EU AI Act & DSGVO-konforme KI-Nutzung

Rechtssicherheit für KMU: Praxishandbuch

Inhaltsverzeichnis

Vorwort: KI-Nutzung im Mittelstand

Liebe Unternehmerinnen und Unternehmer,

wenn Sie dieses Handbuch in den Händen halten, gehören Sie wahrscheinlich zu den 78% der bayerischen KMU, die bereits KI-Tools nutzen oder deren Einsatz planen. Vielleicht verwenden Sie ChatGPT für Marketingtexte, Microsoft Copilot für Ihre Office-Dokumente oder branchenspezifische KI-Lösungen für Ihre Kernprozesse.

Seit Februar 2025 gilt der EU AI Act, der erstmals verbindliche Regeln für die Nutzung von KI-Systemen festlegt. Gleichzeitig müssen wir weiterhin die DSGVO beachten. Für Sie als Unternehmer bedeutet das: Sie müssen wissen, wie Sie KI rechtssicher einsetzen können, ohne in teure Haftungsfallen zu tappen.

> *"Ich dachte, ich kann einfach ChatGPT nutzen, ohne mir Gedanken zu machen. Jetzt höre ich von KI-Kompetenz-Pflicht und Dokumentationsanforderungen. Was bedeutet das konkret für mich als Handwerksmeister?" — Thomas Wittleben, Schreinermeister*

Diese Frage stellte ein Teilnehmer in unserem letzten Webinar. Sie bringt auf den Punkt, was viele von Ihnen bewegt. Dieses Handbuch gibt Ihnen praxisnahe Antworten – ohne Juristendeutsch, dafür mit konkreten Handlungsempfehlungen für Ihren Unternehmensalltag.

Wir haben die Inhalte speziell für die Bedürfnisse von KMU-Inhabern und Geschäftsführern aus verschiedenen Branchen aufbereitet – vom Handwerk über IT bis hin zu Gastronomie und Beratung. Dabei berücksichtigen wir sowohl die Anforderungen für Einsteiger als auch für fortgeschrittene KI-Anwender.

Lassen Sie uns gemeinsam den Weg zu einer rechtssicheren KI-Nutzung gehen!

Ihr Arno Schimmelpfennig
DIN-Experte für KI und Leiter der KI-Akademie
Bund der Selbständigen Bayern

Der EU AI Act im Überblick

Was ist der EU AI Act?

Der EU AI Act ist die weltweit erste umfassende Regulierung für Künstliche Intelligenz. Er trat im Februar 2025 in Kraft und betrifft alle Unternehmen, die KI-Systeme anbieten oder nutzen – unabhängig von ihrer Größe.

Die wichtigsten Punkte auf einen Blick:

- **Risikobasierter Ansatz**: KI-Systeme werden in verschiedene Risikokategorien eingeteilt
- **Transparenzpflichten**: Nutzer müssen wissen, wenn sie mit KI interagieren
- **KI-Kompetenz-Pflicht**: Anbieter und Betreiber müssen KI-Kompetenz nachweisen
- **Dokumentationspflichten**: KI-Systeme müssen dokumentiert werden
- **Sanktionen**: Bei Verstößen drohen empfindliche Bußgelder

Was bedeutet das für KMU?

Als KMU sind Sie wahrscheinlich vor allem **Betreiber** von KI-Systemen, nicht deren Entwickler. Das bedeutet:

1. Sie müssen wissen, welche KI-Tools Sie einsetzen und zu welchem Zweck
2. Sie müssen die Risiken dieser Tools einschätzen können
3. Sie müssen sicherstellen, dass Ihre Mitarbeiter kompetent im Umgang mit KI sind
4. Sie müssen die Nutzung dokumentieren

> ***Praxis-Tipp:*** *Erstellen Sie ein einfaches KI-Inventar, in dem Sie alle genutzten KI-Tools mit Einsatzzweck und Risikokategorie auflisten. Dies ist der erste Schritt zur Compliance und hilft Ihnen, den Überblick zu behalten.*

Die Risikokategorien im EU AI Act

Der EU AI Act teilt KI-Systeme in vier Risikokategorien ein:

1. **Unannehmbares Risiko**: Diese KI-Systeme sind verboten (z.B. Social Scoring)
2. **Hohes Risiko**: Strenge Anforderungen an Transparenz, Robustheit und menschliche Aufsicht
3. **Begrenztes Risiko**: Transparenzpflichten (z.B. Chatbots müssen sich als KI zu erkennen geben)
4. **Minimales Risiko**: Keine spezifischen Anforderungen

Die meisten KI-Tools, die KMU einsetzen (wie ChatGPT, Microsoft Copilot oder Google Gemini), fallen in die Kategorien "begrenztes" oder "minimales" Risiko. Es gibt jedoch Ausnahmen, besonders wenn Sie in sensiblen Bereichen tätig sind oder personenbezogene Daten verarbeiten.

