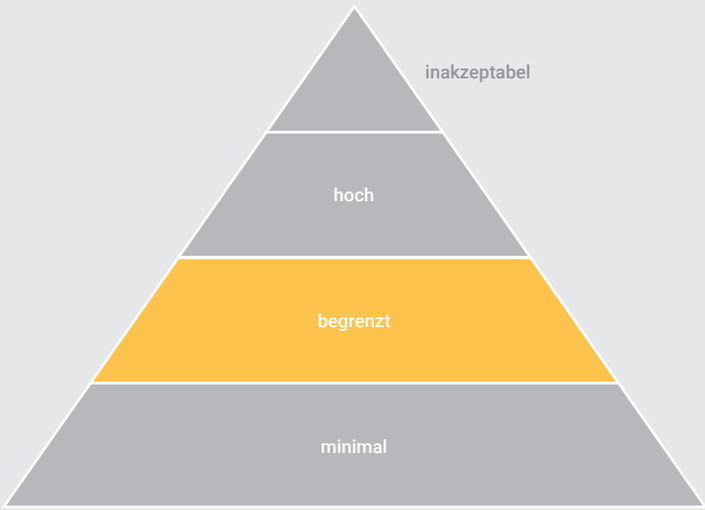
- Automatisch generierte Website/Code, Texte, Bilder und Layout-Vorschläge

KI-Methoden und -Technologien:

- Transformer-basierte Modelle für Textgenerierung
- Generative Adversarial Networks (GANs) für visuelle Inhalte
- Convolutional Neural Networks (CNNs) für Bildanalyse
- **Variational Autoencoder (VAE)** für Designvarianten

Entwicklung:

- Externer Dienstleister (SaaS)
- Sitz: USA
- Branche: Softwareentwicklung



Fachliche Beschreibung:

Die Tools dienen der Erstellung und Planung von Websites und Online-Shops mit eingebauten Iterationen und Feedbackschleifen unter Einhaltung von Design- und SEO-Richtlinien.

Technische Umsetzung:

Ein externer SaaS-Dienst generiert Websites und Online-Shops.

Risiken:

- Fehlerhafte Inhalte
- Schlechte SEO-Optimierung
- Abhängigkeit vom Anbieter
- Mögliche Stillstände des Online-Shops mit Umsatzverlusten

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Begrenztes" Risiko/Transparenzrisiko
- Ausschlaggebender Faktor: Das KI-System interagiert mit dem Menschen. Das KI-System erzeugt oder manipuliert Bild-, Ton-, oder Videoinhalte, die ein Deepfake sein können.

Handlungsbedarf und Verpflichtungen:

01 Transparenzanforderungen des Art. 50 Abs. 1 KI-VO zur Information natürlicher Personen über die Interaktion mit KI treffen den Anbieter und damit nicht die Hagemann Dreh- und Frästechnik GmbH.

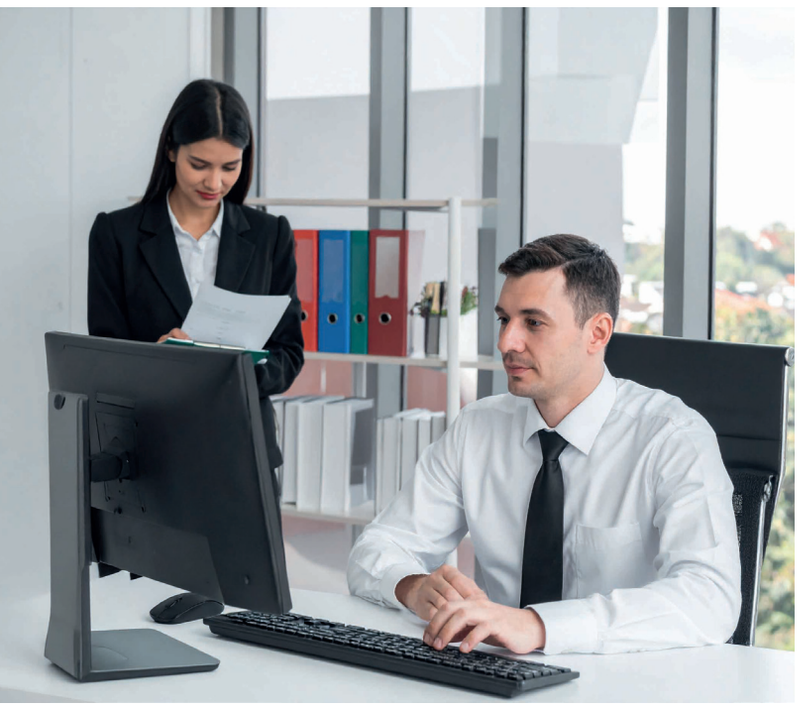
02 Die Transparenzanforderungen gelten auch für Betreiber bei der Verwendung von Output von generativer KI. Künstlich erzeugte Bilder, bei denen es sich um Deepfakes i.S.d. Art. 3 Nr. 60 KI-VO handelt, müssen nach Art. 50 KI-VO als künstlich erzeugt gekennzeichnet werden und die Transparenzverpflichtungen müssen eingehalten werden. Gleiches gilt auch für Audio- und Video-Dateien, sowie für Texte, welche über Angelegenheiten von öffentlichem Interesse informieren.

