SCHÜRMANN
ROSENTHAL
DREYER

Version: März 2025



inklusive
KI-Schnell-
Check

Praxis-Leitfaden

KI sicher nutzen: In 9 einfachen Schritten zur AI-Compliance

So setzen Sie AI sicher ein – nach den Vorgaben des AI Act.

SICHER
RADIKAL
DIGITAL

Herzlich Willkommen!



Schön, dass Sie diesen Praxisleitfaden heruntergeladen haben.

Künstliche Intelligenz (KI) hat bereits Einzug in den Arbeitsalltag gehalten. Ob ChatGPT für E-Mails, KI-gestützte Analysen oder automatisierte Prozesse – Mitarbeitende nutzen KI-Tools oft, ohne sich der rechtlichen Implikationen bewusst zu sein. Doch mit dem **AI Act** stehen nun klare, gesetzliche Vorgaben zur sicheren und rechtskonformen Nutzung von KI auf europäischer Ebene.

Was bedeutet das konkret für Sie als Unternehmen? Welche Risiken müssen Sie vermeiden, um rechtssicher zu agieren? Und wie stellen Sie sicher, dass der Einsatz von KI im Einklang mit den neuen Vorschriften steht?

Hier sind **9 einfache Schritte** (+ Bonus und Checkliste), mit denen Sie KI sicher und strukturiert im Einklang mit den Vorgaben des AI Act in Ihrem Unternehmen einsetzen können. Sie werden durch die wichtigsten rechtlichen Anforderungen geführt, ohne dass Sie sich durch die komplexen Details des Gesetzes arbeiten müssen.

Und falls später Fragen aufkommen, wissen Sie genau, wo Sie rechtliche Unterstützung anfordern können.

Ich wünsche Ihnen viel Freude und Erfolg beim Anwenden.

Ich durfte bereits viele Unternehmen dabei begleiten, Künstliche Intelligenz sicher und rechtskonform in ihren Geschäftsalltag zu integrieren – vom Einsatz einfacher KI-Tools bis hin zu komplexen KI-Systemen. In meiner Arbeit zeigt sich immer wieder: Wer frühzeitig klare Strukturen schafft und rechtliche Stolpersteine kennt, nutzt die Chancen von KI effizienter und risikobewusster. Mein Ziel: Innovation zu ermöglichen – ohne rechtliche Unsicherheiten. Die wichtigsten Erkenntnisse und praktischen Lösungen aus meiner Beratungspraxis stecken in diesem Leitfaden.

Ihr Philipp Müller-Peltzer

Rechtsanwalt und Partner bei Schürmann Rosenthal Dreyer



Inhalts-verzeichnis

01 Überblick verschaffen: Welche KI-Tools werden genutzt?

02 Anbieter-/Betreiberrolle bestimmen

03 KI-Systeme in Risikoklassen einteilen

04 Einfache „KI-Nutzungsregeln“ aufstellen

05 Risiken checken: Was kann schiefgehen?

06 Datenschutz & Geheimhaltung absichern

07 Haftung & Urheberrecht verstehen

08 Nur geprüfte KI-Tools nutzen

09 Schulung & Feedback – Ihr Team einbinden

10 KI-Schnell-Check

01 Überblick verschaffen: Welche KI-Tools werden genutzt?

ZIEL

Eine Bestandsaufnahme der eingesetzten KI-Tools vornehmen und potenzielle rechtliche Relevanz identifizieren.

FRAGE AN IHR TEAM

- Welche KI-Tools werden derzeit verwendet?
- Für welche konkreten Anwendungen werden diese KI-Tools eingesetzt?
- Welche Datenarten werden dabei verarbeitet (z. B. personenbezogene Daten, Betriebsgeheimnisse)?

EINFACHE MASSNAHME

Starten Sie eine interne Umfrage oder führen Sie Interviews mit Mitarbeitenden aus verschiedenen Abteilungen (z. B. HR, Marketing, Produktentwicklung). Dokumentieren Sie die verwendeten KI-Tools sowie die damit verbundenen Datenverarbeitungsprozesse.

WARUM WICHTIG?

Viele Unternehmen unterschätzen, wie tief KI bereits in die Arbeitsprozesse integriert ist, oft ohne formelle Genehmigung oder die nötige rechtliche Prüfung. Die Bestandsaufnahme ist unerlässlich, um die **Risikoklassifizierung, datenschutzrechtliche Compliance** oder mögliche **Haftungsrisiken** zu bewerten.

ERGEBNIS

Sie Sie haben eine detaillierte Liste von KI-Tools (AI-Inventory) und deren Einsatzbereichen sowie eine erste Grundlage für die rechtliche Bewertung.

