WIRTSCHAFTSKAMMERN ÖSTERREICHS

KI-GUIDELINES FÜR KMU

3. Auflage, April 2026

Inhaltsverzeichnis

Vorwort 4
Was ist KI? 6
Bedeutung für Unternehmen 6
Welche praxisnahen Anwendungsfelder gibt es bereits? 7
Tipps für Unternehmerinnen und Unternehmer 10
Richtlinien für Mitarbeitende 14
Rahmenbedingungen zur Nutzung schaffen 14
Grenzen von KI – der Mensch als wichtigste Instanz 16
Kundenbezogene Daten und KI 17
Unternehmensbezogene Daten und Geheimhaltung 19
KI und rechtliche Rahmenbedingungen 20
Sicherheit und Qualität von Daten 22
Ethik. Vielfalt. Inklusion 23
Transparenz und Kennzeichnungen 24
Schulungen und Weiterbildungen 25
KI-generierte externe Kommunikation 27
Gastbeitrag der KI-Servicestelle 28
Rechtliche Rahmenbedingungen und Unterstützung durch die KI-Servicestelle 28
Die Rollen im AI Act 29
Verbotene KI und Hochrisiko-KI 30
GPAI-Modelle 31
Transparenzpflichten bei KI-Inhalten 32
KI-Kompetenz 33
KI-Servicestelle der RTR 34
Entwicklung und Integration von KI-Systemen 35
Prompt Engineering 35
Retrieval Augmented Generation (RAG) 37
Vorteile für Ihr Unternehmen 38
KI-Agenten: Der nächste Schritt 38
Was geht darüber hinaus? 39
Erfolgreich starten: Praktische Empfehlungen 39
ROI ermitteln 40

Kontinuierliche Optimierung..... 40
Vom Piloten zur Produktion..... 40

Dies ist nur eine für den Ausdruck optimierte Gesamtversion unserer KI-Guidelines. Die barrierefreie und möglicherweise aktualisierte Version findet sich unter KI-Guidelines für KMU - Niederösterreich - WKO
Nutzen sie auch unser Formular zur Generierung ihrer eigenen KI-Guidelines für ihre Mitarbeiter! Online unter KI-Guidelines: Nutzen für Ihr Unternehmen - WKO.

VORWORT

Noch vor zwei bis drei Jahren war der Einsatz von künstlicher Intelligenz im unternehmerischen Alltag futuristisch und kaum vorstellbar. Heute ist die Situation eine völlig andere: KI ist nicht mehr „auf dem Vormarsch", sie ist bereits da. Dabei vermischen sich die private und die berufliche Nutzung von KI-Anwendungen zunehmend.

Die Entwicklung schreitet weiter voran: Neben textbasierten Assistenten können KI-Systeme inzwischen auch Bilder, Videos und Audio verarbeiten und erstellen. Autonome KI-Agenten übernehmen immer komplexere Aufgaben. Einerseits versuchen immer mehr Unternehmen, die Chancen dieser neuen Systeme zu nutzen. Gerade für kleine und mittlere Unternehmen bieten KI-Anwendungen zahlreiche Möglichkeiten, beispielsweise zur Effizienzsteigerung, Kostensenkung, zum Datenmanagement oder zur Verbesserung der Interaktion mit Kundinnen und Kunden.

Die konkreten Einsatzmöglichkeiten variieren je nach Branche – von Textverarbeitung über Bildanalyse bis hin zur Prozessautomatisierung. Andererseits gibt es aber auch Unternehmen, die aus Sorge vor möglichen Problemen die Nutzung generativer KI-Dienste wie ChatGPT, Claude, Gemini oder Microsoft Copilot durch ihre Mitarbeitenden am Arbeitsplatz einschränken oder sogar ganz verbieten.

Die WKO unterstützt Unternehmen dabei, das Potenzial von KI-Anwendungen für den eigenen Betrieb zu entdecken und fit für die Nutzung der Schlüsseltechnologie der kommenden Jahrzehnte zu werden. Das sichert den Erfolg ihres Betriebes und den Wirtschaftsstandort Österreich auf Dauer.

Aus diesem Grund hat die WKO diesen Leitfaden entwickelt und nun aktualisiert, der Unternehmen bei der Nutzung und Integration von KI-Anwendungen unterstützt und wichtige Aspekte des Einsatzes einfach erklären soll.

Ziele der KI-Guidelines

- Bereitstellung von Orientierungshilfen und Ratschlägen im Umgang mit KI
- Schaffung klarer Rahmenbedingungen für die Geschäftsführung und Mitarbeitenden
- Bereitstellung eines Fundaments für die Integration und strategische Planung
- Hervorhebung der Vorteile und Anleitung zur optimalen Nutzung von KI-Anwendungen

- Identifikation potenzieller Gefahren und Anleitung zur Umsetzung von Schutzmaßnahmen
- Aufbau von Vertrauen durch Leitlinien, sowohl nach innen als auch nach außen
- Unterstützung bei der Einhaltung rechtlicher Vorgaben (AI Act)

Künstliche Intelligenz, die darauf basierenden Anwendungen und Services sowie die rechtlichen Rahmenbedingungen dieser neuen Technologie unterliegen einem stetigen Wandel. Mit dem Artificial Intelligence Act (AI Act) der Europäischen Union trat das weltweit erste Gesetz in Kraft, das den Einsatz von KI-Systemen regelt. Dieses geht auf die konkreten Gefahren ein, die von KI ausgehen können, und reguliert den Einsatz risikoorientiert. Die Bestimmungen des AI Acts werden schrittweise zwischen Februar 2025 und August 2027 anwendbar. Für KMU besonders relevant dabei: Verbote bestimmter KI-Praktiken bereits ab Februar 2025, Hochrisiko-KI-Systeme ab August 2026.

Schon morgen können neue Anwendungen gänzlich neue Nutzungsformen ermöglichen und auch neue Richtlinien erfordern. Daher sind die vorliegenden Guidelines als „Work in progress" zu betrachten – die jeweils aktuelle Version finden Sie online unter **www.wko.at/ki**. Für Feedback und Anregungen sind wir dankbar. Bitte wenden Sie sich dazu an das Expertenteam vom E-Center der WKÖ: **ecenter@wko.at**

Wir bedanken uns bei der KI-Servicestelle der RTR (Rundfunk und Telekom Regulierungs-GmbH), die in einem Gastbeitrag die neuen rechtlichen Rahmenbedingungen erklärt, sowie bei Bernhard Landrichter (GesetzeFinden.at) für seinen Input zur Entwicklung von KI-Systemen im Unternehmen.

WAS IST KI?

Künstliche Intelligenz (KI) imitiert menschliches Denken, Lernen und Verhalten. Moderne KI-Systeme sind zunehmend multimodal, das heißt, sie können Text, Bilder, Audio und Video gleichzeitig verarbeiten und erstellen. KI kann damit ein breites Aufgabenspektrum übernehmen – von der Ausführung einfacher Befehle über das selbstständige Treffen von Entscheidungen bis hin zur komplexen Datenverarbeitung. Einsatzgebiete gibt es in den unterschiedlichsten Branchen: im Gesundheitswesen, in der Automobilindustrie, der Telekommunikation, im Einzelhandel, in der Gastronomie, im Tourismus und vielen mehr.

Die Entwicklung schreitet rasant voran: Neue Modelle und Funktionen erscheinen im Monatsrhythmus, weshalb kontinuierliche Weiterbildung erforderlich ist. Deshalb wird es für uns alle immer wichtiger, sich mit KI vertraut zu machen, um für die aufkommenden Chancen und Herausforderungen bereit zu sein.

Bedeutung für Unternehmen

Größere Unternehmen gehen die Verwendung von KI-Anwendungen meist offensiv an. Es werden Arbeitsgruppen oder sogar ganze Abteilungen eingerichtet, um die Möglichkeiten für das Unternehmen auszuloten. Doch auch kleine Betriebe können von KI profitieren und ihr Potenzial ausschöpfen. Im Umgang mit künstlicher Intelligenz ist es daher wichtig, einerseits die sich bietenden Chancen zu erkennen und andererseits auch mögliche Risiken abzuwägen.

„Der Aufstieg einer leistungsstarken KI wird entweder das Beste oder das Schlimmste sein, was der Menschheit je widerfahren ist."
Stephen Hawking, Physiker († 2018)

Chancen	Risiken
Verbesserte Personalisierung und Betreuung von Kundinnen und Kunden	Datenschutz- und Sicherheitsbedenken
Effizienzsteigerung und Kostenreduktion	Abhängigkeit von Technologie und anbietenden Unternehmen

Chancen	Risiken
Wissens- und Kompetenzerweiterung im Team	Aufwand im Schulungsbedarf
Automatisierung von wiederkehrenden Aufgaben, Fokus auf das Kerngeschäft	Veränderung der Arbeit und Tätigkeitsbereiche der Beschäftigten
Innovationspotenzial und Wettbewerbsvorteil	Ethik und rechtliche Herausforderungen
Skalierbarkeit und schnelle Reaktion auf Trends	Schwierigkeiten bei der Integration in bestehende Systeme und Prozesse
Vorhersage und Prävention von Problemen, datenbasierte Entscheidungsfindung	Qualität und Verlässlichkeit der KI-Algorithmen
Unterstützung bei kreativen Prozessen und Ideenfindung	Fehlinformationen und "Halluzinationen" durch KI-generierte Inhalte
Aufwertung der Tätigkeitsbereiche der Beschäftigten	Verdichtung des Leistungsdrucks, Überforderung von Beschäftigten bei der Weiterqualifizierung
24/7-Verfügbarkeit ohne zusätzliche Personalkosten	Mögliche Vorurteile und Diskriminierung durch trainierte Daten
Mehrsprachigkeit und globale Erreichbarkeit ohne erhebliche zusätzliche Ressourcen	Mangelnde Nachvollziehbarkeit von KI-Entscheidungen („Black Box")
Kostengünstigerer Zugang zu Expertise und Spezialwissen	Hoher Energieverbrauch und Umweltauswirkungen großer KI-Modelle

Welche praxisnahen Anwendungsfelder gibt es bereits?

Hinweis: Viele moderne KI-Systeme kombinieren bereits mehrere Fähigkeiten. KI-Tools reichen von kostenlosen bis zu umfangreichen Enterprise-Lösungen – viele bieten Freemium-Modelle für den Einstieg.

- **Chatbots & Konversation:** KI kann menschenähnliche Konversationen führen und im Servicebereich oder für Informationsdienste eingesetzt werden (z.B. ChatGPT https://chatgpt.com/, Google Gemini https://gemini.google.com, Claude https://claude.ai, Microsoft Copilot https://copilot.microsoft.com)
  Textproduktion: KI kann eigenständig Texte in verschiedensten Sprachen und Tonalitäten schreiben bzw. umformulieren (z.B. https://chatgpt.com, Google Gemini https://gemini.google.com, Claude https://claude.ai,)
- **Textbearbeitung:** KI kann Texte bearbeiten, korrigieren und optimieren (z.B. DeepL Write https://www.deepl.com/de/write, Grammarly https://www.grammarly.com, LanguageTool https://languagetool.org/de)
- **Übersetzungen:** KI übersetzt einzelne Passagen oder ganze Dokumente in hunderte Sprachen (z.B. DeepL Translate https://languagetool.org/de, Google Translate https://translate.google.com)
- **Bildgenerierung:** KI kann Bilder, Grafiken und visuelle Inhalte erstellen (z.B. Midjourney https://www.midjourney.com, DALL-E https://openart.ai/home, Adobe Firefly https://www.adobe.com/products/firefly.html, Flux https://flux-ai.io, Ideogram https://www.imagine.art, Leonardo.ai https://leonardo.ai/, Google Nano Banana https://gemini.google/overview/image-generation)
- **Videogenerierung:** KI kann Videos aus Text oder Bildern erstellen (z.B. Google Veo 3 https://gemini.google/overview/video-generation/, Runway https://runwayml.com, Pika https://deevid.ai, HeyGen https://www.heygen.com, Synthesia https://www.synthesia.io)
- **Sprachgenerierung:** KI kann geschriebenen Text in realitätsnahe Tonaufnahmen umwandeln und sogar ihre Stimme klonen, etwa für die Vertonung von Präsentationen, Anleitungen, Durchsagen uvm. (z.B. ElevenLabs https://elevenlabs.io, HeyGen https://www.heygen.com)
- **Musik-Generierung:** KI komponiert Musik und Songs (z.B. Suno https://suno.com/home, Udio) https://www.udio.com
- **Programmierung & Code:** KI unterstützt beim Schreiben, Überprüfen und Erklären von Programmcode (z.B. GitHub Copilot https://github.com/features/copilot, Cursor https://cursor.com, Replit https://replit.com)
- **Datenanalyse:** KI kann große Datenmengen analysieren, um Muster und Erkenntnisse zu gewinnen. Auch die Marktanalyse liegt hier im Anwendungsbereich (z.B. Julius https://julius.ai, Tableau AI https://www.tableau.com, Power BI Copilot https://learn.microsoft.com/en-us/power-bi/create-reports/copilot-introduction)
- **Prozessautomatisierung:** KI kann Geschäftsprozesse automatisieren, um Aufgaben effizienter zu erledigen und Kosten zu senken (z.B.Make

https://www.make.com/en, Zapier https://zapier.com/, SaneBox https://www.sanebox.com, Microsoft Power Automate https://www.microsoft.com/en/power-platform/products/power-automate, Langdock https://www.langdock.com)

