## EU AI Act für Unternehmen

# Umfassender Leitfaden zur KI-Regulierung am Arbeitsplatz

Ein detaillierter Überblick über die europäische KI-Verordnung und ihre praktische Umsetzung in Unternehmen – von den rechtlichen Grundlagen bis zur operativen Implementierung

Kapitel 1

# Warum wird KI reguliert?

Die digitale Transformation hat KI von einer Spezialtechnologie zu einem integralen Bestandteil der Wertschöpfungskette gemacht. Diese Entwicklung bringt sowohl enorme Chancen als auch erhebliche Risiken mit sich, die eine umfassende Regulierung erforderlich machen.

### Digitale Transformation

KI durchdringt alle Unternehmensbereiche

### Chancen & Risiken

Balance zwischen Innovation und Schutz

### Rechtlicher Rahmen

Harmonisierte EU-weite Standards

# KI in der Unternehmenspraxis

## Rolle von KI in Vertrieb, Verwaltung, Produktion und Service

Die Studien betonen, dass KI nicht mehr als Spezialtechnologie in isolierten Forschungsabteilungen auftritt, sondern quer durch die Wertschöpfungskette eingesetzt wird – gerade in typischen Unternehmensfunktionen wie Vertrieb, Verwaltung, Produktion und Service.

In der **Verwaltung** reicht die Spannweite von einfachen Dokumenten-Workflows über Chatbots im Kundenservice bis hin zu komplexen Entscheidungsunterstützungssystemen, etwa bei der Bewilligung von Leistungen oder der Risikobewertung von Geschäftsvorgängen.

Im **Vertrieb** werden KI-Systeme zur Profilbildung, personalisierten Werbung, dynamischen Preisgestaltung und automatisierten Kreditwürdigkeitsprüfungen eingesetzt, wodurch sehr detaillierte, teilweise hochsensible Profile von Kunden und potenziellen Kundengruppen entstehen.

In der **Produktion** dominieren intelligente, vernetzte Systeme, die auf umfangreichen Sensordaten und Machine-Learning-Modellen basieren, um Wartung zu optimieren, Qualitätsmängel frühzeitig zu erkennen und Abläufe zu automatisieren. Gerade dort entsteht ein enger Nexus zu Arbeitsschutz und funktionaler Sicherheit, weil falsch arbeitende Modelle unmittelbar physische Schäden und Gefährdungen von Beschäftigten verursachen können.

Im **Service-Umfeld** – etwa im technischen Support, im Gesundheitsbereich oder in der Finanzberatung – verschieben KI-gestützte Systeme zunehmend Aufgaben von Menschen auf algorithmische Agenten, die Anfragen vorstrukturieren, Entscheidungen vorbereiten oder sogar vollautomatisch treffen.

# Neue Rollen am Arbeitsplatz

Für den Arbeitsplatz bedeutet das: Beschäftigte interagieren mit KI-Systemen als Nutzer (z.B. in HR-Software), als Gegenstand von KI-Bewertungen (z.B. Performance-Scoring), oder als Verantwortliche für Überwachung, Eingriff und Dokumentation dieser Systeme.

Insbesondere in HR, Compliance und Fachabteilungen entstehen neue Rollenprofile, die technische, rechtliche und organisatorische Kompetenzen verbinden. Diese Entwicklung erfordert eine grundlegende Neuausrichtung der Qualifikationsprofile und Verantwortlichkeiten in Unternehmen.

Die Integration von KI-Systemen schafft komplexe Interaktionsmuster zwischen Mensch und Maschine, die sorgfältig gestaltet und überwacht werden müssen, um sowohl Effizienz als auch Grundrechtsschutz zu gewährleisten.

# Typische Risiken von KI-Systemen

Die Literatur zeigt, dass KI-Anwendungen gerade in arbeitsplatznahen Kontexten typische Risiken bündeln: Diskriminierung, Intransparenz, Sicherheitsrisiken und systematische Grundrechtsbeeinträchtigungen.

## Diskriminierung

KI-gestützte Systeme in Personalgewinnung, Beförderungsentscheidungen, Schichtplanung oder Leistungsbewertung können bestehende Vorurteile und gesellschaftliche Ungleichheiten verstärken, wenn Trainingsdaten verzerrt sind oder geschützte Merkmale indirekt abgebildet werden. Dies betrifft insbesondere Geschlecht, ethnische Herkunft, Alter, Behinderung, soziale Herkunft und andere Merkmale, die im Arbeitsleben ohnehin sensibel sind.

Im Bereich Kreditvergabe, Versicherungen und Scoring-Systeme kann diskriminierende Behandlung Beschäftigte mittelbar treffen, etwa wenn arbeitgebernahe Daten in Scoring-Verfahren einfließen oder wenn Beschäftigtengruppen systematisch benachteiligt werden.

## Intransparenz

KI-Systeme sind häufig hochkomplex und für Endanwender, Betriebsräte oder Betroffene kaum nachvollziehbar. Black-Box-Modelle erschweren es Beschäftigten, Entscheidungen nachzuvollziehen oder anzufechten, etwa wenn ein algorithmisches System für Dienstplanoptimierung bestimmte Mitarbeitende systematisch mit ungünstigen Schichten belegt.

Diese Intransparenz kollidiert mit arbeitsrechtlichen Transparenz- und Begründungspflichten sowie mit dem Anspruch auf faire Verfahren. Die fehlende Nachvollziehbarkeit untergräbt das Vertrauen in automatisierte Entscheidungsprozesse.

# Weitere kritische Risikobereiche

## Sicherheitsrisiken

Vernetzte, autonome Systeme in Produktion, Logistik und kritischer Infrastruktur können bei Fehlfunktionen physische Schäden anrichten, etwa durch fehlerhafte Maschinensignale, falsch interpretierte Sensordaten oder gehackte Steuerungssysteme.

Auch im Bürobereich existieren Sicherheitsrisiken, etwa wenn KI-basierte Entscheidungsunterstützung im Gesundheitswesen oder in der Verkehrssteuerung falsche Empfehlungen gibt und Personal diese ungeprüft übernimmt. Zusätzlich verschärfen Vernetzung und Autonomie Cyberrisiken und Angriffsflächen.

## Grundrechtsbeeinträchtigungen

Die Studien machen deutlich, dass KI-Anwendungen in Arbeitskontexten eine Vielzahl von Grundrechten berühren, darunter Datenschutz, Privatsphäre, Gleichbehandlung, Meinungs- und Versammlungsfreiheit, aber auch das Recht auf gute Verwaltung und fairen Zugang zu Leistungen.

So können etwa umfassende Überwachungssysteme im Betrieb (Video, Wearables, Performance-Tracking) das Recht auf Privatleben und kollektive Betätigung der Beschäftigten einschränken, während algorithmische Bewertungssysteme für Sozialleistungen oder arbeitsmarktpolitische Maßnahmen den Zugang zu Unterstützungsleistungen beeinflussen.

# Politische und wirtschaftliche Gründe für Regulierung

**Politisch** verfolgt die EU mit der KI-Regulierung das Ziel, eine Balance zwischen technologischer Innovation und dem Schutz von Grundrechten, Demokratie und sozialer Gerechtigkeit zu wahren.

Die KI-Verordnung fügt sich in eine breitere digitale Strategie ein (u.a. DSGVO, DSA, DMA) und soll verhindern, dass KI-Entscheidungen rechtliche Lücken ausnutzen, die zu systematischer Diskriminierung, willkürlichen Eingriffen und einer Erosion demokratischer Prozesse führen. Für das Arbeitsleben bedeutet dies, dass etwa KI-gestützte Überwachung, algorithmische Lohnfindung oder automatische Leistungsbewertung nicht in einem rechtsfreien Raum stattfinden dürfen, sondern klaren Regeln und Aufsicht unterliegen sollen.

