



EU Artificial Intelligence Act

Fit für den EU AI Act

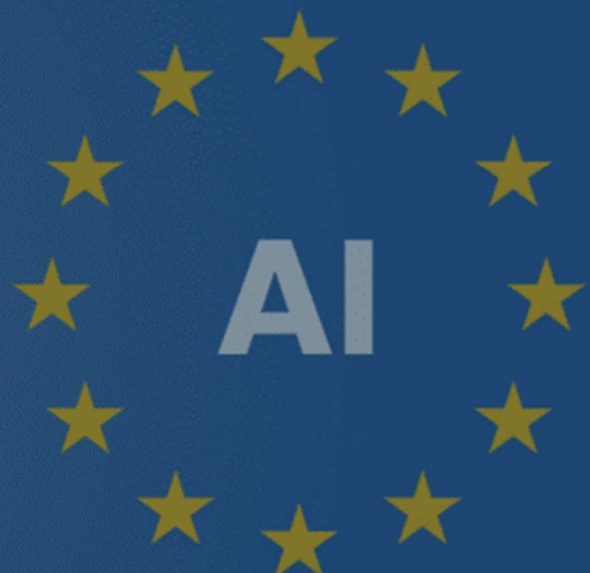
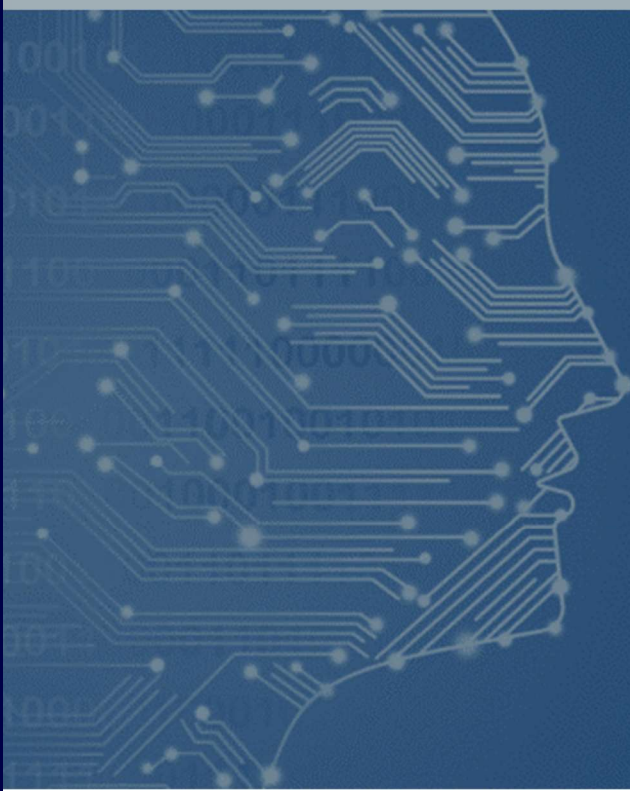
Wie Unternehmen sich jetzt auf den EU AI Act vorbereiten sollten. Ein praktischer Leitfaden – von den Anforderungen bis zur Umsetzung.

September 2025

oetti-ds - AI for Excellence

oetti-ds - AI for Excellence

oetti-ds -



Was ist der EU AI Act?

- Weltweit erste umfassende gesetzliche Regelung zur Entwicklung, Nutzung und Vermarktung von Künstlicher Intelligenz.
- Der AI Act soll Vertrauen in KI und Innovationen „made in Europe“ fördern und Rechtssicherheit für Unternehmen schaffen.

Der EU AI Act ist die weltweit erste umfassende gesetzliche Regelung zur Entwicklung, Nutzung und Vermarktung von Künstlicher Intelligenz (KI) in der Europäischen Union. Ziel ist es, KI sicher, transparent und ethisch vertretbar zu gestalten und dabei Grundrechte, Sicherheit und Demokratie zu schützen.

Der AI Act legt einheitliche Regeln fest und nutzt einen risikobasierten Ansatz: Je nach Risiko für Nutzer und Gesellschaft gelten unterschiedliche Anforderungen – von striktem Verbot (z. B. manipulative oder diskriminierende KI-Systeme) über strenge Vorgaben (hochriskante KI-Systeme wie biometrische Überwachung, kritische Infrastruktur, Medizin und Personalmanagement) bis hin zu geringeren oder minimalen Pflichten für risikoarme Anwendungen (z. B. Chatbots, Spamfilter).

Ziele und Prinzipien

Der AI Act fördert Vertrauen in KI und Innovationen „made in Europe“ und soll Rechtssicherheit für Unternehmen schaffen. Neben dem Schutz der Verbraucher werden auch Anforderungen an Dokumentation, technische Sicherheit, Transparenz und Risikomanagement eingeführt. Die EU verfolgt dabei das Leitbild einer menschenzentrierten und verantwortungsvollen KI.

Wer ist vom EU AI Act betroffen?

- Der AI Act richtet sich **an alle** Unternehmen, die KI-Systeme in der EU **entwickeln**, in den Verkehr bringen, **vertreiben** oder **nutzen**.
- Privatpersonen, die KI „ausschließlich privat“ nutzen, sind vom AI Act ausgenomm.