02 Anbieter-/Betreiberrolle bestimmen

→ **ZIEL**

Identifizieren Sie zu jedem KI-Asset, ob Sie Betreiber oder Anbieter sind.

→ **SCHNELLE PRÜFUNG**

- Entwickeln Sie ein KI-System oder -Modell bzw. lassen Sie es entwickeln?
- Bringen Sie es unter eigenem Namen oder Marke in Verkehr oder in Betrieb?
- Haben Sie wesentliche Änderungen an einem KI-System durchgeführt?

ACHTUNG: Wenn Sie diese Fragen mit "Ja" beantworten, sind Sie möglicherweise Anbieter im Sinne des AI Act. Andernfalls sind Sie wahrscheinlich Betreiber.

→ **WARUM WICHTIG?**

Die Compliance-Anforderungen an Anbieter von KI-Systemen und -Modellen sind deutlich strenger und die Haftungsrisiken größer als die der Betreiber. Deshalb ist es entscheiden, dass Sie Ihre Rolle korrekt einschätzen.

→ **ERGEBNIS**

Sie kennen Ihre Rolle und wissen, welche Anforderungen des AI Act für Sie gelten.

03 KI-Systeme in Risikoklassen einteilen

ZIEL

Finden Sie heraus, zu welcher Risikoklasse Ihre KI-Systeme gehören.

SCHNELLE PRÜFUNG

- Handelt es sich überhaupt um ein KI-System im Sinn des AI Act?
- Handelt es sich um eine verbotene KI-Praktik gemäß Artikel 5 AI Act?
- Handelt es sich um ein Hochrisiko-System gemäß Artikel 6 und Anhang III AI Act?

ACHTUNG: Wenn das KI-System weder verboten noch hochriskant ist, gehört es wahrscheinlich zur Kategorie der geringeren Risiken, was weniger strenge Compliance-Vorgaben bedeutet.

WARUM WICHTIG?

Wie die Rolleneinteilung, bestimmt auch die Risikoklasse über die Compliance-Anforderungen.

ERGEBNIS

Sie kennen die Risikoklassen Ihrer KI-Systeme und wissen, welche Anforderungen des AI Act für Sie gelten.

04 Einfache „KI-Nutzungsregeln“ aufstellen

→ **ZIEL**

Grundlegende **Compliance-Vorgaben** für den KI-Einsatz schaffen.

→ **SCHNELLE PRÜFUNG**

Entwickeln Sie klare, einfache **Nutzungsrichtlinien** für den Einsatz von KI im Unternehmen.

Beispiele für Regeln:

- KI darf verwendet werden, aber keine vertraulichen oder personenbezogenen Daten dürfen eingegeben werden.
- KI-generierte Inhalte müssen vor der Nutzung auf **rechtliche und inhaltliche Korrektheit** geprüft werden.
- Bei Unsicherheit über den Einsatz von KI, muss vorab eine **Rechtsprüfung** oder **Compliance-Abklärung** erfolgen.

→ **WARUM WICHTIG?**

Die Festlegung klarer **Richtlinien** trägt zur Vermeidung von **Datenschutzverletzungen** und **Haftungsrisiken** bei. Eine solche Regelung hilft, den **innerbetrieblichen Umgang mit KI** zu steuern und die rechtliche Absicherung zu gewährleisten.

→ **ERGEBNIS**

Mitarbeitende wissen genau, was sie tun dürfen und was nicht – dies reduziert die rechtlichen Risiken erheblich.

05 Risiken checken: Was kann schiefgehen?

→ **ZIEL**

Identifizierung von rechtlichen Risiken im Zusammenhang mit dem Einsatz von KI.

→ **SCHNELLE PRÜFUNG**

- Werden **personenbezogene Daten** verarbeitet? (z. B. **DSGVO**-Verletzungen)
- Verlässt unternehmensinternes Wissen das Unternehmen (Verletzung von **Geschäftsgeheimnissen**)?
- Werden KI-generierte Inhalte ohne **menschliche Kontrolle** verwendet? (Fehlerpotenzial und Haftung)
- **Transparenzpflichten**: Müssen KI-generierte Inhalte als solche gekennzeichnet werden, um den Anforderungen der **AI Act** zu entsprechen?

→ **EINFACHE MASSNAHMEN**

- Führen Sie ein **Gespräch** mit Ihren Mitarbeitenden: „Was genau gebt ihr in die KI ein? Werden dabei personenbezogene oder vertrauliche Daten genutzt?“
- Überprüfen Sie, ob durch den Einsatz der KI-Tools die **Informationssicherheitsanforderungen** erfüllt werden.

