



Unternehmensleitlinien zum Einsatz von KI

MARTIN FOLZ



Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital



aufgrund eines Beschlusses
des Deutschen Bundestages

Künstliche Intelligenz (KI) kann Arbeitsabläufe erleichtern, Wissen schneller verfügbar machen und Mitarbeitende entlasten. Damit der Einsatz im Unternehmen sicher und nachvollziehbar bleibt, brauchen KMU klare Leitlinien. Sie legen fest, welche KI-Anwendungen erlaubt sind, welche Daten geschützt bleiben müssen und wie unerlaubte Nutzung organisatorisch und technisch begrenzt werden kann.

In diesem Nachgelesen erfahren Sie:

- Warum KI-Leitlinien wichtig sind,
- Wie die KI-Verordnung Unternehmen einstuft, die KI anwenden
- Wie Sie Schatten-KI begrenzen,
- Wie Risikoeinstufung als Entscheidungshilfe dienen kann,
- Wie Sie KI-Inhalte kennzeichnen und
- Welche Bausteine zu einer praxisnahen Leitlinie beitragen.

Impressum

HERAUSGEBER

Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG UND PRODUKTION

PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL Bild generiert mit KI

VERÖFFENTLICHUNG Juli 2026





↑ © muqddas65 - Magnific.com

Hinweis: Dieser Beitrag bietet eine erste Orientierung und ersetzt keine Rechtsberatung. Bei konkreten rechtlichen Fragen, etwa zu Datenschutz, Arbeitsrecht, Haftung oder Pflichten nach der KI-Verordnung, sollten Unternehmen anwaltliche Unterstützung einholen.

Warum KI-Leitlinien vor allem Organisationshilfe sind

Viele Unternehmen starten mit KI nicht durch ein großes Strategieprojekt. Häufig beginnt die Nutzung im Kleinen: Eine Fachkraft lässt sich eine E-Mail formulieren, eine Abteilung testet ein Übersetzungstool oder ein Team nutzt Chatbots für Recherchen. Das kann hilfreich sein. Problematisch wird es, wenn Verantwortliche nicht wissen, welche Anwendungen tatsächlich genutzt werden, welche Daten dort landen und ob Ergebnisse geprüft werden.

KI-Leitlinien schaffen dafür einen klaren Rahmen. Sie beantworten einfache, aber wichtige Fragen: Welche KI-Anwendungen dürfen Mitarbeitende nutzen? Welche Aufgaben eignen sich für KI? Welche Daten dürfen nicht eingegeben werden? Wer prüft neue Anwendungen? Wer ist Ansprechperson bei Unsicherheiten?

Der Fokus sollte nicht auf Verboten liegen, sondern auf sicherer Nutzung. Eine gute Leitlinie macht Mitarbeitende handlungsfähig. Sie erklärt, was erlaubt ist, was geprüft werden muss und was ausgeschlossen bleibt. So entsteht Orientie-

rung im Arbeitsalltag. Gerade für KMU ist das wichtig, weil sie oft keine großen Compliance-, IT- oder Rechtsabteilungen haben.

Unternehmen, die KI nutzen, fallen nach der KI-Verordnung unter Betreiber

Die KI-Verordnung unterscheidet verschiedene Rollen. Anbieter entwickeln oder vermarkten KI-Systeme. Betreiber nutzen KI-Systeme im beruflichen Kontext. Viele KMU sind daher vor allem Betreiber, wenn sie externe KI-Anwendungen einsetzen, etwa für Textarbeit, Kundenkommunikation, Personalprozesse, Produktion, Qualitätsprüfung oder interne Wissensarbeit.

Für Betreiber steht die Organisation der Nutzung im Mittelpunkt. Sie müssen nicht automatisch alle Pflichten eines Anbieters erfüllen. Sie sollten aber wissen, welche KI-Systeme im Unternehmen laufen, wofür sie genutzt werden und ob daraus besondere Risiken entstehen. Die Bundesnetzagentur beschreibt die KI-Verordnung als risikobasierten Rechtsrahmen. Je höher das Risiko eines KI-Systems, desto strenger sind die Anforderungen an Transparenz, Sicherheit und Compliance^[1].

