LEITFADEN

KI-Richtlinien für Unternehmen verstehen und richtig gestalten

proliance

Unternehmen, die Künstliche Intelligenz (KI) einsetzen, brauchen wirksame KI-Governance. Eine zentrale Rolle spielen dabei KI-Nutzungsrichtlinien: Sie zeigen den Mitarbeitern klar, wo Vorteile und Grenzen der Technologie liegen und wie sie sicher mit KI arbeiten. Unser Leitfaden gibt Tipps, mit denen Sie Ihre eigene AI Policy erstellen können.

Was ist eine AI Policy?

Eine AI Policy ist eine verbindliche Richtlinie zum Einsatz von Künstlicher Intelligenz im Unternehmen. Sie ist wichtiger Bestandteil der KI-Governance, also den Leitplanken für den internen Umgang mit der Technologie.

Ziel der Richtlinie ist es, Unternehmen die Arbeit mit KI zu ermöglichen gleichzeitig die Risiken zu kontrollieren, die von Tools wie ChatGPT und Co. ausgehen können. Damit wird die AI Policy zu einer wichtigen Grundlage für Compliance mit geltenden Vorschriften wie der DSGVO oder der KI-Verordnung.

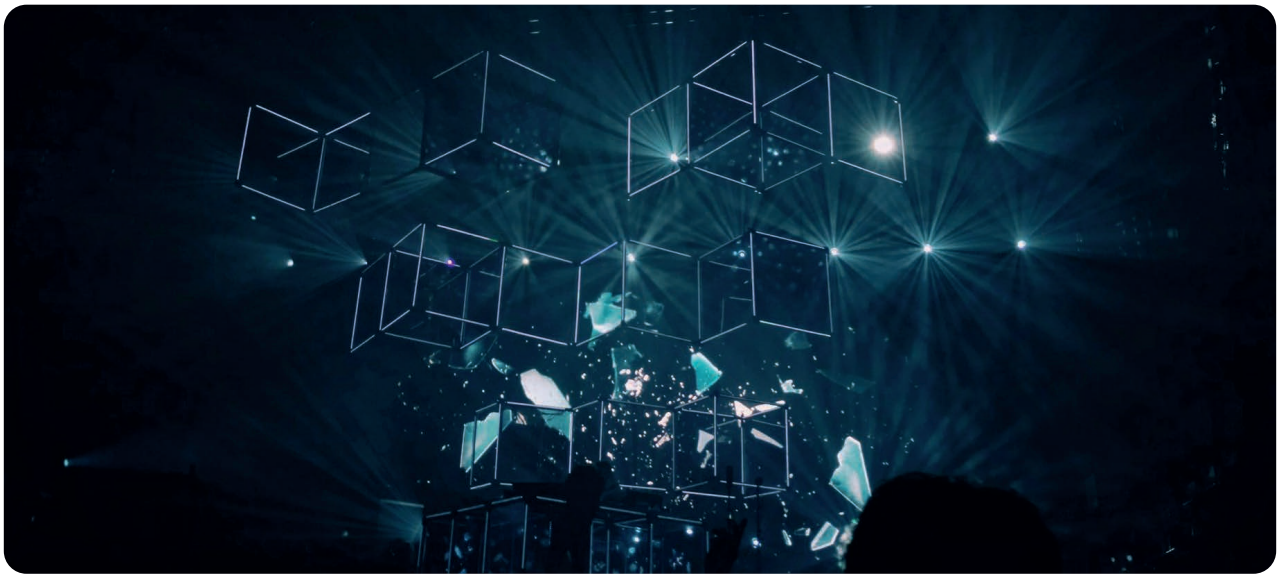
Eine Nutzungsrichtlinie für Unternehmens-KI

- übersetzt ethische und regulatorische Anforderungen in konkrete, verbindliche Vorgaben und Prozesse.
- schützt vor Datenschutzverletzungen, Datenlecks, Urheberrechtsverstößen, Bias und anderen rechtlichen Risiken, die durch KI entstehen können.
- fördert Innovation, indem sie klare Rahmenbedingungen für den verantwortungsvollen Einsatz von KI schafft.