→ **ERGEBNIS**

Sie haben eine erste Einschätzung der Risiken und wissen, wo gegebenenfalls ein **Anpassungsbedarf** besteht, z. B. durch zusätzliche **Datenschutzmaßnahmen** oder die Notwendigkeit einer **Transparenzpflicht** nach dem AI Act.

06 Datenschutz & Geheimhaltung absichern

→ **ZIEL**

Sicherstellen, dass der **Datenschutz** und die **Vertraulichkeit** der Daten im Einklang mit der **DSGVO** und dem **Geschäftsgeheimnisgesetz** gewahrt bleiben.

→ **EINFACHE MASSNAHME**

Führen Sie einen „**KI-Datenschutz-Check**“ durch:

- Prüfen Sie, ob die AGB des KI-Anbieters eine **Datenverarbeitung** und **Speicherung** von vertraulichen oder personenbezogenen Daten vorsehen.
- Falls personenbezogene Daten verarbeitet werden: Prüfen Sie, ob der Anbieter eine **Datenverarbeitungsvereinbarung (DPA)** abgeschlossen hat.
- Ermitteln Sie, ob das Tool interne **Betriebsgeheimnisse** verarbeitet und ob dies durch geeignete **Vertraulichkeitsvereinbarungen** abgesichert ist.
- Falls KI-Tools in der Cloud laufen, prüfen Sie, ob Sie durch **vertragliche Vereinbarungen** die Datenhoheit und **Zugangskontrollen** sichern können.

→ **WARUM WICHTIG?**

Unternehmen können unabsichtlich gegen die **DSGVO** verstoßen, wenn sensible Daten ohne ausreichende **Zustimmung** oder **Schutzmaßnahmen** verarbeitet werden. Darüber hinaus ist der Schutz von **Geschäftsgeheimnissen** und **Vertraulichkeit** für die Vermeidung von **Wettbewerbsnachteilen** unerlässlich.

→ **ERGEBNIS**

Sie haben eine **Datenschutzprüfung** durchgeführt und wissen, welche KI-Tools **DSGVO-konform** sind und welche nicht.

07 Haftung & Urheberrecht verstehen

→ **ZIEL**

Klarheit über die **Haftung** im Falle von KI-generierten Fehlern und **Urheberrechtsfragen** erlangen.

→ **EINFACHE MASSNAHME**

Stellen Sie sich die folgenden Fragen:

- Wer ist im Falle einer **Fehlentscheidung** durch die KI verantwortlich? Liegt die Haftung beim Unternehmen oder dem KI-Anbieter?
- Wer hat das **Urheberrecht** an einem von KI generierten Werk (z. B. Texten, Bildern)? Besteht eine ausreichende menschliche "Schöpfungshöhe"?

→ **GRUNDREGEL**

- **Haftung**: KI-Systeme sind **nicht fehlerfrei**. Entscheidungen, die auf KI basieren, sollten immer durch eine **menschliche Instanz** überprüft werden.
- **Urheberrecht**: KI-generierte Inhalte sind häufig nicht durch das **Urheberrecht** geschützt, es sei denn, es liegt eine kreative **menschliche Schöpfung** vor.

→ **ERGEBNIS**

Sie haben eine fundierte Entscheidung über die **Haftung** und **Urheberrechtsfragen** und wissen, welche Vorkehrungen notwendig sind, um Risiken zu vermeiden.

08 Nur geprüfte KI-Tools nutzen

→ **ZIEL**

Die Nutzung von **unsicheren oder nicht-konformen** KI-Tools verhindern.

→ **EINFACHE MASSNAHME**

Erstellen Sie eine Liste von **zugelassenen KI-Tools**, die Ihre **Compliance-Anforderungen** erfüllen.

Überprüfen Sie alle Tools auf Aspekte wie:

- **Dokumentations-, Transparenz- und Risikobewertungsanforderungen** gemäß AI Act.
- **datenschutzrechtliche Absicherungen, insbesondere durch Datenverarbeitungsvereinbarungen (DPA).**

→ **WARUM WICHTIG?**

Die **Rechtskonformität** des eingesetzten Tools ist entscheidend, um sicherzustellen, dass alle datenschutzrechtlichen und **Compliance-Vorgaben** eingehalten werden und keine rechtlichen Probleme entstehen.

→ **ERGEBNIS**

Sie haben eine **Liste sicherer und geprüfter KI-Tools** und gewährleisten die rechtliche Absicherung des Einsatzes.