- **Autonome Agenten:** KI führt komplexe Aufgaben selbstständig aus und nutzt dabei verschiedene Tools (z.B. AutoGPT https://agpt.co, AgentGPT https://agentgpt.reworkd.ai/de, Relevance AI https://relevanceai.com)
- **Literaturrecherche:** KI durchsucht Literatur und beantwortet Fragen mit Quellenangaben (z.B. Perplexity https://www.perplexity.ai, Google Gemini https://gemini.google.com)
- **Vertrieb:** KI kann die Entlastung der Mitarbeitenden von administrativen Aufgaben bieten (z.B. Microsoft Dynamics 365 Copilot https://learn.microsoft.com/en-us/microsoft-cloud/dev/copilot/copilot-for-dynamics365, Einstein GPT von Salesforce https://www.salesforce.com/agentforce)
- **Projektmanagement:** KI kann Echtzeit-Updates sowie automatisierte Unterstützung bei der Entscheidungsfindung liefern (z.B. ChatGPT https://chatgpt.com, Asana AI https://asana.com, ClickUp AI https://clickup.com)
- **Online-Präsenz:** KI kann auf Basis zuvor analysierter Inhalte SEO-Optimierungen vornehmen, die Websites und deren Inhalte aufwerten (z.B. SurferSEO https://surferseo.com, Clearscope https://www.clearscope.io, Frase https://www.frase.io)
- **Sicherheit:** KI kann Bedrohungen für Cyberangriffe in Echtzeit erkennen (z.B. Darktrace https://www.darktrace.com)
- **Feedback-Tools:** KI kann Feedback von Benutzerinnen und Benutzern oder Kundinnen und Kunden sammeln und analysieren (z.B. MonkeyLearn https://www.welcome.ai/solution/monkeylearn, Qualtrics AI https://www.qualtrics.com/platform)

Weitere Ressourcen:

- Viele österreichische KI-Anwendungen: https://www.awsconnect.at/KI-Marktplatz und https://www.tip-noe.at/plattform-ki/
- Internationale Tool-Übersichten:https://theresanaiforthat.com/ und https://futurepedia.io/
- Weitere Anwendungstipps: Trendguide Künstliche Intelligenz der WKO

TIPPS FÜR UNTERNEHMERINNEN UND UNTERNEHMER

Finden Sie die passende KI-Strategie für Ihr Unternehmen

Wie und ob man künstliche Intelligenz als Unternehmen einsetzt, ist eine strategische Entscheidung, die für jedes Unternehmen individuell getroffen werden muss. Damit Sie leichter zu einer praxisorientierten KI-Strategie für Ihr Unternehmen kommen, haben die Expertinnen und Experten der WKO Tipps zum Erstellen der passenden KI-Strategie für Ihr Unternehmen zusammengestellt.

Tipp 1 - Status Quo erheben und Ziele definieren

Klären Sie zuerst die Ziele und Erwartungen an den Einsatz von KI. Was möchten Sie mit KI erreichen? Wo gibt es Probleme, die sich eventuell mit Hilfe von fertigen KI-Anwendungen lösen lassen? Starten Sie dann mit Pilotprojekten in einem begrenzten Bereich, bevor Sie unternehmensweit ausrollen. Wie viele Mitarbeitende sollen in welchem Umfang eingesetzt werden? Welche Tools sollen genutzt werden? Wie und zu welchem Zweck sollen diese genutzt werden? Kalkulieren Sie realistisch: Lizenzkosten, Schulungszeit und erwartete Effizienzgewinne. Beziehen Sie Mitarbeitende laufend ein, die an den Geschäftsprozessen beteiligt sind. Denken Sie daran: KI-Anwendungen sind immer als Unterstützung für die Beschäftigten zu sehen.

Tipp 2 – Wann macht der Einsatz von KI Sinn?

Um beurteilen zu können, ob und wie der Einsatz von KI für Ihr Unternehmen sinnvoll ist, prüfen Sie zuerst, ob die Arbeitsprozesse stark datenabhängig sind und die benötigten Daten bereits digitalisiert vorliegen. Denn KI kann mit großen Datenmengen wertvolle Erkenntnisse liefern und fundierte Entscheidungen unterstützen. Darüber hinaus lohnt sich der Einsatz von KI, wenn damit wiederkehrende Aufgaben automatisiert werden können, was Zeit spart, und die Effizienz steigert. Auch Projekte, die regelmäßige Prognosen und Analysen erfordern oder komplexe Muster und Trends erkennen müssen,

profitieren von KI-Technologien. Ein weiteres Kriterium ist die Notwendigkeit, große Textmengen zu verarbeiten oder Kundeninteraktionen effizienter zu gestalten, etwa durch automatisierte Support-Antworten. Nicht zuletzt muss ein Team bereit sein, neue Technologien einzuführen und zu nutzen. Der Erfolg einer KI-Lösung hängt maßgeblich von der Akzeptanz und Schulung der Mitarbeitenden ab.

Tipp 3 – Machen Sie sich mit dem AI Act vertraut

Mit dem Artificial Intelligence Act (AI Act) der Europäischen Union trat das weltweit erste Gesetz in Kraft, das den Einsatz von KI-Systemen regelt. Die Bestimmungen werden schrittweise zwischen Februar 2025 und August 2027 anwendbar. Ab Februar 2025 gelten erste Bestimmungen, insbesondere Verbote bestimmter KI-Praktiken. Unternehmen, die Hochrisiko-KI-Systeme einsetzen oder entwickeln (ab August 2026 anwendbar), müssen entsprechende KI-Kompetenz nachweisen und dokumentieren können. Dabei sollten technische, rechtliche und ethische Fragen beleuchtet werden. Bei der Verwendung von Chatbots ist weniger Fachkompetenz nötig als bei einem IT-Unternehmen, das KI-Systeme entwickelt. Lesen Sie dazu mehr im Gastbeitrag der österreichischen KI-Servicestelle (siehe Seite 20).

Tipp 4 – Den Einsatz von KI-Systemen fördern oder verbieten?

Entscheiden Sie nicht leichtfertig und vorschnell, Ihren Mitarbeitenden die Nutzung von KI-Anwendungen einzuschränken oder gänzlich zu verbieten. Bedenken Sie: Verbote führen oft zu unkontrollierter Nutzung privater Tools ohne Wissen der IT-Abteilung („Shadow AI"). Besser: Sichere Alternativen anbieten.

Nur wer sich selbst mit neuen Themen auseinandersetzt, kann als Vorbild in der Branche auftreten und rechtzeitig auf Trends und Möglichkeiten reagieren. Sich für KI-Tools im Unternehmen zu entscheiden bedeutet, zwischen verschiedenen Modellen zu wählen: Kostenlose Versionen speichern oft Eingaben für Modellverbesserung, während Business-Tarife meist Datenschutzgarantien, Service Level Agreements und erweiterte Funktionen bieten. Enterprise-Lösungen bieten zusätzlich dedizierte Unterstützung und können oft on-premise betrieben werden. Achten Sie dabei auf Datenexportierbarkeit und vermeiden Sie zu starker Abhängigkeit von einzelnen Anbietern.

Wie Sie sich auch entscheiden: Kommunizieren Sie Ihren Entschluss klar an alle Mitarbeitenden und vereinbaren Sie unmissverständlich, was für Ihr Personal bei deren Aktivitäten mit künstlicher Intelligenz erwünscht bzw. erlaubt ist und was nicht. Die KI-Guidelines für KMU sollen Ihnen dabei helfen.

Tipp 5 – Sensibilisierung und Information der Mitarbeitenden

Es sollte immer auf alle Personen – Entscheidungstragende und Mitarbeitende – eingegangen werden. Auch jene, die noch wenig Erfahrung mit künstlicher Intelligenz und KI-Anwendungen haben. Diskutieren Sie offen die möglichen Auswirkungen auf Ihr Unternehmen und den Arbeitsplatz. Klären Sie Ihre Arbeitskräfte über Chancen und Risiken von KI-Systemen auf und unterstützen Sie sie bei ihren ersten Aktivitäten.

Sorgen Sie dafür, dass sich Ihre Mitarbeitenden in einer neuen Arbeitsumgebung mit KI sicher fühlen. Schaffen Sie dazu in Ihrem Unternehmen eine Vertrauenskultur und fördern Sie dieses Vertrauen auch im Umgang mit Künstlicher Intelligenz. Informieren Sie sie laufend über Tipps und Erfahrungsberichte zum Einsatz von KI in Unternehmen. Zudem ist ein interdisziplinärer Austausch der verschiedenen Abteilungen von Vorteil, um gemeinsam zu lernen und Erfahrungen zu teilen.

In Betrieben mit Betriebsrat sollte dieser frühzeitig eingebunden werden, insbesondere wenn KI-Systeme Aspekte der Leistungskontrolle oder Überwachung berühren könnten.

Tipp 6 – Möglichkeiten zum Training anbieten

Um erste Erfahrungen zu sammeln und das theoretische Wissen in der Praxis anwenden zu können, ist es wichtig, Möglichkeiten und Zeit zum Testen zur Verfügung zu stellen. Schulen Sie Mitarbeitende auch in Prompt Engineering – der Fähigkeit, KI die richtigen Fragen zu stellen bzw. präzise Anweisungen zu geben, um bessere Ergebnisse zu bekommen. Dies ist eine Grundkompetenz für die effektive Nutzung von KI-Systemen.

Vielleicht gibt es eine Person im Unternehmen, die privat bereits erste Erfahrungen mit KI-Anwendungen gesammelt hat und sich dafür interessiert. Sie könnte anderen Mitarbeitenden beim Testen unterstützen. Nutzen Sie auch externe Ressourcen wie Online-Kurse (z.B. LinkedIn Learning, Coursera) oder WKO-Workshops zur Weiterbildung.

Weisen Sie darauf hin, dass dabei keine sensiblen Unternehmensdaten, personenbezogenen Daten oder Geschäftsinformationen verwendet werden sollen. Eine gute Möglichkeit ist es, Anregungen und Aufgaben zu Freizeit- und Hobby-Themen zu stellen, die mithilfe unterschiedlicher KI-Anwendungen gelöst werden können.

Tipp 7 – KI-Guidelines im Unternehmen entwickeln

Entwickeln Sie für Ihr Unternehmen eigene maßgeschneiderte KI-Guidelines. Was ist erwünscht, was ist im Unternehmen keinesfalls erlaubt? Bedenken Sie, dass alle Unternehmensbereiche betroffen sind und eingebunden werden sollten. Als Grundlage können diese von der WKO entwickelten Muster-KI-Guidelines dienen. Beachten Sie, dass eine etwaige bestehende Datenschutzvereinbarung bereits einige Themen abdecken könnte.

Definieren Sie klare Zugriffsrechte: Wer darf welche KI-Tools nutzen? Wer darf Daten hochladen? Wer trägt die Verantwortung bei kritischen Entscheidungen? Klären Sie auch rechtliche Fragen: Wer haftet bei KI-Fehlern? Wem gehören KI-generierte Inhalte? Bei welchen Anwendungsfällen ist menschliche Überprüfung verpflichtend?