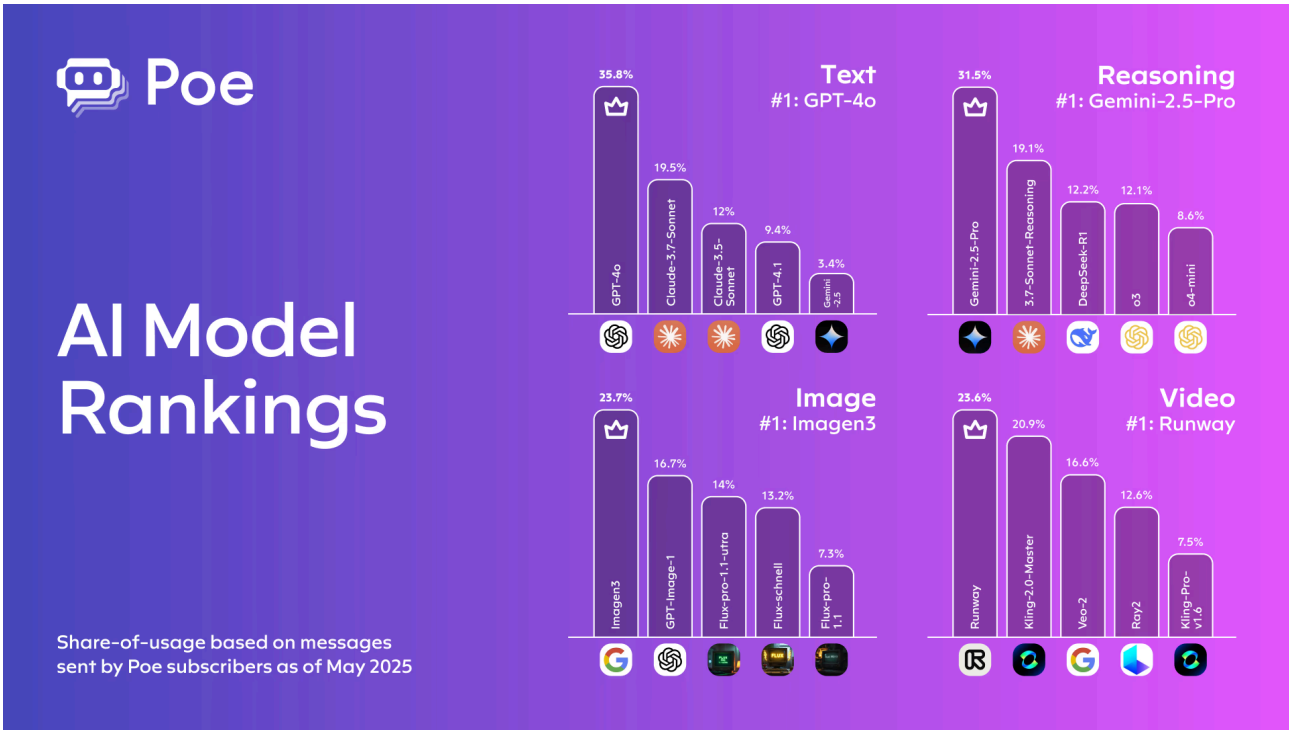

Abbildung: Marktanteile verschiedener KI-Modelle (Stand: Mai 2025)

KI-Kompetenz nach Artikel 4: Was bedeutet das für mein Unternehmen?

Die gesetzliche Grundlage

Artikel 4 des EU AI Acts führt eine neue Pflicht ein: KI-Kompetenz. Diese gilt für alle Anbieter und Betreiber von KI-Systemen – also auch für Ihr Unternehmen, wenn Sie KI-Tools einsetzen.