**Wirtschaftlich** zielt die Regulierung darauf, Vertrauen in KI-Systeme zu schaffen, einheitliche Marktbedingungen im EU-Binnenmarkt zu etablieren und Fragmentierung durch divergierende nationale Ansätze zu verhindern. Statt eines Flickenteppichs aus Einzelregulierungen sollen Unternehmen – inklusive KMU – klare, vorhersehbare Rahmenbedingungen erhalten, die Investitionen in „vertrauenswürdige KI" erleichtern.

Zugleich wird anerkannt, dass KI-Regulierung Kosten verursacht; Impact-Studien zeigen jedoch, dass klare Regeln die Rechtssicherheit erhöhen und langfristig Innovation eher fördern als behindern können, insbesondere wenn Standards und „Safe-Harbour"-Mechanismen gut ausgestaltet sind.

# Der europäische Rechtsrahmen

## Zusammenspiel von AI Act, DSGVO, Digital Services Act und anderen Regelungen

Der europäische Rechtsrahmen für KI am Arbeitsplatz ist kein Monolith, sondern ein Geflecht aus horizontalen Digitalgesetzen und sektorspezifischen Regelungen. Der AI Act adressiert primär die Sicherheit, Qualität und Governance von KI-Systemen als Produkten bzw. Systemen, während die DSGVO die Verarbeitung personenbezogener Daten regelt und der Digital Services Act (DSA) Pflichten von Plattformen und Vermittlungsdiensten, insbesondere im Hinblick auf systemische Risiken und Inhalte, festlegt.

In arbeitsbezogenen Kontexten überschneiden sich diese Regime: Wenn ein Unternehmen etwa eine Plattform nutzt, die KI einsetzt, um Bewerbungen zu filtern, oder einen großen Online-Dienst (VLOP/VLOSE) mit generativen KI-Funktionen integriert, greifen sowohl die KI-spezifischen Anforderungen (z.B. Risikomanagement, Transparenz) als auch die datenschutzrechtlichen Pflichten (Rechtsgrundlage, Zweckbindung, Betroffenenrechte) und ggf. DSA-Pflichten zur Risikobewertung bei systemischen Auswirkungen (z.B. Diskriminierung, Desinformation).

Hinzu kommt sektorales Recht, etwa Finanzmarktrecht, Medizinprodukte-, Verkehrs- oder Arbeitsschutzregelungen, die zusätzliche Anforderungen an KI-gestützte Systeme stellen.

# Abgrenzung zwischen Rechtsakten

Der AI Act bezieht sich bewusst auf bestehende Rahmen, ohne diese zu verdrängen; er „tritt zurück", wo z.B. DSGVO oder sektorale Sicherheitsnormen spezieller sind, betont aber zugleich, dass Unternehmen beide Regime erfüllen müssen. Für Arbeitgeber bedeutet das: Ein KI-System in HR oder Compliance muss sowohl die materiellen Vorgaben der KI-Verordnung (z.B. Datenqualität, Dokumentation, menschliche Aufsicht) als auch die Datenschutzanforderungen (z.B. Informationspflichten, Datenschutz-Folgenabschätzung) erfüllen; eine alleinige DSGVO-Compliance genügt nicht.

### Horizontaler Ansatz

AI Act als Querschnittsregel für alle KI-Systeme im Binnenmarkt

### Lex Specialis

Sektorale Normen gehen als speziellere Regel vor

### Verantwortungsrollen

Provider vs. Controller – unterschiedliche Zuständigkeiten

Im Datenschutzrecht ist die Verteilung der Verantwortlichkeiten unterschiedlich: Während der AI Act primär den „Provider" eines Systems adressiert, liegt die Verantwortung für Datenverarbeitung (Controller) nach DSGVO meist beim Betreiber/Anwender – etwa dem Arbeitgeber, der ein KI-HR-System nutzt. Dieses Auseinanderfallen der Verantwortungsrollen erzeugt Schnittstellen- und Haftungsfragen, die durch abgestimmte Leitlinien, Standardisierung und teils gesetzliche Klarstellungen (z.B. Ausnahmen für Bias-Messung in Art. 10 Abs. 5 AI Act) entschärft werden sollen.

# Ziele des EU AI Act

## Schutz von Gesundheit, Sicherheit und Grundrechten

Zentrales Ziel des AI Act ist der Schutz von Gesundheit, Sicherheit und Grundrechten, insbesondere vor systemischen Risiken durch KI. Die Verordnung reagiert auf empirische Evidenz, dass KI-gestützte Entscheidungen in Bereichen wie Beschäftigung, Bildung, Kreditvergabe, Sozialleistungen oder Gesundheitsversorgung erhebliche Auswirkungen auf die Lebensverhältnisse von Menschen haben können und dabei häufig verzerrt, intransparent oder schwer angreifbar sind.

Für den Arbeitsplatz bedeutet das, dass etwa automatisierte HR-Systeme, KI-gestützte Leistungsbewertungen oder KI-basierte Sicherheitsfunktionen strengen Anforderungen unterliegen, wenn sie das Risiko bergen, Beschäftigte zu diskriminieren, ihre Sicherheit zu gefährden oder ihre Grundrechte zu beeinträchtigen.

## Gewährleistung eines funktionierenden Binnenmarktes

Der AI Act soll zugleich einen funktionierenden Binnenmarkt für KI-Produkte sichern, indem er harmonisierte Regeln und Konformitätsmechanismen schafft, die grenzüberschreitenden Einsatz erleichtern.

Unternehmen, die KI-Systeme in mehreren EU-Staaten einsetzen wollen – etwa standardisierte HR-Tools, Assistenzsysteme in der Produktion oder Risikomanagementlösungen im Finanzbereich – sollen nicht mit unterschiedlichen nationalen Zulassungen und Anforderungen konfrontiert sein, sondern auf ein einheitliches CE-Kennzeichnungs- und Marktüberwachungssystem zurückgreifen.

Dies soll auch den Wettbewerb fairer gestalten, indem unregulierte Anbieter mit niedrigen Standards keinen Kostenvorteil gegenüber regelkonformen Unternehmen erhalten.

# Förderung von Innovation durch klare Regeln

Die Regulierung wird explizit als Innovationspolitik verstanden: klare und vorhersehbare Regeln sollen Investitionen in „vertrauenswürdige KI" stimulieren und insbesondere für KMU Hürden senken, da diese sich auf Standards, Leitlinien und Codes of Practice stützen können.

Der AI Act sieht vor, dass technische Normen als „Safe Harbour" dienen können – wer diese einhält, kann vermuten, die gesetzlichen Anforderungen zu erfüllen. In Verbindung mit Koordinationsmechanismen (AI Office, nationale Aufsichtsbehörden, Standardisierungsorganisationen) soll sich eine lernende Regulierung entwickeln, die auf neue Risiken und technologische Entwicklungen reagiert, ohne Innovation unnötig zu bremsen.

Diese Balance zwischen Schutz und Innovation ist entscheidend für die Wettbewerbsfähigkeit europäischer Unternehmen im globalen Kontext und schafft Anreize für die Entwicklung ethischer, vertrauenswürdiger KI-Lösungen.

Kapitel 2

# Aufbau und Systematik des EU AI Act

# Anwendungsbereich und zentrale Begriffe

Der AI Act definiert KI bewusst breit, um nicht nur „moderne" Deep-Learning-Modelle, sondern auch klassische Verfahren wie statistische Modelle, regelbasierte Systeme und maschinelles Lernen im Allgemeinen zu erfassen. Annex I umfasst maschinelles Lernen, logik- und wissensbasierte Ansätze sowie statistische Methoden, die zu Outputs wie Vorhersagen, Empfehlungen oder Entscheidungen führen, die ihre Umgebung beeinflussen.