03 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Das bedeutet u.a.: Der Arbeitgeber hat die Arbeitnehmenden, die mit dem System arbeiten über das System zu schulen (Vermeidung personenbezogener Daten). Die Vorgaben der Leitlinien schließen aus, dass Anbieter eigegebene Daten zum Training der KI verwenden. Von den betroffenen Mitarbeitenden soll Einwilligung eingeholt werden. In aller Regel muss ein Datenauftragsverarbeitungsvertrag mit dem SaaS-Dienstleister abgeschlossen werden. Eine **Datenschutzfolgenabschätzung** muss durchgeführt werden. Auch urheberrechtliche Aspekte sind u.a. zu berücksichtigen.

04 Zu Haftungsfragen gilt, dass für durch Generatoren erstellte Websites, das Impressum und den Datenschutzleitlinien oft keine Haftung für die Richtigkeit und Vollständigkeit übernommen wird. Es ist daher ratsam, hierfür einen externen Datenschutzbeauftragten oder Dienstleister zu beauftragen, welche die Haftung für ihre Dienste übernehmen.

KI IM PERSONALWESEN

Schröder Bautechnik GmbH | Branche: Hochbauzulieferer, Baubranche



Ausgangssituation:

Die Personalabteilung des rapide wachsenden Unternehmens benötigt effiziente Unterstützung bei der Bearbeitung von Bewerbungen.

Ziel:

Ziel ist die Beschleunigung der Bearbeitungszeit und die Reduzierung des Workloads des Personals.

Zielgruppe:

Personalabteilung

Interaktion mit Menschen:

Ja

Input:

- Bewerbungsunterlagen
- Stellenausschreibung

KI-Themenfelder:

- Allzweck-KI
- Empfehlungssystem

Vorgehen:

Durch den Einsatz von KI-Tools wie ChatGPT und Gemini werden eingehende Lebensläufe und Anschreiben gemeinsam mit der Stellenausschreibung auf ihrer Eignung und Übereinstimmung überprüft, indem ein entsprechender Übereinstimmungswert berechnet wird, der als Empfehlungsgrundlage für die Personalabteilung genutzt werden kann. Sichtung und Analyse der Bewerbungsunterlagen werden dadurch beschleunigt und automatisiert. In der Folge kann die höhere Auftragslage der Personalabteilung besser bewältigt werden.

KI-Systeme mit hohem Risiko

Nach Anhang III der KI-VO gelten bestimmte KI-Systeme im Bereich Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit zu Hochrisiko-KI-Systemen. Dazu gehören Systeme, die für Einstellung oder Auswahl von Personen genutzt werden. Ebenfalls erfasst sind Systeme, die Entscheidungen zu Arbeitsbedingungen, Beförderungen oder Kündigungen beeinflussen, Aufgaben auf Basis persönlicher Merkmale zuweisen oder Leistung und Verhalten beobachten.

Ausnahmen bilden Systeme, die zwar in diesen Bereich fallen, aber kein Profiling vornehmen und kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte besteht. Das ist z. B. der Fall, wenn ein System das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit verbessert.