> ***Definition laut AI Act, Artikel 3 Nr. 56:*** *"KI-Kompetenz bezeichnet die Fähigkeiten, Kenntnisse und das Verständnis, um KI-Systeme sachkundig einzusetzen und sich dabei der Chancen und Risiken bewusst zu sein."*

Die vier Grundsteine der KI-Kompetenz

1. **Individuellen Bedarf ermitteln**
2. Wer arbeitet mit welchen KI-Systemen zu welchem Zweck?
3. Welche Vorkenntnisse sind vorhanden?
4. Welche Risiken bestehen bei der Nutzung?
5. **Maßnahmen ausgestalten**
6. Schulungen und Trainings entwickeln
7. Lernmaterialien bereitstellen
8. Externe Expertise einbinden, wenn nötig
9. **Regelmäßige Auffrischung**
10. KI-Kompetenz ist kein einmaliges Projekt
11. Kontinuierliche Anpassung an technologische Entwicklungen
12. Regelmäßige Updates für Mitarbeiter
13. **Ausreichende Dokumentation**
14. Art, Umfang und Inhalte der Maßnahmen festhalten
15. Teilnehmer und Termine dokumentieren
16. Nachweise für Behörden vorhalten

Flexibler Ansatz statt starrer Regeln

Die Bundesnetzagentur betont in ihrem Hinweispapier einen flexiblen Ansatz. Es gibt keine starren Regeln, sondern die Maßnahmen müssen angemessen sein – abhängig von:

- Ihrer Rolle (Anbieter oder Betreiber)
- Dem Risiko des KI-Systems
- Dem Einsatzkontext
- Den Vorkenntnissen Ihres Personals

Praxisbeispiel: Schreinerei Holzdesign GmbH

Die Schreinerei Holzdesign GmbH mit 12 Mitarbeitern nutzt ChatGPT für Marketingtexte und eine KI-gestützte Planungssoftware für Küchendesigns. Inhaber Christoph Heinzl hat folgende Maßnahmen umgesetzt:

1. **Bedarfsermittlung**: Zwei Mitarbeiter nutzen ChatGPT, vier arbeiten mit der KI-Planungssoftware
2. **Maßnahmen**:
3. Teilnahme an einem halbtägigen Webinar zu "KI-Grundlagen für Handwerker"
4. Interne Schulung zur KI-Planungssoftware durch den Anbieter
5. Erstellung eines kurzen Leitfadens für die ChatGPT-Nutzung
6. **Auffrischung**: Vierteljährliches Update-Meeting zu KI-Themen
7. **Dokumentation**: Einfache Excel-Tabelle mit Schulungsterminen, Teilnehmern und Inhalten

> ***Praxis-Tipp:*** *Für kleine Unternehmen reicht oft eine einfache Dokumentation. Wichtig ist, dass Sie nachweisen können, dass Sie sich mit dem Thema KI-Kompetenz auseinandergesetzt haben und angemessene Maßnahmen ergriffen haben.*

Der 3-Stufen-Compliance-Check

Um die Anforderungen des EU AI Acts und der DSGVO zu erfüllen, empfehlen wir einen pragmatischen 3-Stufen-Compliance-Check. Dieser hilft Ihnen, schnell und effizient die wichtigsten Maßnahmen umzusetzen.

Stufe 1: KI-Inventar erstellen

Ziel: Überblick über alle genutzten KI-Tools gewinnen

Vorgehen: 1. Liste aller genutzten KI-Tools erstellen 2. Einsatzzweck für jedes Tool dokumentieren 3. Betroffene Daten identifizieren (besonders personenbezogene Daten) 4. Verantwortliche Mitarbeiter benennen

Beispiel-Tabelle:

KI-Tool	Einsatzzweck	Betroffene Daten	Verantwortlicher
ChatGPT	Marketingtexte	Keine personenbezogenen Daten	Fr. Müller, Marketing
Microsoft Copilot	Office-Dokumente	Interne Geschäftsdaten	Hr. Schmidt, IT
KI-Buchhaltungssoftware	Rechnungsverarbeitung	Kundendaten, Finanzdaten	Fr. Weber, Buchhaltung

Stufe 2: Risikobewertung durchführen

Ziel: Risikokategorie der KI-Tools bestimmen und entsprechende Maßnahmen ableiten

Vorgehen: 1. Für jedes KI-Tool die Risikokategorie bestimmen 2. Besonders auf Hochrisiko-Anwendungen achten 3. Spezifische Anforderungen für jede Kategorie identifizieren

Risikokategorien und typische KMU-Anwendungen:

- **Minimales Risiko:**
- Textgeneratoren ohne Personenbezug

- Einfache Bildbearbeitungs-KI
- KI-gestützte Übersetzungstools
- **Begrenztes Risiko:**
- Kundensupport-Chatbots
- KI-gestützte Marketinganalysen
- Personalisierte Produktempfehlungen
- **Hohes Risiko:**
- KI-gestützte Bewerberauswahl
- Kreditwürdigkeitsprüfung
- Medizinische Diagnose-Unterstützung

Stufe 3: Dokumentation anlegen

Ziel: Compliance nachweisbar machen

Vorgehen: 1. KI-Kompetenz-Maßnahmen dokumentieren 2. Datenschutz-Folgenabschätzung für Hochrisiko-Anwendungen 3. Technische und organisatorische Maßnahmen festhalten 4. Regelmäßige Überprüfung und Aktualisierung