Wichtig ist auch die KI-Kompetenz. Anbieter und Betreiber sollen dafür sorgen, dass Personen, die in ihrem Auftrag mit



KI-Systemen umgehen, über ein ausreichendes Maß an KI-Kompetenz verfügen. Dazu zählen technisches Grundverständnis, Erfahrung, Schulung und der konkrete Nutzungskontext^[2]. Für KMU heißt das: Mitarbeitende sollten verstehen, wo KI helfen kann, wo Fehler entstehen können und was deren Konsequenzen sein können sowie wann Ergebnisse geprüft werden müssen.

Whitelist statt Blacklist: Nur freigegebene KI-Anwendungen nutzen

Für Unternehmen empfiehlt sich ein **Whitelist-Ansatz**. Das bedeutet: Es dürfen nur KI-Anwendungen genutzt werden, die ausdrücklich geprüft und freigegeben wurden. Dieser Ansatz ist meist besser als eine Blacklist, bei der einzelne unerwünschte Anwendungen verboten werden. Der Grund ist einfach: Neue KI-Tools entstehen sehr schnell. Eine Blacklist ist daher oft schon veraltet, bevor sie vollständig gepflegt wurde.

Eine Whitelist kann in KMU übersichtlich starten. Zum Beispiel mit drei Kategorien:

- **Freigegeben:** Anwendungen, die geprüft wurden und für bestimmte Aufgaben genutzt werden dürfen.
- **Prüfung erforderlich:** Anwendungen, die interessant sind, aber noch nicht bewertet wurden.
- **Nicht erlaubt:** Anwendungen, die nicht genutzt werden dürfen, etwa weil Datenschutz, IT-Sicherheit oder Vertragsbedingungen unklar sind. (Entspricht dem Blacklist-Ansatz)

Zu jeder freigegebenen Anwendung sollte das Unternehmen festhalten: Wofür darf sie genutzt werden? Welche Daten dürfen eingegeben werden? Wer ist fachlich verantwortlich? Welche Ergebnisse müssen geprüft werden? Gibt es Einschränkungen, zum Beispiel keine Nutzung für personenbezogene Daten, Kundendaten oder Geschäftsgeheimnisse?

Der Vorteil: Mitarbeitende erhalten sichere Optionen, statt auf eigene Lösungen auszuweichen. Gleichzeitig behält das Unternehmen den Überblick.

Schatten-KI begrenzen: Organisatorische und technische Maßnahmen

Schatten-KI entsteht, wenn Mitarbeitende KI-Anwendungen ohne Freigabe nutzen. Das passiert oft nicht aus böser Absicht, sondern aus Zeitdruck, Arbeitserleichterung oder Neugier. Trotzdem kann es riskant werden. Vertrauliche Informationen können in externe Systeme gelangen. Ergebnisse können ungeprüft übernommen werden. Außerdem fehlt dem Unternehmen die Grundlage, um Datenschutz, Sicherheit und Pflichten nach der KI-Verordnung zu bewerten.

Unternehmen sollten Schatten-KI deshalb mit organisatorischen und technischen Maßnahmen begrenzen.

Organisatorisch sinnvoll sind:

- Eine klare KI-Leitlinie mit Whitelist-Ansatz,
- ein einfaches Verfahren zur Freigabe neuer KI-Anwendungen,
- feste Ansprechpersonen für KI-Fragen,
- kurze Schulungen zur sicheren Nutzung,
- Beispiele für erlaubte und nicht erlaubte Eingaben,
- regelmäßige Überprüfung der tatsächlich genutzten Anwendungen,
- klare Regeln für KI-generierte Inhalte durch z.B. Kennzeichnung, Quellenprüfung und menschliche Kontrolle.