Output:

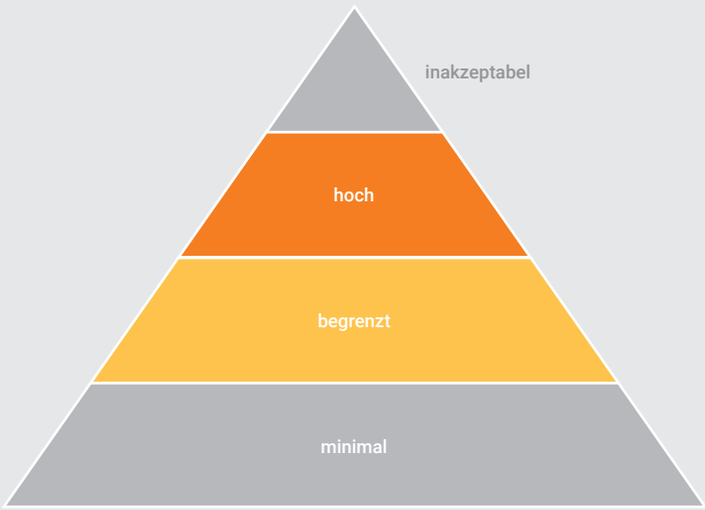
- Maßnahmen und Empfehlungen für die Personalabteilung

KI-Methoden und -Technologien:

- Multimodale Modelle wie
- Large Language Models (LLMs)
- Generative Adversarial Networks (GANs)
- Convolutional Neural Networks (CNNs) etc.

Entwicklung:

- Externer Dienstleister (SaaS)
- mehrere Bezüge von Unternehmen wie OpenAI, Google, etc.; mit Sitz in den USA
- Branche: Softwareentwicklung



Fachliche Beschreibung:

Die Tools dienen der Erstellung von Bewertungen der Bewerber*innen auf Grundlage der Stellenausschreibung. Dazu werden die Informationen aus der Bewerbung mit den Anforderungen der Stellenausschreibung durch das System verglichen und eine entsprechende Empfehlung ausgesprochen.

Technische Umsetzung:

Externe SaaS-Dienst werden genutzt, um die Inputdaten auszuwerten und eine Empfehlung auszusprechen.

Risiken:

- Fehleinschätzungen
- Datenschutzrechtliche Probleme

Einstufung nach KI-Verordnung:

- Rolle: Betreiber
- Risikoklasse: „Hohes" Risiko und „Begrenztes" Risiko (Transparenzpflichten betreffen den Anbieter)
- Das KI-System sichtet und filtert Bewerbungen und bewertet Bewerber*innen. Das KI-System interagiert mit dem Menschen.

Handlungsbedarf und Verpflichtungen:

01 Transparenzanforderungen des Art. 50 Abs. 1 KI-VO zur Information natürlicher Personen über die Interaktion mit KI treffen den Anbieter und damit nicht die Schröder Bautechnik GmbH.

02 Den Betreiber von Hochrisiko-KI-Systemen treffen einige spezifische Verpflichtungen (Art. 26 KI-VO). U.a.:

- Durchführung der Datenschutzfolgenabschätzung
- Treffen geeigneter Maßnahmen bzgl. der ordnungsgemäßen Verwendung
- Übertragen der menschlichen Aufsicht an eine kompetente Person
- Verantwortung für die Eingabedaten (hinsichtlich der Übereinstimmung mit der Zweckbestimmung/Gebrauchsanweisung des KI-Systems, Repräsentativität etc.)
- Überwachung des Betriebs; z.B.: Aufbewahrung automatisch erzeugter Protokolle (i.d.R. 6 Monate)
- Informationspflichten bzgl. der Verwendung des Hochrisiko-KI-Systems ggü. der Arbeitnehmervertretung und Arbeitnehmenden

03 Die Anforderungen an den Aufbau von KI-Kompetenz (Art. 4 KI-VO) im Unternehmen gelten. Der Arbeitgeber hat die Arbeitnehmer, die mit dem System arbeiten nach Bedarf über das System zu schulen. In unternehmensinternen Leilinien sollten Vorgaben für den Einsatz des KI-Systems und die Überwachung seines Betriebs formuliert werden.

04 Im vorliegenden Fall sind neben den Anforderungen der KI-VO umfangreiche datenschutzrechtliche Vorgaben zu erfüllen.

3. VERBOTENE SYSTEME

Verboten sind KI-Systeme, die mit den Werten der EU nicht vereinbar sind. Das ist der Fall, wenn die Menschenwürde nicht geachtet wird oder die KI inakzeptable Risiken für Freiheit, Gleichheit, Demokratie und Rechtsstaatlichkeit sowie die in der Charta der Menschenrechte verankerten Grundrechte birgt. Zu der in der Charta aufgelisteten Grundrechte zählen u.a. das Recht auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie Rechte des Kindes.