Mindestumfang der Dokumentation:

- Beschreibung der KI-Systeme und ihrer Einsatzzwecke
- Risikobewertung und Einstufung
- Durchgeführte Schulungen und Kompetenzmaßnahmen
- Verantwortlichkeiten und Ansprechpartner
- Maßnahmen zur DSGVO-Konformität
- Aktualisierungshistorie

> ***Praxis-Tipp:*** *Nutzen Sie unsere Vorlage "AI Act Artikel 4 Checkliste" im Anhang dieses Handbuchs. Sie führt Sie Schritt für Schritt durch den 3-Stufen-Compliance-Check und hilft Ihnen, keine wichtigen Punkte zu übersehen.*

DSGVO-konforme KI-Nutzung

Die DSGVO gilt natürlich weiterhin, auch wenn KI im Spiel ist – und sie stellt besondere Anforderungen an die KI-Nutzung.

Die DSGVO-Basics für KI-Tools

1. **Auftragsverarbeitung**: Wenn Ihre KI-Tools personenbezogene Daten verarbeiten, benötigen Sie einen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO mit dem Anbieter.
2. **Datenübermittlung**: Achten Sie besonders auf den Serverstandort. EU-Serverstandorte sind zu bevorzugen, bei US-Anbietern sind zusätzliche Maßnahmen erforderlich.

3. **Besondere Datenkategorien**: Gesundheitsdaten, biometrische Daten und andere besonders sensible Daten unterliegen strengeren Anforderungen.
4. **Datenschutzerklärung**: Die KI-Nutzung muss in Ihrer Datenschutzerklärung transparent gemacht werden.

DSGVO-konforme Alternativen im Vergleich

KI-Tool	AVV möglich	Datennutzung für Training	Serverstandort	Empfehlung für KMU
ChatGPT (kostenfreie Version)	Nein	Ja	USA	Nur ohne personenbezogene Daten
ChatGPT Enterprise	Ja	Nein (konfigurierbar)	USA	Mit AVV geeignet
Microsoft Copilot	Ja (über Microsoft Cloud-Vertrag)	Konfigurierbar	USA/EU	Mit AVV geeignet
Mistral (EU-Anbieter)	Ja	Nein	EU	Besonders geeignet
On-Premise-Lösungen	Nicht nötig	Nein	Eigene Server	Maximale Kontrolle, höherer Aufwand

Typische Fallstricke und wie Sie sie vermeiden

1. **Fallstrick: Eingabe personenbezogener Daten in kostenlose KI-Tools**
   Lösung: Daten vor der Eingabe anonymisieren oder pseudonymisieren
2. **Fallstrick: Fehlende AVV bei KI-Nutzung**
   Lösung: Nur KI-Tools mit AVV-Möglichkeit für personenbezogene Daten nutzen
3. **Fallstrick: Unzureichende Information in der Datenschutzerklärung**
   Lösung: Datenschutzerklärung um KI-spezifische Abschnitte ergänzen (siehe Mustervorlage im Anhang)
4. **Fallstrick: Unbeabsichtigte Weitergabe von Geschäftsgeheimnissen**
   Lösung: Klare Richtlinien für Mitarbeiter erstellen, welche Informationen in KI-Tools eingegeben werden dürfen

> ***Praxis-Tipp:*** *Nutzen Sie unsere "DSGVO-KI-Matrix" im Anhang, um schnell zu prüfen, welche KI-Anwendungen unter welchen Bedingungen DSGVO-konform eingesetzt werden können.*

Praxisbeispiel: Autohaus Höß GmbH

Das Autohaus Höß mit 25 Mitarbeitern wollte ChatGPT für die Kundenkommunikation einsetzen. Dabei sollten Kundendaten für personalisierte Angebote genutzt werden.

Herausforderung: Die kostenfreie Version von ChatGPT bietet keinen AVV und speichert Eingaben für das Modelltraining.

Lösung: 1. Upgrade auf ChatGPT Enterprise mit AVV und Deaktivierung des Trainings 2. Erstellung einer Verfahrensbeschreibung für die KI-Nutzung 3. Anpassung der Datenschutzerklärung 4. Schulung der Mitarbeiter zum datenschutzkonformen Umgang mit KI

"Wir haben zunächst überlegt, ob wir die Daten anonymisieren können. Aber das hätte den Nutzen für die personalisierte Kommunikation stark eingeschränkt. Das Upgrade auf die Enterprise-Version war für uns die

praktikabelste Lösung," erklärt Geschäftsführer Markus Höß.

Haftungsrisiken bei KI-Einsatz

Der Einsatz von KI birgt nicht nur Chancen, sondern auch Haftungsrisiken. Als Unternehmer sollten Sie diese kennen und entsprechende Vorsichtsmaßnahmen treffen.

Die drei Haftungsdimensionen

1. **Unternehmenshaftung**
2. Ein Mangel an KI-Kompetenz kann als Verletzung der Sorgfaltspflicht gewertet werden
3. Haftung für Schäden durch fehlerhafte KI-Entscheidungen
4. Besondere Risiken bei Kundendaten und Beratungsleistungen
5. **Produkthaftung**
6. Haftung für KI als fehlerhaftes Produkt über den gesamten Lebenszyklus
7. Einschließlich Cybersicherheit und Updates
8. Relevant für Unternehmen, die KI-gestützte Produkte anbieten
9. **Führungskräftehaftung**
10. Persönliche Haftung von Geschäftsführern und Vorständen
11. Organisationsverschulden bei mangelnder KI-Governance
12. Besondere Sorgfaltspflichten bei der Implementierung von KI-Systemen

Praktische Beispiele für Haftungsszenarien

Szenario 1: Der falsche Rat
Ein KI-Chatbot auf Ihrer Website gibt falsche Rechtsauskünfte, die zu Schäden bei Kunden führen. Als Betreiber des Chatbots können Sie haftbar gemacht werden, wenn Sie keine angemessenen Maßnahmen zur Qualitätssicherung getroffen haben.

Szenario 2: Die diskriminierende Entscheidung
Ein KI-System zur Bewerberauswahl diskriminiert systematisch bestimmte Personengruppen. Dies kann zu Schadensersatzansprüchen und Reputationsschäden führen.

Szenario 3: Das Datenleck
Personenbezogene Kundendaten werden in einem US-basierten KI-Tool ohne ausreichende Rechtsgrundlage verarbeitet. Bei einem Datenschutzverstoß drohen Bußgelder von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes.

Absicherungsstrategien

1. **Dokumentation**
2. Lückenlose Dokumentation aller KI-Systeme, Schulungen und Maßnahmen
3. Regelmäßige Überprüfung und Aktualisierung

4. Nachweisbarkeit im Streitfall
5. **Schulung**
6. Regelmäßige Schulungen für Mitarbeiter und Führungskräfte
7. Klare Richtlinien für den Umgang mit KI-Tools
8. Sensibilisierung für Risiken und Grenzen der KI
9. **Verträge**
10. Rechtssichere Verträge mit KI-Anbietern
11. Klare Haftungsregelungen und Service Level Agreements
12. Prüfung der Versicherungsdeckung für KI-Risiken

> ***Praxis-Tipp:*** *Lassen Sie Ihre KI-Nutzung regelmäßig von einem Rechtsexperten prüfen. Die Kosten für eine präventive Rechtsberatung sind deutlich geringer als die potenziellen Kosten eines Rechtsstreits oder Bußgelds.*

Praxisbeispiel: Das ChatGPT-Dilemma

Ein häufiges Dilemma für KMU ist die Nutzung von ChatGPT für die Kundenberatung. Dabei sollen Kundendaten in Prompts verwendet werden, um personalisierte Antworten zu generieren. Wie gehen Sie rechtssicher vor?

Die Herausforderungen

- ChatGPT Standard speichert Eingaben für Modelltraining
- Datenverarbeitung außerhalb der EU
- Kein standardmäßiger AVV bei kostenfreier Version
- Risiko der Datenweitergabe und Zweckentfremdung

Lösungsansätze für verschiedene Unternehmenstypen

Für Einsteiger: Drei Standardlösungen

1. **Upgrade auf ChatGPT Enterprise**
2. Vorteile: AVV möglich, kein Training mit Ihren Daten, höhere Sicherheit
3. Nachteile: Kostenpflichtig, weiterhin US-Serverstandort
4. Geeignet für: Mittlere Unternehmen mit regelmäßigem KI-Bedarf
5. **Anonymisierung personenbezogener Daten**
6. Vorteile: Kostengünstig, auch mit kostenfreier Version nutzbar
7. Nachteile: Aufwändig, eingeschränkte Personalisierung
8. Geeignet für: Kleine Unternehmen mit gelegentlichem KI-Bedarf
9. **Wechsel zu EU-basierten Anbietern**

10. Vorteile: EU-Serverstandort, DSGVO-konform
11. Nachteile: Teilweise weniger leistungsfähig, weniger bekannt
12. Geeignet für: Unternehmen mit hohen Datenschutzanforderungen

Für Fortgeschrittene: Drei komplexere Lösungen

1. **On-Premise LLM auf lokaler Infrastruktur**
2. Vorteile: Volle Kontrolle, keine Datenabflüsse
3. Nachteile: Hoher technischer Aufwand, Ressourcenbedarf
4. Geeignet für: IT-Unternehmen, größere Mittelständler mit IT-Abteilung
5. **Hybrid-Lösung**
6. Vorteile: Sensible Daten lokal, allgemeine Anfragen extern
7. Nachteile: Komplexe Implementierung, zwei Systeme zu warten
8. Geeignet für: Unternehmen mit gemischten Anforderungen
9. **Maßgeschneiderte KI-Lösung**
10. Vorteile: Optimal auf Ihre Bedürfnisse zugeschnitten
11. Nachteile: Hohe Kosten, längere Entwicklungszeit
12. Geeignet für: Spezialanwendungen, größere Unternehmen

Erfahrungsberichte aus der Praxis

Axel Koch, Transferstärke Coaching: "Ich wollte einen KI-Coach entwickeln, der Menschen hilft, Gewohnheiten zu verändern. Da hier potenziell sensible persönliche Daten verarbeitet werden, habe ich mich für eine Hybrid-Lösung entschieden: Die Grundfunktionen laufen über eine EU-basierte KI, während für allgemeine Inhalte auch ChatGPT zum Einsatz kommt. Die Dokumentation der KI-Kompetenz war anfangs lästig, gibt mir jetzt aber Sicherheit."

Birgit Meindl-Köhle, Steuerberatung: "In unserer Kanzlei nutzen wir KI für die Analyse von Steuerdokumenten. Wir haben uns für eine On-Premise-Lösung entschieden, da wir mit hochsensiblen Mandantendaten arbeiten. Der Initialaufwand war hoch, aber die Rechtssicherheit ist es wert. Zudem haben wir alle Mitarbeiter geschult und klare Richtlinien erstellt."

> ***Praxis-Tipp:*** *Es gibt keine Einheitslösung – die richtige Wahl hängt von Ihrer spezifischen Situation, Ihren Ressourcen und Ihrem Risikoprofil ab. Beginnen Sie mit einer einfachen Lösung und entwickeln Sie diese weiter, wenn Ihr KI-Einsatz wächst.*

Branchenspezifische Compliance-Strategien

Je nach Branche stehen Sie vor unterschiedlichen Herausforderungen bei der KI-Compliance. Hier finden Sie maßgeschneiderte Strategien für verschiedene Unternehmenstypen.

IT und Software

Typische KI-Anwendungen: - Codeunterstützung (GitHub Copilot, Amazon CodeWhisperer) - Automatisierte Tests und Debugging - Kundenservice-Chatbots

Compliance-Strategie: 1. Detaillierte Dokumentation der KI-Systeme und ihrer Funktionsweise 2. Regelmäßige Schulungen für Entwickler und Produktmanager 3. Code-Reviews für KI-generierte Inhalte 4. Automatisierte Compliance-Checks in der CI/CD-Pipeline

Besondere Risiken: - Urheberrechtsverletzungen durch KI-generierte Inhalte - Sicherheitslücken in KI-generiertem Code - Datenschutzrisiken bei der Verarbeitung von Kundendaten

> ***Praxis-Tipp für IT-Unternehmen:*** *Implementieren Sie ein "KI-Governance-Board", das neue KI-Tools vor dem Einsatz prüft und freigibt. Dies reduziert das Risiko von Schatten-IT und unbemerkten Compliance-Verstößen.*

Handwerk und Produktion

Typische KI-Anwendungen: - KI-gestützte Planungs- und Designtools - Predictive Maintenance - Automatisierte Qualitätskontrolle

Compliance-Strategie: 1. Fokus auf Standard-Tools mit AVV 2. Einfache Checklisten für Mitarbeiter 3. Klare Nutzungsrichtlinien für KI-Tools 4. Regelmäßige Überprüfung der Datenqualität

Besondere Risiken: - Haftung für KI-gestützte Planungsfehler - Datenschutz bei Kundenprojekten - Abhängigkeit von KI-Anbietern

> ***Praxis-Tipp für Handwerksbetriebe:*** *Nutzen Sie branchenspezifische KI-Lösungen, die bereits auf Ihre Anforderungen zugeschnitten sind und idealerweise von Ihrem Branchenverband oder einer Innung empfohlen werden.*

Handel und Dienstleistung

Typische KI-Anwendungen: - Personalisierte Kundenansprache - Bedarfsprognosen und Lagerhaltung - KI-gestützte Preisoptimierung

Compliance-Strategie: 1. Besonderer Fokus auf Kundendatenschutz bei KI-Profilierung 2. Transparente Kommunikation gegenüber Kunden 3. Regelmäßige Überprüfung der KI-Empfehlungen 4. Schulung der Mitarbeiter im Kundenkontakt

Besondere Risiken: - Diskriminierung durch KI-Algorithmen - Intransparente Preisgestaltung - Übermäßige Personalisierung

> ***Praxis-Tipp für Händler:*** *Informieren Sie Ihre Kunden proaktiv über den Einsatz von KI in Ihrem Unternehmen. Dies schafft Vertrauen und reduziert das Risiko von Beschwerden.*

Beratung und freie Berufe

Typische KI-Anwendungen: - Recherche- und Analyseunterstützung - Dokumentenerstellung und -analyse - Terminplanung und Kundenkommunikation

Compliance-Strategie: 1. Strikte Trennung von KI-Unterstützung und professioneller Beurteilung 2. Besonders hohe Anforderungen an Datenschutz und Vertraulichkeit 3. Klare Kennzeichnung KI-generierter Inhalte 4. Regelmäßige Überprüfung der KI-Outputs

Besondere Risiken: - Haftung für fehlerhafte KI-gestützte Beratung - Verletzung von Berufsgeheimnissen - Übermäßiges Vertrauen in KI-Ergebnisse

> ***Praxis-Tipp für Berater:*** *Definieren Sie klar, welche Aufgaben an KI delegiert werden können und welche zwingend menschliche Expertise erfordern. Dokumentieren Sie diese Abgrenzung in Ihren internen Richtlinien.*

Checklisten und Vorlagen

In diesem Abschnitt finden Sie praktische Checklisten und Vorlagen, die Ihnen die Umsetzung der KI-Compliance erleichtern.

12-Punkte-Sofortcheck für KI-Kompetenz

Nutzen Sie diese Checkliste, um schnell zu prüfen, wo Sie in Sachen KI-Kompetenz stehen:

1. [ ] KI-Inventar erstellt (Welche KI-Tools werden genutzt?)
2. [ ] Einsatzzwecke dokumentiert (Wofür werden die Tools genutzt?)
3. [ ] Risikokategorien bestimmt (Welches Risiko haben die Tools?)
4. [ ] Verantwortlichkeiten festgelegt (Wer ist für welches Tool zuständig?)
5. [ ] Schulungsbedarf ermittelt (Welche Kompetenzen fehlen noch?)
6. [ ] Schulungsplan erstellt (Wie werden die Kompetenzen aufgebaut?)
7. [ ] Erste Schulungen durchgeführt (Sind die Grundlagen vermittelt?)
8. [ ] Nutzungsrichtlinien erstellt (Wie dürfen die Tools genutzt werden?)
9. [ ] Dokumentation angelegt (Sind alle Maßnahmen dokumentiert?)
10. [ ] DSGVO-Konformität geprüft (Sind die Tools datenschutzkonform?)
11. [ ] Aktualisierungsprozess definiert (Wie werden die Maßnahmen aktuell gehalten?)
12. [ ] Notfallplan erstellt (Was tun bei KI-bedingten Problemen?)

> ***Praxis-Tipp:*** *Beginnen Sie mit den ersten vier Punkten – sie bilden die Grundlage für alle weiteren Maßnahmen und lassen sich meist in wenigen Stunden umsetzen.*

Vorlage: KI-Inventar

KI-Tool	Version	Anbieter	Einsatzzweck	Betroffene Daten	Risikokategorie	Verantwortlicher	AVV vorhanden?	Letzte Prüfung
[Tool 1]								
[Tool 2]								
[Tool 3]								

Vorlage: Dokumentation der KI-Kompetenz-Maßnahmen

Datum	Maßnahme	Teilnehmer	Inhalte	Nachweis	Nächste Wiederholung
[Datum]					
[Datum]					
[Datum]					

Vorlage: KI-Nutzungsrichtlinie für Mitarbeiter

1. Zugelassene KI-Tools - Liste der freigegebenen Tools - Wo und wie sie zu finden sind - Wer die Nutzung genehmigen muss

2. Datenschutzregeln - Welche Daten dürfen eingegeben werden - Welche Daten müssen anonymisiert werden - Wie erfolgt die Anonymisierung

3. Qualitätssicherung - Wie sind KI-Ergebnisse zu prüfen - Wer trägt die Verantwortung - Dokumentationspflichten

4. Weiterbildung - Pflichtschulungen - Weiterführende Ressourcen - Ansprechpartner bei Fragen

5. Meldepflichten - Vorgehen bei Problemen - Meldewege bei Datenschutzvorfällen - Eskalationsprozess

> ***Praxis-Tipp:*** *Passen Sie diese Vorlagen an Ihre spezifischen Bedürfnisse an. Eine schlanke, aber durchdachte Dokumentation ist besser als ein umfangreiches Regelwerk, das niemand liest oder umsetzt.*

Glossar und weiterführende Ressourcen

Glossar: Die wichtigsten Begriffe erklärt

AI Act (Artificial Intelligence Act): Die umfassende KI-Regulierung der Europäischen Union, die im Februar 2025 in Kraft trat.