Empfohlen wird die Benennung einer Ansprechperson, die bei Fragen zur Nutzung von KI-Anwendungen das letzte Wort hat. Testen Sie die Guidelines über einen definierten Zeitraum und aktualisieren Sie diese regelmäßig. Um Klarheit zu schaffen, können Sie nach der Probephase eine bindende Unternehmensvereinbarung zur Nutzung von KI-Anwendungen treffen. Das Schließen einer Unternehmensvereinbarung ist zwar nicht verpflichtend, kann aber auch im Hinblick auf etwaige Haftungsfragen nützlich und wichtig sein. Lassen Sie diese Vereinbarung aus Dokumentationsgründen von allen Mitarbeitern unterzeichnen.

Tipp 8 – Feedbackprozesse einführen und Erfolg messen

Für die Optimierung ihrer Geschäftsprozessen und den wirtschaftlichen Erfolg spielt Feedback eine entscheidende Rolle. Es ist sowohl wichtig, die Zufriedenheit von Kundinnen und Kunden beim Einsatz von künstlicher Intelligenz zu erheben, als auch die Zufriedenheit und Sicherheit der Mitarbeitenden beim Umgang mit KI abzufragen. Deren Feedback ist essenziell, um sicherzustellen, dass KI-Anwendungen positiv und nahtlos in den Arbeitsalltag integriert werden.

Definieren Sie messbare Kennzahlen (KPIs) wie Zeitersparnis, Fehlerrate, Nutzerakzeptanz oder Return on Investment. Etablieren Sie auch Prozesse für den Umgang mit KI-Fehlern oder problematischen Outputs (Incident Management). Bestimmen Sie im Unternehmen Personen, die für den Support für eingesetzte KI-Anwendungen verantwortlich sind. Diese müssen die Tools auch regelmäßig im Hinblick auf Funktionen und den gesetzmäßigen Einsatz evaluieren.

Überprüfen Sie Ihre KI-Strategie mindestens halbjährlich – neue Tools, Methoden und rechtliche Anforderungen entstehen laufend.

Tipp 9 – Durch eigene KI-Systeme von der Masse abheben

Der Einsatz von KI-basierten Anwendungen im Unternehmensalltag kann nützlich sein und dabei helfen, Zeit und Ressourcen zu sparen. Wenn es im Betrieb jedoch aufwändige und stark datenbasierte Prozesse gibt und die Datenbasis bereits qualitativ gut digitalisiert ist, wird die Integration eines eigenen KI-Systems interessant.

Dabei sollten Unternehmer abwägen, wo allgemeine KI-Modelle ausreichen und wo eine maßgeschneiderte Lösung sinnvoller ist – insbesondere bei Anwendungen und Prozessen, die für den USP (Unique Selling Proposition) des Unternehmens relevant sind. Eine kosteneffiziente Alternative zu vollständigen Unternehmens relevant sind. Eine kosteneffiziente Alternative zu vollständigem Finetuning ist RAG (Retrieval Augmented Generation), bei dem KI auf Ihre Unternehmensdokumente zugreift, ohne das Modell selbst anzupassen.

Für umfassendere Anpassungen lohnt sich der Einsatz eines lizenzierten, eigenen Modells. Open-Source-Modelle wie Meta Llama können Sie lokal betreiben und auf die Datenwelt des Unternehmens anwenden. Welche Möglichkeiten zur Integration eigener KI-Systeme im Unternehmen es gibt und was dabei zu beachten ist, lesen Sie ab Seite 24.

RICHTLINIEN FÜR MITARBEITENDE

KI-Guidelines (Muster für KMU) – Richtlinien für Mitarbeitende für den Umgang mit künstlicher Intelligenz

Die vorliegenden Guidelines wurden von der WKO entwickelt. Sie sollen Unternehmen als Grundlage dienen, um individuelle Guidelines zur Nutzung von KI-basierten Anwendungen im Unternehmen zu entwickeln. Wir empfehlen, die folgenden Themen und Paragrafen in jeder Vereinbarung zu berücksichtigen. Sie sollten an die Unternehmenserfordernisse angepasst werden und dabei helfen, eine verständliche Vereinbarung zur Nutzung von KI-Anwendungen mit Ihren Mitarbeitenden zu treffen.

Rahmenbedingungen zur Nutzung schaffen

#1 Vereinbarungen kennen und beachten

Das Unternehmen _____ nutzt Anwendungen und Services auf Basis von künstlicher Intelligenz zu _____ (z.B.: Recherchezwecken / zur

Verbesserung des Service im Umgang mit Kundinnen und Kunden / zur Inspiration / als Analyse-Instrument ...) / nutzt künstliche Intelligenz derzeit nicht.

Beschäftigten des Unternehmens ist die Nutzung von KI-Anwendungen und Services _____ (erlaubt / nur nach Einschulung erlaubt / ebenfalls nicht gestattet).

Die Verwendung der Unternehmens-E-Mail-Adresse zur Registrierung bei KI-Systemen zum Zweck der geschäftlichen Nutzung ist Beschäftigten _____ (gestattet / nicht gestattet). Wird die Erlaubnis zur Nutzung der betrieblichen E-Mail-Adresse erteilt, bestehen folgende interne Meldepflichten:
_____

Mitarbeitende nutzen starke Passwörter und aktivieren Zwei-Faktor-Authentifizierung bei KI-Accounts. Bei kostenpflichtigen Services sind vereinbarte Budget-Limits einzuhalten. Die Nutzung experimenteller oder Beta-Funktionen bedarf gesonderter Freigabe durch die Unternehmensleitung.

Unternehmensangehörige halten sich bei allen Aktivitäten an die Gesetze und arbeitsrechtlichen Verpflichtungen sowie die vorliegenden KI-Guidelines.

Erläuterungen:

Wenn es um den Einsatz von KI-Systemen in Ihrem Unternehmen geht, trifft allein die Unternehmensleitung die Entscheidung, ob die Anwendung zulässig ist. Im Umgang mit KI sollten ähnliche Regeln wie im herkömmlichen Arbeitsalltag gelten. Beispielsweise dürfen Mitarbeitende auch sonst üblicherweise keine Software ohne Rücksprache herunterladen. Alle Aktivitäten im Zusammenhang mit KI und KI-basierten Systemen müssen mit den geltenden Gesetzen, dem Arbeitsvertrag und den daraus resultierenden Geheimhaltungspflichten vereinbar sein. Dabei ist es wichtig, sich immer vor Augen zu halten, welche übergeordneten Ziele das Unternehmen mit dem Einsatz von KI verfolgt.

In den Richtlinien muss klar definiert werden, ob, in welchem Rahmen und in welchem Ausmaß die Nutzung von Anwendungen und Services, die auf KI beruhen, im dienstlichen Zusammenhang erlaubt ist. Wenn die Nutzung der betrieblichen E-Mail-Adresse zur Registrierung bei KI-Systemen erlaubt ist, kann eine interne Meldepflicht vereinbart werden, beispielsweise die Bekanntgabe aller verwendeten Services bzw. kostenpflichtiger Services. Dies kann Klarheit über die genutzten KI-Systeme, anfallende Kosten sowie etwaige Haftungsfragen schaffen.

TIPPS FÜR DIE PRAXIS

- Erstellen Sie eine Liste genehmigter KI-Tools nach Abteilung und Verwendungszweck
- Definieren Sie klare Freigabeprozesse für neue KI-Anwendungen
- Legen Sie fest, wer Ansprechperson für KI-Fragen ist

Grenzen von KI – der Mensch als wichtigste Instanz

#2 Der Mensch hat im Einsatz der KI das letzte Wort

Der Einsatz und die Freigabe von KI-generierten Inhalten unterliegen einer gewissenhaften Aufsicht und menschlichen Kontrolle. Die Beschäftigten verpflichten sich, KI-basierte Inhalte erst dann zu übernehmen, wenn diese zuvor von mindestens einer qualifizierten Person auf Richtigkeit, Faktentreue und Kontext überprüft wurden. Bei kritischen Outputs ist das Vier-Augen-Prinzip anzuwenden.

Erläuterungen:

So gut KI-basierte Systeme auch sind, sie sind keineswegs fehlerfrei und auch keine Alleskönner. Im Gegensatz zur menschlichen Intelligenz, die von einer Vielzahl von Faktoren wie Erfahrung, sozialen Beziehungen, kulturellen Einflüssen und komplexen Emotionen geprägt ist, beruhen die Fähigkeiten von KI auf den ihr zur Verfügung stehenden Daten, Informationen und Algorithmen.

Das bedeutet, dass menschliche Fähigkeiten wie Wahrnehmung, Intuition und emotionale Intelligenz weiterhin unersetzlich sind. Die Einzigartigkeit und Verantwortung des Menschen liegen in seiner Fähigkeit, menschliche Aspekte in die tägliche Arbeit einzubringen, Beziehungen zu berücksichtigen und kontextbezogen zu denken und zu handeln.

Menschliche Fähigkeiten bleiben in folgenden Bereichen zentral:

- Empathie und emotionales Verständnis
- Moralische und ethische Urteilsbildung
- Kontextverständnis und Intuition
- Ironie, Sarkasmus und Nuancen
- Kreative Problemlösung jenseits von Mustern

Sollte durch den Einsatz von KI-Ergebnissen ein Schaden entstehen, haftet das Unternehmen, das diese verwendet hat. Um das Haftungsrisiko zu minimieren, ist es daher umso wichtiger, klare Richtlinien für den Umgang mit KI einzuführen. Die Verantwortung für den angemessenen Einsatz von KI-Technologien liegt dabei nicht nur bei den entwickelnden und anbietenden Unternehmen, sondern auch bei den

einzelnen Personen, die diese Systeme nutzen oder die von ihnen erzeugten Informationen weiterverwenden. Es muss sichergestellt werden, dass die eingesetzten KI-Anwendungen im Einklang mit dem jeweiligen Wissensstand sowie den Unternehmenswerten und -zielen handeln.

TIPPS FÜR DIE PRAXIS

Hilfreiche Fragen im Zusammenhang mit KI-Anwendung können sein:

- Ist das Ergebnis der KI für Ihre Anwendungszwecke relevant?
- Ist das Ergebnis im Einklang mit Ihren Zielen?
- Wie gut ist die Datenqualität?
- Wie sicher sind die Daten?
- Ist der generierte Inhalt ethisch und moralisch vertretbar?
- Enthält der Inhalt Verzerrungen oder wirkt er gegenüber bestimmten Personen(gruppen) diskriminierend?

Kundenbezogene Daten und KI

#3 Kundinnen und Kunden über den Einsatz von KI aufklären

Vor der Nutzung von KI-Anwendungen im Rahmen von Projekten mit Kundinnen und Kunden werden diese über den geplanten Einsatz von KI informiert und aufgeklärt. Ab August 2026 gelten gemäß AI Act erweiterte Dokumentationspflichten für Hochrisiko-Systeme.

Erläuterungen:

Die aktuellen Entwicklungen im Bereich KI bringen eine Reihe von Herausforderungen für den Schutz von Unternehmens- und personenbezogenen Daten sowie der Privatsphäre mit sich. Sowohl die Bestimmungen des AI Act als auch weitere aktuell geltende Vorschriften – etwa zum Datenschutz, zum Urheberrecht oder zu Markenrechten – sind einzuhalten, und vertrauliche Informationen sind mit größter Sorgfalt zu behandeln. Welche Daten auf welche Weise in KI-Anwendungen eingegeben werden dürfen, muss im Unternehmen klar geregelt sein.

Im Umgang mit Kundendaten ist es immer nötig, eine Grundlage für die Verarbeitung dieser Daten zu haben. Das kann ein Vertrag sein (z. B. eine entsprechende Regelung im Vertrag mit den Kundinnen und Kunden). Generell wird empfohlen, keine sensiblen Unternehmensdaten, Geschäftsgeheimnisse und idealerweise auch keine personenbezogenen Daten (Namen, Adressen, Telefonnummern o. Ä.) in KI-Tools einzupflegen. Derartige Informationen können nur sehr schwer oder gar nicht

wieder gelöscht werden. Sollten diese Informationen jedoch mit KI verarbeitet werden, muss für sensible Daten von Kundinnen und Kunden (z. B. Gesundheitsdaten, Gewerkschaftszugehörigkeit o. Ä.) eine Einwilligung für die Verarbeitung via KI eingeholt werden. Gleiches gilt für die Verarbeitung von Geschäfts- und Betriebsgeheimnissen.