In Artikel 5 listet die KI-VO eine Reihe verbotener KI-Praktiken auf. Hierzu zählen:

01 Unterschwellige Beeinflussung oder absichtliche Manipulation oder Täuschung (z.B. Einsatz von **„Dark Pattern"**)

02 Missbräuchliche Ausnutzung von Vulnerabilität oder Schutzbedürftigkeit (Alter, Behinderung, soziale oder wirtschaftliche Situation)

03 Social Scoring

04 Individuelle Risikobewertung und Vorhersage von Straftaten (allein auf Grundlage von Profilen oder Persönlichkeitsmerkmalen)

05 Erstellen/Erweitern von Gesichtserkennungsdatenbanken durch gezieltes Auslesen von Gesichtsbildern aus dem Internet oder über Überwachungsaufnahmen

06 Emotionserkennung (am Arbeitsplatz oder in Bildungseinrichtungen; Ausnahme medizinische Gründe oder Sicherheitsgründe)

07 Biometrische Kategorisierung (Rückschlüsse auf Ethnie, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugung, Sexualleben; Ausnahme: Filterung rechtmäßig erworbener biometrischer Datensätze)

08 Biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken.

Neben diesen in der KI-VO genannten verbotenen KI-Praktiken können bestimmte KI-Anwendungen auch ohne Nennung in der KI-VO nach anderen Gesetzen verboten sein und bleiben. Verbote können sich etwa weiterhin auch aus Datenschutzrecht oder Verbraucherschutzrecht ergeben. Grundsätzlich ist festzuhalten, dass Verhaltensweisen, die ohne KI-Einsatz verboten sind, es auch mit KI-Einsatz bleiben.

4. SCHLUSSFOLGERUNG

Der Einsatz von KI-Systemen bietet auch für KMU zahlreiche Chancen, Arbeitsprozesse effektiver und kostengünstiger zu gestalten. Jedoch erfordert jeder Einsatz von IT-Technologie im Unternehmen die Einhaltung rechtlicher Anforderungen, auch produktsicherheitsrechtlicher. Dies gilt umso mehr für innovative KI-Lösungen, an welche mit der KI-Verordnung spezifische Anforderungen bestehen.

Die Analyse und Einordnung der für KMU repräsentativen Use Cases zeigt, dass die überwiegende Anzahl dieser KI-Anwendungen in der Regel nicht in hohe Risikoklassen der KI-Verordnung einzuordnen ist. Dies hat zur Folge, dass die damit verbundenen rechtlichen Anforderungen überschaubar und weniger komplex sind. Allerdings verbieten sich pauschale Aussagen bezogen auf „Systeme für KMU". Wie aus den aufgeführten Anwendungsfällen deutlich wird, ist insbesondere der Einsatzzweck ausschlaggebend für die Bestimmung der Risikoklasse. So kann der Einsatz eines Systems im Bereich „Human Resources" zu der Einstufung in die Kategorie des „hohen Risikos" führen.

> ***Für jedes System und für jede geplante Art der Verwendung muss daher die Analyse und Einordnung immer gesondert erfolgen.***

Neben der zumeist niedrigeren Risikoklasseneinstufung von in KMU verwendeten Systemen agieren KMU in den meisten Fällen als Betreiber von KI-Anwendungen (siehe rechtliche Bewertung der Rolle der repräsentativen Use Cases). Die Hauptverantwortung für die Einhaltung der produktsicherheitsrechtlichen Vorgaben der KI-Verordnung bezieht sich jedoch auf die Entwicklung der Systeme und liegt hiermit bei den Anbietern. Allerdings gehen die bei KMU am häufigsten auftretenden Anwendungsfälle auch für diese mit einem überschaubaren administrativen und rechtlichem Aufwand einher.

Dennoch bleibt es wichtig, sich der eigenen Verantwortung bewusst zu sein und sicherzustellen, dass die genutzten Anwendungen den grundlegenden rechtlichen Standards entsprechen. Durch eine klare Abgrenzung der Verantwortlichkeiten und eine bewusste Auswahl vertrauenswürdiger Anbieter können KMU den Einsatz von KI-Systemen effizient und rechtssicher gestalten.

Ein zentraler Schwerpunkt der Verwendung von KI-Anwendungen im KMU liegt auf dem Aufbau von KI-Kompetenz, wie in der Zusammenstellung der rechtlichen Anforderungen im Rahmen der Einordnung der Systeme in die Risikoklassen gezeigt wurde. Es ist essenziell, das notwendige Wissen und die Fähigkeiten im Unternehmen zu etablieren, um die verwendeten KI-Anwendungen effektiv und verantwortungsvoll zu betreiben. Dies umfasst nicht nur technische Kompetenzen, sondern auch ein fundiertes Verständnis der rechtlichen Rahmenbedingungen, die den Einsatz solcher Technologien leiten.