09 Schulung & Feedback – Ihr Team einbinden

→ **ZIEL**

KI-Kompetenz gemäß. Art. 4 AI Act sicherstellen.

→ **EINFACHE MASSNAHME**

- **Rechtliche Schulung** zum AI Act: Mitarbeitende müssen sich mit den Rechten und Pflichten auskennen, die die Verordnung mit sich bringt.
- **Technische Schulung**: Mitarbeitende müssen sich mit dem sachgerechten Einsatz von KI-Systemen auskennen.
- **Ethische Schulung**: Mitarbeitende müssen über die sozialen und ethischen Chancen und Risiken der KI-Nutzung im Klaren sein.

→ **WARUM WICHTIG?**

Ein kontinuierlicher **Compliance-Prozess** und regelmäßige **Schulungen** tragen dazu bei, dass Ihr Team immer auf dem neuesten Stand ist und **rechtliche Fehler** frühzeitig erkannt werden.

→ **ERGEBNIS**

Ihr Team arbeitet sicher mit KI und trägt zur **rechtssicheren Nutzung** im Unternehmen bei.

BONUS-TIPP

Benennen Sie einen AI-Officer im Unternehmen

ZIEL

Eine **zentrale Ansprechperson** für alle KI-relevanten Fragen, um rechtliche Unsicherheiten zu minimieren und die Nutzung effizient zu steuern.

EINFACHE MASSNAHME

Bestimmen Sie einen Mitarbeitenden oder ein kleines Team, das als AI-Officer fungiert und für alle KI-bezogenen Themen zuständig ist. Diese Person kann:

- **Fragen zur KI-Nutzung** beantworten und dafür sorgen, dass die internen Prozesse rechtskonform sind.
- **Neue KI-Tools auf rechtliche Risiken** prüfen, insbesondere im Hinblick auf Datenschutz und Haftung.
- **Im Zweifel juristischen Rat** einholen und als Schnittstelle zu externen Rechtsexperten fungieren, um rasch fundierte Entscheidungen zu treffen.

WARUM WICHTIG?

Ein dedizierter **AI-Officer** stellt sicher, dass es im Unternehmen eine klare Zuständigkeit gibt, was sowohl die **rechtliche Compliance** als auch den **sicheren Einsatz von KI** betrifft. Diese Ansprechperson trägt dazu bei, dass alle Mitarbeitenden wissen, an wen sie sich wenden können, sodass **rechtliche Unsicherheiten** schnell und effizient gelöst werden.

ERGEBNIS

Sie haben eine **klare Zuständigkeit** für alle KI-relevanten Fragen und können die **rechtliche Sicherheit** im Unternehmen erhöhen, ohne dass jede Anfrage eine Rechtsberatung erfordert.

WEN ERNENNT MAN ALS AI OFFICER?

Die Person im Unternehmen sollte im Vorfeld **spezielle Kompetenzen** besitzen. Am besten werden diese Kompetenzen durch eine zweitägige Ausbildung mit Zertifikat ("**AI Compliance Specialist**") erworben. Wir können Sie bei der Ausblidung unterstützen – sprechen Sie uns an.

Ihr „KI-Schnell-Check“: Lücken erkennen, reagieren und schließen

1. Werden KI-Tools bereits genutzt? (z. B. ChatGPT, Midjourney, Jasper AI)	**ja** ☐	**nein** ☐
2. Verarbeitet eines dieser Tools personenbezogene Daten? (z. B. Kundendaten, Mitarbeiterdaten, Bewerberdaten)	**ja** ☐	**nein** ☐
3. Werden diese Daten ohne ausreichende Einwilligung oder Transparenz durch Dritte verarbeitet? (z. B. externe Anbieter von KI-Tools)	**ja** ☐	**nein** ☐
4. Geben Sie interne Firmeninformationen in ein KI-Tool ein? (z. B. vertrauliche Geschäftsdaten, Know-how, betriebsinterne Prozesse)	**ja** ☐	**nein** ☐
5. Haben Sie eine erlaubte KI-Tool-Liste erstellt? (Liste der geprüften und zugelassenen Tools)	**ja** ☐	**nein** ☐
6. Wissen alle Mitarbeitenden, welche KI-Tools erlaubt oder verboten sind? (z. B. Know-how über Nutzungsrichtlinien)	**ja** ☐	**nein** ☐
7. Haben Sie eine Grundregel für die KI-Nutzung? (z. B. Verbot vertraulicher Daten oder Prüfung vor Veröffentlichung)	**ja** ☐	**nein** ☐
8. Wird KI-generierter Content immer von einer Person geprüft, bevor er verwendet wird? (z. B. Prüfung der Qualität und rechtlichen Compliance von KI-Inhalten)	**ja** ☐	**nein** ☐
9. Wird beim Einsatz von KI sichergestellt, dass keine Rechte Dritter verletzt werden? (z. B. Urheberrechte, Markenrechte, Patente)	**ja** ☐	**nein** ☐
10. Haben Sie klare Regelungen für den Umgang mit Fehlentscheidungen oder Fehlern, die von der KI getroffen werden? (z. B. Haftungsklärung bei Fehlern der KI)	**ja** ☐	**nein** ☐
11. Gibt es jemanden im Unternehmen, der Fragen zu KI beantworten kann? (z. B. Benennung eines KI-Officers oder Compliance-Beauftragten)	**ja** ☐	**nein** ☐
12. Haben Sie ein Verfahren, um neue KI-Tools auf Risiken zu prüfen? (z. B. Datenschutzrisiken, Haftungsfragen)	**ja** ☐	**nein** ☐