Warum brauchen Unternehmen eine AI Policy?

KI-Tools dürfen in Organisationen nur eingesetzt werden, wenn sie zuvor von IT, Compliance und Datenschutzbeauftragten geprüft wurden. So ist gewährleistet, dass die eingesetzten Tools zu den Unternehmensprozessen und -zwecken passen und die IT-Sicherheit nicht gefährdet ist.

Ohne klare Regelung besteht auf der anderen Seite die Gefahr, dass Mitarbeitende KI eigenständig mit privaten Accounts nutzen („Schatten-KI"). Dies birgt erhebliche Sicherheitsrisiken und kann zu Haftungsfällen führen, wenn Compliance-Vorgaben verletzt werden.



Was muss eine AI Policy konkret enthalten – und wie formuliert man die Inhalte?

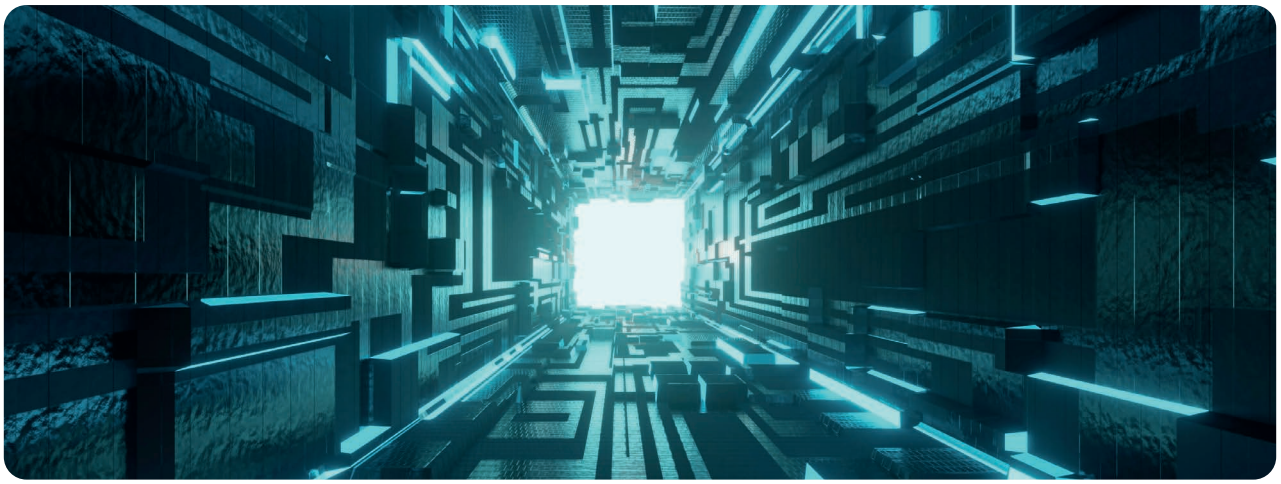
Für den Aufbau und Inhalt einer KI-Nutzungsrichtlinie gibt es keine gesetzlichen Vorgaben. Es gibt jedoch wichtige Punkte, die in Ihrer AI Policy nicht fehlen sollten, damit Ihre Belegschaft KI sicher nutzen kann.

Zulässige Tools und Zwecke

Legen Sie fest,

- welche KI-Tools
- für welche Zwecke und
- mit welchen Daten
- von welchen Personen oder Abteilungen

genutzt werden dürfen.



Definieren Sie darüber hinaus, welche KI-Systeme konkret erlaubt, eingeschränkt oder verboten bzw. nicht freigegeben sind und für welche Personen und KI-Systeme Ihre KI-Richtlinie gilt.