Es ist festzuhalten, dass die rechtlichen Anforderungen zwar einheitlichen Prinzipien folgen, jedoch in ihrer konkreten Ausgestaltung variieren können. Betreiber müssen sich bewusst sein, dass selbst innerhalb derselben Risikoklasse Unterschiede existieren können, die sich aus spezifischen Anwendungsbereichen oder den technischen Eigenschaften der jeweiligen KI-Lösung ergeben. Neben der Einhaltung allgemeiner Vorgaben kommt es darauf an, branchenspezifische Besonderheiten und eventuell

zusätzliche regulatorische Anforderungen zu berücksichtigen. Dies kann bedeuten, dass für bestimmte Anwendungen ergänzende Maßnahmen erforderlich sind. Einen entscheidenden Aspekt bezüglich datengetriebener KI-Anwendungen kann im Fall der Verarbeitung personenbezogener Daten der Datenschutz darstellen. Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) bleibt eine unverzichtbare Grundlage, unabhängig von der Risikoklasse der eingesetzten KI-Anwendung nach der KI-Verordnung. Daneben könnten branchenspezifische Regelungen, arbeitsrechtliche Bestimmungen oder Vorgaben zum Verbraucherschutz die Verwendung von KI im Betrieb ergänzend regeln.

> ***Eine umfassende rechtliche Prüfung und gegebenenfalls die Konsultation von Fachanwälten können daher sinnvoll sein, um sicherzustellen, dass alle relevanten Vorschriften beachtet werden.***

Insgesamt bleibt die strategische Herangehensweise damit unverzichtbar, um sowohl den allgemeinen als auch den spezifischen Anforderungen innerhalb der Risikoklasse gerecht zu werden und die Grundlage für eine verantwortungsvolle und rechtskonforme Nutzung von KI-Systemen zu schaffen.

Zusammenfassend lässt sich sagen, dass die rechtlichen Anforderungen für den Einsatz von KI-Systemen mit minimalem Risiko für KMU zwar überschaubar sind, aber dennoch eine strategische Herangehensweise erfordern.

> ***Der Aufbau von KI-Kompetenzen, die konsequente Beachtung des Datenschutzes und die Berücksichtigung weiterer rechtlicher Rahmenbedingungen sind wesentliche Bausteine für einen erfolgreichen und rechtskonformen Einsatz von KI.***

Indem KMU diese Aspekte aktiv adressieren, können sie rechtliche Risiken minimieren und ihre Innovationskraft durch Nutzung von KI stärken.

WEITERFÜHRENDE INFORMATIONEN

Für weiterführende Informationen und den direkten Zugang zum Gesetzestext finden Sie im Folgenden einige Links, die für den Umgang mit der KI-VO im Unternehmen hilfreich sein können.

OFFIZIELLE QUELLEN

- **Die KI-VO –** Offizielle Quelle der finalen KI-VO in diversen Sprachen. Veröffentlicht von der Europäischen Union unter eur-lex.europa ↗.
- **Hinweispapier der BNetzA.** bundesnetzagentur.de ↗.
- **Veröffentlichte Leitlinien und Materialien (Mai 2025) –** "Leitlinien für verbotene KI". Veröffentlicht digital-strategy.ec ↗.
- **EU-Leitlinien zur Definition von KI-Systemen.** Veröffentlicht von der Europäischen Kommission unter digital-strategy.ec ↗.
- **Antworten auf häufig gestellte Fragen.** Veröffentlicht von der Europäischen Kommission unter digital-strategy.ec ↗.
- **Erklärung und Überblick zur KI-VO.** Veröffentlicht vom Europäischen Rat unter consilium.europa ↗.
- **KI-Compliance Kompass der Bundesnetzagentur.** Veröffentlicht unter bundesnetzagentur.de ↗.
- **Europäisches KI-Büro der Europäischen Union.** Veröffentlicht unter digital-strategy.ec ↗.
- **Der AI Pact –** Initiative zur praktischen Umsetzung der KI-VO, an der sich außer- und innereuropäische Unternehmen beteiligen können. Veröffentlicht unter digital-strategy.ec ↗.
- **KI-Service-Desk.** Veröffentlicht von der Bundesnetzagentur unter bnetza.de/ki ↗

INOFFIZIELLE VERSIONEN DES GESETZESTEXTES

- **KI-VO mit interaktivem Inhaltsverzeichnis auf Deutsch und Englisch.** Veröffentlicht von Intersoft Consulting unter ai-act-law.eu.↗
- **KI-VO mit interaktivem Inhaltsverzeichnis in mehreren Sprachen.** Veröffentlicht vom Future of Life Institute unterartificialintelligenceact.eu. ↗

SONSTIGE INFORMATIONEN UND TOOLS

- **Speziell trainierte Chatbots –** KI-basierte Chatbots, die Fragen zur KI-VO beantworten.