Technisch können Unternehmen ergänzend arbeiten mit:

- DNS-Blocking bekannter nicht freigegebener KI-Domains,
- Webfilter oder Secure Web Gateway,



- Firewall-Regeln für unerwünschte Dienste,
- Sperrung nicht freigegebener Browser-Erweiterungen,
- Geräteverwaltung für Unternehmensgeräte,
- Rollen- und Rechtekonzepten,
- Protokollierung der Nutzung freigegebener Anwendungen,
- zentralem Zugriff über Unternehmensaccounts statt privater Konten.

Auch wenn alle oben genannten technischen Maßnahmen ergriffen wurden, besteht keine 100-prozentige Sicherheit. Neue Domains, mobile Geräte, private Zugänge, VPN-Verbindungen oder KI-Funktionen in bereits genutzter Software können solche Sperren umgehen. Außerdem bieten Suchmaschinen wie Google bereits KI-Antworten an. Der wichtigste Punkt bleibt: Unternehmen sollten sichere, freigegebene Alternativen bereitstellen und erklären, warum bestimmte Anwendungen nicht genutzt werden dürfen.

Risiko-Einstufung als einfache Entscheidungshilfe

Nicht jede KI-Nutzung ist gleich kritisch. Eine interne Risiko-Einstufung hilft, Anwendungen im Unternehmen schnell zu sortieren. Für KMU reicht häufig ein einfaches Modell:

Niedriges Risiko:

KI unterstützt bei Formulierungen, Ideen, Übersetzungen oder allgemeinen Zusammenfassungen. Es sollten keine vertraulichen oder personenbezogenen Daten eingegeben werden. Ergebnisse prüft ein Mensch.

Mittleres Risiko:

KI unterstützt interne Prozesse, Auswertungen oder Kundenkommunikation. Hier braucht es klare Regeln zu Daten, Prüfung, Freigabe und Transparenz.

Hohes Risiko:

KI beeinflusst Entscheidungen über Menschen, zum Beispiel in Personalprozessen, Qualifizierung, Leistungsbewertung, Kreditwürdigkeit oder sicherheitsrelevanten Bereichen. Solche Anwendungen brauchen eine besonders sorgfältige Prüfung.

Nicht zulässig oder nicht freigeben:

Anwendungen, die gegen interne Regeln, Datenschutzvorgaben oder die KI-Verordnung verstoßen können, dürfen nicht genutzt werden. Dazu können etwa manipulative Anwendungen, unzulässige biometrische Verfahren oder nicht geprüfte KI-Systeme in sensiblen Entscheidungsprozessen gehören.

Für Hochrisiko-KI-Systeme gelten besondere Pflichten. Betreiber müssen unter anderem geeignete technische und organisatorische Maßnahmen treffen, das System nach Anleitung nutzen, menschliche Aufsicht sicherstellen, Eingabedaten kontrollieren, den Betrieb beobachten und bestimmte Protokolle aufbewahren^[3].

KI-Inhalte kennzeichnen

KI-Leitlinien sollten auch regeln, wann KI-generierte Inhalte gekennzeichnet werden. Das betrifft zum Beispiel Bilder, Videos, Audioinhalte, Chatbot-Kommunikation oder Texte, die öffentlich eingesetzt werden. Die EU stellt dafür Icons bereit, mit denen KI-generierte oder KI-veränderte Inhalte kenntlich gemacht werden können. Die Icons sind freiwillig nutzbar, wenn es sich nicht um Deep Fakes oder KI-manipuliertes Material handelt. Die Kennzeichnungspflichten nach Artikel 50 der KI-Verordnung bleiben davon unabhängig^[4].

Für KMU kann eine einfache Regel helfen: Immer, wenn KI-Inhalte extern veröffentlicht werden oder bei Kundschaft, Partnern oder Öffentlichkeit einen falschen Eindruck erwecken könnten, sollte eine Kennzeichnung geprüft werden. Das gilt besonders bei KI-generierten Bildern von Personen, Produktvisualisierungen, Deepfakes, automatisiert erzeugten Nachrichten oder Inhalten zu Themen von öffentlichem Interesse. Für interne Inhalte sollte ein pragmatischer Ansatz gewählt werden und müssen nicht gekennzeichnet werden.