Die Policy sollte zudem beschreiben, wie Mitarbeitende vorgehen können, wenn sie ein neues Tool nutzen möchten, und welche Prüfungen der KI-Beauftragte vor der Freigabe neuer Tools vornehmen muss.

Formulierungsbeispiele

Ziele dieser Policy:

- ✓ Verantwortungsvolle und innovative Nutzung von KI
- ✓ Identifikation & Minimierung von Risiken beim KI-Einsatz
- ✓ Förderung von KI-Kompetenz, Ermöglichung effizienter und sachgemäßer KI-Nutzung
- ✓ Sicherstellung von Transparenz, Nachvollziehbarkeit und menschlicher Kontrolle
- ✓ Vermeidung diskriminierender, manipulativer oder rechtswidriger KI-Anwendungen
- ✓ Schutz von Unternehmensdaten, Geschäftsgeheimnissen & personenbezogener Daten

Name des zugelassenen Tools	Zugelassen für (Personengruppe)	Zugelassene Einsatzzwecke
[z.B. ChatGPT Teams]	[z.B. für alle Mitarbeiter mit Account-Freischaltung auf Anfrage]	[z.B. Recherche, Content-Creation, Dokumenterstellung]

Definition wichtiger Begriffe

Definieren Sie zentrale Begriffe wie „Künstliche Intelligenz“ oder „KI-Anwendung“, um ein einheitliches Verständnis der Technologie in Ihrem Unternehmen zu schaffen. Orientierung können etablierte Standards von Organisationen wie OECD oder NIST bieten sowie die Legaldefinition in Art. 3 Nr. 1 KI-VO.

Formulierungsbeispiel

Künstliche Intelligenz (KI): bezeichnet Systeme, die auf maschinellem Lernen, Wissensrepräsentation und anderen Techniken basieren, um Aufgaben zu erfüllen, die normalerweise menschliche Intelligenz erfordern wie beispielsweise die Analyse großer Datenmengen, Mustererkennung oder das Treffen von Entscheidungen.

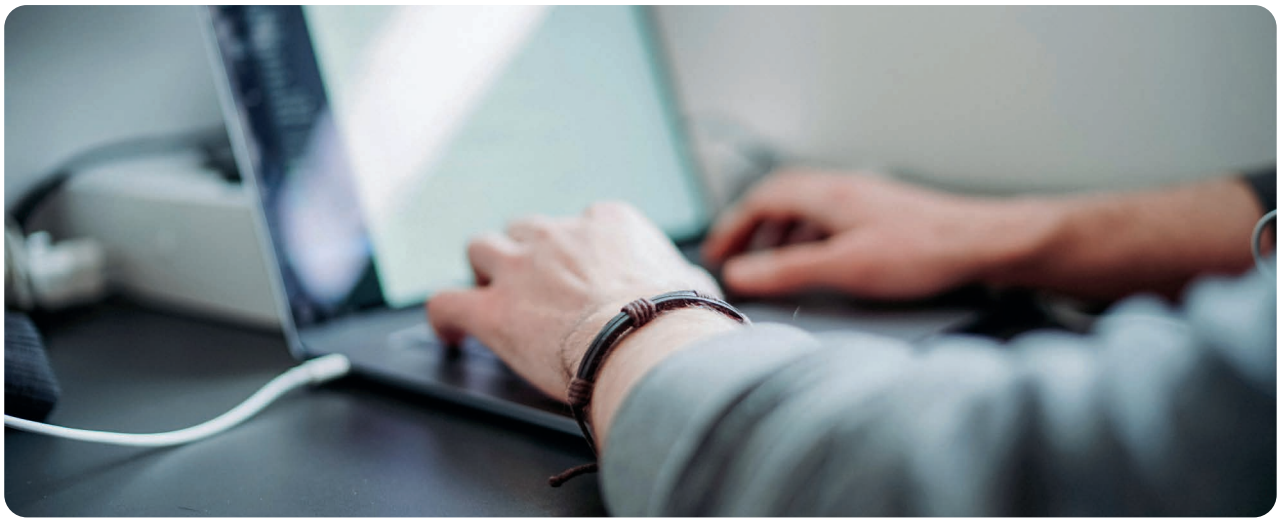
Regeln zur Einhaltung des Datenschutzes

Eine der größten Gefahren bei der Arbeit mit KI-Tools ist, dass vertrauliche Informationen in die Trainingsdaten der KI gelangen. Erlauben Sie die Eingabe von personenbezogenen oder unternehmensbezogenen Daten deshalb in Ihrer Richtlinie nur für zugelassene Tools und Anwendungsfälle.

⚠ **Wichtig:** Die Eingabe sensibler personenbezogener Daten gemäß. Art. 9 DSGVO muss grundsätzlich untersagt sein.

Formulierungsbeispiel

Die Eingabe sensibler personenbezogener Daten gemäß. Art. 9 DSGVO ist nicht gestattet. Hierzu zählen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, genetische Daten, biometrischen Daten, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung.



Verantwortlichkeiten und Rollen

Definieren Sie klar, wer für die Steuerung, Überwachung und Freigabe von KI-Systemen verantwortlich ist. Das kann zum Beispiel ein IT-Verantwortlicher oder der KI- oder Datenschutzbeauftragter sein. Legen Sie fest, wie die Zusammenarbeit und Kommunikation zwischen diesen Rollen erfolgt.

Formulierungsbeispiel

Der KI-Beauftragte übernimmt die Aufgaben bezüglich des KI-Einsatzes in Abstimmung mit der Unternehmensleitung sowie dem KI Governance Team. Der KI-Beauftragte nimmt insbesondere folgende Aufgaben wahr:

1. die Prüfung der Zulassung und Dokumentation neuer KI-Anwendungen
2. die Überwachung und Verwaltung von Zugriffsrechten
3. die Bearbeitung sonstiger operativer Aufgaben und Themen
4. die Beantwortung von Anfragen zu KI insgesamt und spezifischen KI-Anwendungen
5. Die Vorbereitung und Durchführung des quartalsweisen und jährlichen KI-Reviews
6. Organisation und Überwachung der KI-Kompetenz Schulungen
7. Verwaltung der Dokumentation

Umgang mit KI-Vorfällen und Meldewege

Legen Sie fest, wie mit Sicherheitsvorfällen, Fehlfunktionen oder Verdacht auf diskriminierende, manipulative oder rechtswidrige KI-Anwendungen umzugehen ist. Definieren Sie Meldewege und Verantwortlichkeiten für die Bearbeitung solcher Vorfälle.

Beispiel für eine Meldematrix

Kategorie	Meldung an	Frist	Meldepflicht
Datenschutzverletzung	• KI-Beauftragter • DSB	72h	Meldepflicht an AB & Betroffene, Art. 33, 34 DSGVO
Diskriminierung/Bias	• KI-Beauftragter • DSB	48h	
Schwere Fehlfunktion (Hochrisiko-KI)	• KI-Beauftragter • Compliance • IT-Sicherheit	72h	Meldepflicht an Anbieter & AB, Art. 26 Abs. 5, 73 KI-VO
Sicherheitsvorfall	• KI-Beauftragter • Compliance • IT-Sicherheit	sofort	
Compliance-Verstoß	• KI-Beauftragter	5 Werktage	

Zusammenfassung der Meldepflichten

Schulung und Kompetenzaufbau

Regeln Sie in Ihrer KI-Richtlinie, wie Mitarbeitende regelmäßig zu KI, Datenschutz und Compliance geschult werden. Fördern Sie den Aufbau von KI-Kompetenz und Sensibilität für Risiken.

Verknüpfung mit anderen Policies und rechtlichen Anforderungen

Stellen Sie klar, dass die AI Policy im Einklang mit anderen internen Richtlinien und externen gesetzlichen Anforderungen steht und zählen Sie die die konkret einzuhaltenden Vorgaben im Anhang auf.

Formulierungsbeispiel

Bei der Nutzung zugelassener KI-Anwendungen sind die gesetzlichen Vorgaben, insbesondere die datenschutzrechtlichen Normen der DSGVO sowie des BDSG und der KI-Verordnung einzuhalten.

Sanktionen und Ausnahmen

Geben Sie genau an, welche Konsequenzen bei Verstößen gegen die Policy drohen und wie mit begründeten Ausnahmen umzugehen ist.

Formulierungsbeispiel

Mitarbeiter*innen sind dazu verpflichtet, der vorliegenden Richtlinie im Rahmen des Weisungsrechts des Arbeitgebers Folge zu leisten. Verstöße können z. B. Schadensersatzansprüche sowie straf-, zivil- und arbeitsrechtliche Konsequenzen nach sich ziehen.

Das sollten Unternehmen beim Erstellen und Implementieren einer AI Policy beachten

Do's

- Definieren Sie den Geltungsbereich und die Ziele der Nutzungsrichtlinie so genau wie möglich.
- Legen Sie konkrete KI-Tools für konkrete Zwecke fest.
- Gleichen Sie die AI Policy mit den Werten und Strategien Ihres Unternehmens ab.
- Bestimmen Sie klare Verantwortlichkeiten.
- Etablieren Sie nachvollziehbare Prozesse, zum Beispiel mit Vorlagen, Checklisten, Aufgaben und Rollen.
- Kommunizieren Sie die KI-Richtlinien transparent und aktiv und schulen Sie Mitarbeitende regelmäßig.

Don'ts

- Festlegung von Spielregeln für KI-Nutzung wird versäumt – so entsteht gefährliche „Schatten-KI".
- Verantwortlichkeiten und Prozesse bleiben ungeklärt.
- Vernachlässigung von Schulungen zur Richtlinie sowie der KI-Kompetenz von Mitarbeitenden.
- Die Eingabe personenbezogener Daten nur zu untersagen reicht als KI-Nutzungsrichtlinie nicht aus.
- Fehlender Abgleich der KI-Richtlinie mit anderen internen und externen Regelwerken sowie die Beseitigung von Widersprüchen.

Nächste Schritte für Ihre AI Policy

Eine Nutzungsrichtlinie für den KI-Einsatz schützt Ihr Unternehmen vor Risiken, fördert Innovation und sorgt für Compliance. Sie muss verständlich formuliert sein, damit alle Mitarbeitenden sie anwenden können. Nach der Verabschiedung sind die Prozesse und Maßnahmen gemeinsam mit den Mitarbeitenden zu implementieren und regelmäßig zu überprüfen.

Lassen Sie sich von unseren KI-Experten beraten

Sie wünschen Unterstützung bei der Erstellung und Implementierung Ihrer AI Policy? Erfahren Sie, wie die KI-Experten von Proliance Ihnen Arbeit abnehmen.

Jetzt unverbindlichen Termin buchen

Sie haben Fragen?
Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung
zu Compliance in Ihrem Unternehmen?

Rufen Sie uns gerne an oder schreiben Sie uns
eine E-Mail!

proliance.ai
+49 (0)89 250 039 220
info@proliance.ai

Alexander Ingelheim
Geschäftsführung

Compliance. Sicher erledigt.
Proliance ist die Datenschutz- und Compliance-Plattform für den Mittelstand. Wir kombinieren smarte Software mit persönlicher Beratung durch TÜV- und Dekra-zertifizierte Experten und Compliance-Enthusiasten, damit Sie DSGVO, NIS2, ISO 27001, TISAX® u.a. mühelos erfüllen. Risikofrei, unkompliziert, zeitsparend. Über 2.500 Kunden aus 50+ Branchen vertrauen seit 2017 auf uns.

proliance

Join the movement
Wir sind Mitglied

We take
Climate
Action
lfca.earth/co2