Für Unternehmen bedeutet das, dass auch lang etablierte Score- oder Entscheidungsmodelle, die in HR, Compliance oder Kreditvergabe eingesetzt werden, als KI gelten können, sofern sie algorithmisch Ergebnisse generieren, die Entscheidungen beeinflussen.

Der Anwendungsbereich ist extraterritorial: Erfasst sind nicht nur Akteure mit Sitz in der EU, sondern auch Anbieter außerhalb, deren Systeme im EU-Binnenmarkt bereitgestellt werden oder deren Outputs in der EU genutzt werden. Für global tätige Unternehmen in Deutschland – etwa mit zentral entwickelten HR- oder Risikomodellen – bedeutet dies, dass die EU-Regeln faktisch als Referenzrahmen für weltweit einheitliche Lösungen dienen können.

# Rollen in der Wertschöpfungskette

Die Systematik lehnt sich an das europäische Produktsicherheitsrecht an und unterscheidet mehrere Rollen:

## Anbieter (Provider)

Natürliche oder juristische Personen, die ein KI-System entwickeln oder in eigenem Namen oder unter eigener Marke in Verkehr bringen oder in Betrieb nehmen. Für interne Eigenentwicklungen kann ein Unternehmen selbst zum Anbieter werden, auch wenn das System nicht als Produkt verkauft wird.

## Nutzer (Deployer/User)

Natürliche oder juristische Personen, die ein KI-System unter eigener Verantwortung nutzen. Im Arbeitskontext ist der Arbeitgeber typischerweise Nutzer von HR-Systemen, Entscheidungsunterstützung oder Produktions-KI. Anders als im DSGVO-Sprachgebrauch bezeichnet „user" hier nicht den Endnutzer oder Betroffenen, sondern die Organisation, die KI einsetzt.

## Importeure und Distributoren

Unternehmen, die KI-Systeme aus Drittstaaten in den EU-Markt bringen oder innerhalb des Binnenmarkts vertreiben; sie haben Pflichten zur Überprüfung von Konformität und Kennzeichnung, ähnlich wie bei anderen CE-pflichtigen Produkten.

Diese Rollen sind entscheidend für die Verteilung von Pflichten: Während Anbieter die Hauptverantwortung für Design, Konformitätsbewertung und CE-Kennzeichnung tragen, müssen Nutzer sicherstellen, dass Systeme entsprechend der vorgesehenen Verwendung, im Rahmen der rechtlichen Vorgaben und unter angemessener menschlicher Aufsicht betrieben werden.

# Besonderheiten bei Forschung, Open Source und nicht-professioneller Nutzung

Die Quellen betonen Besonderheiten bei Forschung, Open-Source-Systemen und nicht-professionellen Anwendungen, die für die praktische Anwendung des AI Act von erheblicher Bedeutung sind.

## Forschung und Prototyping

Reine Forschung und Prototyping-Phasen ohne Inverkehrbringen oder betriebliche Nutzung sind teilweise von Anforderungen ausgenommen bzw. unterliegen erleichterten Pflichten, solange die Systeme nicht in realen Entscheidungsprozessen eingesetzt werden.

Dies ermöglicht Unternehmen und Forschungseinrichtungen, innovative Ansätze zu erproben, ohne sofort die volle Regulierungslast tragen zu müssen. Allerdings endet diese Ausnahme, sobald Systeme in den produktiven Betrieb überführt werden.

## Open Source und nicht-professionelle Nutzung

Open-Source-Komponenten und allgemein zugängliche Modelle werden nur dann in die volle Regulierung einbezogen, wenn sie als „General Purpose AI" oder im Rahmen eines konkreten Hochrisiko-Anwendungsfalls bereitgestellt werden; andernfalls gelten primär Transparenz- und Informationspflichten.

Nicht-professionelle Nutzung – etwa private Experimente mit KI-Tools – fällt weitgehend aus dem Anwendungsbereich; maßgeblich ist der Einsatz im beruflichen oder kommerziellen Umfeld. Das bedeutet zugleich, dass Unternehmen sich nicht auf Open-Source-Charakter oder private Herkunft eines Modells berufen können, um Pflichten zu umgehen, wenn sie es im Geschäftsbereich einsetzen.

# Der risikobasierte Ansatz

## Vier Risikoklassen im Überblick

Der AI Act strukturiert KI-Systeme nach ihrem Risikopotenzial in vier Kategorien, die jeweils unterschiedliche regulatorische Anforderungen nach sich ziehen. Dieser risikobasierte Ansatz ermöglicht eine proportionale Regulierung, die Hochrisikobereiche streng kontrolliert, während Niedrigrisikoanwendungen mehr Flexibilität erhalten.

