



# UNTERNEHMENSRICHTLINIE FÜR VERANTWORTUNGSVOLLEN EINSATZ VON KÜNSTLICHER INTELLIGENZ (KI)

*Version 1.0 – [Datum]*



# UNTERNEHMENSRICHTLINIE FÜR VERANTWORTUNGSVOLLEN EINSATZ VON KÜNSTLICHER INTELLIGENZ (KI)

*Version 1.0 – [Datum]*

## 1. Einführung und Zweck der Richtlinie

Die Nutzung von Künstlicher Intelligenz (KI) verändert grundlegend die Art und Weise, wie Unternehmen arbeiten, Entscheidungen treffen und Innovation gestalten. [Unternehmensname] erkennt das enorme Potenzial von KI-Technologien zur Steigerung von Effizienz, Qualität und Innovationskraft – ebenso wie die damit verbundenen Risiken in Bezug auf Ethik, Datenschutz und Diskriminierung.

Diese Richtlinie verfolgt das Ziel, eine unternehmensweite Grundlage für den **verantwortungsvollen, rechtssicheren und transparenten Einsatz von KI-Systemen** zu schaffen. Sie definiert klare Grundsätze, Zuständigkeiten und Rahmenbedingungen für die Entwicklung, den Erwerb und den Einsatz von KI in allen Unternehmensbereichen.

Wir verstehen verantwortungsvolle KI als die Verpflichtung, Innovation im Einklang mit gesellschaftlichen Werten, gesetzlichen Anforderungen (z. B. DSGVO, KI-Verordnung (EU)) und unternehmensinternen Leitlinien umzusetzen. Die Richtlinie trägt dazu bei, Vertrauen bei Beschäftigten, Partnern und der Öffentlichkeit zu stärken – und gleichzeitig die Innovationsfähigkeit von [Unternehmensname] zu sichern.

## 2. Anwendungsbereich

Diese KI-Richtlinie gilt für:

- **alle Mitarbeitenden** (inkl. Teilzeitkräfte, Werkstudent:innen, Praktikant:innen und externe Auftragnehmer),
- **alle Einheiten und Standorte** von [Unternehmensname],
- **sämtliche KI-Anwendungen**, unabhängig davon, ob sie selbst entwickelt, eingekauft, in der Cloud betrieben oder über Drittanbieter bezogen werden.

Sie umfasst **alle Phasen des KI-Lebenszyklus** – von der Idee und Beschaffung über Entwicklung, Implementierung, Nutzung und Wartung bis zur Evaluierung und ggf. Außerbetriebnahme.

Für Fragen zur Anwendbarkeit dieser Richtlinie auf konkrete Systeme, Technologien oder Prozesse steht das KI-Governance-Team bzw. die benannten Ansprechpersonen zur Verfügung (siehe Abschnitt „Governance & Rechenschaftspflicht“).

## 3. Begriffsdefinitionen

### **KI-System (gemäß EU-KI-Verordnung, Art. 3 Nr. 1):**

Ein maschinengestütztes System, das für einen autonomen Betrieb in unterschiedlichem Umfang ausgelegt ist, nach seiner Betriebsaufnahme anpassungsfähig sein kann und Eingaben verwendet, um Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen zu erzeugen, die physische oder virtuelle Umgebungen beeinflussen können.

### **Beispiele:**

- *KI-System*: ChatGPT, Text-zu-Bild-Generatoren, Spracherkennung mit lernfähiger Auswertung
- *Kein KI-System*: Regelbasierte Skripte oder Excel-Makros ohne autonome Entscheidungslogik

**Schatten-KI:**

Darunter versteht man KI-Anwendungen, die ohne Wissen oder Zustimmung des Unternehmens – insbesondere außerhalb des offiziellen IT-Freigabeprozesses – genutzt werden. Diese Systeme stellen ein erhebliches Risiko für Datenschutz, Sicherheit und Compliance dar. Die Nutzung nicht freigegebener KI-Tools ist untersagt und kann disziplinarische Konsequenzen nach sich ziehen.