  - **“ISMS” –** Veröffentlicht von BETTER ISMS und abrufbar unter ismscopilot.com ↗.

  oder

  - **“CustomGPT” –** Veröffentlicht von open AI und abrufbar unter chatgpt.com ↗.

KI-REGULIERUNG AUSSERHALB DER EU

Die Europäische Union hat mit ihrer KI-Verordnung weltweit das erste Gesetz zur Regulierung des Umgangs mit Künstlicher Intelligenz geschaffen. Auch in anderen Staaten wird an Entwürfen für Richtlinien und Gesetze gearbeitet.

- AI Watch: Global regulatory tracker – Übersicht über außereuropäische KI-Regelungen. Veröffentlicht von White & Case LLP unter whitecase.com ↗. Offizielle Beispiele

  - Das Vereinigte Königreich entwickelt einen prinzipienbasierten Rahmen, anhand derer bestimmte Behörden für ihre jeweiligen Sektoren Regelungen aufbauen können. Veröffentlicht unter europarl.europa ↗.

  - Die USA setzen mehr auf Freiwilligkeit, um in hohem Maße Innovationen zu fördern. Neben diversen weiteren offiziellen Institutionen hat das National Institute of Standards and Technology eine Richtlinie herausgegeben, die Unternehmen bei einem verantwortungsvollen Umgang mit KI unterstützen soll. Veröffentlicht unter nist.gov ↗.

  - China verfolgt mit den sehr spezifischen Vorschriften der „Interim Measures for the Management of Generative AI Services“ einen hierarchisch kontrollierten Ansatz. Veröffentlicht auf Chinesisch unter cac.gov ↗.

GLOSSAR

A/B-Testing	Methode zum systematischen Vergleich zweier Systemvarianten, der Originalversion und der modifizierten Version
Allzweck-KI	Systeme, die mehreren verschiedenen Zwecken und unterschiedlichen Kontexten dienen und sogar in andere KI-Systeme integriert werden können (engl.: General Purpose AI)
Anomalieerkennung	Erkennung von unerwarteten / ungewollten Abweichungen von Datenverhalten in einem System, sogenannte Inkonsistenzen
Cloudbasierte Anwendungen	Systeme, die nicht auf eigenen Rechnern installiert sind, sondern über Server in Rechenzentren ("Cloud"), beispielsweise eines externen Dienstleisters, laufen
Computer Vision	Bereich der KI, bei dem Computer die Fähigkeit besitzen, Bilder und Videos zu sehen und auszuwerten
Convolutional Neural Networks (CNNs)	künstliches neuronales Netz, was im Rahmen der Computer Vision Bilder und Videos analysieren kann
Dark Patterns	Design-Elemente, deren Ziel es ist, Menschen zu einem bestimmten Verhalten zu bewegen, was insbesondere dem Anbieter nützt
Datenschutzfolgenabschätzung	Vorausschau, die prüft, ob neue Technologien oder Projekte ein Risiko für die Privatsphäre von Menschen und ihre persönlichen Daten darstellen könnten
Dialogorientierte KI	KI-gestützte Anwendungen, die per Text oder Sprache Konversationen führen können (engl.: Conversational AI)
Empfehlungssystem	System, was personalisierte Empfehlungen für die Anwender*innen generiert (engl.: Recommender System)
Fine-Tuning	bezeichnet das gezielte Anpassen eines bestehenden KI-Modells an spezielle Anforderungen oder Datensätze, um die Leistung in einem bestimmten Anwendungsbereich zu verbessern
Generative Adversarial Networks (GANs)	Netzwerk, das aus zwei neuralen Netzen besteht, die gegeneinander ("adversarial") trainiert werden: einem Generator, der neue Daten wie Bilder erzeugt, und einem Diskriminator, der die Echtheit dieser Daten bewertet
Generative KI	KI, die mithilfe von neuronalen Netzwerken und erlernten Mustern eigenständig neue Inhalte wie Texte, Bilder oder Musik erzeugen kann