01

### Verbotene KI-Praktiken

Unacceptable Risk – Systeme, die grundlegende EU-Werte verletzen

02

### Hochrisiko-Systeme

High Risk – Umfassende Regulierung mit Konformitätsbewertung

03

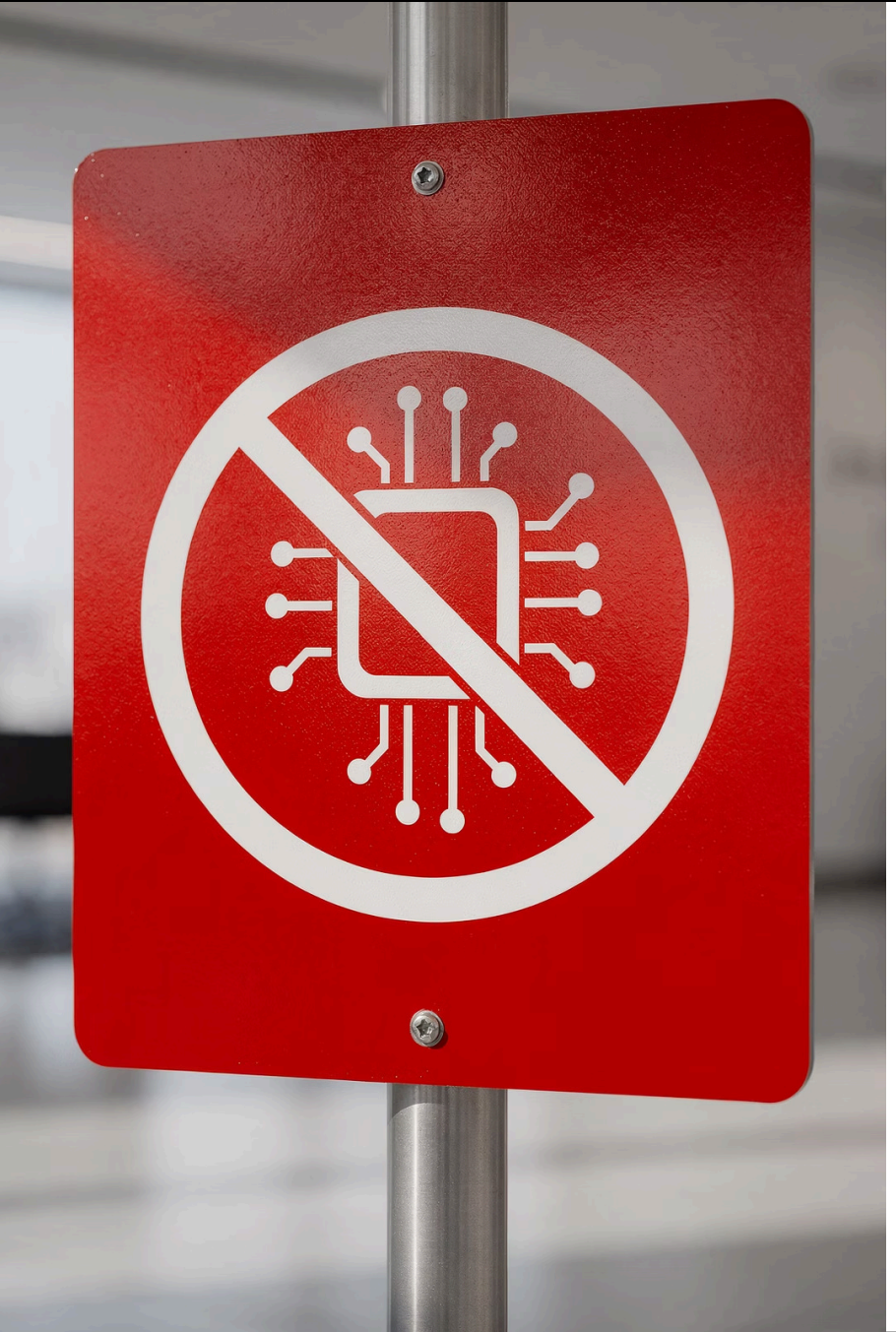
### Systeme mit begrenztem Risiko

Limited Risk – Primär Transparenzpflichten

04

### Niedrigrisiko-Systeme

Minimal Risk – Freiwillige Codes of Conduct



# Verbotene KI-Praktiken

## Unacceptable Risk

Der AI Act enthält einige „rote Linien", also Praktiken, die als mit EU-Werten unvereinbar gelten und grundsätzlich verboten sind. Dazu gehören u.a. manipulative Systeme, die Vulnerabilitäten bestimmter Personengruppen ausnutzen, bestimmte Formen von Social Scoring durch öffentliche Stellen und der Einsatz biometrischer Echtzeit-Identifikationssysteme im öffentlichen Raum für Strafverfolgungszwecke mit eng begrenzten Ausnahmen.

Im engeren Arbeitsumfeld sind vor allem Szenarien relevant, in denen Beschäftigte durch KI-basierte Überwachungs- oder Bewertungssysteme so stark gesteuert oder manipuliert werden, dass ihre Autonomie und Würde ernsthaft beeinträchtigt werden – etwa durch permanente emotionale Überwachung oder verdeckte Verhaltensbeeinflussung.

Diese Verbote sind absolut und gelten unabhängig von möglichen Vorteilen oder Rechtfertigungen. Unternehmen müssen sicherstellen, dass ihre KI-Systeme nicht in diese Kategorien fallen, da Verstöße mit den höchsten Sanktionen belegt werden können.

# Hochrisiko-Systeme

## High-Risk AI im Detail

Hochrisiko-KI steht im Zentrum der Regulierung. Zwei Kategorien sind relevant:

**Erstens:** KI als Sicherheitskomponente eines bereits regulierten Produkts (z.B. Maschinen, Medizinprodukte, Fahrzeuge), die im Rahmen bestehender Harmonisierungsrechtsakte bereits Konformitätsbewertungspflichten haben.

**Zweitens:** In Annex III explizit aufgeführte Anwendungen mit erheblichem Risiko für Grundrechte und Sicherheit, u.a.:

- Bildung und berufliche Ausbildung (Zugang, Bewertung)
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (z.B. automatisierte Auswahl, Beförderung, Überwachung)
- Zugang zu wesentlichen privaten und öffentlichen Dienstleistungen, einschließlich Krediten und Sozialleistungen
- Strafverfolgung und Rechtspflege
- Migration, Asyl und Grenzkontrolle
- Kritische Infrastruktur

Insbesondere HR-Systeme zur Bewerbervorauswahl, Scoring von Mitarbeitenden, algorithmische Dienstplanung oder automatisierte Performance-Bewertung können in die Hochrisikokategorie fallen, wenn sie entscheidend über Zugang zu Beschäftigung oder Karriere bestimmen.

# Systeme mit begrenztem und minimalem Risiko

## Limited Risk

Systeme mit begrenztem Risiko unterliegen primär Transparenzpflichten. Dazu zählen beispielsweise Chatbots, emotionserkennende Systeme oder Deepfake-Generatoren, sofern sie nicht in Hochrisiko-Kontexte eingebettet sind.

Im Arbeitsalltag bedeutet das etwa, dass Mitarbeitende und Kunden klar erkennen müssen, wenn sie mit einem KI-System interagieren, sowie gegebenenfalls Hinweise auf synthetische Inhalte erhalten. Die Verantwortung liegt hier stärker auf Information und Kennzeichnung als auf umfassenden Konformitätsprozessen.

Diese Transparenzpflichten sind nicht zu unterschätzen: Sie erfordern klare Kommunikationsstrategien und technische Implementierungen, um Nutzer angemessen zu informieren.

## Minimal Risk

Die große Mehrheit der KI-Anwendungen – etwa Spamfilter oder KI-gestützte Spielelemente – gilt als minimal risk; hier sieht der AI Act primär freiwillige Codes of Conduct und Eigenregulierung vor.

Gleichwohl wird erwartet, dass Unternehmen auch bei Niedrigrisikoanwendungen ethische Leitlinien beachten und sich in Richtung guter Praxis bewegen, insbesondere wenn diese Systeme mit Beschäftigteninteressen interagieren.

Die Einstufung als Minimal Risk entbindet nicht von anderen rechtlichen Verpflichtungen, insbesondere aus DSGVO, Arbeitsrecht oder Verbraucherschutz. Unternehmen sollten auch hier dokumentieren, warum sie ein System als Minimal Risk einordnen.

# Pflichten von Anbietern

## Provider-Verantwortlichkeiten im Detail

Anbieter von Hochrisiko-KI müssen ein umfassendes Pflichtenprogramm erfüllen, das den gesamten Lebenszyklus eines Systems abdeckt:

1. **Risikomanagement**
   Ein systematisches Risikomanagement über den gesamten Lebenszyklus eines Systems etablieren, das sowohl technische als auch grundrechtliche Risiken identifiziert, bewertet, mitigiert und überwacht.

2. **Datenqualität**
   Datenqualität und -governance sicherstellen (Repräsentativität, Relevanz, Genauigkeit, Verzerrungsminimierung). Trainingsdaten müssen frei von systematischen Bias sein.

3. **Dokumentation**
   Umfassende technische Dokumentation erstellen und pflegen (Architektur, Trainingsdaten, Annahmen, Leistungsgrenzen, Risikobewertungen).

4. **Logging**
   Automatische Protokollierung (Logging) und Nachvollziehbarkeit sicherstellen, um Entscheidungen rekonstruieren zu können.

5. **Menschliche Aufsicht**
   Geeignete Maßnahmen zur menschlichen Aufsicht vorsehen und implementieren, einschließlich UI-Design und Eskalationsmechanismen.

6. **Robustheit**
   Robustheit, Genauigkeit und Cybersicherheit des Systems gewährleisten, einschließlich Schutz vor Adversarial Attacks.

7. **Konformität**
   Eine Konformitätsbewertung durchführen und die CE-Kennzeichnung anbringen, bevor das System in Verkehr gebracht oder in Betrieb genommen wird.

Diese Pflichten wirken sich unmittelbar auf Unternehmensfunktionen aus, die KI-Systeme entwickeln oder anpassen – etwa Data-Science-Teams, IT, Compliance und Qualitätsmanagement. Sie definieren zugleich den Rahmen, in dem KMU als Anbieter agieren müssen, wenn sie eigene KI-Produkte entwickeln.

# Pflichten von Nutzern

## Deployer-Verantwortlichkeiten

Nutzer von Hochrisiko-Systemen – typischerweise Unternehmen, die KI in Geschäftsprozessen einsetzen – haben ergänzende Pflichten, die über die reine Anwendung hinausgehen:

### Zweckgebundene Nutzung

Nutzung im Einklang mit der vom Anbieter vorgesehenen Zweckbestimmung und den bereitgestellten Anweisungen. Abweichungen erfordern neue Bewertungen und können den Nutzer zum Provider machen.