**Beispiele:**

- Nutzung von ChatGPT über einen privaten Account zur Bearbeitung interner Dokumente
- Verwendung von Bild-KI zur Logoentwicklung ohne Abstimmung mit dem KI-Kern-Team

**Personenbezogene Daten (gemäß DSGVO, Art. 4 Abs. 1):**

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

**Beispiele:**

- Direkte Identifikatoren: Name, E-Mail-Adresse, Telefonnummer, Sozialversicherungsnummer
- Indirekte Identifikatoren: Nutzer-ID, IP-Adresse, Standortdaten in Kombination mit anderen Merkmalen

**Sensible Daten (Datenklasse I – „Streng vertraulich“):**

Informationen, deren Verlust oder Offenlegung erhebliche wirtschaftliche, rechtliche oder reputative Schäden verursachen kann.

**Beispiele:**

- Beschäftigtendaten (z. B. Lohnabrechnungen, Personalakten)
- Geschäftliche Geheimnisse (z. B. Preismodelle, technische Designs, geplante M&A-Projekte)

- Kundenverträge, nicht veröffentlichte Jahresabschlüsse oder interne Strategieunterlagen
- Sicherheitsrelevante Systeme oder Quellcodes

#### **Abgrenzung zu öffentlichen Daten (Datenklasse IV):**

Öffentliche Daten sind Informationen, deren Veröffentlichung keinen Schaden verursacht. Sie dürfen grundsätzlich zur Interaktion mit freigegebenen KI-Systemen verwendet werden, sofern dies nicht im Einzelfall eingeschränkt ist.

#### **Beispiele für öffentliche Daten:**

- Produktbroschüren, Pressemitteilungen, veröffentlichte Preislisten
- Unternehmenswebsite, öffentliche Termine, Fachartikel oder Marktstudien mit Freigabe

Die genaue Einordnung von Informationen in Datenklassen erfolgt gemäß der internen **Datenschutz- und Informationssicherheitsrichtlinie**. Im Zweifel ist das **KI-Kern-Team** zu konsultieren.

## **4. Rechtliche & ethische Grundprinzipien**

Der Einsatz von KI bei [Unternehmensname] erfolgt unter Achtung rechtlicher Verpflichtungen und ethischer Werte. Diese Prinzipien gelten unabhängig vom Einsatzbereich – ob intern, extern oder im Kundenkontext. Sie bilden das Fundament für Vertrauen, Compliance und nachhaltige Innovationskraft.

### **4.1 Datenschutz & Privatsphäre**

KI-Systeme dürfen nur in Einklang mit geltendem Datenschutzrecht (insbesondere DSGVO) eingesetzt werden. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine rechtliche Grundlage besteht oder eine ausdrückliche Einwilligung vorliegt.

**Verpflichtend gilt:**

- Datenminimierung: Nur notwendige personenbezogene Daten dürfen verwendet werden.
- Zweckbindung: Daten dürfen nur für den konkreten Verwendungszweck genutzt werden.
- Transparenz: Betroffene müssen über die Datenverarbeitung verständlich informiert werden.
- Betroffenenrechte: Auskunft, Löschung, Korrektur und Widerspruch sind jederzeit sicherzustellen.

**4.2 Sicherheit & Schutz**

KI-Systeme müssen so gestaltet und betrieben werden, dass die Sicherheit von Daten, Prozessen und Personen jederzeit gewährleistet ist.

**Konkret bedeutet das:**

- Technische und organisatorische Maßnahmen gemäß ISO 27001 und interner Sicherheitsrichtlinien
- Regelmäßige Tests auf Funktionalität, Fehlertoleranz und Missbrauchsmöglichkeiten
- Keine Verarbeitung sicherheitskritischer Informationen ohne vorherige Freigabe durch das KI-Kern-Team

**4.3 Rechenschaftspflicht**

Jede KI-Anwendung muss nachvollziehbar, dokumentiert und verantwortet sein. Die Verantwortung für die korrekte Nutzung von KI liegt beim Fachbereich, der das System betreibt – unterstützt vom KI-Kern-Team.

**Praktisch umfasst das:**

- Dokumentation der eingesetzten Modelle, Datenquellen und Entscheidungen
- Zuordnung von Zuständigkeiten im KI-Inventar
- Durchführung von Risiko- und Rechtsbewertungen vor Inbetriebnahme

**4.4 Transparenz & Erklärbarkeit**

Nutzer:innen – intern wie extern – müssen nachvollziehen können, wann und wie KI-Systeme in Entscheidungsprozesse eingebunden sind.