Large Language Models	KIs, die mithilfe von Textdaten trainiert werden, um menschliche Sprache zu verstehen und nachzuahmen bzw. Texte zu lesen und zu generieren
Long Short-Term Memory (LSTMs)	RNNs, die insbesondere sequenzielle Daten analysieren und langfristige Abhängigkeiten erkennen können
Machine-Learning-Algorithmen	Algorithmen, die auf dem Prinzip des maschinellen Lernens basieren, also aus Daten lernen und darauf basierend Vorhersagen treffen können
Manufacturing Execution System (MES)-System	System, das in der industriellen Fertigung angewandt wird, um die Produktion zu planen und zu steuern
Metaheuristiken	algorithmische Näherungslösungen zu komplexen Optimierungsproblemen / Aufgaben
Natürliche Sprachverarbeitung (NLP)	Bereich der KI, der sich mit der Verarbeitung und Analyse von menschlicher Sprache befasst (engl.: Natural Language Processing)
Neuronale Netze	künstliche, mathematische Modelle, die die Funktionsweise des menschlichen Hirns nachahmen, zum Beispiel Mustererkennung oder Vorhersage
On Premise	Systeme, die auf eigenen Rechnern und Servern installiert und betrieben werden
Open Source	Softwares, die frei zugänglich und deren Quellcodes bearbeitbar sind, meist kostenlos
Open Source nach KI-Verordnung	frei verfügbare und kostenlose Software oder KI-Modelle, deren Nutzung, Änderung und Weiterverbreitung erlaubt ist. Es bedarf der Offenlegung von Parametern und Architektur unter Nennung des Anbieters und Einhaltung vergleichbarer Lizenzbedingungen **(Vgl. hierzu Erwägungsgrund 102 und 103 der KI-Verordnung)**

Erwägungsgründe der KI-Verordnung

Die Erwägungsgründe der KI-Verordnung sind rechtlich nicht unmittelbar verbindliche, aber dennoch sehr wichtige Abschnitte im Gesetzestext. Sie stehen am Anfang der Verordnung und dienen dazu, die Ziele, Hintergründe und Absichten des Gesetzgebers zu erläutern. Erwägungsgrund 102 und 103 setzen sich genauer mit Open-Source-Modellen auseinander. Erwägungsgrund 102 betont, dass KI-Modelle mit allgemeinem Verwendungszweck aus Transparenzgründen unter kostenloser, quelloffener Lizenz veröffentlicht werden können. Erwägungsgrund 103 spezifiziert anschließend, was als freie und quelloffene KI-Komponente gilt.

Predictive Analytics	analytische Verfahren zum Treffen einer Vorhersage
Random Forests	Maschinelles Lernverfahren, das mehrere unterschiedliche Entscheidungsbäume zum Treffen von Vorhersagen nutzt. Jeder Baum trifft eine Entscheidung, am Ende wird die Mehrheitsentscheidung aller Bäume als Ergebnis verwendet
Rechenleistung	bezeichnet die Fähigkeit eines Computers oder eines technischen Systems, Daten zu verarbeiten und Berechnungen innerhalb einer bestimmten Zeit durchzuführen
Recurrent Neural Network (RNNs)	künstliche neuronale Netze, die Zusammenhänge in der Auswertung sequenzieller Daten erkennen können
Retrieval-Augmented Generation (RAG)	Teilbereich der natürlichen Sprachverarbeitung, bei der ein Modell zusätzlich Information aus Datenbänken abruft (Retrieval), um einen Output zu generieren
Search Engine Optimization (SEO)-Richtlinien	Sammlung von Handlungsempfehlungen, die darauf abzielen, eine Website so zu optimieren, dass sie in Suchmaschinen besser / sichtbarer platziert wird
Software as a Service (SaaS)	cloudbasiertes Software-Modell, in dem die Software als Dienstleistung angeboten wird
überwachtes Lernen (Supervised Learning)	KI-Modell, das mit gelabelten Daten trainiert wird; sowohl die Eingabedaten als auch die richtigen Ausgabendaten sind bekannt (engl.: Supervised Learning)
unüberwachtes Lernen (Unsupervised Learning)	KI-Modell, das mit ungelabelten Daten trainiert wird, wobei es keine vorgegebenen Ausgaben gibt, und das Modell selbst Muster oder Strukturen in den Daten erkennen muss (engl.: Unsupervised Learning)
Use Case	beschreibt eine konkrete Situation, in der beispielsweise ein KI-System eingesetzt wird, um aufzuzeigen inwiefern es ein Problem lösen kann, und welche spezifischen Folgen einhergehen (deutsch: Anwendungsfall)
Variational Autoencoder (VAE)	generative Modelle, die im maschinellen Lernen verwendet werden, um Variationen der Eingabedaten, mit denen sie trainiert wurden, zu generieren
verstärkendes Lernen	Bereich des Machine-Learning, in dem ein Programm lernt, wie es richtige Entscheidungen trifft mithilfe eines Bestrafungs- und Belohnungssystem (engl.: Reinforcement Learning)
Wearables	tragbare Geräte oder Kleidung, die mit Sensoren ausgestattet sind