### Folgenabschätzungen

Durchführung eigener Risiko- und ggf. Grundrechtsfolgenabschätzungen, insbesondere im öffentlichen Sektor oder bei sensiblen Anwendungsfällen (z.B. HR, Kredit, Sozialleistungen). Diese müssen dokumentiert und regelmäßig aktualisiert werden.

### Menschliche Aufsicht

Sicherstellung angemessener menschlicher Aufsicht im Betrieb (z.B. Schulung von Mitarbeitenden, Definition von Eingriffs- und Abschaltmöglichkeiten). Mitarbeitende müssen befähigt werden, KI-Entscheidungen zu hinterfragen.

### Monitoring und Meldung

Monitoring der Systemleistung, Protokollierung relevanter Ereignisse, Meldung schwerwiegender Vorfälle an Anbieter und ggf. Aufsichtsbehörden. Systematische Überwachung auf Drift und Bias.

### Qualifikation

Gewährleistung, dass beteiligte Mitarbeitende qualifiziert und sensibilisiert sind, insbesondere hinsichtlich Grenzen, Bias-Risiken und Anfechtungsmöglichkeiten.

Wenn Nutzer eigenmächtig wesentliche Änderungen an einem System vornehmen, können sie rechtlich als neue Anbieter mit entsprechend vollem Pflichtenprogramm gelten. Das ist für Unternehmen relevant, die bestehende Modelle stark anpassen oder mit eigenen Daten „weitertrainieren".

# General Purpose AI

## Besonderheiten bei allgemeinen KI-Modellen

General Purpose AI (GPAI) – also Modelle, die viele verschiedene Aufgaben erfüllen können, etwa große Sprachmodelle – stellen besondere Herausforderungen dar. Die Verantwortung verlagert sich hier teilweise von den ursprünglichen Modellanbietern auf die nachgelagerten Integratoren, die GPAI in konkrete Anwendungen einbetten.

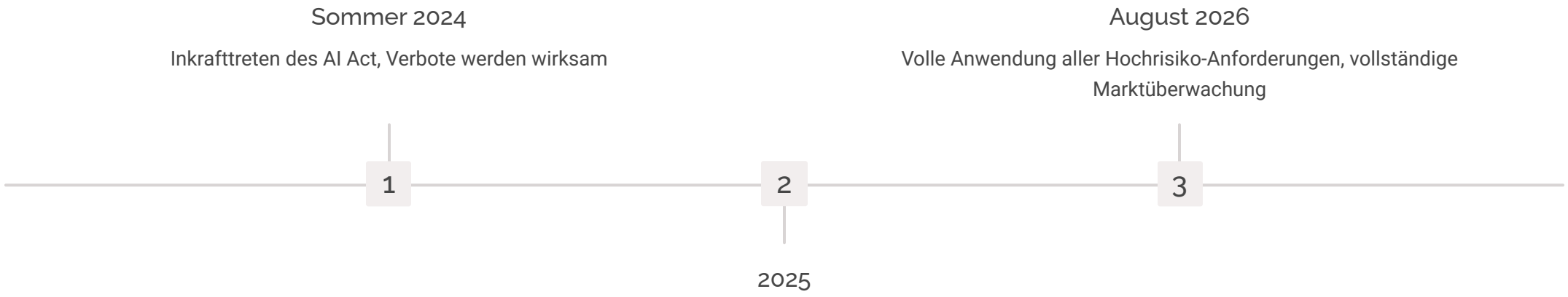
Das bedeutet: Ein Unternehmen, das ein generatives Modell eines Dritten in einem HR-Kontext oder für sicherheitskritische Entscheidungen einsetzt, kann als „Provider" des konkreten Hochrisiko-Systems gelten und muss die entsprechenden Pflichten (Risikomanagement, Dokumentation, CE) erfüllen, selbst wenn es nur eine API nutzt.

Diese Regelung ist besonders relevant für Unternehmen, die Large Language Models oder andere Foundation Models in ihre Geschäftsprozesse integrieren. Die bloße Nutzung einer API entbindet nicht von der Verantwortung, wenn das resultierende System in einen Hochrisikobereich fällt.

GPAI-Anbieter haben eigene Pflichten bezüglich Transparenz, Dokumentation und Risikomanagement, die sich von den Anforderungen an spezifische Hochrisiko-Systeme unterscheiden. Die genaue Abgrenzung und Verantwortungsverteilung wird durch nachgelagerte Leitlinien weiter konkretisiert.

# Zeitplan und Übergangsfristen

Der AI Act ist im Sommer 2024 in Kraft getreten; seine Anwendung erfolgt stufenweise bis August 2026. Diese gestaffelte Implementierung gibt Unternehmen Zeit zur Vorbereitung, erfordert aber auch frühzeitiges Handeln.




Verbotene KI-Praktiken werden früh in Geltung kommen, während Pflichten für Hochrisiko-Systeme, GPAI und Marktüberwachung in gestaffelten Übergangszeiträumen wirksam werden. Parallel werden technische Normen erarbeitet, die den gesetzlichen Rahmen konkretisieren und voraussichtlich bis 2026 maßgebliche Orientierung bieten.

Für Unternehmen und insbesondere KMU bedeutet die Übergangsphase eine kritische Vorbereitungszeit: Es besteht die Erwartung, bestehende und geplante KI-Anwendungen zu inventarisieren, vorläufig zu klassifizieren und erste Governance- und Dokumentationsstrukturen aufzubauen, bevor die vollen Sanktionsmechanismen greifen.

Gleichzeitig bleibt ein Zeitfenster, in dem Leitlinien, Praxisstandards und Codes of Practice entstehen, an denen sich Unternehmen orientieren können, um Compliance effizient und ressourcenschonend umzusetzen. Wer frühzeitig Strukturen schafft, kann Wettbewerbsvorteile durch vertrauenswürdige, rechtskonforme Systeme erzielen.

Kapitel 3

# Pflichten für Unternehmen

## Insbesondere für KMU

Die praktische Umsetzung des AI Act stellt Unternehmen vor vielfältige Herausforderungen. Besonders KMU müssen mit begrenzten Ressourcen komplexe Anforderungen erfüllen. Dieses Kapitel bietet einen detaillierten Überblick über typische KI-Anwendungen und ihre regulatorischen Implikationen.

### HR & Personalwesen

Bewerberauswahl, Leistungsbewertung, Schichtplanung

### Vertrieb & Marketing

Empfehlungssysteme, Pricing, Scoring

### Produktion

Predictive Maintenance, Qualitätskontrolle, Robotik

### Finanzbereich

Kreditscoring, Risikobewertung, Betrugserkennung

# Typische KI-Anwendungen im Detail

## HR und Personalwesen

In HR zählen zu typischen KI-Anwendungen:

- Automatisierte Bewerbervorauswahl (CV-Screening, Ranking)
- Algorithmische Matching-Systeme für Stellenbesetzung
- KI-gestützte Leistungsbewertung und Zielerreichungs-Analysen
- Automatisierte Schicht- und Personaleinsatzplanung
- Tools zur Analyse von Mitarbeiterkommunikation oder -zufriedenheit

## Vertrieb und Marketing

Im Vertrieb kommen etwa zum Einsatz:

- Empfehlungssysteme für Produkte und Dienstleistungen
- Dynamische Preisgestaltung basierend auf Nachfrage und Kundenverhalten
- Kunden-Scoring- und Lead-Priorisierung
- KI-basierte Betrugserkennung in Zahlungsprozessen
- Personalisierte Werbung und Content-Delivery

