DOSSIER

EU AI Act - Konkrete Pflichten

Der EU AI Act - Konkrete Pflichten

Vom Gesetzestext zur Praxis: Klarheit, Zuständigkeiten, Nachweise

Vom Überblick zum Handeln

Das **Dossier "Der EU AI Act - Grundlagen"** allgemein zum Rahmen und den Bestimmungen hat gezeigt: Der EU AI Act bringt klare Pflichten für alle Organisationen – unabhängig davon, ob sie KI selbst entwickeln oder einfach nur einsetzen.

Dieses **Vertiefungsdossier** übersetzt die Pflichten in die Praxis. Es geht darum, **was Organisationen konkret beachten müssen** und wie sie diese Pflichten so umsetzen, dass nicht nur Compliance entsteht, sondern auch Vertrauen.

1. Transparenzpflicht – sichtbar machen, wo KI eingesetzt wird

Ein Kunde ruft im Servicecenter an. Die Antwort wirkt flüssig, sachlich, freundlich. Erst nach Minuten fragt er irritiert: „War das eigentlich gerade ein Mensch – oder eine Maschine?" Genau in diesem Moment entscheidet sich Vertrauen.

Was die Pflicht verlangt

Der EU AI Act verpflichtet Organisationen, offen zu legen, wenn KI im Einsatz ist. Das klingt unspektakulär, ist aber grundlegend: Niemand darf glauben, mit einem Menschen zu sprechen, wenn es in Wahrheit eine Maschine ist. Niemand soll Bewerbungsbescheide oder Leistungsentscheidungen erhalten, ohne zu wissen, dass KI beteiligt war.

Warum das mehr ist als ein Hinweistext

Viele stellen sich unter Transparenz einen kleinen Zusatz am Seitenende vor: „Dieses Angebot wurde KI-gestützt erstellt." Doch das reicht nicht. Transparenz heißt: Klarheit zum richtigen Zeitpunkt.

- Ein Chatbot muss sofort signalisieren, dass er KI-basiert antwortet – nicht erst im Impressum.
- Ein Bewerber muss wissen, wenn sein Lebenslauf von einem Algorithmus vorbewertet wird – nicht erst, wenn er abgelehnt wurde.

Die Führungsdimension

Transparenz ist nicht nur eine juristische Vorschrift, sondern eine Haltung. Wenn eine Organisation bewusst offenlegt, wann KI beteiligt ist, signalisiert sie: Wir haben nichts zu verbergen.

Das verändert die Wahrnehmung – bei Kunden, Bürgern, Bewerbern gleichermaßen. Statt den Verdacht auszulösen, etwas werde verschwiegen, entsteht Vertrauen: Hier wird ehrlich kommuniziert.

Stolperfallen aus der Praxis

Viele Organisationen unterschätzen, wie schnell Intransparenz wirkt:

- Ein Chatbot, der sich „Anna“ nennt, aber keine KI-Hinweise gibt.
- Ein automatischer Textvorschlag im CRM, der ungekennzeichnet an Kunden versendet wird.
- Eine standardmäßig aktivierte KI-Funktion in HR-Software, die unbemerkt Screening-Entscheidungen trifft.

Jede dieser Situationen kann rechtlich problematisch werden – aber noch wichtiger: Sie schadet der Glaubwürdigkeit.

Was Führungskräfte beachten sollten

Die entscheidende Frage lautet nicht: Mit wie wenig Transparenz kommen wir durch?
Sondern: Wie gestalten wir Transparenz so, dass sie Vertrauen stärkt?

Das ist eine Führungsentscheidung. Sie betrifft Kommunikation, Außenauftritt und Kultur. Wer KI einsetzt, ohne dies klarzumachen, verspielt nicht nur rechtlich, sondern auch in der Wahrnehmung.

2. Schulungspflicht – Wissen als Pflicht, nicht als Kür

In vielen Organisationen läuft es so: Ein kurzer Vortrag zur „KI im Alltag“, eine Präsentation mit ein paar Folien – und damit gilt die Schulung als erledigt.

Doch genau hier beginnt das Missverständnis.