Nehmen Sie die Bedenken von Kundinnen und Kunden, Lieferunternehmen und anderen Geschäftskontakten ernst und zeigen Sie Einfühlungsvermögen. Bedenken entstehen oft, wenn es an Wissen über neue Technologien mangelt. Informieren Sie Ihr Gegenüber deshalb darüber, was künstliche Intelligenz ist, in welche Prozesse KI integriert ist und unter welchen Rahmenbedingungen sie in Ihrem Unternehmen eingesetzt wird. Vermeiden Sie übermäßigen Fachjargon und erklären Sie die Prozesse auf verständliche Weise. Nur so kann sich Ihr Gegenüber ein klares Bild davon machen, ob und inwieweit es mit dem Einsatz von KI-Anwendungen einverstanden ist.

TIPPS FÜR DIE PRAXIS

- Überlegen Sie von Fall zu Fall: Welche Informationen dürfen geteilt werden – und welche nicht?
- Beachten Sie, dass Sie bei vielen kostenlos frei verfügbaren KI-Tools implizit der Weiterverarbeitung der eingegebenen Daten durch das anbietende Unternehmen zustimmen.
- Achten Sie darauf, dass beim Kopieren von Daten in die Zwischenablage häufig auch persönliche Informationen mitkopiert werden.
- Eine gute Lösung ist die Anonymisierung der Daten, um keine Rückschlüsse auf kundenbezogene Daten ziehen zu können (durch Entfernung von Namen und anderen Identifikatoren).
- Wenn keine vollständige Anonymisierung möglich ist, sollen Daten pseudonymisiert werden, um Datensicherheitsstandards einzuhalten (z.B. Ersetzen der realen Daten durch randomisierte Namen).
- Eine Datenverarbeitung personenbezogener Daten durch KI-Systeme muss in der Datenschutzerklärung an Kundinnen und Kunden, aber auch in jener für Mitarbeitende, falls deren Daten erfasst sind, ausgewiesen werden. Das gilt auch für pseudonymisierte Daten.
- Zeigen Sie Verständnis für Bedenken der Kundinnen und Kunden, Lieferunternehmen und sonstiger geschäftlicher Kontakte.
- Schaffen Sie Klarheit und Transparenz zu internen Arbeitsweisen und kommunizieren Sie auf verständliche Art und Weise, um Missverständnisse zu vermeiden.

- Fördern Sie den Dialog mit den Kundinnen und Kunden und ermutigen Sie diese zum Feedback als Chance zur Beziehungsverbesserung und Prozessoptimierung.
- Werden Daten außerhalb des EWR gehostet, müssen Vorschriften des Internationalen Datenverkehrs beachtet werden.

Unternehmensbezogene Daten und Geheimhaltung

#4 Geheimhaltungsverpflichtung beachten

In KI-Anwendungen dürfen keine vertraulichen Informationen über Ihr Unternehmen oder über Dritte verwendet werden. Holen Sie im Zweifel die Erlaubnis der Unternehmensleitung zur Verwendung ein. API-Zugriffsschlüssel sind wie Passwörter zu behandeln und dürfen nicht geteilt oder öffentlich gemacht werden. Die Nutzung unternehmenseigener KI-Systeme für außerbetriebliche oder konkurrierende Zwecke ist untersagt.

Erläuterungen:

Auch bei unternehmensbezogenen Daten ist es wichtig, den Mitarbeitenden Leit- und Richtlinien zum Umgang mit KI zur Verfügung zu stellen. Beachten Sie bitte, dass Sie der Verschwiegenheit verpflichtet sind und Geschäfts- und Betriebsgeheimnisse keinesfalls weitergeben dürfen. Dies betrifft auch die Weitergabe solcher Informationen an KI-Systeme. Bei vielen KI-Systemen, vor allem bei kostenlos verfügbaren, sind der Speicherort und die Verwertung der Daten noch nicht ausreichend transparent. Dadurch besteht das Risiko, dass wichtige Daten in falsche Hände geraten. Mehr Sicherheit bieten unternehmenseigene KI-Anwendungen, die lokal gehostet werden und so verhindern, dass eingegebene Daten außerhalb des Unternehmens einsehbar werden.

Als Mitarbeitende eines Unternehmens gehören Sie oft zu den Ersten, die von neuen Entwicklungen erfahren. Das können noch nicht fixierte Aufträge, Informationen über die finanzielle Lage des Unternehmens oder neue Geschäftsideen sein, die noch nicht in der Öffentlichkeit präsentiert wurden. Das berechtigt Sie jedoch nicht dazu, diese Informationen zu verbreiten. Unternehmensinterne Richtlinien sollen hierfür einen Rahmen bieten und ausreichende Schutzmaßnahmen gewährleisten. Empfehlenswert ist eine Abstimmung mit der Datenschutzbeauftragten bzw. dem Datenschutzbeauftragten des Unternehmens.

Seien Sie besonders wachsam bei ungeprüften Prompts aus externen Quellen, da diese manipulativ sein könnten (Prompt Injection). Nutzen Sie Sandbox- oder Test-Umgebungen für Experimente mit nicht sensiblen Daten.

TIPPS FÜR DIE PRAXIS

Überlegen Sie:

- Wurden die Daten bzw. Informationen bereits für alle zugänglich veröffentlicht (z.B. auf der Unternehmenswebsite, in einer Pressemitteilung, durch weitere Informationen)?
- Betreffen die Daten Kategorien, die der Geheimhaltung unterliegen? Überprüfen Sie ggf. die Geheimhaltungserklärung Ihres Unternehmens.
- Besteht die Möglichkeit, ein unternehmensinternes KI-System zu verwenden, das lokal bzw. innerhalb Europas gehostet wird?

KI und rechtliche Rahmenbedingungen

#5 Rechtliche Rahmenbedingungen

Unternehmensangehörige halten sich an geltendes Recht und berücksichtigen bei der Nutzung von KI-Anwendungen sowie bei allen Veröffentlichungen von KI-generierten Inhalten insbesondere die Urheber-, Persönlichkeits- und Markenrechte sowie die Datenschutzbestimmungen. Schwerwiegende KI-Fehler oder Datenschutzverletzungen sind umgehend der zuständigen Stelle zu melden.

Erläuterungen:

Wer mit KI-Systemen und -Services arbeitet, sollte über die allgemeine Rechtslage informiert sein. Mit der Einführung des AI Acts sind neue Vorgaben zu berücksichtigen, die über die bisherigen Anforderungen hinausgehen. Der AI Act gilt als weltweit erster länderübergreifender KI-Standard und soll ein neues Maß an Sicherheit und Vertrauen in KI schaffen. Die Bestimmungen werden schrittweise anwendbar: Im Februar 2025 treten die Verbote bestimmter Praktiken in Kraft, im August 2026 die Regelungen für Hochrisiko-Systeme und im August 2027 die Regelungen für alle Systeme.

Da das österreichische Urheberrechtsgesetz nur eine „natürliche Person" als Urheber vorsieht, kann die KI aus heutiger Sicht selbst kein Urheber bzw. Inhaber von Rechten sein. Die der KI zugeführten und verarbeiteten Daten können jedoch sehr wohl

urheberrechtlich geschützt sein. Nicht alles, was öffentlich verfügbar ist, darf auch verwendet werden. Auch an den Ergebnissen der KI hat man kein geistiges Eigentum und somit keine gesicherte Exklusivität. Die Übertragung von Datenbanken, die Extraktion von Webseiten oder auch nur die Nutzung von Bildern im Internet sind geregelt und können im Umgang mit KI rechtliche Konsequenzen haben. Um Urheberrechtsverletzungen durch unerlaubte Vervielfältigung, Bearbeitung oder Veröffentlichung zu vermeiden, muss sichergestellt werden, dass …

- im Einklang mit unternehmensinternen Richtlinien gehandelt wird.
- Mitarbeitende über alle notwendigen Berechtigungen / Lizenzvereinbarungen für die Verwertung der Inhalte verfügen.
- alle rechtlichen Vereinbarungen eingehalten werden.

Verantwortung und Haftung

Wer haftet, wenn KI falsch eingesetzt wird oder wenn wichtige Informationen öffentlich gemacht werden? Im Datenschutz haftet das „Unternehmen" für schuldhaftes Fehlverhalten von Personen, die diesem zuzurechnen sind (Leitungsorgane, Mitarbeitende, etc.). In anderen Rechtsmaterien kann die Geschäftsführung unter Umständen direkt für das Verschulden von Mitarbeitenden haften, wenn diese ihre Organisations- und/oder Aufsichtspflichten verletzen. Verursachen Mitarbeitende durch fahrlässiges Verhalten oder die Nichteinhaltung von KI-Richtlinien einen Schaden, könnte die Unternehmensleitung persönlich dafür haftbar gemacht werden. Obwohl die Rechtslage in Bezug auf KI aktuell noch sehr dynamisch ist, dürfen die Pflichten einer Führungsperson nicht außer Acht gelassen werden. Um dieses Haftungsrisiko zu minimieren, ist es ratsam, klare und verbindliche KI-Richtlinien für die Mitarbeitenden einzuführen, umfassende Schulungen bereitzustellen, regelmäßige Kontrollen durchzuführen und sicherzustellen, dass alle Beteiligten die ethischen und rechtlichen Aspekte der KI-Nutzung im Unternehmen verstehen und einhalten.

In Betrieben mit Betriebsrat ist dieser bei mitbestimmungspflichtigen Themen frühzeitig einzubeziehen, insbesondere wenn KI-Systeme Aspekte der Leistungskontrolle berühren.

Zu konkreten Anwendungsfällen und auch rechtlichen Detailfragen bietet die WKO eine eigene Webinar-Reihe (auch als Aufzeichnung) an.
https://www.wko.at/digitalisierung/ki-loesungen-fuer-die-praxis

TIPPS FÜR DIE PRAXIS

- Können Sie ausschließen, dass Daten, Textbausteine oder Bilder, die Sie in die KI-Anwendung eingeben, urheberrechtlich geschützt sind?

- Falls die verwendeten Daten, Textbausteine oder Bilder urheberrechtlich geschützt sind, verfügen Sie über die notwendigen Berechtigungen oder Lizenzen zur Verwertung?

Sicherheit und Qualität von Daten

#6 Umgang mit der Qualität von KI-generierten Inhalten

Unternehmensangehörige dürfen Informationen aus KI-Systemen nur verwenden, nachdem sie deren Richtigkeit und Zuverlässigkeit überprüft haben.

Erläuterungen:

Die Ergebnisse von KI-Systemen sind nicht immer wahr oder aktuell. KI-Systeme haben nicht immer oder nur eingeschränkten Echtzeit-Zugriff und können daher nur auf Daten bis zu einem bestimmten Zeitpunkt zugreifen. Selbst bei Systemen mit Web-Zugriff ist eine gründliche Quellenprüfung ratsam. Das bedeutet, dass neue, für Ihr Interesse relevante Erkenntnisse, Ereignisse, Daten und Informationen möglicherweise noch nicht im Produkt der KI berücksichtigt sind. Aus diesem Grund ist ein Abgleich mit gesichertem menschlichem Fachwissen sowie mit aktuellen Daten von vertrauenswürdigen Quellen empfehlenswert.

Bei der Suche nach Informationen ist es darüber hinaus wichtig, nicht nur auf deren Aktualität, sondern auch auf die Zuverlässigkeit der Quelle zu achten. Dies kann bereits bei der Auswahl der passenden KI-Anwendung eine Rolle spielen. Denn Modelle wie ChatGPT oder Google Gemini sind zwar beeindruckend, aber nicht unbedingt für alle Recherchezwecke die besten Werkzeuge. Da sie möglicherweise mit fehlerhaften Daten trainiert wurden, kann es zu sogenannten „Halluzinationen" oder erfundenen Quellen kommen, also zu nichtexistierenden oder falschen Quellenangaben. Auch wenn Sie ein anderes KI-Recherche-Tool mit höherer Genauigkeit bei der Quellenangabe verwenden, ist es dennoch ratsam, die Herkunft der Informationen zu überprüfen. Verlassen Sie sich niemals allein auf das KI-Tool und wählen Sie Ihre Quellen mit Bedacht aus.