## Produktion und Logistik

In der Produktion sind verbreitet:

- Vorausschauende Wartung (Predictive Maintenance)
- Visuelle Inspektionssysteme für Qualitätskontrolle
- Autonome oder teilautonome Robotik und Fördertechnik
- KI-gestützte Kapazitäts- und Ressourcenplanung
- Supply Chain Optimierung

## Finanzbereich

Im Finanzbereich nutzen Unternehmen und Finanzinstitute KI u.a. für:

- Kreditwürdigkeitsprüfungen (Scoring)
- Risikobewertung und -pricing
- Betrugserkennung und Geldwäscheprävention
- Algorithmische Handelsstrategien
- Automatisierte Kundenberatung (Robo-Advisory)

# Erste Orientierung zur Risikokategorie

Eine erste Einordnung orientiert sich an Annex III und der Systemfunktion. Unternehmen sollten für jedes KI-System systematisch prüfen, in welche Risikokategorie es fällt:

1

## HR-Systeme

HR-Systeme, die über Zugang zu Beschäftigung, Beförderung oder wesentliche arbeitsbezogene Leistungen entscheiden, sind typischerweise Hochrisiko. Dies umfasst Bewerberauswahl, Performance-Bewertung und Überwachungssysteme.

2

## Produktion und Logistik

KI in Produktion und Logistik ist Hochrisiko, wenn sie Bestandteil regulierter Produkte (z.B. Maschinen) oder sicherheitskritischer Infrastruktur ist; reine Assistenzsysteme können in niedrigere Kategorien fallen.

3

## Finanzdienstleistungen

Kredit- und Versicherungs-Scoring für natürliche Personen gilt als Hochrisiko, insbesondere bei Lebens- und Gesundheitsversicherungen. Auch Betrugserkennung kann je nach Auswirkung hochriskant sein.

4

## Marketing und Vertrieb

Marketing- und Vertriebs-KI ohne unmittelbare gravierende Auswirkungen auf Grundrechte ist häufig „limited" oder „minimal risk", unterliegt aber dennoch DSGVO und ggf. DSA.

Für KMU ist es wichtig, diese Einordnung pragmatisch über Checklisten oder Standardkataloge vorzunehmen, die nach Anwendungsfall, betroffenem Grundrecht und Sektor strukturieren. Eine falsche Einordnung kann erhebliche rechtliche und finanzielle Konsequenzen haben.

# Grundpflichten im Detail

## Anforderungen für Anbieter

Die Impact-Studien identifizieren fünf Kernanforderungen, die für Hochrisiko-Systeme besonders kostenrelevant sind: Training Data (Datenqualität und -governance), Dokumentation und Record-Keeping, Informationsbereitstellung und Transparenz, Menschliche Aufsicht sowie Robustheit und Genauigkeit.

### Risikomanagement

Einrichtung eines formalen Systems, das Risiken über den gesamten Lebenszyklus identifiziert, bewertet, mitigiert und überwacht; Einbezug sowohl technischer als auch grundrechtlicher Risiken (z.B. Diskriminierung im HR-Kontext). Das Risikomanagement muss dokumentiert, regelmäßig überprüft und an neue Erkenntnisse angepasst werden.

### Datenqualität

Sicherstellung, dass Trainings-, Validierungs- und Testdaten relevant, repräsentativ, hinreichend vollständig, akkurat und frei von systematischen Verzerrungen sind; in Hochrisikokontexten können Ausnahmen für die Verarbeitung sensibler Daten zur Bias-Messung greifen, sofern Schutzmaßnahmen implementiert sind. Die Datenherkunft muss nachvollziehbar dokumentiert werden.

### Technische Dokumentation

Erstellung detaillierter Unterlagen zu Modellarchitektur, Annahmen, Datenquellen, Trainingsprozessen, Leistungskennzahlen, Einsatzgrenzen und Vorkehrungen gegen Fehlfunktionen; diese Dokumentation ist Grundlage für Konformitätsbewertung und behördliche Kontrolle.

### Transparenz

Bereitstellung verständlicher Informationen für Nutzer (Deployer) über Zweck, Funktionsweise, Grenzen, erforderliche Aufsicht und erwartete Genauigkeit; ggf. Informationen für Betroffene über den Einsatz von KI in sie betreffenden Entscheidungen. Die Informationen müssen in klarer, verständlicher Sprache verfasst sein.

### Menschliche Aufsicht

Konzeption von Systemen so, dass menschliche Akteure Ergebnisse verstehen, überwachen, korrigieren oder übersteuern können; dies umfasst UI-Design, Eskalationsmechanismen sowie Instruktionen für Bedienende. Die Aufsichtsmechanismen müssen praktikabel und effektiv sein.

### Robustheit und Genauigkeit

Gewährleistung, dass Systeme unter verschiedenen Bedingungen zuverlässig funktionieren, gegen Cyberangriffe geschützt sind und ihre Leistung über die Zeit aufrechterhalten. Regelmäßige Tests und Updates sind erforderlich.

# Anforderungen für Nutzer

Nutzer müssen – zusätzlich zu den Pflichten als Arbeitgeber, Datenschutzverantwortliche und ggf. Produktbetreiber – umfassende Maßnahmen ergreifen:

### Zweckgebundene Nutzung

KI-Systeme werden nur für die vom Anbieter vorgesehenen und dokumentierten Zwecke verwendet; Zweckänderungen erfordern erneute Bewertung und ggf. Konformitätsverfahren. Jede Abweichung muss dokumentiert und rechtlich geprüft werden.

### Monitoring

Laufende Überwachung von Systemleistung und Nebenwirkungen im realen Einsatz; Erkennung von Drift, Leistungsverlust oder unerwarteten Bias-Effekten; Meldung schwerwiegender Vorkommnisse. Systematische Auswertung von Logs und Metriken.

### Protokollierung

Sicherstellung, dass Logs erstellt, gesichert und im Bedarfsfall ausgewertet werden können, etwa zur Rekonstruktion von Fehlentscheidungen oder zur Beweisführung in Streitfällen. Aufbewahrungsfristen müssen eingehalten werden.

### Qualifizierte Mitarbeitende

Schulung derjenigen, die Systeme bedienen, interpretieren oder beaufsichtigen; Aufbau grundlegender KI-Kompetenz in Management, Fachbereichen und Compliance. Regelmäßige Weiterbildung ist erforderlich.

Gerade KMU sind hier gefordert, angemessene, aber pragmatische Strukturen aufzusetzen – etwa schlanke Risikoregister, klare Verantwortlichkeiten und standardisierte Checklisten für die Bewertung von KI-gestützten Entscheidungen. Die Dokumentation muss nachweisen, dass alle Pflichten erfüllt werden.

# Konformitätsbewertung und CE-Kennzeichnung

Hochrisiko-KI-Systeme dürfen nur mit gültiger Konformitätsbewertung und CE-Kennzeichnung in Verkehr gebracht werden. Die Systematik folgt dem New Legislative Framework (NLF) und setzt stark auf Selbstbewertung anhand harmonisierter technischer Normen; externe Prüfstellen sind nur in bestimmten Konstellationen (z.B. bestimmte biometrische Systeme oder bereits streng regulierte Produkte) zwingend.

### Interne Kontrolle

Prüfung des Qualitäts- und Risikomanagementsystems, Dokumentation aller relevanten Prozesse

### Technische Prüfung

Bewertung von Datenqualität, Sicherheitsanforderungen, Robustheit und Genauigkeit

### Dokumentation

Erstellung vollständiger technischer Unterlagen und Registrierung in EU-Datenbanken

### Post-Market-Monitoring

Implementierung kontinuierlicher Überwachung und Berichterstattung nach Markteinführung

Notifizierte Stellen (Prüfstellen) spielen vor allem bei Systemen eine Rolle, die bereits unter andere CE-Regime fallen oder besonders sensibel sind (z.B. Biometrie). Nationale Marktüberwachungsbehörden kontrollieren stichprobenartig und anlassbezogen die Konformität von Systemen, können technische Unterlagen und Zugang zu Daten verlangen und Produkte bei Gefahr vom Markt nehmen.