Dank

Wir bedanken uns bei allen KI-Trainer*innen der Mittelstand-Digital Zentren sowie allen Teilnehmenden der AG Künstliche Intelligenz und dem Forum Recht von Mittelstand-Digital, die bei der inhaltlichen Gestaltung der Publikation mitgewirkt haben:

Enes Alp	Mittelstand-Digital Zentrum Ländliche Regionen
Stefanie Baade	Mittelstand-Digital Zentrum Franken
Stephan Blank	Mittelstand-Digital Zentrum Handwerk
Kristina Bodrožić-Brnić	Mittelstand-Digital Zentrum Fokus Mensch
Robert Falkenstein	Mittelstand-Digital Zentrum Handwerk
Susanne Fischer	Mittelstand-Digital Zentrum Rostock
Dagmar Gesmann-Nuissl	Mittelstand-Digital Zentrum Chemnitz
Steffen Gießmann	Mittelstand-Digital Zentrum Handwerk
Hannah Japp	Mittelstand-Digital Zentrum Franken
Frederic Kerber	Mittelstand-Digital Zentrum Handel
Natalja Kleiner	Mittelstand-Digital Zentrum Klima.Neutral.Digital
Heiko Matheis	Mittelstand-Digital Zentrum Smarte Kreisläufe
Michael Rätze	Mittelstand-Digital Zentrum Chemnitz
Sarah Rübel	Mittelstand-Digital Zentrum Kaiserslautern
Martina Schneller	Mittelstand-Digital Zentrum Handwerk
Sina Scholz	Mittelstand-Digital Zentrum Schleswig-Holstein
Marc Schubhan	Mittelstand-Digital Zentrum Handel
André Stöhr	Mittelstand-Digital Zentrum Leipzig-Halle
Ines Tacke	Mittelstand-Digital Zentrum Chemnitz
Larissa Theis	Mittelstand-Digital Zentrum Kaiserslautern

IMPRESSUM

HERAUSGEBER:
Technologie-Initiative SmartFactory KL e. V.
Trippstadter Str. 122
67663 Kaiserslautern
Tel.: 0631 343 773 10
Vorsitzender:
Prof. Dr. Martin Ruskowski
Vereinsregisternummer: VR 2458 Kai

IN KOOPERATION MIT:
Mittelstand-Digital Zentrum Kaiserslautern
c/o Technologie-Initiative SmartFactory KL e. V.
Trippstadter Straße 122
67663 Kaiserslautern
Verantwortlich: Jonas Metzger

Deutsches Forschungszentrum
für Künstliche Intelligenz GmbH (DFKI)
Trippstadter Str. 122
67663 Kaiserslautern
Geschäftsführung:
Prof. Dr. Antonio Krüger (Vorsitzender)
Helmut Ditzer
Amtsgericht Kaiserslautern, HRB 2313

MIT UNTERSTÜTZUNG VON:
Mittelstand-Digital Zentrum Chemnitz
c/o Technische Universität Chemnitz
09107 Chemnitz
Verantwortlich: Prof. Dr. Gesmann-Nuissl

REDAKTION:
Sarah Rübel, Larissa Theis, Lena Rauber
Gestaltung: Andrea Bräuning
Bildnachweis: freepik, flaticon, Adobe Firefly

Mittelstand-Digital

Die Mittelstand-Digital Zentren gehören zu Mittelstand-Digital.
Mittelstand-Digital gibt kleinen und mittleren Unternehmen sowie dem Handwerk Orientierung bei der digitalen Transformation und informiert über die Chancen und Herausforderungen der Digitalisierung. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote. Kleine und mittlere Unternehmen profitieren dabei von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Die in den Zentren angesiedelten KI-Trainerinnen und -Trainer bieten zudem besondere Unterstützung bei allen Fragen zum Einsatz Künstlicher Intelligenz – vom Einsteiger bis hin zu erfahrenen Anwenderinnen und Anwendern.

Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Stand: 01.07.2025