TIPPS FÜR DIE PRAXIS

- Überprüfen und bestätigen Sie die Richtigkeit von Informationen, Daten und Analysen, bevor Sie sie in Ihre Arbeit einfließen lassen.
- Vergleichen Sie Informationen mit aktuellen und glaubwürdigen Quellen, um die Authentizität und Zuverlässigkeit zu überprüfen.
- Nutzen Sie Fact-Checking-Tools zur Verifikation von KI-Aussagen.

- Stellen Sie sicher, dass Sie mit KI-Ergebnissen nicht versehentlich Desinformation verbreiten oder irreführende Darstellungen fördern.

Ethik. Vielfalt. Inklusion.

#7 Kontrolle von KI-generierten Inhalten im Hinblick auf ethische Grundlagen

KI-generierte Inhalte müssen von den Unternehmensangehörigen auf Verzerrungen überprüft und ggf. korrigiert werden.

Erläuterungen:

Aktuell sind KI-Systeme noch nicht in der Lage, selbstständig zu entscheiden, was ethisch richtig oder falsch ist. Dies ist auch Gegenstand des AI Acts, der ethische Rahmenbedingungen festlegt. Um die Verbreitung oder Förderung von voreingenommenen Informationen zu vermeiden, ist es von entscheidender Bedeutung, KI-Systeme mit Daten zu trainieren, die frei von Vorurteilen und Diskriminierung sind.

Obwohl sich KI-Systeme kontinuierlich verbessern, bleiben Bias-Risiken bestehen. Ein anschauliches Beispiel für das Problem der Voreingenommenheit in KI-Systemen ist die Übersetzung von Texten. In Sprachen, in denen die Geschlechterrollen neutral bezeichnet werden, wie es im Englischen häufig der Fall ist, neigen viele KI-basierte Systeme dazu, bestehende Stereotype in Übersetzungen zu übernehmen. Die folgenden Beispiele verdeutlichen dies:

Beispiel 1 –*The doctor asked if the customer was satisfied with the result*.
Der Arzt fragte, ob der Kunde mit dem Ergebnis zufrieden sei

Ein KI-System übersetzt eine geschlechtsneutrale Bezeichnung in eine männliche Form, was ein stereotypisches Rollenbild widerspiegelt.

Beispiel 2 – *The elementary school teacher asked the class a question*.
Die Grundschullehrerin stellt der Klasse eine Frage

Hier wird dieselbe geschlechtsneutrale Bezeichnung in eine weibliche Form übersetzt, was ebenfalls ein Stereotyp darstellt.

Beispiel 3 – *Hospital Nurses are crucial to providing quality patient care*.
Krankenschwestern und Krankenpfleger sind für eine hochwertige Patientenversorgung von entscheidender Bedeutung

In diesem Fall liefert das KI-System zwar eine Übersetzung beider Geschlechter, die jedoch auch nicht zeitgemäß ist. "Pflegefachkräfte" wäre die zeitgemäße, geschlechtsneutrale Form.

Auch Analysetools und Bildgeneratoren stehen vor ähnlichen Herausforderungen. Ein Beispiel dafür ist die Tendenz einiger KI-Modelle, häufiger Bilder von weißen Männern in renommierten Positionen (z.B. CEO, Richter oder Arzt) zu erzeugen, während vergleichsweise selten Bilder von Frauen oder Angehörigen von Minderheiten erscheinen. Einige Herstellungsunternehmen sind sich dieses Problems bewusst und arbeiten bereits an einer Lösung.

TIPPS FÜR DIE PRAXIS

Überprüfen Sie:

- Ist der KI-generierte Inhalt frei von Vorurteilen und Diskriminierung?
- Betrifft mein Input ein gesellschaftlich oder sozial kontroverses Thema, wo besonders viele Miss- und Desinformationen kursieren?
- Wer könnte an einer Verzerrung Interesse haben?
- Wie kann ich mögliche Verzerrungen richtigstellen?
- Gibt es unternehmensinterne Richtlinien, an denen ich mich orientieren kann?

Transparenz und Kennzeichnungen

#8 Kennzeichnung KI-generierter Inhalte

KI-generierte Inhalte werden in unserem Unternehmen wie folgt gekennzeichnet: _____ (Erklärung der Kennzeichnung einfügen).

Erläuterungen:

KI-basierte Technologien sind mittlerweile so weit fortgeschritten, dass es für Menschen oft schwer ist, zu erkennen, ob ein Inhalt von einer KI oder von einem Menschen erstellt wurde. Ein verantwortungsvoller Einsatz von KI ist daher besonders wichtig, um Täuschungen und irreführende Informationen zu vermeiden. Dazu sollte transparent gemacht werden, wann und wie KI-Systeme in den jeweiligen Prozessen eingesetzt werden. Eine Möglichkeit dazu ist die Kennzeichnung oder ein Hinweis, der dem Zielpublikum signalisiert, dass der Inhalt durch oder mit Unterstützung von KI erstellt wurde.

Dies wird nun auch durch den AI Act gefordert. Unternehmen sind demnach verpflichtet, Personen zu informieren, wenn diese mit einer KI oder KI-generierten Inhalten interagieren. Dies gilt insbesondere für Chatbots oder Deepfakes. Ausnahmen sind vorgesehen, wenn für die Nutzenden offensichtlich ist, dass sie mit KI kommunizieren, oder wenn das System für legale Zwecke genutzt wird. Bereits vor Inkrafttreten des AI Acts hatten sich viele Unternehmen freiwillig verpflichtet, KI-generierte Inhalte zu kennzeichnen.

Besondere Vorsicht ist bei Audio und Video geboten: Mithilfe von Voice Cloning und Video-Deepfakes ist eine täuschend echte Imitation von Stimmen und Personen möglich. Dies birgt erhebliche Betrugsrisiken. Seien Sie daher besonders wachsam bei KI-generierten E-Mails, Anrufen oder Videos, die vortäuschen, von Kollegen, Vorgesetzten oder Geschäftspartnern zu stammen. Verifizieren Sie bei sensiblen Anfragen (z. B. Überweisungen, vertrauliche Informationen) die Identität durch einen direkten Rückruf über bekannte Kontaktwege.

TIPPS FÜR DIE PRAXIS

Die Art und Weise, in der KI-generierte Inhalte gekennzeichnet werden, kann variieren. Hier sind einige Beispiele:

- „Künstlich generiert" oder „Mit Hilfe von KI generiert und von ____ freigegeben": Ob Bilder, Tabellen, Texte, Audiodateien oder Videos, diese beiden Zusätze können den Nutzerinnen und Nutzern auf einen Blick verdeutlichen, wie der Inhalt erstellt wurde.
- Kennzeichnung in Metadaten: Metadaten können in digitalen Inhalten verwendet werden, um Informationen über die KI-Generierung zu liefern.
- Wasserzeichen oder visuelle Kennzeichnungen: Visuelle Kennzeichnungen in Bildern, Grafiken oder Illustrationen können verwendet werden, um zu zeigen, dass sie mit der Unterstützung von KI erstellt wurden.
- AGB der Anbieter beachten: Auch in den AGB einiger KI-Anbieter lassen sich bereits konkrete Vorgaben zu Quellenverweisen finden.

Schulungen und Weiterbildungen

#9 Aus- und Weiterbildungen zu künstlicher Intelligenz

Das Unternehmen stellt sicher, dass Aus- und Weiterbildungsmöglichkeiten für das Personal sowie für andere Personen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, angeboten werden. Dadurch soll ein ausreichendes Maß an KI-Kompetenz erworben werden. Die Beschäftigten verpflichten sich, im Bereich KI

weiterzubilden und die erworbenen Kenntnisse verantwortungsbewusst im beruflichen Alltag anzuwenden.

Erläuterungen:

KI-Anwendungen können zwar viele Aufgaben übernehmen, ihr Einsatz ist jedoch auf das Wissen und die Expertise der Anwenderinnen und Anwender angewiesen. Ähnlich wie bei der Bedienung eines neuen Tools muss auch das Wissen über und der Umgang mit KI erst erarbeitet werden. Die Bereitstellung von Schulungsressourcen, Webinaren und praxisnahen Beispielen schafft eine Grundlage für die erfolgreiche Integration von KI-Systemen in das Unternehmen und stärkt das Vertrauen in die sichere und verantwortungsbewusste Nutzung von KI-Anwendungen. Bieten Sie Ihren Mitarbeitenden zudem Experimentierräume und fördern Sie den Aufbau einer internen Wissensbasis. Durch ein aktives Change-Management fördern Sie die Integration von KI in den Arbeitsalltag.

Darüber hinaus verpflichtet der AI Act Unternehmen ausdrücklich zur Sicherstellung der KI-Kompetenz derjenigen Beschäftigten, die für den Betrieb und die Nutzung von KI zuständig sind. Die Anforderungen des AI Acts zur KI-Kompetenz gelten seit Ende 2025 für alle Unternehmen, unabhängig von ihrer Größe oder der Risikoeinstufung der eingesetzten KI.

Schulungen helfen dabei,

- das Bewusstsein für die Chancen und Risiken des Einsatzes von KI zu fördern.
- das Risiko eines fahrlässigen und unbedachten Einsatzes zu verringern.
- Überforderung der Anwenderinnen und Anwender zu vermeiden und sie zu motivieren.
- Mitarbeitende durch Kompetenzerweiterung an Ihr Unternehmen zu binden.
- Innovation in Ihrem Unternehmen zu fördern.

TIPPS FÜR DIE PRAXIS

Schulen Sie Ihre Mitarbeitenden in Bezug auf:

- Das Verständnis für KI und ihre Anwendungsbereiche
- Die Auswahl und den Einsatz von geeigneten Tools
- Bedarfsanalysen und Anwendungsfälle im Unternehmen
- Die technischen Grenzen von KI
- Ethische Aspekte: Vorurteile und Auswirkung auf Dritte
- Rechtliche Aspekte: Datenschutz, Haftung und Urheberrecht
- Sicherheitsaspekte und Cybersecurity

KI-generierte externe Kommunikation

#10 Besondere Sorgfalt bei externer Kommunikation

Externe Kommunikation (E-Mails, Angebote, Verträge, Marketing-Materialien), die mit KI generiert wurde, muss von einer qualifizierten Person freigegeben werden, bevor sie versendet wird. Besondere Vorsicht ist bei rechtsverbindlichen Dokumenten, Verträgen und offiziellen Stellungnahmen geboten.

Erläuterungen:

Die externe Kommunikation Ihres Unternehmens repräsentiert Ihre Marke und kann rechtliche sowie geschäftliche Konsequenzen haben. KI-generierte Inhalte können Fehler, Ungenauigkeiten oder unangemessene Formulierungen enthalten. Solche Fehler wären in der internen Kommunikation tolerierbar, in der externen Kommunikation können sie jedoch zu Missverständnissen, Reputationsschäden oder rechtlichen Problemen führen.