**Dazu gehört:**

- Kennzeichnung von KI-generierten Inhalten oder Entscheidungen
- Erläuterung, welche Rolle die KI spielt und welche Daten sie nutzt
- Offenlegung automatisierter Entscheidungsprozesse, z. B. bei personalisierten Angeboten

**4.5 Fairness & Nichtdiskriminierung**

KI darf keine benachteiligenden oder diskriminierenden Wirkungen entfalten – weder direkt noch indirekt.

**Verpflichtend gilt:**

- Bias-Prüfung bei Trainingsdaten und Modellen
- Keine Bewertung oder Steuerung emotionaler oder persönlicher Merkmale von Mitarbeitenden
- Keine algorithmischen Entscheidungen in arbeitsrechtlichen Belangen ohne menschliche Prüfung

## 4.6 Menschliche Aufsicht & Befähigung

KI darf niemals vollständig autonom agieren. Entscheidungen mit wesentlichen Folgen sind durch qualifizierte Mitarbeitende zu prüfen und freizugeben.

### Konkret heißt das:

- „Human in the loop“-Pflicht bei kritischen Prozessen
- Schulung der Mitarbeitenden im Umgang mit dem jeweiligen KI-System
- Förderung eines positiven Innovationsklimas mit klaren Leitplanken

## 5. Nachhaltigkeit

KI-Systeme müssen effizient, ressourcenschonend und im Einklang mit unseren Umweltzielen eingesetzt werden.

### Beispiele für nachhaltige KI-Praxis:

- Energieeffiziente Modellwahl und Cloud-Nutzung
- Vermeidung unnötiger Datenverarbeitung
- Berücksichtigung ökologischer Auswirkungen bei neuen KI-Projekten

Für Fragen zur praktischen Umsetzung dieser Prinzipien steht das **KI-Kern-Team** beratend zur Seite. Bei Unsicherheiten gilt: lieber einmal zu viel fragen als einmal zu wenig.

## 6. Umgang mit sensiblen und öffentlichen Daten

Für die Verarbeitung unterschiedlicher Daten gelten differenzierte Regeln:

<b>Datenklasse</b>	<b>Behandlung in KI-Systemen</b>
<b>Streng vertraulich</b> (z. B. M&A-Pläne, Löhne, Patente)	<b>Verarbeitung in KI nur mit schriftlicher Freigabe</b> durch das KI-Kern-Team
<b>Vertraulich</b> (z. B. Schulungspläne, interne Analysen)	<b>Nur nach Risikoabwägung</b> und dokumentierter Prüfung durch Fachbereich
<b>Eingeschränkt zugänglich</b> (z. B. Lieferanteninfos, Projektzeitpläne)	Nutzung mit <b>vermerkter Zweckbindung</b> und Zugangskontrolle
<b>Öffentlich</b> (z. B. Website-Inhalte, veröffentlichte Pressemitteilungen)	<b>Nutzung zulässig</b> , sofern keine Vermischung mit sensiblen Informationen erfolgt

Im Zweifel gilt stets: sensible Daten dürfen **niemals** unverschlüsselt oder außerhalb freigegebener Tools in KI-Systeme eingegeben werden.

### 6.1 Vorgehen bei Unsicherheiten

Wenn unklar ist, ob ein System oder ein Anwendungsfall unter diese Richtlinie fällt, sind folgende Schritte einzuhalten:

1. Dokumentation des Anwendungsfalls
2. Rücksprache mit der zuständigen Führungskraft
3. Kontaktaufnahme mit dem KI-Kern-Team

**Es gilt das Vorsichtsprinzip:** Keine KI-Nutzung ohne klare rechtliche und technische Freigabe.

## 6.2 Dokumentationspflichten

Alle freigegebenen KI-Systeme und ihre Einsatzszenarien müssen im zentralen **KI-Inventar** registriert werden. Dazu zählen:

- Name und Version des Tools
- verantwortlicher Fachbereich
- Beschreibung des Einsatzes
- verarbeitete Datenarten
- Risiko- und Zweckbeschreibung
- Ergebnisse von Vorabprüfungen (z. B. Datenschutzfolgeabschätzung, Bias-Screening)

Diese Dokumentation ist regelmäßig zu aktualisieren – mindestens einmal jährlich oder bei wesentlichen Änderungen.

Die Einhaltung dieser Verhaltensregeln wird regelmäßig überprüft. Verstöße können zu Einschränkungen beim KI-Zugang, Projektstopps oder disziplinarischen Maßnahmen führen.

## 7. Governance & Rechenschaftspflicht

Eine wirksame KI-Richtlinie braucht klare Verantwortlichkeiten und transparente Eskalationswege. Dieser Abschnitt beschreibt, wer im Unternehmen wofür zuständig ist, wie Mitarbeitende bei Fragen oder Vorfällen Unterstützung erhalten – und welche Konsequenzen bei Verstößen gegen die Richtlinie vorgesehen sind.

### 7.1 Aufgaben und Rolle des KI-Kern-Teams

Das **KI-Kern-Team** ist das zentrale Gremium für Governance, Koordination und Beratung beim Einsatz von KI-Systemen. Es setzt sich interdisziplinär zusammen – typischerweise aus Vertretungen von Datenschutz, IT, Recht, Strategie, Kommunikation und ggf. HR.

**Hauptaufgaben:**

- Prüfung und Genehmigung neuer KI-Anwendungen
- Führung und Pflege des unternehmensweiten KI-Inventars
- Beratung bei rechtlichen und ethischen Fragen
- Koordination von Risikoanalysen und Folgeabschätzungen
- Bereitstellung von Schulungs- und Weiterbildungsangeboten
- Monitoring von Compliance und technischer Entwicklung

**Kontakt:** [Kontakt-E-Mail oder internes Ticket-System angeben]

**7.2 Ansprechpartner:innen und Eskalationswege****Wer hilft weiter, wenn...**

<b>Situation</b>	<b>Zuständig</b>
Ich bin unsicher, ob ich ein KI-Tool verwenden darf.	KI-Kern-Team
Ich habe datenschutzrechtliche Fragen.	Datenschutzbeauftragte:r
Ich entdecke eine fehlerhafte oder riskante Entscheidung durch ein KI-System.	Fachverantwortliche:r + KI-Kern-Team
Ich sehe einen möglichen Verstoß gegen diese Richtlinie.	Unmittelbar Führungskraft, optional KI-Kern-Team oder Vertrauensstelle

**Grundsatz:**

Fragen stellen ist ausdrücklich erwünscht. Fehler dürfen passieren – Verschweigen jedoch nicht.

### 7.3 Meldeverfahren bei Vorfällen

Sollte ein KI-System nicht wie erwartet funktionieren, unerwünschte Ergebnisse liefern oder Datenlecks auftreten, gilt:

- **Sofortige Meldung** an das KI-Kern-Team oder die Datenschutzstelle
- Interne Vorfallsbewertung (technisch, rechtlich, ethisch)
- Falls erforderlich: Information der Geschäftsführung und ggf. externer Stellen (z. B. Aufsichtsbehörden)
- Unterstützung bei Maßnahmen zur Schadensbegrenzung

**Wichtig:** Auch **vermutete** Verstöße oder Risiken müssen gemeldet werden.

### 7.4 Konsequenzen bei Verstößen

[Unternehmensname] verfolgt eine lernorientierte Fehlerkultur. Wir erwarten jedoch die **ernsthafte Beachtung dieser Richtlinie**. Abweichungen, die gemeldet und offen angesprochen werden, ziehen **keine Sanktionen** nach sich.

**Folgende Reaktionen sind möglich:**

<b>Verstoßart</b>	<b>Mögliche Folgen</b>
Leicht fahrlässiger Verstoß bei Erstverwendung	Aufklärung, Schulung
Wiederholte oder grob fahrlässige Missachtung	Projektausschluss, formelle Abmahnung
Vorsätzlicher Regelbruch, z. B. vorsätzliche Datenweitergabe	Disziplinarmaßnahmen bis hin zur Kündigung, ggf. strafrechtliche Schritte

Verantwortungsvolles Handeln heißt auch, **Grenzen zu respektieren** und im Zweifel Rat einzuholen.

Diese Governance-Regeln unterstützen unser Ziel, KI transparent, sicher und im Einklang mit unseren Werten einzusetzen – nicht, um Mitarbeitende zu kontrollieren, sondern um sie zu befähigen.

## 8. Schulung & Bewusstseinsbildung

Der verantwortungsvolle Umgang mit KI erfordert mehr als technische Fähigkeiten: Er verlangt ein fundiertes Verständnis rechtlicher Rahmenbedingungen, ethischer Leitplanken und konkreter Anwendungsrisiken. [Unternehmensname] fördert gezielt die **KI-Kompetenz seiner Mitarbeitenden** – durch Schulung, Praxisnähe und Austauschformate.

### 8.1 Grundlagenvermittlung & Pflichtformate

Alle Mitarbeitenden, die KI-Systeme nutzen, müssen eine **Grundlagenschulung zur verantwortungsvollen KI-Nutzung** absolvieren. Die Teilnahme ist verpflichtend, sobald ein neues KI-Tool eingesetzt wird oder eine neue Rolle im KI-Kontext übernommen wird.

#### Inhalte der Grundlagenschulung (mindestens):

- Was ist ein KI-System?
- Rechte und Pflichten laut EU-KI-VO und DSGVO
- Datenarten und Schutzmaßnahmen (inkl. Schatten-KI-Verbot)
- Beispiele für ethische Dilemmata und gute Praxis
- Meldepflichten und Anlaufstellen im Unternehmen

#### Format:

Online-Modul mit Wissenstest (wird dokumentiert), ergänzt durch Präsenzangebote bei Bedarf

## 8.2 Weiterführende Schulungen nach Zielgruppe

Je nach Rolle bieten wir vertiefende Qualifizierungen an:

Zielgruppe	Schwerpunkte
Fachverantwortliche / Product Owner	KI-Anforderungsdefinition, Risikobewertung, Modellverständnis
Entwickler:innen / Tech	Modellwahl, Trainingsdatenprüfung, Bias-Kontrolle, Dokumentation
Führungskräfte	Risikomanagement, Verantwortung in der KI-Wertschöpfungskette
Datenschutz / Legal / Compliance	Schnittstellen zur DSGVO, Urheberrecht, Transparenzanforderungen
HR & Kommunikation	Einsatz von KI in Bewerbungsprozessen, Kommunikation und Change-Management

Alle Schulungsangebote werden vom **KI-Kern-Team** in Kooperation mit externen Fachstellen regelmäßig aktualisiert.

## 8.3 Informelles Lernen & Austauschkultur

Neben formalen Schulungen setzt [Unternehmensname] auf kontinuierlichen Austausch:

- **„KI-Check-ins“**: Regelmäßige kurze Updates zu Neuerungen, Praxisfällen oder Richtlinien
- **KI-Ethik-Botschafter:innen** in den Fachabteilungen als lokale Ansprechpersonen
- **Themendialoge / Lunch & Learn** zu aktuellen Fragen, Use Cases oder regulatorischen Entwicklungen
- **Feedbackkanäle** für Ideen, Fragen oder Probleme im Umgang mit KI-Systemen

Ziel ist es, **eine Unternehmenskultur zu etablieren, in der KI als Werkzeug mit Verantwortung verstanden wird** – nicht als Risiko oder Blackbox.

Der Aufbau von KI-Kompetenz ist keine einmalige Maßnahme, sondern ein kontinuierlicher Prozess. [Unternehmensname] stellt sicher, dass Wissen und Haltung gemeinsam wachsen.

## 9. KI-Inventar & Prüfprozess

Transparenz ist ein zentrales Prinzip beim verantwortungsvollen Einsatz von KI. Um den Überblick über alle eingesetzten KI-Systeme zu behalten, führt [Unternehmensname] ein zentrales **KI-Inventar**. Es bildet die Grundlage für rechtssichere Nutzung, regelmäßige Überprüfung und gezieltes Risikomanagement.

### 9.1 Aufnahme und Registrierung neuer KI-Systeme

Vor der erstmaligen Nutzung eines KI-Systems muss dieses über das KI-Kern-Team im Inventar erfasst werden. Die Registrierung ist Voraussetzung für den rechtskonformen Einsatz.

#### Der Ablauf umfasst folgende Schritte:

1. **Vorabmeldung durch den Fachbereich**, der das System einsetzen will (z. B. via Anfrageformular)
2. **Einreichung einer Systembeschreibung**, inkl. geplanter Nutzung, Funktionsweise und verarbeiteter Datenarten
3. **Risikoprüfung durch das KI-Kern-Team**, insbesondere auf:
  - Datenschutzkonformität (z. B. Notwendigkeit einer Datenschutzfolgeabschätzung)
  - Relevanz im Sinne der EU-KI-Verordnung (z. B. Hochrisikosysteme)
  - Ethik- und Transparenzanforderungen
4. **Freigabeentscheidung** mit ggf. Auflagen, Einschränkungen oder Schulungspflichten
5. **Eintrag ins KI-Inventar** mit allen relevanten Metadaten (siehe unten)

Das Inventar wird durch das KI-Kern-Team gepflegt, ist nicht öffentlich zugänglich und dient ausschließlich dem internen Compliance-Management.

## 9.2 Pflichtangaben im KI-Inventar

Folgende Informationen sind für jedes registrierte KI-System vollständig zu erfassen:

- Bezeichnung des KI-Systems und Versionsstand
- Verantwortlicher Fachbereich und benannte:r Ansprechpartner:in
- Zweck und Einsatzszenarien
- Verarbeitete Datenarten (inkl. Klassifikation nach Datenklassen)
- Technische Beschreibung (z. B. Modelltyp, Trainingsdaten, Anbieter)
- Ergebnisse der rechtlichen und ethischen Vorprüfung
- Klassifizierung nach Risikokategorie (basierend auf EU-KI-VO)
- Schulungs- und Kontrollbedarf
- Letzter Prüfzeitpunkt, Status (aktiv/inaktiv/ausgephast)

## 9.3 Aktualisierungspflichten

- **Der Fachbereich** ist verantwortlich für die Pflege der Angaben im Inventar.
- **Mindestens jährlich** erfolgt ein Review durch das KI-Kern-Team.
- Bei **wesentlichen Änderungen** (z. B. neue Datenbasis, Änderung des Einsatzzwecks) ist eine neue Freigabe erforderlich.

Das KI-Inventar stellt sicher, dass [Unternehmensname] KI nicht nur innovativ, sondern auch nachvollziehbar und kontrolliert einsetzt. Es ist integraler Bestandteil der Governance-Struktur nach EU-KI-Verordnung und interner Compliance-Strategie.

## 10. Überprüfung & Aktualisierung der Richtlinie

Künstliche Intelligenz ist ein dynamisches Feld. Technologien entwickeln sich rasant, gesetzliche Rahmenbedingungen verändern sich, und neue Erkenntnisse aus der Praxis verlangen nach Anpassungen. Aus diesem Grund ist diese Richtlinie kein statisches Dokument, sondern wird **regelmäßig überprüft, weiterentwickelt und an neue Gegebenheiten angepasst**.

### 10.1 Regelmäßige Überprüfung

Die Richtlinie wird mindestens **einmal jährlich** durch das KI-Kern-Team inhaltlich und formal überprüft. Dabei werden insbesondere folgende Aspekte berücksichtigt:

- Änderungen in der nationalen und europäischen Gesetzgebung (z. B. KI-VO, DSGVO, Urheberrecht)
- Erkenntnisse aus internen Audits, Vorfallanalysen oder Compliance-Reviews
- Feedback aus den Fachbereichen oder von Mitarbeitenden
- Entwicklungen in der KI-Technologie und deren Anwendung im Unternehmen

Die Ergebnisse der Überprüfung werden dokumentiert und fließen in die nächste Version ein.

### 10.2 Anlassbezogene Anpassung

Unabhängig vom regelmäßigen Review kann eine sofortige Anpassung erforderlich werden, wenn:

- neue gesetzliche oder regulatorische Anforderungen in Kraft treten,
- ein sicherheits- oder datenschutzrelevanter Vorfall im Zusammenhang mit einem KI-System eintritt,
- strategische Neuausrichtungen im Umgang mit KI erfolgen,
- ein neuer Risikobereich erkannt wird (z. B. neue Hochrisiko-Kategorie nach EU-KI-VO).

In solchen Fällen koordiniert das KI-Kern-Team die kurzfristige Revision der relevanten Abschnitte in Abstimmung mit betroffenen Fachbereichen und der Geschäftsleitung.

### 10.3 Versionierung

Jede Änderung an der Richtlinie wird durch eine neue Versionsnummer und ein **Änderungsprotokoll** dokumentiert. Die aktuelle Version wird zentral zugänglich gemacht. Vorherige Versionen werden archiviert und stehen für Prüfzwecke zur Verfügung.

Version	Datum	Änderungen	Freigegeben durch	Nächste Überprüfung
1.0	[TT.MM.JJJJ]	Erstfassung	KI-Kern-Team	[TT.MM.JJJJ]

Die kontinuierliche Pflege dieser Richtlinie ist Ausdruck unseres Anspruchs, KI nicht nur technisch, sondern auch rechtlich, ethisch und organisatorisch **auf dem neuesten Stand** zu halten – als lernende Organisation mit Verantwortung.

## 11. Verknüpfte Richtlinien und mitgeltende Dokumente

Diese KI-Richtlinie steht **nicht isoliert**, sondern ist Teil des umfassenden Regelwerks von [Unternehmensname] für verantwortungsbewusstes, rechtssicheres und nachhaltiges Handeln. Sie ergänzt bestehende interne Richtlinien, Standards und Leitlinien – und verweist auf diese, wo sinnvoll.

## 11.1 Interne Richtlinien mit Relevanz für den KI-Einsatz

Folgende unternehmensinterne Dokumente gelten ergänzend zur KI-Richtlinie und sind im Zweifel vorrangig zu berücksichtigen:

- **Datenschutzrichtlinie**  
Regelt die Verarbeitung personenbezogener Daten gemäß DSGVO, inkl. Betroffenenrechte, Datenschutzfolgenabschätzungen und Löschkonzepte.
- **Informationssicherheitsrichtlinie**  
Definiert technische und organisatorische Schutzmaßnahmen für Daten, Systeme und Prozesse – inklusive Anforderungen an Systemhärtung und Zugriffskontrolle.
- **Richtlinie zur Klassifikation von Unternehmensdaten**  
Enthält Vorgaben zur Einordnung von Daten in Schutzklassen (z. B. „öffentlich“, „vertraulich“, „streng vertraulich“) und deren zulässige Verwendung, auch im Kontext von KI
- **Code of Conduct / Verhaltenskodex**  
Formuliert Grundprinzipien zu Integrität, Fairness, Diskriminierungsverbot und verantwortungsbewusstem Handeln – auch bei automatisierten Entscheidungen.
- **Richtlinie für IT-Systembeschaffung**  
Legt Prozesse und Kriterien für die Auswahl, Beschaffung und Freigabe neuer technischer Systeme fest, inkl. Einbindung des KI-Kern-Teams bei KI-Komponenten.
- **Richtlinie für Innovations- oder Digitalprojekte** (falls vorhanden)  
Regelt Pilotprojekte, Testphasen und Governance für neue Technologien – inkl. Berücksichtigung ethischer und regulatorischer Anforderungen.

## 11.2 Externe Bezugsnormen

Neben internen Regelungen orientiert sich diese Richtlinie u. a. an folgenden externen Standards:

- **EU-KI-Verordnung (AI Act)**
- **Datenschutz-Grundverordnung (DSGVO)**
- **ISO/IEC 27001 (Informationssicherheit)**
- **OECD-Prinzipien für vertrauenswürdige KI**
- **Ethik-Leitlinien der Europäischen Kommission zur vertrauenswürdigen KI**
- [Branchenrelevante Gesetze oder Leitlinien ergänzen]

## 11.3 Umgang mit Widersprüchen

Im Fall von Widersprüchen zwischen dieser Richtlinie und anderen Unternehmensregelwerken gilt:

- Die jeweils **strikttere Regelung** hat Vorrang.
- Bei Zweifeln oder Unklarheiten ist das **KI-Kern-Team** zu konsultieren.

Diese Querverbindungen stellen sicher, dass KI nicht als Sonderthema behandelt wird – sondern **integriert in unsere gesamte Governance-Struktur**.

## 12. Versionierung

Diese Richtlinie unterliegt einem dokumentierten Änderungs- und Freigabeprozess. Jede neue Version wird eindeutig gekennzeichnet und zentral archiviert. So stellen wir sicher, dass alle Mitarbeitenden jederzeit mit der **aktuellen und gültigen Version** arbeiten – und dass Änderungen transparent nachvollzogen werden können.

## 12.1 Änderungsdocumentation

Die folgende Tabelle dokumentiert alle bisherigen Versionen der Richtlinie für verantwortungsvollen KI-Einsatz bei [Unternehmensname]:

Versio n	Datum der Veröffentlichu ng	Art der Änderung	Geprüf t durch	Freigabe durch	Nächste geplante Überprüfun g
1.0	[TT.MM.JJJJ]	Erstfassung (Neuerstellun g)	KI- Kern- Team	Geschäftsführu ng	[TT.MM.JJJ J]

*Weitere Einträge folgen bei künftigen Anpassungen.*

## 12.2 Zuständigkeit

Für die Pflege, Freigabe und Kommunikation der jeweils aktuellen Version ist das **KI-Kern-Team** verantwortlich. Vorschläge zur Weiterentwicklung der Richtlinie können jederzeit formlos eingereicht werden – idealerweise mit kurzer Begründung oder Praxisbezug.

Durch die konsequente Versionierung und Verantwortungszuordnung bleibt diese Richtlinie **lebendig, nachvollziehbar und handhabbar** – auch über Jahre hinweg.

## Abschluss & Inkrafttreten

Diese Richtlinie für den verantwortungsvollen Einsatz von Künstlicher Intelligenz wurde durch das KI-Kern-Team in Abstimmung mit der Geschäftsleitung von [Unternehmensname] erstellt und freigegeben.

Sie tritt mit Wirkung zum **[Datum einsetzen]** in Kraft und gilt bis auf Weiteres. Bei wesentlichen Änderungen der rechtlichen Rahmenbedingungen, organisatorischen Strukturen oder technischen Einsatzszenarien wird eine zeitnahe Aktualisierung vorgenommen.

Alle Mitarbeitenden sind verpflichtet, die Inhalte dieser Richtlinie zu beachten und etwaige Fragen oder Unsicherheiten frühzeitig mit dem zuständigen Fachbereich oder dem KI-Kern-Team zu klären.

Die jeweils aktuelle Version ist im Intranet unter **[Pfad oder Link einfügen]** verfügbar.

## Freigabe und Unterzeichnung

### Verantwortlich für Inhalt & Pflege

[Vorname Name],  
Leitung KI-Kern-Team

### Freigabe durch

[Vorname Name],  
Geschäftsführung

### Beteiligung des Betriebsrats

[Vorname Name],  
Betriebsratsvorsitzende:r

[Ort], den [Datum]

Unterschrift: \_\_\_\_\_  
(Leitung KI-Kern-Team)

Unterschrift: \_\_\_\_\_  
(Geschäftsführung)

Unterschrift: \_\_\_\_\_  
(Betriebsrat)

## Rechtlicher Hinweis / Disclaimer

Diese Mustervorlage für eine Unternehmensrichtlinie zum verantwortungsvollen Einsatz von Künstlicher Intelligenz (KI) wurde auf Basis bewährter Praktiken, regulatorischer Anforderungen (insbesondere DSGVO und EU-KI-Verordnung) sowie ethischer Leitlinien erstellt. Sie dient ausschließlich zu **Orientierungs- und Diskussionszwecken** innerhalb von Unternehmen.

### Wichtiger Hinweis:

Diese Vorlage stellt **keine Rechtsberatung** dar. Sie ersetzt weder eine individuelle juristische Prüfung noch die Berücksichtigung der spezifischen Gegebenheiten Ihres Unternehmens – insbesondere in Bezug auf Branche, Betriebsgröße, eingesetzte Technologien, bestehende Richtlinien oder tarifliche/betriebsverfassungsrechtliche Rahmenbedingungen.

Die Nutzung dieser Vorlage erfolgt auf eigene Verantwortung. Für eine rechtsverbindliche Umsetzung, insbesondere bei der Gestaltung von Arbeitsprozessen, Datenschutzregelungen oder Pflichten aus dem AI Act, wird die **Einbindung qualifizierter Fachjurist:innen sowie ggf. des Betriebsrats** ausdrücklich empfohlen.

Durch die Verwendung dieser Vorlage erkennt das Unternehmen an, dass individuelle Anpassungen erforderlich sind und dass die Autoren keine Haftung für etwaige Folgen der Anwendung übernehmen.