Im Finanz- und Medizinbereich wird häufig die bestehende Aufsicht (z.B. BaFin, Medizinproduktebehörden) zugleich für die Durchsetzung des AI Act zuständig sein, was die Koordination von KI-Regeln mit sektoralen Anforderungen erleichtern soll. Für Unternehmen empfiehlt sich eine frühzeitige Abstimmung von Produkt-, Compliance- und Rechtsabteilungen, um Mehrfachprüfungen zu vermeiden und Synergien zu nutzen.

Kapitel 4

# Umsetzung im Unternehmen

## Vom Gesetz zur Praxis

Die praktische Implementierung des AI Act erfordert systematische Prozesse, klare Verantwortlichkeiten und kontinuierliche Weiterentwicklung. Dieses Kapitel zeigt, wie Unternehmen die regulatorischen Anforderungen in ihre tägliche Praxis übersetzen können.

# Bestandsaufnahme

## Analyse bestehender KI- oder Automationssysteme

Als erster Schritt empfiehlt sich eine systematische Bestandsaufnahme aller Systeme, die algorithmische Entscheidungen treffen oder vorbereiten – inklusive „älterer" Scoring-Verfahren, Decision Trees und automatisierter Regelwerke. Entscheidend ist nicht das Label „KI", sondern die Funktion: Wo werden Entscheidungen automatisiert, Vorhersagen oder Empfehlungen erzeugt, die Mitarbeitende oder Dritte wesentlich betreffen? In HR, Compliance, Produktion, Vertrieb und Service sollten dazu Inventarlisten erstellt werden, die Systemzweck, Datenquellen, Betroffenenkreise und Schnittstellen dokumentieren.

### HR

- Bewerberauswahl
- Leistungsbewertung
- Schichtplanung

### Compliance

- Risikoscoring
- Fraud Detection
- Monitoring

### Produktion

- Qualitätskontrolle
- Predictive Maintenance
- Prozessoptimierung

### Vertrieb

- Lead-Scoring
- Preisoptimierung
- Empfehlungssysteme

### Service

- Chatbots
- Ticketpriorisierung
- Kundensegmentierung

# Erste Risikoeinordnung anhand gesetzlicher Kriterien

Auf Basis des Inventars können Systeme grob in die Risikokategorien des AI Act eingeordnet werden. Diese erste Einordnung dient dazu, Prioritäten zu setzen: Hochrisiko-Kandidaten werden vertieft bewertet, Niedrigrisiko- und Minimalrisiko-Anwendungen können zunächst mit leichteren Maßnahmen (z.B. Transparenz, einfache Checks) adressiert werden.

Liegt ein in Annex III genannter Bereich vor (z.B. HR, Kredit, kritische Infrastruktur)?

Hat das System direkten Einfluss auf Zugang zu Beschäftigung, Bildung, Leistungen oder auf physische Sicherheit?

Werden besonders schutzwürdige Gruppen betroffen oder sensible Daten verarbeitet?

# Governance-Strukturen und Verantwortlichkeiten

## Einbettung von KI in bestehende Organisationsstrukturen

KI sollte in bestehende Compliance-, Risiko- und Qualitätsmanagementstrukturen integriert statt isoliert betrachtet werden. Dafür ist es sinnvoll, KI-Governance als Querschnittsthema zu verankern, das mit Datenschutz, IT-Sicherheit, Arbeitsschutz, Produkt- und Dienstleistungsqualität sowie Rechtsabteilung koordiniert wird. In vielen Unternehmen werden bestehende Gremien (z.B. Compliance Committee, Datenschutz-Board) um KI-Kompetenzen ergänzt, statt neue Parallelstrukturen zu schaffen.

# Rollenverteilung zwischen Technik, Fachbereichen, Rechtsabteilung und Management

Die Quellen empfehlen eine klare Rollenverteilung. Gerade im HR-Kontext ist die Einbindung von Arbeitnehmervertretungen (Betriebs-/Personalräte) essenziell, da KI-Einsatz oft mit Mitbestimmungsrechten und Vereinbarungen zu Arbeits- und Leistungsüberwachung verbunden ist.

## Technik/Data Science

Modellentwicklung, Datenmanagement, technische Robustheit und Dokumentation

## Fachbereiche

Use Case Definition, fachliche Angemessenheit, operative Risikoabwägungen

## Rechtsabteilung/Compliance

Rechtliche Risikobewertung (AI Act, DSGVO, Sektorrecht), Konformitätsbewertung, Vertragsgestaltung

## Management

Strategischer Rahmen, Risk Appetite, Ressourcenzuteilung, regulatorische Verantwortung

# Prozesse, Richtlinien und Dokumentation

## Bausteine einer internen KI-Richtlinie

Eine interne KI-Richtlinie sollte mindestens regeln:

- Kriterien für Zulässigkeit und Zielsetzung von KI-Use-Cases (insbesondere im HR- und Beschäftigungskontext)
- Anforderungen an Datenbeschaffung, -qualität und -schutz
- Verfahren zur Risikobewertung (inkl. Grundrechtsfolgenabschätzungen) und Freigabe neuer KI-Systeme
- Prinzipien für menschliche Aufsicht, Eskalation und Abschaltung
- Anforderungen an Transparenz gegenüber Mitarbeitenden und ggf. Kunden
- Dokumentationspflichten und Verantwortlichkeiten

Diese Richtlinien dienen als interne „Übersetzung" des AI Act in konkrete Prozesse und bieten Orientierung für Projektteams und Führungskräfte.

# Dokumentationsanforderungen und Monitoringprozesse

Die Studien zeigen, dass substantielle Compliance-Kosten gerade aus laufender Dokumentation und Monitoring resultieren, die aber zugleich zentrale Grundlage für Rechtssicherheit und Lernfähigkeit sind.

## Dokumentation

- Standardisierte Dokumentationspakete pro System (Use Case, Datenquellen, Modelle, Tests, Risiken, Maßnahmen)
- Regelmäßige Reviews von Systemleistung und Nebeneffekten
- Klare Prozesse zur Meldung und Bearbeitung von Vorfällen

## Monitoring

- Überwachung auf Diskriminierung, Fehlerraten und neue Risiken
- Systematische Auswertung von Logs und Metriken
- Erkennung von Drift, Leistungsverlust oder unerwarteten Bias-Effekten

# Umgang mit Vorfällen und Fehlern

Für Vorfälle sollten definierte Workflows bestehen, die technische, rechtliche und kommunikative Aspekte verbinden. Gerade bei Hochrisiko-Anwendungen im HR-, Finanz- oder Sicherheitsbereich ist ein strukturierter Umgang mit Fehlern entscheidend, um Vertrauen zu erhalten und regulatorische Konsequenzen zu vermeiden.