Stellen Sie sicher, dass alle nach außen gerichteten KI-generierten Inhalte:

- Fachlich korrekt und aktuell sind
- Im angemessenen Ton und Stil verfasst wurden
- Keine vertraulichen oder unangebrachten Informationen enthalten
- Rechtlich einwandfrei sind (insbesondere bei Verträgen, AGBs, Datenschutzerklärungen)
- Die Unternehmenswerte und -standards widerspiegeln

TIPPS FÜR DIE PRAXIS

- Definieren Sie klare Freigabeprozesse für KI-generierte externe Kommunikation
- Legen Sie fest, welche Personen für welche Art von externer Kommunikation freigabeberechtigt sind
- Erstellen Sie Templates und Leitfäden für häufige Kommunikationsszenarien
- Dokumentieren Sie wichtige Kommunikation für Nachvollziehbarkeit und Compliance

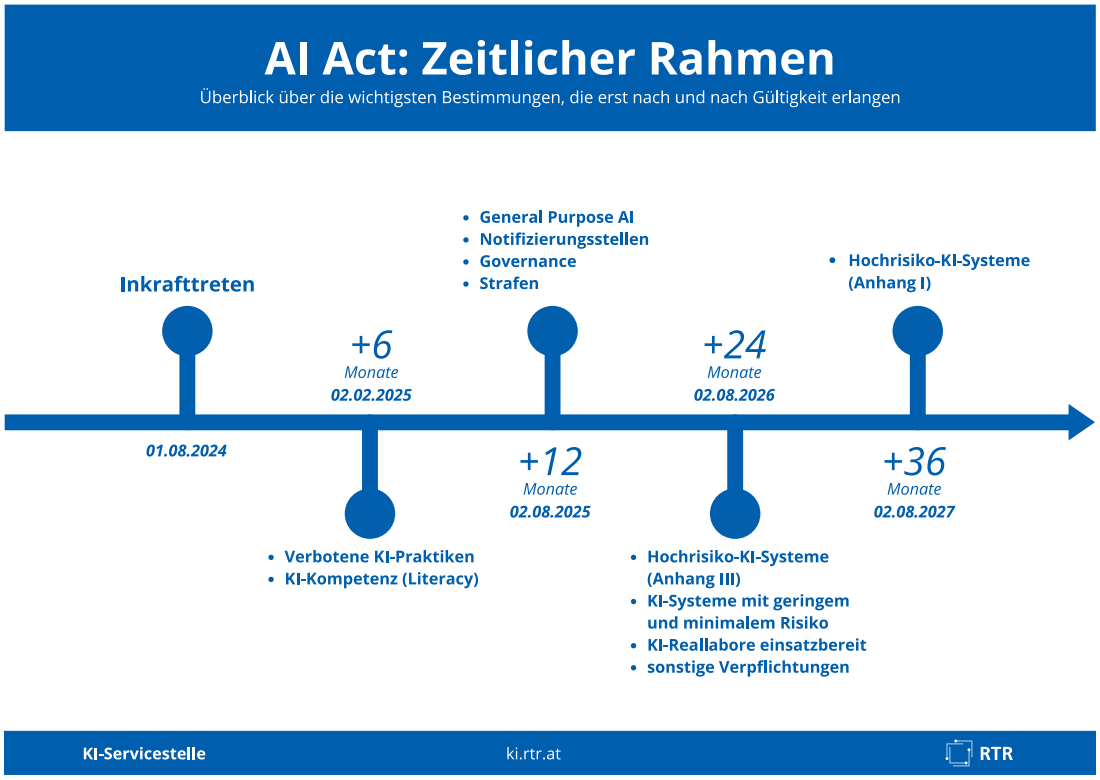
GASTBEITRAG DER KI-SERVICESTELLE

Rechtliche Rahmenbedingungen und Unterstützung durch die KI-Servicestelle

Der europäische AI Act enthält als Produktsicherheitsgesetz Sicherheitsvorschriften insbesondere in besonders heiklen Bereichen. Manche Praktiken werden in Europa verboten.

Der AI Act und sein Inkrafttreten

Der am 1.8.2024 in Kraft getretene AI Act sieht einen abgestuften Rahmen für den zeitlichen Geltungsbereich der Bestimmungen vor. Die folgende Abbildung stellt einen Überblick über die wichtigsten Bestimmungen, die erst nach und nach Gültigkeit erlangen, dar. Die Übergangsfristen ermöglichen es, zeitgerecht die betroffenen Produkte anzupassen.



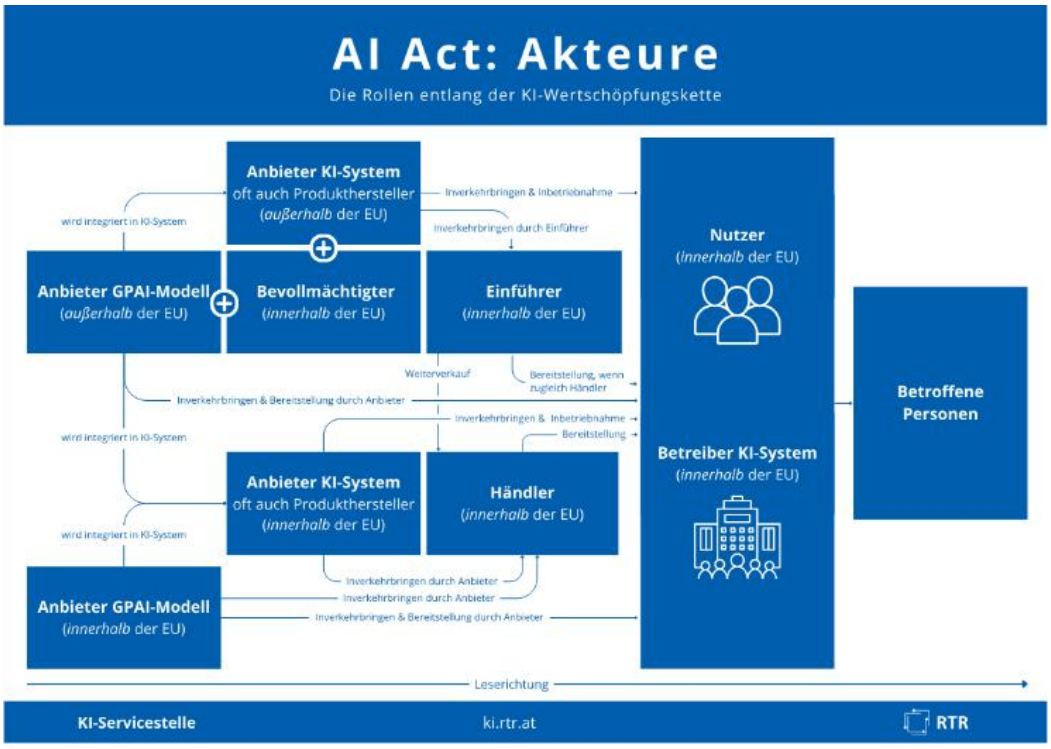
Mit 02.02.2025 sind die Bestimmungen zu verbotenen KI-Praktiken sowie zur KI-Kompetenz in Kraft getreten. Mit 2. 8.2025 erfolgte insbesondere das Inkrafttreten der

Bestimmungen zu KI-Modellen mit allgemeinem Verwendungszweck und den Sanktionen Die ersten Verpflichtungen zu Hochrisiko-KI-Systemen werden am 2.8.2026 in Kraft treten.

Die Rollen im AI Act

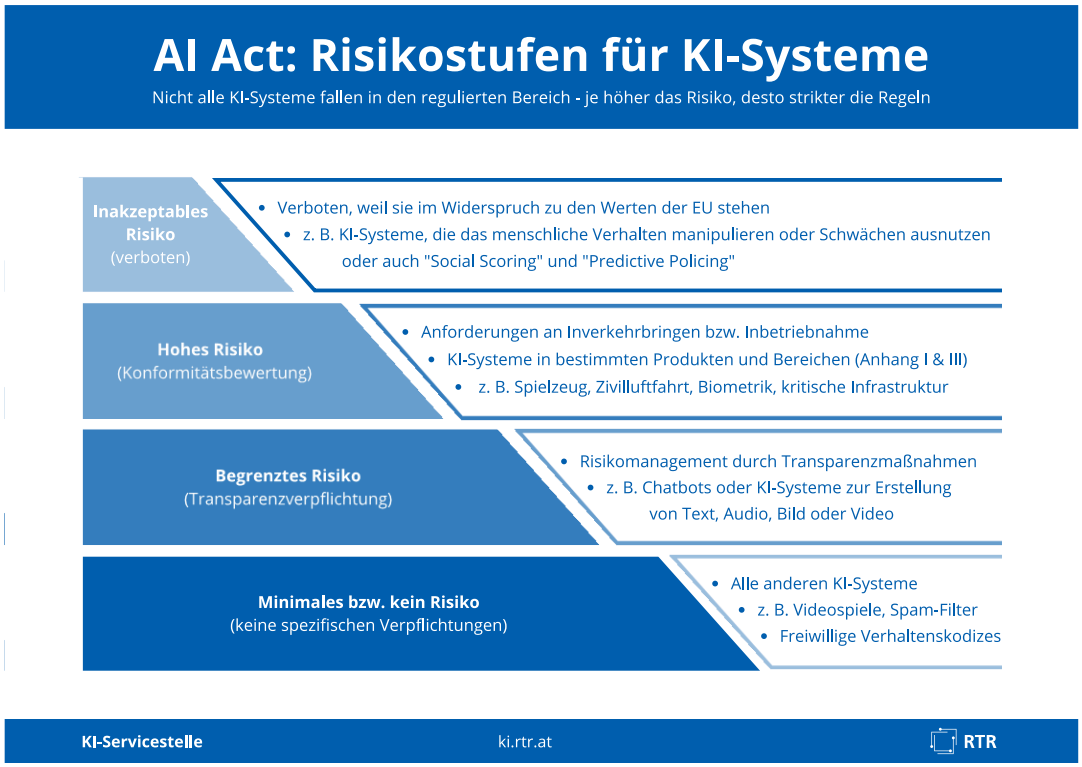
Der AI Act sieht viele Rollen in der KI-Wertschöpfungskette vor, die darin verschiedene Tätigkeiten übernehmen. Unterschieden wird dabei zwischen „Inverkehrbringen", „Bereitstellen" und „Inbetriebnahme". Zu den Akteuren im AI Act zählen etwa „Anbieter", „Produkthersteller", „Betreiber", und „Händler".

Wenn KMUs am Markt befindliche KI-Systeme in eigener Verantwortung für die Erfüllung diverser Aufgaben verwenden, sind sie meist als „Betreiber" gemäß Art 3 Z 4 AIA einzustufen. In der KI-Wertschöpfungskette sind sie den Anbietern nachgelagert – sie entwickeln KI-Systeme nicht, führen diese aber in der unternehmerischen Praxis aus. Eine Ausnahme besteht nur, falls KI-Systeme entgegen ihrer Zulassung eingesetzt werden – in diesem Fall zählen auch die einsetzenden Unternehmen als „Anbieter" (vgl. Art 25 AIA).



Eine risikobasierte Regulierung

Der AI Act verfolgt einen risikobasierten Ansatz, um ein verhältnismäßiges, wirksames und verbindliches Regelwerk für KI-Systeme einzuführen. KI-Systeme werden entsprechend ihrem Risikopotential nach inakzeptablem, hohem, begrenztem und minimalem Risiko kategorisiert. Die folgende Grafik dient zur besseren Veranschaulichung der Risikostufen für KI-Systeme.



Verbotene KI und Hochrisiko-KI

Manche Praktiken in Zusammenhang mit KI-Systemen bergen ein zu hohes Risiko im Hinblick auf die Wahrscheinlichkeit eines Schadenseintritts und auch des Schadensausmaßes an individuellen oder öffentlichen Interessen, weshalb sie verboten sind – etwa KI-Systeme für Social Scoring oder Predictive Policing.

Um diese Verbote in der Praxis besser einordnen zu können, hat die Kommission Leitlinien veröffentlicht, die als unverbindliche Auslegungshilfe dienen. Sie enthalten rechtliche Erläuterungen und praktische Beispiele, um den AI Act zu verstehen und einzuhalten. Die Leitlinien stehen auch in deutscher Sprache zur Verfügung. Den Link zu den Leitlinien finden Sie auf der Webseite der KI-Servicestelle unter der Rubrik „Ergänzende Leitlinien und Dokumente“ (https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/erg-leitlinien-und-dokumente.de.html).

Hochrisiko-KI-Systeme stellen – wie bereits der Name sagt – im Hinblick auf die Wahrscheinlichkeit eines Schadenseintritts und auch des Schadensausmaßes an individuellen oder öffentlichen Interessen ein hohes Risiko dar, sind aber gemäß Art 6

AIA nicht per se verboten. Das Inverkehrbringen oder die Inbetriebnahme ist unter Einhaltung bestimmter Anforderungen erlaubt. Derartige KI-Systeme sind unter anderem im Anhang I und III des AI Act aufgelistet (z.B. KI-Systeme im Bereich des Mitarbeiterrecruitings sind als Hochrisiko-KI-Systeme gemäß Anhang III Z 4 lit a AIA einzustufen). Für Betreiber sind die Verpflichtungen in Zusammenhang mit dem Betrieb von Hochrisiko-KI-Systemen in Artikel 26 AIA aufgelistet.