Was die Pflicht verlangt

Der EU AI Act spricht nicht von „Sensibilisierung“, sondern von **nachweisbarer Schulung**. Jede Mitarbeiterin und jeder Mitarbeiter, der mit KI in Berührung kommt, muss verstehen:

- Was kann das System?
- Wo liegen seine Grenzen?
- Welche Risiken bestehen?

Warum oberflächliche Ansätze scheitern

Ein einziges Webinar reicht nicht. Wer nur oberflächlich informiert wird, übersieht Risiken – oder nutzt KI blindlings. Typisches Beispiel: Ein Recruiter verlässt sich voll auf die Vorauswahl des KI-Systems, ohne die Kriterien zu hinterfragen. Die Folge: Bewerber:innen werden diskriminiert, ohne dass es jemand merkt.

So sollte es gemacht werden

- **Klarer Rahmen**: Schulung ist nicht Event, sondern Prozess.
- **Praxisnah**: Mitarbeitende müssen die Anwendung üben, die sie tatsächlich nutzen.
- **Nachweisbar**: Es braucht Dokumentation, wer wann wie geschult wurde.

Führungsperspektive

Schulung ist Organisationslernen. Wer sie als Pflicht abhakt, verfehlt den Kern. Wer sie strategisch begreift, baut Kompetenz auf – und genau das unterscheidet Organisationen, die KI souverän einsetzen, von jenen, die stolpern.

3. Risikoprüfung – Klarheit vor dem Einsatz

Im Vorstandsgespräch kommt die Frage auf: „Wir haben da ein neues KI-Tool im HR – müssen wir das wirklich prüfen, oder reicht es, wenn wir sagen: alle nutzen es?“

Genau hier beginnt die Kernpflicht: **Vor dem Einsatz einer KI muss klar sein, welche Risiken sie birgt und welche Pflichten dadurch ausgelöst werden.**

Welche Risiken der AI Act anspricht

Der Gesetzgeber unterscheidet nicht abstrakt, sondern sehr konkret:

- **Diskriminierung** – KI kann systematisch Menschen benachteiligen (z. B. Bewerber:innen mit bestimmten Namen, Frauen bei Kreditentscheidungen, bestimmte Gruppen bei Prognosen).
- **Fehleranfälligkeit** – Systeme können Ergebnisse liefern, die faktisch falsch oder verzerrt sind. Ein Diagnosetool mit hoher Fehlerquote kann Leben gefährden.
- **Mangelnde Nachvollziehbarkeit** – „Black-Box“-Entscheidungen, die weder Fachleute noch Betroffene nachvollziehen können.
- **Technische Robustheit** – Systeme, die bei Datenfehlern, Angriffen oder Veränderungen instabil werden.
- **Reputations- und Vertrauensrisiken** – auch wenn nicht explizit im Gesetz, entstehen sie automatisch: Eine intransparente KI-Nutzung kann Vertrauen in die Organisation untergraben.

Wie sich daraus Pflichten ergeben

1. Vor dem Einsatz prüfen

2. Jede Organisation muss klären: Welche Risikoklasse gilt?

- Minimal/Begrenzt: Kurze Abwägung, dokumentiert – Pflicht erfüllt.
- Hochrisiko: Detaillierte Risikobewertung, oft mit externen Prüfungen.

3. Konkrete Prüfpunkte

- **Datenbasis**: Sind Trainings- oder Entscheidungsdaten diskriminierungsfrei und aktuell?
- **Genauigkeit**: Welche Fehlerraten gibt es? Werden diese regelmäßig getestet?
- **Transparenz**: Kann die Entscheidung nachvollzogen werden – intern wie extern?
- **Einsatzkontext**: Wo werden Ergebnisse kritisch? (Kundenschnittstelle, Personal, Finanzen, Gesundheit).

4. Dokumentation & Nachweisbarkeit

- Jede Prüfung muss nachvollziehbar dokumentiert sein.
- „Wir haben geprüft“ reicht nicht – es muss klar sein: Wie, wann, mit welchen Ergebnissen.
- Bei Hochrisiko-Systemen zusätzlich: Registrierung im EU-Register.