### Sofortmaßnahmen

Deaktivierung bestimmter Funktionen, Notfallmodus

### Ursachenermittlung

Datenproblem, Modellfehler, Missbrauch

### Information

Mitarbeitende, Aufsichtsbehörden, ggf. Betroffene

### Remediation

Datenbereinigung, Modellanpassung, Prozessänderung

### Lessons Learned

Anpassung von Richtlinien und Schulungsinhalten


# Schulung und Sensibilisierung

## Kompetenzen für Management, Fachabteilungen und Technikteams

Die Quellen betonen, dass KI-Regulierung ohne Kompetenzaufbau im Unternehmen nicht effektiv umgesetzt werden kann. Benötigt werden abgestufte Schulungsformate:

### Management

- Grundverständnis von KI-Funktionsweisen
- Risikokategorien
- Haftungs- und Reputationsrisiken
- strategische Chancen vertrauenswürdiger Systeme

### Fachabteilungen

- Verständnis der spezifischen KI-Use-Cases
- ihrer Grenzen
- typischen Bias-Risiken
- und der eigenen Rollen bei Überwachung und Eingriff

### Technikteams

- Vertiefte Kenntnisse in Datenschutz
- AI Act-Anforderungen
- Dokumentation und erklärbarer KI
- zusätzlich zur Modellierungskompetenz

# Konkrete Szenarien, in denen Mitarbeitende Compliance beachten müssen

Schulungen sollten praxisnahe Szenarien behandeln. Solche Szenarien schärfen das Bewusstsein dafür, dass KI-Empfehlungen nicht blind übernommen werden dürfen und dass Mitarbeitende eine aktive Rolle im Schutz von Grundrechten und Sicherheit spielen.

> Wie geht ein HR-Mitarbeiter vor, wenn ein KI-System eine qualifizierte Bewerberin niedrig rankt, obwohl andere Indikatoren für hohe Eignung sprechen?

> Wie reagiert ein Produktionsleiter, wenn ein KI-basiertes Qualitätskontrollsystem auffällig viele Fehlalarme generiert?

> Welche Schritte muss ein Kundenbetreuer einleiten, wenn ein KI-System einer Person einen Kredit verweigert und diese eine Begründung verlangt?

# Blick nach vorn

## Bedeutung zukünftiger Leitlinien und Standards

Die endgültige Wirkung des AI Act wird stark von nachgelagerten Leitlinien, Standards und Codes of Practice abhängen. Europäische und nationale Behörden (AI Office, Datenschutzgremien, Marktaufsichten) werden Auslegungshilfen für Schnittstellen mit DSGVO, DSA und sektoralen Normen entwickeln – etwa zum Umgang mit Trainingsdaten, zur Abgrenzung von Hochrisiko-Use-Cases oder zu Anforderungen an Erklärbarkeit. Technische Normungsorganisationen (CEN/CENELEC, ISO/IEC, IEEE) arbeiten an Standards, die Anforderungen an Datenqualität, Risikomanagement und Governance konkretisieren und für Unternehmen zur praktischen „Gebrauchsanleitung" der Regulierung werden können.

# Entwicklung von Best Practices auf EU- und Branchenebene

Branchenspezifische Best Practices – etwa im Finanzsektor, im Gesundheitswesen, in der Industrieproduktion oder in HR-Dienstleistungen – werden eine Schlüsselrolle spielen, um KI-Regulierung effizient umzusetzen und dennoch Raum für Innovation zu lassen. Diese können aus Kooperationen zwischen Unternehmen, Verbänden, Gewerkschaften, Wissenschaft und Zivilgesellschaft hervorgehen und als Grundlage für Codes of Practice nach dem AI Act dienen. Gerade für KMU sind solche Best Practices essenziell, um nicht jedes Problem selbst lösen zu müssen, sondern bewährte Musterlösungen adaptieren zu können.

## Kooperationspartner

- Unternehmen und Verbände
- Gewerkschaften
- Wissenschaft
- Zivilgesellschaft

## Anwendungsbereiche

- Finanzsektor
- Gesundheitswesen
- Industrieproduktion
- HR-Dienstleistungen

# Sanktionen und Haftung

## Sanktionsrahmen

Der AI Act sieht empfindliche Bußgelder vor, die sich an der Systematik der DSGVO orientieren und sich prozentual am weltweiten Jahresumsatz bemessen können. Verstöße gegen Verbote oder Kernanforderungen Hochrisiko-Systeme können daher erhebliche finanzielle und reputative Folgen haben, insbesondere für größere Unternehmen.

KMU sollen durch verhältnismäßige Durchsetzung und unterstützende Maßnahmen entlastet werden, bleiben aber grundsätzlich adressiert. Die Behörden werden bei der Bemessung von Sanktionen die Größe und Ressourcen des Unternehmens berücksichtigen.

Neben Bußgeldern können auch andere Maßnahmen verhängt werden, etwa Produktrückrufe, Verkaufsverbote oder die Verpflichtung zur Nachbesserung. In schweren Fällen können auch strafrechtliche Konsequenzen drohen.

## Haftungsschnittstellen

Regulatorische Verstöße nach AI Act und zivilrechtliche Haftung greifen ineinander. Die Studien zeigen, dass Unternehmen, die gegen KI-Anforderungen verstoßen, typischerweise auch nach Produkthaftungsrecht oder Deliktsrecht haftbar sein können – etwa bei Schäden durch fehlerhafte Entscheidungen oder mangelnde Überwachung.

Umgekehrt entbindet die Einhaltung des AI Act nicht automatisch von zivilrechtlicher Haftung, kann aber als Indiz für die Einhaltung des Stands der Technik und damit zur Haftungsbegrenzung dienen.

Eine Harmonisierung über technische Standards als „Safe Harbour" für KI- und Haftungsregime ist in Diskussion: Wer anerkannte Standards erfüllt, soll in der Regel als konform gelten, was sowohl regulatorische als auch haftungsrechtliche Risiken reduziert. Für Unternehmen ist es daher strategisch sinnvoll, sich an entstehenden Normen zu orientieren und ggf. aktiv in Standardisierungsgremien mitzuwirken.

# Besondere Herausforderungen für KMU

KMU stehen vor besonderen Herausforderungen: Ihnen fehlen oft spezialisierte Rechts- und Compliance-Teams, tiefe Datenexpertise und finanzielle Reserven, um komplexe Konformitätsprozesse zu etablieren. Gleichzeitig sind sie zunehmend auf KI-Lösungen angewiesen, um wettbewerbsfähig zu bleiben – etwa durch Automatisierung von Routineaufgaben, gezielte Kundenansprache oder effizientere Produktion.

Studien zeigen, dass Compliance-Kosten gerade bei Hochrisiko-Systemen einen spürbaren Anteil am Entwicklungsbudget ausmachen können; dennoch sind viele Teilaktivitäten ohnehin best practice und würden auch ohne spezifische Regulierung anfallen.

### Standards und Vorlagen

Für KMU sind branchenspezifische Leitfäden, standardisierte Vorlagen (z.B. für DPIA, Fundamental Rights Impact Assessments) und praxisnahe technische Standards besonders wichtig. Sie können den Aufwand reduzieren, indem sie rechtliche Anforderungen operationalisieren und als Checklisten oder Musterprozesse bereitstellen.

### Unterstützungsangebote

Unabhängige Prüfinstanzen und Beratungsangebote – etwa gefördert durch staatliche Programme – können KMU beim Aufbau von Governance-Strukturen, Datenmanagement und Dokumentation unterstützen. Branchenverbände und Kammern bieten zunehmend spezialisierte Hilfestellungen an.

### Wettbewerbsvorteile

Frühzeitige Auseinandersetzung mit KI-Compliance schafft nicht nur Rechtskonformität, sondern kann auch als Qualitäts- und Vertrauensmerkmal im Wettbewerb genutzt werden. Unternehmen, die nachweislich faire, transparente und robuste KI einsetzen, können sich gegenüber Kunden, Mitarbeitenden, Regulierern und Investoren positiv positionieren.

In Branchen mit hohem Reputationsrisiko – etwa HR-Dienstleistungen, Finanzservices oder Gesundheitsanwendungen – kann vertrauenswürdige KI zum entscheidenden Differenzierungsfaktor werden. Die Investition in Compliance zahlt sich langfristig durch Risikominimierung, Vertrauensgewinn und Marktzugang aus.