Auf europäischer Ebene gibt es bereits Leitlinien zur Interpretation des „KI-Systems". Zur Auslegung der Hochrisiko-KI-Bereiche werden Leitlinien für das Jahr 2026 erwartet. Der Link zu den gegenständlichen Leitlinien ist unter https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/erg-leitlinien-und-dokumente.de.html abrufbar

GPAI-Modelle

Sogenannte General Purpose AI Models (KI-Modelle mit allgemeinem Verwendungszweck) sind KI-Modelle, die ein breites Spektrum von Aufgaben bewältigen können, anstatt für eine spezifische Aufgabe oder Anwendung optimiert worden zu sein. Diese Modelle sind oft in der Lage, große Mengen an unstrukturierten Daten wie Text, Bildern, Audio und Videos zu verarbeiten. Beispiele für solche GPAI-Modelle sind die großen Sprachmodelle von OpenAI und anderen Anbietern.

Um die Umsetzung des AI Acts zu gewährleisten und die Verständlichkeit zu verbessern, haben das AI-Office und die Europäische Kommission Begleitmaterialien veröffentlicht.

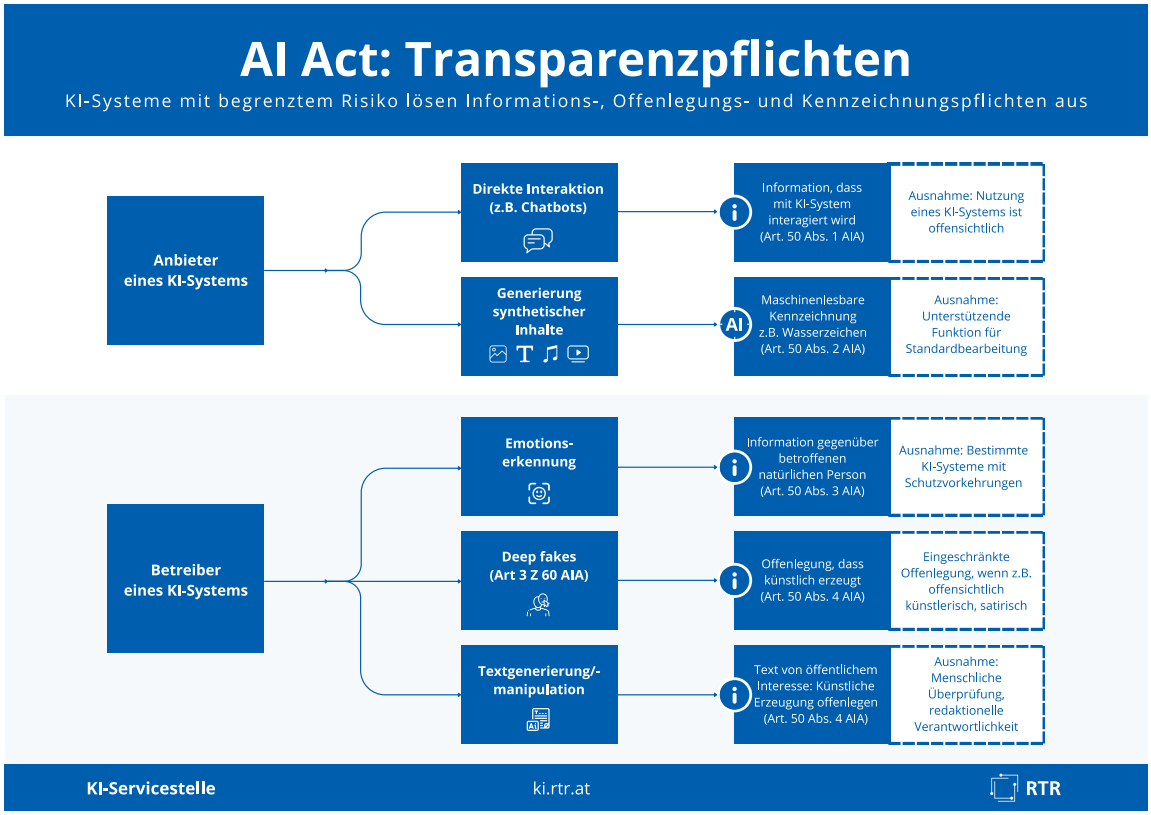
Ein vom AI-Office am 10.7.2025 veröffentlichter Praxisleitfaden - sogenannter „Code of Practice" (CoP) - besteht aus drei Dokumenten und enthält Informationen zu Transparenzmaßnahmen und zur Ermittlung und Analyse systemischer Risiken sowie Regelungen zur Beachtung des Urheberrechts.

Die von der Europäischen Kommission am 18.07.2025 veröffentlichten Leitlinien für Anbieter von KI - Modellen mit allgemeinem Verwendungszweck enthalten technische Kriterien, die die Kategorisierung von KI-Modellen erleichtern sollen und präzisieren die Ausnahme für Open-Source klar. Zudem wurde darin festgestellt, dass nur wesentliche Änderungen unter Aufwendung massiver Rechenkapazität dazu führt, dass es zu einem Angebot neuer KI-Modelle führt.Eru Es lässt sich deshalb aus den Leitlinien ableiten, dass österreichische Unternehmen nur im absoluten Ausnahmefall eine Rolle als Anbieter einnehmen werden.

Die Links zum Praxisleitfaden und den Leitlinien können der Webseite der KI-Servicestelle entnommen werden (https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/erg-leitlinien-und-dokumente.de.html).

Transparenzpflichten bei KI-Inhalten

Den Anbietern und Betreibern von KI-Systemen, die der Risikostufe „begrenztes Risiko“ einzustufen sind, legt der AI Act Offenlegungs-, Kennzeichnungs- bzw Informationspflichten gemäß Art 50 AIA auf (siehe folgende Grafik). Dies betrifft insbesondere auch die Nutzung von generativer KI.



Erzeuger von „Deep Fakes“ – Bild-, oder Videoinhalten, die wirklichen Personen, Objekten, Gegenständen, Orten, Einrichtungen und Ereignissen zum Verwechseln ähneln – haben (mit Ausnahmen) offenzulegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Für alle anderen Bild-, Ton- und Videoinhalte besteht keine Offenlegungspflicht (Art. 50 Abs. 4 UAbs. 1 AIA).

Bei der Nutzung von generativer KI zur Erzeugung von Text ist die KI-Nutzung offenzulegen, wenn der Text veröffentlicht werden soll, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren und keine menschliche Überprüfung oder redaktionelle Verantwortung vorliegt. Ansonsten besteht auch hier keine Transparenzpflicht (Art. 50 Abs. 4 UAbs. 2 AIA).

KI-Kompetenz

Der AI Act sieht vor, dass unabhängig des Risikos der eingesetzten KI-Systeme in Unternehmen die mit der Entwicklung, dem Betrieb und der praktischen Anwendung der KI-Systeme betrauten Personen über ein ausreichendes Maß an KI-Kompetenz verfügen (Art 3 Z 56 AIA iZm Art 4 AIA). Die Bestimmungen zur KI-Kompetenz traten mit 2.2.2025 in Kraft. Die KI-Kompetenz trifft alle relevanten Akteure auf der KI-Wertschöpfungsebene im Kontext ihrer Rolle entlang der Wertschöpfungskette (vgl. ErwG 20). Dabei ist zu beachten, dass je nach Risikoklasse und Einsatzbereich ein unterschiedliches Maß an KI-Kompetenz erforderlich ist. Die technischen Kenntnisse der Mitarbeitenden, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, sind zu berücksichtigen. KI-Kompetenz ist ein interdisziplinäres Feld, es umfasst nicht nur technische, sondern auch rechtliche und ethische Aspekte (siehe Erwägungsgrund 20 AIA). So haben sich Anbieter, die sich mit der Entwicklung eines Chatbots beschäftigen naturgemäß mit anderen Thematiken auseinanderzusetzen als ein Betreiber, der dieses System in seinem Unternehmen lediglich anwendet. Diese Präzisierung der unternehmerischen Sorgfaltspflichten soll sicherstellen, dass Mitarbeitende speziell für die für KI neuen Aspekte geschult sind.

Betroffen von der Verpflichtung zu KI-Kompetenz sind damit folgende Personengruppen:

- **Mit der Entwicklung von KI betrauten Personen**
- **Mit dem Betrieb von KI-Systemen betrauten Personen**
- **Personen innerhalb eines Unternehmens, die KI-Systeme einsetzen.**

Über die Art und Weise der zu treffenden Schulungsmaßnahmen bleibt der AI Act offen. Die Kompetenzvermittlung kann intern oder extern, durch e-Learnings oderFortbildungsveranstaltungen erfolgen. In der Praxis empfiehlt sich, die Arten, Inhalte, Zeitpunkte und geschulten Personen zu dokumentieren. Weiters ist auch ratsam laufende Erhebungen hinsichtlich des Status der vorhandenen KI-Kompetenzen zu tätigen und strategische wie operative Maßnahmen zu setzen. a

Detaillierte Informationen zur KI-Kompetenz finden Sie auf der Webseite der KI-Servicestelle (https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/ki-kompetenz.de.html).

KI-Servicestelle der RTR

Die in der RTR eingerichtete Servicestelle für Künstliche Intelligenz dient als Ansprechpartner und Informationshub einer breiten Öffentlichkeit zum Thema KI. Sie unterstützt auch bei der Umsetzung des europäischen AI Act. Unter ki.rtr.at finden Sie Informationen rund um regulatorische Rahmenbedingungen beim Einsatz von künstlicher Intelligenz sowie den Aspekten im Hinblick auf Cybersecurity, Datenökonomie und deren Einsatz im Medienbereich.

Fragen rund um regulatorische Rahmenbedingungen zum Thema KI können gerne per E-Mail an ki@rtr.at gerichtet werden. Wir sind stets bemüht alle Anfragen so rasch als möglich zu beantworten.

ENTWICKLUNG UND INTEGRATION VON KI-SYSTEMEN

Die Entwicklung der künstlichen Intelligenz hat sich in den letzten Jahren bereits grundlegend gewandelt. Was lange Zeit großen Technologieunternehmen in Form abstrakter KI-Modelle zur Lösung spezifischer Probleme vorbehalten war, ist heute auch für kleine und mittlere Unternehmen zugänglich geworden. Die seit 2022 öffentlich verfügbaren großen KI-Sprachmodelle (Large Language Models – LLM) haben sich rasant weiterentwickelt und bieten in der Praxis vielen Unternehmen eine enorme Produktivitätssteigerung. Moderne Systeme sind zunehmend multimodal, das heißt, sie verarbeiten Text, Bilder, Audio und Dokumente gemeinsam. Es gibt auch andere KI-Modelle außerhalb der Sprachverarbeitung, beispielsweise in der Medizin. In diesem Artikel liegt der Fokus jedoch auf der Nutzung von LLMs.

Prompt Engineering

Für Unternehmen, die in die KI-Entwicklung einsteigen möchten, bieten sich verschiedene Wege an, die sich in ihrer Komplexität und dem erforderlichen Ressourceneinsatz unterscheiden. Der einfachste und zugleich praktischste Einstieg erfolgt über das sogenannte Prompt Engineering. Dieser Ansatz lässt sich gut mit einem Einarbeitungsprozess vergleichen: Ähnlich wie Sie neuen Mitarbeitenden genaue Arbeitsanweisungen geben, formulieren Sie beim Prompt Engineering präzise Anweisungen für das KI-System. Der große Vorteil dieser Methode liegt darin, dass keine Programmierkenntnisse erforderlich sind. Stattdessen ist vor allem ein gutes Verständnis der eigenen geschäftlichen Anforderungen sowie die Fähigkeit, diese klar zu kommunizieren, gefragt.

Tools für den Einstieg: ChatGPT Enterprise, Claude for Work, Google Gemini Business ermöglichen Team-Nutzung mit Datenschutz-Garantien. Moderne No-Code-Plattformen wie Zapier AI, Make.com oder n8n ermöglichen KI-Integration in bestehende Workflows ohne Programmierung.

Kostengröße: 20-200€ pro Monat pro Nutzer für Business-Lizenzen.

Ein praktisches Beispiel verdeutlicht dies: Nehmen wir an, Sie betreiben einen Online-Shop und möchten KI im Kundenservice einsetzen. Sie würden dem System dann genaue Anweisungen geben, wie es auf verschiedene Kundenanfragen reagieren soll. Diese Anweisungen könnten beispielsweise festlegen, wie Kunden begrüßt werden sollen, wie bei Reklamationen vorzugehen ist oder wann ein menschlicher Mitarbeiter hinzugezogen werden muss. Durch eine sorgfältige Formulierung dieser Anweisungen stellen Sie sicher, dass die KI in Ihrem Sinne und nach Ihren Qualitätsstandards arbeitet.

BEISPIEL: Kundenservice-Prompt

„Du bist der erste Kundenservice-Kontakt für unseren Online-Shop [Unternehmensname], der Kleidung und Accessoires verkauft. Befolge diese Richtlinien in deiner Kommunikation:

- Beginne ein Gespräch stets freundlich mit ‚Willkommen bei [Unternehmensname]', gehe hiernach konkret auf die Frage der Kundschaft ein
- Frage aktiv nach weiteren Details, wenn die Anfrage unklar ist
- Bei Fragen zu Größen und Passform: Bitte nach genauen Körpermaßen und gewünschtem Tragegefühl
- Bei Reklamationen: Drücke Verständnis aus und frage nach der Bestellnummer und dem genauen Problem
- Bei Lieferzeitanfragen: Erkläre, dass die Standard-Lieferzeit 2-3 Werktage beträgt
- Bei komplexen technischen Problemen oder Beschwerden: Leite die Person höflich an einen menschlichen Mitarbeitenden weiter mit ‚Ich verbinde Sie gerne mit unserem spezialisierten Team für eine ausführliche Beratung'
- Beende jedes Gespräch mit ‚Danke für Ihr Vertrauen in [Unternehmensname]. Kann ich sonst noch etwas für Sie tun?"'

Um die Qualität der KI-Antworten zu prüfen, testen Sie den Prompt mit verschiedenen typischen Anfragen:

Anfrage 1: „Hallo, meine Bestellung ist noch nicht angekommen."
Erwartete KI-Antwort: „Willkommen bei [Unternehmensname]! Um Ihnen bei Ihrer Lieferung bestmöglich zu helfen, benötige ich bitte Ihre Bestellnummer..."

Anfrage 2: „Welche Größe soll ich bei der blauen Hose nehmen?"
Erwartete KI-Antwort: „Willkommen bei [Unternehmensname]! Für eine optimale Größenberatung bei der blauen Hose bräuchte ich von Ihnen bitte folgende Informationen: Ihre übliche Größe und Ihre bevorzugte Trageweise..."

Systematisches Testing: Überprüfen Sie regelmäßig stichprobenartig die KI-Antworten mit Testdatensätzen und definieren Sie KPIs wie Genauigkeit, Antwortzeit und Kundenzufriedenheit. Passen Sie den Prompt basierend auf häufigen Kundenanfragen, typischen Missverständnissen, Feedback und saisonalen Besonderheiten an.

WICHTIG: Die KI sollte nur die erste Kontaktaufnahme übernehmen und bei komplexeren Anliegen an menschliche Mitarbeitende übergeben. Zu diesem Zeitpunkt hat das System jedoch noch keine genaueren Informationen über Ihr Unternehmen, sondern „weiß" nur die im Prompt enthaltenen Informationen.

Retrieval Augmented Generation (RAG)

Um dieses Problem zu lösen, ist Retrieval Augmented Generation (RAG) die Lösung. Diese Technologie verbindet die Fähigkeiten moderner KI-Systeme mit dem spezifischen Wissen Ihres Unternehmens. Stellen Sie sich das wie einen sehr effizienten Assistenten vor, der zunächst in Ihren Unternehmensunterlagen nachschlägt und dann sein Wissen mit den gefundenen Informationen ergänzt. Dies ist besonders nützlich, wenn Sie möchten, dass die KI auf Basis Ihrer aktuellen Unternehmensdokumente arbeitet.

Technisch basiert RAG auf Vector Databases (z.B. Pinecone, Weaviate, Qdrant), die Ihre Dokumente semantisch durchsuchbar machen. Praktische RAG-Plattformen für KMU: Custom GPTs (OpenAI), Claude Projects (Anthropic), Microsoft Copilot Studio, oder spezialisierte Lösungen wie Glean oder Dashworks.

Kostengröße: 100-1.000€ pro Monat, abhängig von Dokumentenvolumen und Nutzerzahl.

BEISPIEL: RAG im Einsatz

Angenommen, eine Kundschaft fragt nach den Garantiebedingungen für ein spezielles Produkt. Ein herkömmliches KI-System könnte nur allgemeine Antworten geben. Ein RAG-System hingegen:

1. durchsucht Ihre spezifischen Garantierichtlinien
2. findet die exakten Bedingungen für das angefragte Produkt
3. formuliert eine präzise Antwort basierend auf Ihren tatsächlichen Unternehmensrichtlinien

Vorteile für Ihr Unternehmen

- Aktualität: Die Antworten basieren immer auf Ihren aktuellen Unternehmensdokumenten
- Genauigkeit: Das System kann nur Informationen verwenden, die Sie explizit zur Verfügung stellen
- Kontrolle: Sie bestimmen genau, welche Dokumente als Wissensbasis dienen

Datenschutz bei RAG: Prüfen Sie, wo Ihre Dokumente gespeichert werden. EU-Hosting bevorzugen. Für besonders sensible Daten: Open-Source-Modelle wie Llama, Mistral oder Phi ermöglichen lokales Hosting ohne Cloud-Abhängigkeit. Lokale Lösungen wie LM Studio, Ollama oder Jan.ai bieten volle Datenkontrolle.

KI-Agenten: Der nächste Schritt

KI-Agenten stellen eine Weiterentwicklung dar, die 2025/2026 für KMU besonders relevant wird. Während Prompt Engineering und RAG auf einzelne Anfragen reagieren, können KI-Agenten eigenständig mehrstufige Aufgaben erledigen, verschiedene Tools nutzen und komplexe Workflows automatisieren.

Praktisches Beispiel: Ein KI-Agent für Kundenreklamationen könnte:

1. Die Beschwerde analysieren
2. Automatisch die Bestellhistorie aus Ihrem System abrufen
3. Relevante Produktinformationen nachschlagen
4. Eine Lösung vorschlagen
5. Bei Genehmigung automatisch eine Gutschrift erstellen
6. Eine personalisierte E-Mail versenden

Tools für KI-Agenten: Zapier Central, Microsoft Copilot Studio, AutoGPT, n8n mit AI-Workflows, oder spezialisierte Plattformen wie Relevance AI.

Kostengröße: 200-2.000€ pro Monat, je nach Komplexität und Integrationstiefe.

Wichtig: Agenten benötigen klare Grenzen – definieren Sie genau, welche Aktionen automatisch erfolgen dürfen und wann menschliche Freigabe erforderlich ist.

Was geht darüber hinaus?

Wenn die Möglichkeiten von Prompt Engineering, RAG und Agenten nicht mehr ausreichen, bietet sich als nächster Schritt das Fine Tuning an. Bei dieser Methode wird ein bestehendes KI-Modell gezielt an die spezifischen Bedürfnisse Ihres Unternehmens angepasst. Dies erfordert zwar mehr technisches Know-how und Ressourcen (ab ca. 1.000-5.000€ monatlich), ermöglicht aber eine bessere Abstimmung auf individuelle Anforderungen. Ein Beispiel: firmenspezifische Verträge, die immer gleich formuliert werden sollen und immer dieselben Passagen enthalten müssen.

Sicherheit bei eigener Entwicklung: Achten Sie auf Datenisolation, Zugriffskontrollen, kontinuierliches Monitoring und Backup-Strategien. Dokumentieren Sie: Welche Prompts/Modelle verwendet werden, welche Daten verarbeitet werden – für Nachvollziehbarkeit und Compliance. Bei eigener Entwicklung: AI Act-Konformität beachten, insbesondere bei Hochrisiko-Anwendungen (ab August 2026).

Erfolgreich starten: Praktische Empfehlungen

5 Quick Wins für den Einstieg

1. E-Mail-Entwürfe: KI formuliert professionelle Antworten auf Standardanfragen
2. Dokumentzusammenfassungen: Lange Berichte in Kernaussagen kondensieren
3. Meeting-Protokolle: Automatische Zusammenfassungen aus Notizen
4. FAQ-Beantwortung: Chatbot für wiederkehrende Kundenfragen
5. Übersetzungen: Mehrsprachige Kommunikation ohne externe Dienstleister

Häufige Fehler vermeiden

- Zu komplexe erste Projekte: Starten Sie klein und überschaubar
- Unklare Erfolgsmetriken: Definieren Sie vorab, woran Sie Erfolg messen
- Fehlende Mitarbeiterschulung: Binden Sie das Team frühzeitig ein
- Keine Iterationen: Planen Sie regelmäßige Optimierungszyklen ein
- Kein Fallback: Halten Sie manuelle Prozesse als Backup bereit

ROI ermitteln

Einfache Formel: Zeitersparnis × Stundensatz - Lizenzkosten - Implementierungsaufwand = Return on Investment

Beispiel: 5 Stunden Zeitersparnis pro Woche × 50€ Stundensatz = 250€/Woche = 1.000€/Monat Nutzen minus 200€ Lizenzkosten = 800€ monatlicher Gewinn.

Kontinuierliche Optimierung

KI-Systeme sind nie „fertig". Planen Sie ein: → Regelmäßige Prompt-Anpassungen basierend auf Feedback

- Aktualisierung der Wissensdatenbank bei RAG
- Performance-Monitoring und Qualitätssicherung
- Anpassung an neue Geschäftsanforderungen

Vom Piloten zur Produktion

Für einen erfolgreichen Einstieg in die KI-Entwicklung empfiehlt sich ein schrittweises Vorgehen:

1. Beginnen Sie klein: Starten Sie mit überschaubaren Projekten im Bereich Prompt Engineering
2. Sammeln Sie Erfahrungen: Bauen Sie intern Expertise auf
3. Messen und lernen: Definieren Sie KPIs und evaluieren Sie regelmäßig
4. Skalieren: Erweitern Sie auf RAG oder Agenten, wenn Anforderungen wachsen
5. Hybride Ansätze: In der Praxis kombinieren viele Unternehmen verschiedene Methoden

Prüfen Sie auch alternative Lösungen wie Partnerschaften mit KI-Beratungsunternehmen, spezialisierten Entwickler-Teams oder WKO-Netzwerkpartnern sowie den Einsatz fertiger Lösungen.

Durch sorgfältige Planung und verantwortungsvolle Umsetzung können auch kleinere Unternehmen die Chancen der künstlichen Intelligenz nutzen und ihre Prozesse zukunftsfähig gestalten. Der Schlüssel zum Erfolg liegt dabei nicht in der Komplexität der gewählten Methode, sondern in der durchdachten Anwendung und der konsequenten Ausrichtung an den eigenen Unternehmenszielen. Künstliche Intelligenz, im Speziellen die großen Sprachmodelle, bieten eine enorme Produktivitätssteigerung, wenn sie richtig eingesetzt werden.

Diese Broschüre ist ein Produkt der Zusammenarbeit aller Wirtschaftskammern.
Bei Fragen wenden Sie sich bitte an die Wirtschaftskammer Ihres Bundeslandes:
Wien, Tel. Nr.: (01) 51450-1144, Niederösterreich, Tel. Nr.: (02742) 851-16600, Oberösterreich, Tel. Nr.: 0590 909,
Burgenland, Tel. Nr.: 0590 907-2000, Steiermark, Tel. Nr.: (0316) 601-601, Kärnten, Tel. Nr.: 0590 904,
Salzburg, Tel. Nr.: (0662) 8888-397, Tirol, Tel. Nr.: 0590 905-1111, Vorarlberg, Tel. Nr.: (05522) 305-1122
Hinweis! Diese Information finden Sie auch im Internet unter https://wko.at/innovation Alle Angaben
erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr.
Eine Haftung der Wirtschaftskammern Österreichs ist ausgeschlossen.
Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter!