

KI-COMPLIANCE-CHECKLISTE

für Geschäftsführer

Stand: August 2026

Die gesetzlichen Regelungen hinsichtlich KI entwickeln sich schnell. Wer die Schlagzeilen verfolgt, gewinnt leicht den Eindruck, dass die Pflichten kaum zu überblicken sind. Dieser Eindruck täuscht aber.

Diese Checkliste gibt Ihnen einen ersten Überblick über die wichtigsten Anforderungen für mittelständische Unternehmen, die KI einsetzen. Sie deckt ab, was für die meisten mittelständischen Unternehmen relevant ist. Was daraus für Ihr Unternehmen konkret folgt, hängt von Ihrer individuellen Situation ab. Denn je nach Branche, Unternehmensgröße, eingesetzten Technologien und individuellem Geschäftsmodell können die konkreten Pflichten abweichen. Deshalb empfehlen wir, die Umsetzung nicht allein anzugehen. Wir begleiten Sie dabei, Ihre individuelle Risikolage einzuschätzen, die notwendigen Maßnahmen zu priorisieren und rechtssicher umzusetzen.

Wenn Sie bei einzelnen Punkten auf Nummer Sicher gehen wollen, melden Sie sich gerne bei Tobias Stephan für rechtliche Fragen und bei Dina für Fragen zur Anwendung.



MAINLY

§ 1 Bestandsaufnahme

Bevor einzelne Anforderungen geprüft werden können, müssen Sie wissen, welche KI-Systeme in Ihrem Unternehmen im Einsatz sind, zu welchem Zweck sie eingesetzt werden und wer dafür verantwortlich ist.

- ☐ Erstellen Sie eine vollständige Liste aller genutzten KI-Tools, einschließlich in ERP oder CRM eingebetteter KI und abteilungsspezifischer Anwendungen.
- ☐ Klären Sie, welche Mitarbeiter welche Tools wie nutzen und ob unautorisierte Tools im Einsatz sind.
- ☐ Halten Sie für jedes Tool fest, wer der Anbieter ist, wo er sitzt und welche Art von Daten eingespeist werden.
- ☐ Sammeln Sie alle bestehenden Verträge mit KI-Anbietern, einschließlich SaaS-Verträge, Lizenzen, Datenschutzverträgen und Nutzungsbedingungen.

§ 2 KI-Verordnung (EU AI Act)

- ☐ Stellen Sie je KI-System Ihre Rolle fest, also ob Sie als Betreiber oder als Anbieter handeln. Achtung: Wenn Sie fremde KI in Ihre eigenen Produkte einbauen oder diese unter Ihrem Namen in den Verkehr bringen, können Sie als Anbieter gelten.

- ☐ Prüfen Sie, ob eines Ihrer Systeme in die Kategorie „verbotene KI“ fällt, etwa Social Scoring, manipulative Systeme oder biometrische Echtzeit-Überwachung im öffentlichen Raum. Bei einem Verdacht sollten Sie dies umgehend rechtlich prüfen lassen. Verbotene Systeme müssen sofort abgeschaltet werden.
- ☐ Prüfen Sie, ob eines Ihrer Systeme als Hochrisiko-KI einzustufen ist, zum Beispiel KI zur Personalauswahl in der HR-Abteilung oder KI, die als Sicherheitsbauteil in einem Produkt fungiert. Für diese gelten zukünftig strenge Anforderungen an Dokumentation, menschliche Aufsicht und Risikomanagement. Im Zweifel sollten Sie die Einordnung und die Folgen rechtlich prüfen lassen.
- ☐ Prüfen Sie, ob Sie ein KI-Modell, das für eine Vielzahl von Aufgaben nutzbar ist anbieten. Denken Sie an das oben beschriebene "White-Label" Risiko.
- ☐ Stellen Sie sicher, dass Sie die Transparenzpflichten einhalten. Kennzeichnen Sie KI-Chatbots und virtuelle Assistenten klar als solche. Kennzeichnen Sie KI-generierte Texte, Bilder und Videos vor der Veröffentlichung als maschinell erzeugt. Informieren Sie Betroffene, wenn ein System Emotionserkennung oder biometrische Kategorisierung einsetzt.
- ☐ Stellen Sie sicher, dass Ihre Mitarbeiter über ausreichende KI-Kompetenz verfügen, um die eingesetzten Systeme verantwortungsvoll zu

nutzen. Die Pflicht wurde zwar abgemildert, Sie tragen aber weiter die Verantwortung für Ihre Mitarbeiter.

§ 3 Datenschutz

- ☐ Legen Sie für jede Verarbeitung personenbezogener Daten mit KI eine Rechtsgrundlage fest.
- ☐ Schließen Sie mit jedem KI-Anbieter einen passenden Datenschutzvertrag ab. Häufig ist das eine Auftragsverarbeitung, aber es sind durchaus auch Situationen von gemeinsamer oder getrennter Verantwortlichkeit denkbar. Achten Sie darauf, ob die Daten für das Modelltraining verwendet werden dürfen.
- ☐ Prüfen Sie, ob Daten in Drittstaaten übermittelt werden, und stellen Sie sicher, dass geeignete Garantien bestehen, zum Beispiel ein Angemessenheitsbeschluss oder Standardvertragsklauseln.
- ☐ Prüfen Sie, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist. Bei KI-Einsatz ist sie häufig verpflichtend. Führen Sie die Abschätzung durch oder lassen Sie diese extern durchführen.
- ☐ Aktualisieren Sie das Verarbeitungsverzeichnis sowie Ihre Datenschutzerklärungen um alle KI-gestützten Verarbeitungen.

- ☐ Prüfen Sie, ob in Ihrem Unternehmen Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung auf Personen — etwa bei Kreditvergabe, Personalauswahl oder Vertragsschluss — vollautomatisiert getroffen werden. Ist das der Fall, muss dafür eine Rechtsgrundlage bestehen (Vertrag, gesetzliche Erlaubnis oder ausdrückliche Einwilligung), die betroffene Person muss vorab informiert werden, und sie muss jederzeit das Recht haben, die Entscheidung anzufechten, ihren Standpunkt darzulegen und eine menschliche Überprüfung zu verlangen.

§ 4 Vertragsrecht

- ☐ Prüfen Sie mit Ihrer Rechts- oder Einkaufsabteilung, ob bestehende Verträge mit Kunden, Lieferanten und Dienstleistern den KI-Einsatz abdecken, insbesondere mit Blick auf Haftung, Datenschutz und Nutzungsrechte an Ergebnissen.
- ☐ Stellen Sie sicher, dass neue Verträge mit KI-Anbietern diese Punkte und die unterschiedlichen Verantwortungen (z.B. für die Richtigkeit und Rechtssicherheit von Inhalten) regeln, bevor Systeme produktiv eingesetzt werden. KI-Anbieter begrenzen ihre Haftung in AGB häufig erheblich.

§ 5 Geschäftsgeheimnisse (GeschGehG)

- ☐ Identifizieren Sie, welche Informationen in Ihrem Unternehmen als Geschäftsgeheimnisse zu qualifizieren sind, etwa Preiskalkulationen, Kundenlisten, Rezepturen oder interne Strategien.
- ☐ Stellen Sie sicher, dass angemessene Schutzmaßnahmen bestehen. Ohne Schutzmaßnahmen greift das GeschGehG nicht. Prüfen Sie, ob Verträge mit KI-Anbietern ein ausdrückliches Verbot des Trainings mit Ihren Daten enthalten.
- ☐ Prüfen Sie, ob Mitarbeiter diese Informationen in externe KI-Tools eingeben. Erstellen Sie eine KI-Richtlinie, welche unter anderem Regelt, welche Informationen wie genutzt werden dürfen.

§ 6 Urheberrecht

- ☐ Prüfen Sie, ob die in KI-Tools eingespeisten Inhalte urheberrechtlich geschützt sind, etwa Texte, Bilder, Code oder Musik von Dritten. Sofern dies der Fall ist, stellen Sie sicher, dass Sie über das Recht verfügen, die Informationen entsprechend zu verarbeiten.
- ☐ Prüfen Sie den rechtlichen Status der von KI generierten Outputs. KI-generierte Inhalte sind in Deutschland grundsätzlich nicht urheberrechtlich geschützt und können daher von Dritten frei genutzt werden. Wenn Sie die Ergebnisse (zum Beispiel als Software)

weiterverkaufen, achten Sie auch darauf, worauf Sie sich gegenüber Ihren Kunden verpflichten.

- ☐ Stellen Sie sicher, dass KI-Outputs nicht geschützte Werke Dritter reproduzieren, bevor Sie sie veröffentlichen oder weiterverwenden.
- ☐ Klären Sie vertraglich, wem KI-generierte Entwicklungen gehören, wenn externe Dienstleister oder Arbeitnehmer beteiligt sind.

§ 7 Arbeitsrecht (BetrVG, AGG).

- ☐ Prüfen Sie, ob der Einsatz von KI ein Mitbestimmungsrecht des Betriebsrats auslöst, insbesondere wenn KI zur Leistungs- oder Verhaltensüberwachung eingesetzt wird. Eine fehlende Betriebsvereinbarung kann ein KI-Projekt stoppen.
- ☐ *Empfehlenswert:* Informieren Sie den Betriebsrat auch dort, wo keine Mitbestimmung besteht.
- ☐ Prüfen Sie, ob KI-Systeme zu Benachteiligungen führen können, etwa nach Alter, Geschlecht, Herkunft oder Behinderung. Das gilt nicht nur in der Personalarbeit, sondern auch im Kundenkontakt und bei automatisierten Entscheidungen.

§ 8 Haftungsrecht

- ☐ Verankern Sie einen Freigabeprozess für KI-generierte Inhalte in Ihrer KI-Richtlinie. Chatbot-Aussagen und andere KI-Outputs gelten rechtlich als eigene Äußerungen des Unternehmens.
- ☐ Dokumentieren Sie den Einsatz von KI-Systemen, insbesondere technische Dokumentation, lückenlos. Bereiten Sie sich auf erweiterte Beweispflichten vor. Ab Dezember 2026 gelten für fehlerhafte KI-Produkte verschärfte Beweislastregeln, Gerichte können Unternehmen künftig verpflichten, technische Unterlagen offenzulegen.
- ☐ Prüfen Sie Ihren Versicherungsschutz. Bestehende Policen decken KI-bedingte Schäden häufig nicht ab.

§ 9 Cybersicherheit

- ☐ Prüfen Sie, ob Ihre Produkte unter den Cyber Resilience Act fallen. Betroffen sind alle Produkte mit digitalen Elementen, einschließlich Produkte mit KI-Komponenten oder KI-Funktionen.
- ☐ Regeln Sie den Einsatz von KI-Tools intern. Geben Sie Anbieter und Anwendungen frei, beschränken Sie den Systemzugriff auf das Notwendige und schulen Sie Mitarbeiter zu KI-spezifischen Angriffsmustern wie Prompt-Manipulation.

IHRE ANSPRECHPARTNER



Dina Kohler

E-Mail info@gpt-pilot.com

Phone +49 176 470 39 335

Web gpt-pilot.com

LinkedIn <https://www.linkedin.com/in/dina-kohler/>



Tobias Stephan

E-Mail t.stephan@mainly-law.com

Phone +49 711 252 485 92

Web mainly-law.com

LinkedIn <https://www.linkedin.com/in/tobias-stephan-65663517b/>