AUSWERTUNG:

🟢 **Wenn Sie überall „Ja“ angekreuzt haben:** Super! Sie haben bereits einen strukturierten und rechtlich sicheren KI-Einsatz im Unternehmen etabliert.

🟠 **Wenn Sie mindestens einmal „Nein“ angekreuzt haben:** Hier könnte Handlungsbedarf bestehen. Überprüfen Sie die betreffenden Punkte & nehmen Sie gegebenenfalls Anpassungen vor.

🔴 **Mehr als drei „Nein“?** Dann sollten Sie dringend prüfen, wie Sie KI sicherer und rechtlich abgesichert einsetzen können. Ein KI-Compliance-Check ist notwendig.

Tech-First-Boutique für Recht, Technologie und digitales Business

Wir unterstützen Sie mit praxisorientierter KI-Rechtsberatung – gepaart mit Technologie-Expertise. Unser erfahrenes und mehrfach ausgezeichnetes Anwalts-Team beträt Sie ganzheitlich und auf höchsten Niveau im Bereich KI-Compliance.

Unser Ansatz: Die Hamonisierung von Künstlicher Intelligenz und Recht – ohne Innovationen zu bremsen. Dabei unterstützen wir Sie in allen rechtlichen Fragen rund um das Thema KI, z.B bei:

- **Regulatory Mapping:** Identifikation relevanter rechtlicher Anforderungen durch detailliertes Mapping gemäß verschiedenen nationalen Vorgaben und EU-Datenregulierungen.
- **Data & AI Governance:** Entwicklung und Anpassung von Governance-Strukturen, Identifizierung der Anforderungen und Vorbereitungen für die KI-Verordnung.
- **Schulungen:** Workshops zur Reichweite und Umsetzung des AI Act, Vermittlung von AI-Kompetenz gem. Art. 4 AI Act für Führungskräfte, Produktteams und Entwickler.
- **AI Inventory:** Unterstützung bei der Erstellung einer Übersicht aller KI Systeme im Unternehmen, einschließlich der Definition als mögliches als KI-System
- **Vertragsgestaltung:** Vertragsgestaltung im Zusammenhang mit KI-Projekten, wie z.B. Entwicklungsverträge, KI-as-a-Service-Verträge (KIaaS) und weitere.
- **Beratung zu Externen KI-Anwendungen:** Beratung und Anleitung zur Nutzung externer KI-Anwendungen und Prüfung von Drittanwendungen.
- **Anonymisierung & Pseudonymisierung:** Ausgestaltung und Beratung zu Anonymisierungs- und Pseudonymisierungskonzepten
- **Risikobewertungen:** Beratung zu Risikobewertungen im Rahmen von Datenschutz- und Grundrechtefolgenabschätzungen in Bezug auf KI-Systeme.
- **Beratung zu Urheberrecht:** Beratung zu urheberrechtlichen Implikationen im Zusammenhang mit GenAI.
- **Rechtskonforme Datennutzung:** Beratung zu rechtskonformer Datennutzung von Big Data, maschinellem Lernen und generativer KI im Zusammenhang mit Datenschutzrecht, Geschäftsgeheimnissen und Datenbankrechten.



Philipp Müller-Peltzer
Rechtsanwalt und Partner

T +49 (0)30 21 30 028-0
E mueller-peltzer@srd-rechtsanwaelte.de

srd-rechtsanwaelte.de

JUVE HANDBUCH 2023|2024

The LEGAL 500 DEUTSCHLAND – TOP KANZLEI 2024

The LEGAL 500 DEUTSCHLAND – BOUTIQUE-KANZLEI DES JAHRES 2025