Pflicht zur kontinuierlichen Überprüfung

Risikoprüfung ist kein einmaliger Akt, sondern ein Prozess. Systeme verändern sich (Updates, neue Versionen, geänderte Daten). Das Gesetz verlangt Monitoring und laufende Anpassungen.

Anwendungen in der Praxis

- **Personalwesen**: Ein Bewerbermanagement-System muss vor Einsatz geprüft werden: Bevorzugt es bestimmte Profile? Wie transparent ist die Auswahl?
- **Finanzwesen**: Eine Kreditentscheidung durch KI gilt als Hochrisiko. Pflicht: Diskriminierungsprüfung, Fehlerquoten, Transparenz der Kriterien, Dokumentation, EU-Register.
- **Kommunikation mit GenAI**: Ein Texttool für interne Berichte gilt als begrenztes Risiko. Pflicht: kurze Abwägung (z. B. Risiko von Fehlinformationen, Umgang mit vertraulichen Daten) und Nachweis, dass Transparenzregeln eingehalten werden.

Führungsperspektive

Risikoprüfung ist kein bürokratischer Akt, sondern ein Instrument der Selbstkontrolle.

- Sie zeigt, dass die Organisation verstanden hat, wo die kritischen Punkte liegen.
- Sie schützt vor Blindflügen mit eingebetteten KI-Funktionen.
- Sie stärkt Glaubwürdigkeit: Wenn Mitarbeitende oder Kunden nachfragen, kann die Organisation zeigen, dass Risiken bewusst geprüft und dokumentiert wurden.

4. Technische & organisatorische Maßnahmen – IT allein reicht nicht

Oft hört man den Satz: „Darum kümmert sich die IT."

Doch genau das ist der Irrtum.

Organisationen müssen Prozesse für Qualitätssicherung, Monitoring und Reaktion auf Fehler einrichten. Das gilt unabhängig davon, ob sie die KI selbst entwickeln oder einkaufen.

Typische Irrtümer

- „Unser Anbieter garantiert Qualität" – reicht nicht.
- „Wenn etwas schiefgeht, merkt die IT es schon" – fatal, denn Fehler tauchen oft in Fachbereichen auf.
- „Wir dokumentieren das später" – zu spät, wenn etwas passiert ist.

Ein Beispiel aus der Praxis

Ein Industrieunternehmen setzt KI für Qualitätskontrolle ein. Die KI übersieht fehlerhafte Teile. Ohne klaren Prozess zur Eskalation und Verantwortlichkeit bleibt der Fehler im System – und landet beim Kunden. Die Folge: Produktionsrückruf, Imageschaden, mögliche Strafen.

Führungsperspektive

Technische & organisatorische Maßnahmen sind kein IT-Detail, sondern Teil der Governance. Führungskräfte müssen sicherstellen:

- Wer überwacht?
- Wer entscheidet im Ernstfall?
- Wer trägt Verantwortung?

5. Verantwortung bei externen Tools – der blinde Fleck

Es ist ein unscheinbarer Moment: Ein Softwareanbieter spielt ein Update ein. Über Nacht ist eine neue KI-Funktion aktiviert – ohne dass jemand in der Organisation davon weiß. Und genau hier beginnt die Verantwortung. Auch wenn eine KI von außen kommt, trägt die Organisation Verantwortung. Externe Anbieter entbinden nicht von der Pflicht, zu prüfen und zu dokumentieren.

Warum das oft übersehen wird

- Standardsoftware wie M365, SAP oder Salesforce enthält längst KI-Funktionen – oft automatisch aktiviert.
- Viele Führungskräfte gehen davon aus: „Wenn Microsoft es anbietet, wird es schon compliant sein." Das ist ein gefährlicher Irrtum.

Praxisbeispiele

- HR-Software wählt Bewerbungen vor – ohne dass HR-Leitung weiß, dass dies KI-basiert läuft.
- CRM-System schlägt automatisiert Kundensegmentierungen vor – ohne dass Sales-Teams verstehen, wie die Kriterien zustande kommen.

Führungsperspektive

Tool-Auswahl ist Compliance. Wer sie als reine IT-Frage behandelt, riskiert Blindflüge.

Führungskräfte müssen gezielt fragen:

- Welche KI-Funktionen sind enthalten?
- Welche Pflichten ergeben sich daraus?
- Wer überprüft, dass diese eingehalten werden?

Unterschiede nach Unternehmensgröße

Der EU AI Act trifft alle Organisationen – aber die Größe einer Organisation beeinflusst, wie Pflichten praktisch umgesetzt werden.

Kleine und mittlere Unternehmen (KMU)

- Nutzen meist Standardsoftware mit eingebetteter KI.
- Selten eigene Entwicklung, aber hohes Risiko, Funktionen unbewusst mitzunutzen.
- Pflichten: Bestandsaufnahme und Schulungssystem sind entscheidend. Risikoprüfungen bleiben überschaubar, solange keine Hochrisiko-Systeme eingesetzt werden.

Große Unternehmen und Konzerne

- Setzen KI strategisch und oft in Kernprozessen ein, teilweise mit Eigenentwicklung.
- Mehrere Abteilungen involviert (Compliance, IT, Fachbereiche).
- Pflichten: Aufbau komplexer Governance-Strukturen, klare Zuständigkeiten, dokumentierte Prüfverfahren, Audit-Trails, externe Prüfungen.

Die Führungsimplikation

Für KMU bedeutet der EU AI Act: Klarheit über bestehende Tools schaffen und Mitarbeitende systematisch schulen.

Für große Organisationen: Risiko- und Compliance-Strukturen dauerhaft verankern – nicht als Projekt, sondern als Bestandteil von Unternehmensführung.

Branchenspezifische Unterschiede

Nicht nur die Größe einer Organisation, sondern auch das Einsatzfeld wirkt sich darauf aus, wie Pflichten praktisch umgesetzt werden.

Öffentliche Verwaltung

- KI ist bereits im Einsatz, oft unbemerkt: Texterkennung bei Formularen, Bürger-Chatbots, Prognosetools.
- **Pflichten**: Transparenz gegenüber Bürger:innen, Schulung der Mitarbeitenden, teils Hochrisiko bei automatisierter Antragsprüfung.

Industrie

- KI wird in der Qualitätskontrolle, in der vorausschauenden Wartung und in Lieferketten-Analysen eingesetzt.
- **Pflichten**: Meist begrenztes Risiko, aber in sicherheitskritischen Branchen (z. B. Automobil, Chemie) Übergang zu Hochrisiko.

Finanzwesen

- Banken und Versicherungen nutzen KI in Kreditvergabe, Risikoanalysen und Anlageberatung.
- **Pflichten**: Strenge Hochrisiko-Anforderungen – inklusive Risikoprüfung, Dokumentation und Registrierung im EU-Register.

Gesundheitswesen

- KI in Diagnostik, Bildanalyse oder Entscheidungsunterstützung.
- **Pflichten**: Nahezu immer Hochrisiko, daher umfassende Prüf- und Dokumentationspflichten.

Dienstleistungen & Wissensarbeit

- Breiter Einsatz von GenAI für Texte, E-Mails, Marketing, interne Analysen.
- **Pflichten**: Begrenztes Risiko – Transparenz und Schulung sind hier die entscheidenden Hebel.

Der Handlungsrahmen für Organisationen

Am Ende münden alle Pflichten in **fünf greifbare Schritte**. Entscheidend ist, dass Sie sie einfach, überprüfbar und anschlussfähig in Ihre bestehende Governance integrieren:

1. **Bestandsaufnahme**: Wo nutzen wir heute bereits KI – sichtbar (Chatbots, HR-Vorauswahl) oder „embedded“ in Standardtools (M365, CRM, ERP)?

2. **Risikoeinstufung**: Welche Anwendungen sind minimales/begrenztes Risiko (kurze Abwägung), wo droht Hochrisiko (formalisierte Prüfung vor Einsatz)?

3. **Zuständigkeiten & Prozesse**: Wer verantwortet Transparenz, Schulung, Dokumentation, Monitoring – und wie läuft Eskalation im Fehlerfall?

4. **Schulung als System**: Rollenbasiert, praxisnah, nachweisbar – nicht als Event, sondern als wiederkehrender Prozess.

5. **Kommunikation**: Transparenz so früh wie möglich – nach innen (Mitarbeitende) und außen (Kund:innen/Bürger:innen). Ziel: Vertrauen statt Überraschungen.

Diese fünf Schritte sind **schlank genug für KMU** – und **skalierbar für große Organisationen**.

Konkretisierende Maßgaben des deutschen Durchführungsgesetzes

Der EU AI Act gilt unmittelbar in allen Mitgliedstaaten. Doch in den Mitgliedsstaaten, also auch Deutschland, wird er durch ein **Durchführungsgesetz** konkretisiert. Ein **Referentenentwurf** des Bundesministeriums für Digitales und Staatsmodernisierung (Stand September 2025) zeigt, wie Aufsicht und Zuständigkeiten organisiert werden sollen.

Kernpunkte:

- Die **Bundesnetzagentur (BNetzA)** übernimmt eine zentrale Rolle und richtet ein **Koordinierungs- und Kompetenzzentrum (KoKIVO)** ein.
- Wo es bereits Aufsichtsstrukturen gibt – etwa in der Produktregulierung – bleiben diese bestehen.
- Für neue Felder wie Biometrie, kritische Infrastrukturen oder KI am Arbeitsplatz wird die BNetzA zuständig.
- Im Finanzsektor übernimmt die BaFin die Marktüberwachung.
- Zudem entsteht innerhalb der BNetzA eine unabhängige **Marktüberwachungskammer (UKIM)**, die ab 2026 jährlich Bericht erstattet.

Für Organisationen bedeutet das: Der AI Act wird nicht nur europäisch geregelt, sondern in Deutschland auch praktisch überprüfbar. Noch handelt es sich um einen Referentenentwurf, aber die Richtung ist eindeutig.

Fazit

Der EU AI Act verlangt keine Bürokratiemonster, sondern nachvollziehbare Verantwortung. Wer Transparenz, Schulung, Risikoprüfung und TOMs in ein schlankes, belastbares Führungssystem übersetzt, gewinnt Rechtssicherheit und Vertrauen – bei Mitarbeitenden, Kund:innen und Aufsicht.

Mit Blick auf den deutschen Referentenentwurf ist jetzt gutes Vorausplanen gefragt: Zuständigkeiten kennen, Kontaktpunkte definieren, Dokumentation robust aufsetzen – und so vorbereitet sein, wenn die nationale Umsetzung in Kraft tritt.

Künstliche Intelligenz weiterdenken

Wenn Sie Interesse an weiterführenden Informationen haben, melden Sie sich gern:

Unverbindliche Beratung: https://calendly.com/freuding/beratung-ki

Kontakt: Dr. Beate Freuding, freuding@digital-leader.eu, 0152 05188026

Weitere Dossiers & E-Books zum Download: ki-briefing.kit.com

Hinweis: Die Regulierung innerhalb Europas entwickelt sich sehr schnell. Dieses Dokument ist im September 2025 erstellt worden. Zum Zeitpunkt des Lesens können die im Dokument genannten Fakten bereits überholt sein.

Dieses Dokument dient der allgemeinen Information und Orientierung und ist in enger Zusammenarbeit mit Künstlicher Intelligenz entstanden. Es stellt keine Rechtsberatung dar und kann eine individuelle juristische Prüfung im Einzelfall nicht ersetzen.

Alle Angaben wurden sorgfältig recherchiert und nach bestem Wissen erstellt. Dennoch übernimmt die Autorin keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit der Inhalte, insbesondere im Hinblick auf sich fortentwickelnde gesetzliche Vorgaben.

Für Entscheidungen, die auf Basis dieses Dokuments getroffen werden, übernimmt die Autorin keine Haftung. Die Umsetzung rechtlicher Anforderungen – insbesondere im Bereich KI-Governance – sollte stets in Abstimmung mit fachkundiger Rechtsberatung erfolgen.