AVV (Auftragsverarbeitungsvertrag): Ein nach Art. 28 DSGVO erforderlicher Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter bei der Verarbeitung personenbezogener Daten.

DSGVO (Datenschutz-Grundverordnung): Die europäische Verordnung zum Schutz personenbezogener Daten, die seit Mai 2018 gilt.

Generative KI: KI-Systeme, die neue Inhalte wie Texte, Bilder oder Code erzeugen können, z.B. ChatGPT oder DALL-E.

KI-Kompetenz: Die Fähigkeiten, Kenntnisse und das Verständnis, um KI-Systeme sachkundig einzusetzen und sich dabei der Chancen und Risiken bewusst zu sein (gemäß AI Act, Art. 3 Nr. 56).

LLM (Large Language Model): Große Sprachmodelle wie GPT-4 oder Gemini, die natürliche Sprache verstehen und generieren können.

On-Premise: Lokale Installation von Software oder KI-Systemen auf eigenen Servern statt in der Cloud.

Prompt: Eine Eingabeaufforderung oder Anweisung an ein KI-System, die dessen Ausgabe steuert.

Risikokategorien: Die vier Risikostufen des AI Acts: unannehmbares Risiko, hohes Risiko, begrenztes Risiko und minimales Risiko.

Tokenisierung: Der Prozess, bei dem Text in kleinere Einheiten (Tokens) zerlegt wird, die von KI-Modellen verarbeitet werden können.

Weiterführende Ressourcen

Offizielle Quellen

- EU AI Act (vollständiger Text)
- Hinweispapier der Bundesnetzagentur zur KI-Kompetenz
- DSGVO-Leitlinien des Europäischen Datenschutzausschusses zu KI

Praxishilfen und Tools

- AI Act Artikel 4 Checkliste (BDS Bayern)
- DSGVO-KI-Matrix (BDS Bayern)
- Muster-Datenschutzerklärung für KI-Nutzung (BDS Bayern)
- Mitarbeiter-Guidelines für KI-Tools (BDS Bayern)

Empfohlene KI-Tools für KMU

- **EU-basierte Anbieter:**
- Mistral AI - Französisches KI-Unternehmen mit leistungsstarken Sprachmodellen
- Aleph Alpha - Deutscher KI-Anbieter mit Fokus auf Vertrauenswürdigkeit
- DeepL Write - KI-gestütztes Schreibtool mit EU-Serverstandort
- **On-Premise-Lösungen:**
- LM Studio - Lokale Ausführung von Sprachmodellen
- Ollama - Einfache lokale Ausführung von Open-Source-Modellen
- LocalAI - Self-hosted Alternative zu OpenAI
- **KI mit Enterprise-Features:**
- ChatGPT Enterprise - Mit AVV und Datenschutzgarantien
- Microsoft Copilot - Integration in Microsoft 365
- Google AI Studio - Enterprise-Version von Google Gemini

Kontakt und Unterstützung

Für weitere Unterstützung bei der Umsetzung der KI-Compliance stehen wir Ihnen gerne zur Verfügung:

Arno Schimmelpfennig
DIN-Experte für KI und Leiter der KI-Akademie
Bund der Selbständigen Bayern

E-Mail: a.schimmelpfennig@bds-bayern.de
Telefon: 089 / 123 456 789
Website: www.bds-akademie-bayern.de

Impressum

Herausgeber:
Bund der Selbständigen Bayern e.V.
KI-Akademie
Musterstraße 123
80123 München

Verantwortlich für den Inhalt:
Arno Schimmelpfennig
DIN-Experte für KI und Leiter der KI-Akademie

Bildnachweise:
Titelbild: iStock/GettyImages-1294458239
KI-Modell-Rankings: Poe, Mai 2025

Stand:
September 2025

Haftungsausschluss:
Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

Dieses Handbuch ersetzt keine rechtliche Beratung. Bei konkreten rechtlichen Fragen wenden Sie sich bitte an einen spezialisierten Rechtsanwalt.