Bausteine einer praxistauglichen KI-Leitlinie

Eine KI-Leitlinie muss nicht lang sein. Wichtig ist, dass sie verständlich und im Arbeitsalltag nutzbar bleibt. Sie sollte mindestens folgende Punkte enthalten:

- 1** Ziel der KI-Nutzung: Wofür möchte das Unternehmen KI einsetzen?
- 2** Geltungsbereich: Für wen und welche Systeme gilt die Leitlinie?
- 3** Whitelist freigegebener KI-Anwendungen: Welche Tools dürfen genutzt werden?
- 4** Freigabeprozess: Wie können Mitarbeitende neue KI-Anwendungen vorschlagen?
- 5** Datenregeln: Welche Informationen dürfen nicht in KI-Systeme eingegeben werden?
- 6** Risikoeinstufung: Wann ist eine vertiefte Prüfung nötig?
- 7** Menschliche Kontrolle: Wann müssen Ergebnisse geprüft oder freigegeben werden?
- 8** Kennzeichnung: Wann werden KI-Inhalte gekennzeichnet?
- 9** Schulung: Wie bauen Mitarbeitende KI-Kompetenz auf?
- 10** Technische Schutzmaßnahmen: Welche Anwendungen werden blockiert oder nur kontrolliert zugänglich gemacht?
- 11** Meldewege: Was tun Mitarbeitende bei Fehlern, Datenpannen oder Unsicherheiten?
- 12** Aktualisierung: Wie oft prüft das Unternehmen die Leitlinie?

tene Tools stehen im Mittelpunkt, sondern eine Liste geprüfter und freigegebener Anwendungen.

Technische Maßnahmen wie DNS-Blocking, Webfilter oder Rechtekonzepte können die unerlaubte Nutzung zusätzlich erschweren. Sie ersetzen aber keine klare Organisation. Entscheidend sind verständliche Regeln, sichere Alternativen, geschulte Mitarbeitende und feste Verantwortlichkeiten.

Der Einstieg kann schlank erfolgen: KI-Inventar erstellen und nach Risiko bewerten, erste Anwendungen freigeben, Datenregeln formulieren, Schulungen anbieten und technische Grundschutzmaßnahmen einführen. Danach sollte die Leitlinie regelmäßig angepasst werden. Denn KI-Anwendungen, rechtliche Anforderungen und Arbeitsprozesse verändern sich schnell.

Für rechtliche Vertiefungen bietet die Wissensbox Recht des Mittelstand-Digital Zentrums Chemnitz kompakte Informationen rund um Digitalisierung und Recht, darunter gesetzliche Vorschriften, Rechtsprechung und Handlungsempfehlungen für Unternehmen.

Fazit und Ausblick

Unternehmensleitlinien zum Einsatz von KI sind ein praktisches Werkzeug für den Arbeitsalltag. Sie helfen KMU, Chancen von KI zu nutzen und Risiken zu begrenzen. Besonders wichtig ist ein klarer Whitelist-Ansatz: Nicht einzelne verbo-



Quellen und weiterführende Informationen

- 1** Bundesnetzagentur - KI. (o. D.). https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/start_ki.html
- 2** AI ACT Service Desk - Artikel 4: KI-Kompetenz. (o. D.). <https://ai-act-service-desk.ec.europa.eu/de/ai-act/article-4>
- 3** AI Act Service Desk - Artikel 26: Pflichten der Betreiber von Hochrisiko-KI-Systemen. (o. D.). <https://ai-act-service-desk.ec.europa.eu/de/ai-act/article-26>
- 4** EU-Icons zur Kennzeichnung von KI-generierten Inhalten. (o. D.). Gestaltung der Digitalen Zukunft Europas. <https://digital-strategy.ec.europa.eu/de/policies/eu-icons-labelling-ai-generated-content>

Verfasst von

MARTIN FOLZ ist wissenschaftlicher Mitarbeiter an der Professur Fabrikplanung und Intralogistik der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz beschäftigt er sich mit den Themen IoT & Automatisierungstechnik, künstliche Intelligenz sowie mobile Endgeräte.

martin.folz@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.





Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital 