KI IM UNTERNEHMEN NUTZEN: DIESE RECHTLICHEN RISIKEN SOLLTEST DU KENNEN



Veröffentlicht am 22. Mai 2026 von Thomas

Unternehmen nutzen KI heute für Content-Erstellung, Kundenservice, Marketingkampagnen, Datenanalysen, Recruiting oder interne Automatisierungen. Was vor wenigen Jahren noch experimentell wirkte, **gehört inzwischen in vielen Betrieben zum Alltag.** Genau darin liegt allerdings auch ein wachsendes Risiko: Während sich die Technologie rasant entwickelt, hinken viele Unternehmen bei rechtlichen Vorgaben, internen Prozessen und Sicherheitsstandards hinterher.

Besonders heikel ist, dass KI häufig spontan und ohne klare Regeln eingesetzt wird. Mitarbeiter kopieren vertrauliche Informationen in Chatbots, Marketingabteilungen veröffentlichen ungeprüfte KI-Texte, und Unternehmen verlassen sich auf automatisierte Inhalte, deren Herkunft oder Richtigkeit kaum nachvollziehbar ist. Gleichzeitig entstehen neue gesetzliche Anforderungen wie der EU AI Act, die Dich künftig stärker in die Verantwortung nehmen.

DIE 5 WICHTIGSTEN RISIKOFELDER BEI DER ARBEIT MIT KI

Wenn Du KI in Deinem Unternehmen einsetzen möchtest, solltest Du deshalb nicht nur die Chancen kennen, **sondern auch die rechtlichen Risiken verstehen**. Die fünf wichtigsten Risikofelder im Überblick:

Risikofeld	Was konkret passieren kann
Datenschutz	DSGVO-Verstöße durch Eingabe personenbezogener Daten in externe KI-Tools
Urheberrecht	Unklare Rechte an KI-Output; Verletzung fremder Werke durch Ähnlichkeit
Halluzinationen	Haftung für veröffentlichte Falschaussagen, erfundene Quellen, falsche Produktangaben
Diskriminierung	Benachteiligung von Bewerbergruppen durch verzerrte Trainingsdaten (AGG)
Regulatorik	Pflichten aus dem EU AI Act: Dokumentation, Transparenz, Schulung, Risikomanagement

WARUM KI PLÖTZLICH EIN COMPLIANCE-THEMA WIRD

Viele Unternehmen betrachten KI vor allem **als Produktivitätswerkzeug**. Texte entstehen schneller, Prozesse werden automatisiert, repetitive Aufgaben lassen sich effizienter bearbeiten. Genau dieser Geschwindigkeitsvorteil sorgt jedoch dafür, dass Risiken häufig übersehen werden.

Im Gegensatz zu klassischer Software erzeugt KI eigenständig Inhalte und Entscheidungen. Dabei kann sie Fehler machen, falsche Informationen liefern oder problematische Inhalte produzieren, ohne dass dies auf den ersten Blick erkennbar ist. Kritisch wird es vor allem dann, wenn Du diese Ergebnisse ungeprüft übernimmst und veröffentlichst.

Hinzu kommt, dass viele KI-Systeme mit großen Datenmengen arbeiten. Werden dabei personenbezogene Informationen, interne Dokumente oder vertrauliche Kundendaten verarbeitet, entstehen schnell Datenschutz- und Haftungsprobleme. Für Dich bedeutet das: KI ist längst nicht mehr nur ein technisches Thema, sondern zunehmend **eine Frage von Compliance, Risikomanagement und Unternehmensverantwortung.**

DATENSCHUTZ: DAS GRÖSSTE EINFALLSTOR

In der Praxis entstehen die meisten Probleme aktuell beim Umgang mit sensiblen Daten. Viele Mitarbeiter nutzen KI-Tools ähnlich wie eine Suchmaschine und geben Informationen ein, ohne über die Folgen nachzudenken. Genau das kann schnell teuer werden.

Folgende Eingaben sollten in öffentlichen KI-Tools wie ChatGPT, Gemini oder Claude grundsätzlich nicht erfolgen, sofern kein abgesicherter Enterprise-Zugang mit klaren Datenschutzgarantien

besteht:

- Kundendaten (Namen, Kontaktdaten, Auftragshistorie)
- Bewerberunterlagen und Lebensläufe
- Verträge, Angebote und interne Preiskalkulationen
- Mitarbeiter- und Gesundheitsdaten
- Zugangsdaten, API-Keys, Passwörter
- Interne Strategie- und Finanzdokumente

Je nach Plattform können eingegebene Inhalte gespeichert, analysiert oder zur Verbesserung der Modelle genutzt werden. Im Hinblick auf die DSGVO ist das relevant, weil personenbezogene Daten nur unter klar definierten Voraussetzungen verarbeitet werden dürfen. **Fehlen interne Richtlinien oder technische Schutzmaßnahmen, entstehen rechtliche Risiken** – bis hin zu Bußgeldern und Meldepflichten an die Aufsichtsbehörde.

Unterschätzt wird zudem, wie unkontrolliert die KI-Nutzung intern bereits stattfindet. Häufig existieren weder Freigabeprozesse noch Vorgaben dazu, welche Tools überhaupt genutzt werden dürfen. Daraus entsteht der sogenannte „Shadow AI"-Effekt: Mitarbeiter arbeiten eigenständig mit KI-Anwendungen, ohne dass die Geschäftsführung weiß, welche Daten dort verarbeitet werden.

KI-GENERIERTE INHALTE UND DAS PROBLEM MIT DEM URHEBERRECHT

Ein weiteres großes Risiko betrifft das Urheberrecht. Viele Unternehmen gehen davon aus, dass KI-generierte Texte, Bilder oder Designs automatisch ihnen gehören. So einfach ist die Rechtslage nicht.

In Deutschland gilt: Urheberrechtlich geschützt sind nach § 2 UrhG **nur persönliche geistige Schöpfungen** – also Werke mit menschlicher Schöpfungshöhe. Rein KI-generierte Inhalte ohne nennenswerten menschlichen Gestaltungsanteil fallen daher nicht unter den klassischen Urheberrechtsschutz. Entscheidend ist, wie groß der eigene kreative Anteil tatsächlich war. Für

Marketingabteilungen, Agenturen und Content-Produzenten ist das durchaus relevant – fremde Dritte können rein KI-erzeugte Inhalte grundsätzlich frei weiterverwenden.

Gleichzeitig besteht das umgekehrte Risiko: KI kann bestehende Werke unbeabsichtigt kopieren oder imitieren. Besonders bei Bildern, Designs, Logos oder kreativen Kampagnen können Ähnlichkeiten zu bestehenden Werken entstehen. Damit läufst Du Gefahr, Urheber- oder Markenrechte Dritter zu verletzen – mit Abmahn- und Schadensersatzfolge.

Hinzu kommt ein praktisches Problem: KI-Systeme erzeugen Inhalte auf Basis riesiger Trainingsdatenmengen. Die Herkunft einzelner Stilrichtungen, Formulierungen oder visueller Elemente **lässt sich kaum nachvollziehen**. Wer KI-Output ungeprüft veröffentlicht, bewegt sich deshalb in einer **rechtlichen Grauzone.**

DAS UNTERSCHÄTZTE RISIKO VON HALLUZINATIONEN

Eines der größten Probleme moderner KI-Systeme ist ihre Fähigkeit, überzeugend falsche Informationen zu erzeugen. Diese sogenannten Halluzinationen wirken oft glaubwürdig und professionell formuliert – **obwohl die Inhalte sachlich falsch sind.**

Gerade im Marketing- oder Content-Bereich entsteht dadurch ein erhebliches Risiko. KI kann falsche Produktangaben generieren, Studien erfinden, Quellen falsch darstellen oder technische Aussagen formulieren, die schlicht nicht stimmen. Für Außenstehende ist häufig nicht erkennbar, dass die Inhalte von einer KI stammen – **verantwortlich bist trotzdem Du**.

Werden falsche Leistungsversprechen kommuniziert oder irreführende Informationen verbreitet, drohen wettbewerbsrechtliche Abmahnungen, Schadensersatzansprüche und Reputationsschäden. In sensiblen Bereichen wie Medizin, Finanzen, Recht oder Gesundheit kann das existenzbedrohend werden.

Es reicht deshalb nicht aus, KI-Texte oberflächlich zu überfliegen. Du brauchst **klare Qualitätskontrollen** und eine **verbindliche menschliche Freigabe**, bevor Inhalte das Haus verlassen.

RECRUITING UND AUTOMATISIERTE

ENTSCHEIDUNGEN BERGEN NEUE GEFAHREN

Auch im Recruiting setzen immer mehr Unternehmen auf KI. Bewerbungen werden automatisiert analysiert, Lebensläufe vorsortiert, Kandidaten anhand bestimmter Kriterien bewertet. Genau hier entstehen erhebliche Diskriminierungsrisiken.

KI-Systeme lernen aus bestehenden Daten. Sind diese Daten verzerrt oder enthalten sie unbewusste Vorurteile, **übernimmt die KI diese Muster**. Bestimmte Personengruppen werden dadurch benachteiligt, ohne dass dies unmittelbar auffällt. Das kollidiert direkt mit dem Allgemeinen Gleichbehandlungsgesetz (AGG).

Für Dein Unternehmen kann das **schwerwiegende Folgen haben**: Diskriminierungsvorwürfe, Imageschäden, rechtliche Auseinandersetzungen, Entschädigungsansprüche abgelehnter Bewerber. Besonders kritisch wird es, wenn Entscheidungen vollständig automatisiert getroffen werden und keine menschliche Kontrolle mehr stattfindet. Genau deshalb stuft der EU AI Act KI-gestützte HR-Systeme als Hochrisiko-Anwendungen ein.



DER EU AI ACT VERÄNDERT DIE SPIELREGELN

Mit dem EU AI Act existiert **erstmals ein umfassender Rechtsrahmen für künstliche Intelligenz in Europa**. Die Verordnung ist am 1. August 2024 in Kraft getreten und gilt schrittweise. Viele Unternehmen unterschätzen aktuell noch, welche Auswirkungen das in den nächsten Monaten konkret hat.

Der AI Act verfolgt einen risikobasierten Ansatz: Je größer das potenzielle Risiko eines KI-Systems, desto strenger sind die Anforderungen. Vier Risikoklassen sind vorgesehen:

Risikoklasse	Beispiele	Folgen für Dich
Inakzeptabel	Social Scoring, manipulative Systeme, Emotionserkennung am Arbeitsplatz	Verboten seit Februar 2025
Hochrisiko	Recruiting-KI, Kreditscoring, biometrische Identifikation, kritische Infrastruktur	Strenge Pflichten: Risikomanagement, Dokumentation, menschliche Aufsicht
Begrenztes Risiko	Chatbots, Deepfakes, KI-generierte Inhalte	Transparenzpflicht: Nutzer muss erkennen können, dass KI im Spiel ist
Minimales Risiko	Spam-Filter, KI in Videospielen	Keine besonderen Pflichten

Die Pflichten gelten gestaffelt. Wichtig für die Planung:

- Seit Februar 2025: Verbot bestimmter KI-Praktiken; verpflichtende KI-Kompetenz (AI Literacy) für Mitarbeitende, die KI einsetzen
- Seit August 2025: Pflichten für Anbieter von General-Purpose-AI-Modellen (etwa GPT, Claude, Gemini)
- Ab August 2026: Die meisten Pflichten für Hochrisiko-Systeme und allgemeine Anwender werden vollständig wirksam
- Ab August 2027: Übergangsfristen für eingebettete Hochrisiko-KI in regulierten Produkten enden

Wichtig: Die AI-Literacy-Pflicht (Art. 4 AI Act) **gilt bereits jetzt und betrifft praktisch jedes Unternehmen, das KI einsetzt**. Wer Mitarbeitende nicht nachweisbar zum verantwortungsvollen KI-

Umgang schult, verstößt schon heute gegen die Verordnung.

WARUM DU JETZT KLARE KI-REGELN BRAUCHST

Die größte Gefahr liegt aktuell oft weniger in der Technologie selbst, sondern in der fehlenden Governance innerhalb der Unternehmen. Viele Betriebe erlauben KI-Nutzung indirekt, ohne klare Prozesse oder Verantwortlichkeiten geschaffen zu haben. Daraus entsteht eine Reihe ungeklärter Fragen:

- Wer darf welche Tools nutzen?
- Welche Daten dürfen eingegeben werden, welche nicht?
- Wie werden KI-Inhalte vor Veröffentlichung geprüft?
- Wer trägt die Verantwortung bei Fehlern oder Verstoßen?
- Wie wird KI-Nutzung dokumentiert?

Eine wirksame KI-Richtlinie deckt mindestens die folgenden Bereiche ab:

- **Tool-Freigabe:** Liste der zugelassenen KI-Tools und der jeweiligen Einsatzbereiche
- **Datenklassen:** klare Regeln, welche Datentypen in welchen Tools verarbeitet werden dürfen
- **Freigabeprozess:** verbindliche menschliche Prüfung vor Veröffentlichung von KI-Inhalten
- **Schulung:** dokumentierte AI-Literacy-Trainings für alle Mitarbeitenden mit KI-Zugriff
- **Kennzeichnung:** Transparenzregeln für KI-generierte externe Kommunikation
- **Vorfallmanagement:** Meldewege und Verantwortlichkeiten bei Datenschutz- oder Compliance-Vorfällen

Entscheidend ist die Erkenntnis: KI ersetzt keine menschliche Verantwortung. Du bleibst für veröffentlichte Inhalte, Entscheidungen und Datenverarbeitung verantwortlich – unabhängig davon,

ob diese von Menschen oder Maschinen erzeugt wurden.

FAZIT: KI BIETET ENORMES POTENZIAL, ABER KEINE RECHTLICHE ABKÜRZUNG

Künstliche Intelligenz wird die Arbeitswelt nachhaltig verändern. Du kannst Prozesse beschleunigen, Kosten reduzieren und neue Möglichkeiten schaffen. Gleichzeitig entstehen rechtliche Herausforderungen, die viele Unternehmen aktuell noch unterschätzen.

Datenschutz, Urheberrecht, Haftung, Diskriminierung und regulatorische Vorgaben werden in den nächsten Jahren massiv an Bedeutung gewinnen. Der gefährlichste Pfad ist die unkontrollierte Nutzung ohne Regeln oder Verantwortlichkeiten.

Wenn Du KI langfristig erfolgreich einsetzen willst, brauchst Du mehr als gute Tools. Entscheidend sind klare Prozesse, geschulte Mitarbeiter, technische Sicherheitsmaßnahmen und ein verantwortungsvoller Umgang mit der Technologie.

Denn KI kann vieles beschleunigen – auch rechtliche Probleme.

Webweisend unterstützt Unternehmen dabei, KI-Prozesse strukturiert und praxisnah in das Marketing zu integrieren. Wir setzen bewusst auf menschliche Kontrolle, klare Qualitätsstandards und einen verantwortungsvollen Umgang mit sensiblen Daten und Inhalten.

Denn gute Ergebnisse entstehen nicht durch unkontrollierte Automatisierung, sondern durch die sinnvolle Verbindung aus Technologie, Fachwissen und Erfahrung.