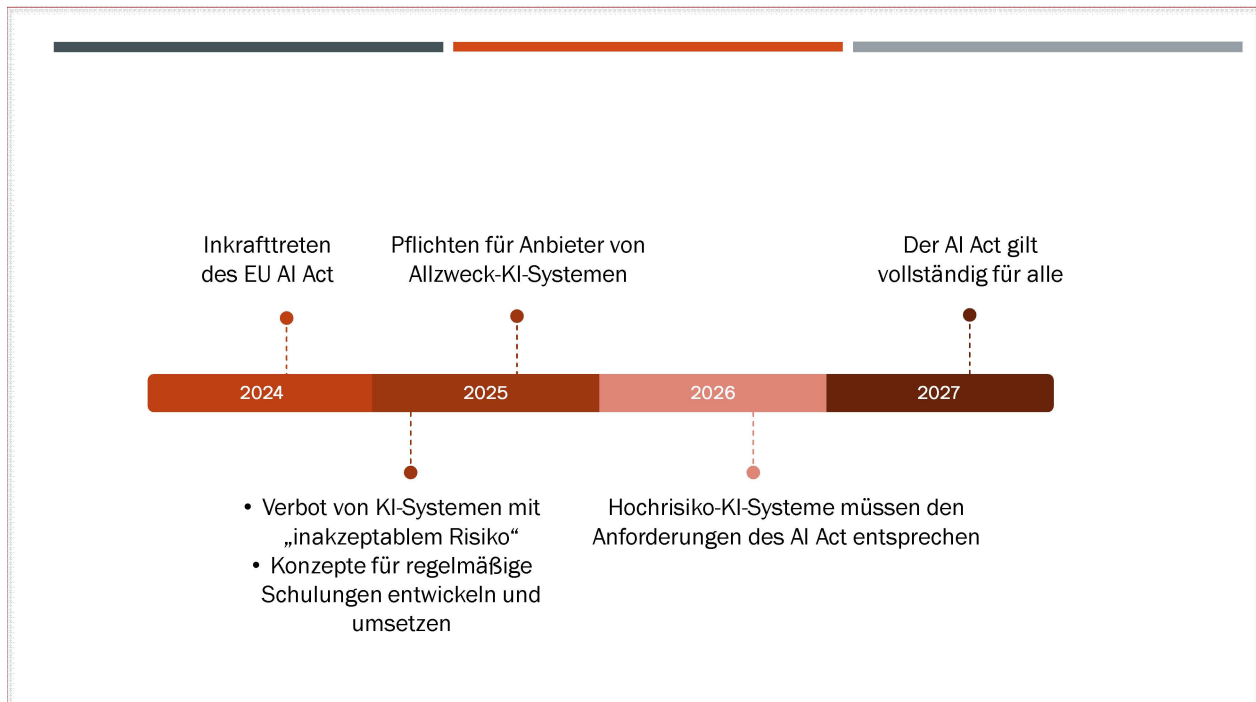
Der AI Act richtet sich an alle, die KI-Systeme in der EU entwickeln, **in den Verkehr bringen**, **vertreiben** oder **nutzen** – unabhängig davon, ob sie in der EU ansässig sind oder nicht.

Dazu gehören:

- **Anbieter/Hersteller von KI-Systemen:** Unternehmen, die KI-Anwendungen oder -Modelle entwickeln und auf den europäischen Markt bringen.
- **Betreiber/Anwender:** Organisationen, die KI-Systeme gewerblich einsetzen, z. B. für Recruiting, Kundenservice, Fertigung oder Medizin.
- **Importeure und Händler:** Unternehmen, die KI-Produkte aus dem Ausland in die EU importieren oder vertreiben.
- **Plattformbetreiber:** Firmen, die KI-Systeme bereitstellen oder als Dienste im EU-Markt anbieten.
- **Bevollmächtigte und Behörden:** Auch juristische Personen, öffentliche Stellen und Unternehmen, die im Auftrag agieren oder KI-Systeme für öffentliche Aufgaben einsetzen.

Privatpersonen, die KI „ausschließlich privat“ nutzen, sind vom AI Act ausgenommen. Entscheidend ist also nicht der Firmensitz, sondern ob das KI-System auf dem europäischen Binnenmarkt eingesetzt oder vermarktet wird.

Wie ist der Zeitplan?



Der **EU AI Act** folgt einem klar strukturierten, mehrstufigen Zeitplan, der sich über mehrere Jahre erstreckt. Das Gesetz tritt am 2. August 2024 in Kraft; die praktische Umsetzung und die Pflichten für Unternehmen erfolgen aber gestaffelt:

Wichtige Meilensteine

- **2. August 2024:** Inkrafttreten des EU AI Act und Start der 24-monatigen Übergangsphase
- **2. Februar 2025:** Verbot von KI-Systemen mit „inakzeptablem Risiko“. Für alle anderen: Konzepte für regelmäßige Schulungen entwickeln und umsetzen.
- **2. August 2025:** Verpflichtungen und Governance-Regeln für Anbieter von Allzweck-KI-Systemen (GPAI), erste behördliche Strukturen und Meldepflichten treten in Kraft.
- **2. August 2026:** Ende der Übergangsphase – Hochrisiko-KI-Systeme müssen den neuen Anforderungen des AI Act entsprechen.
- **2. August 2027:** Übergangsfristen für bereits bestehende KI-Systeme enden, der AI Act gilt vollständig für alle Anwendungsbereiche und Akteure.

Weitere Fristen und Maßnahmen

- In den ersten Monaten nach Inkrafttreten werden die zuständigen nationalen Behörden benannt.
- Unternehmen müssen schrittweise Dokumentationen, Risikobewertungen und Compliance-Strukturen aufbauen.
- Detaillierte Leitlinien und Ergänzungen sollen bis 2026 folgen, insbesondere für Hochrisiko-KI und Allzweck-KI.

Was gilt gemäß EU AI Act als KI System?

Ein KI-System ist Software,

- die mit Daten arbeitet
- und eigenständig Ergebnisse liefert, die wiederum Auswirkungen auf die Realität haben können.

Ein **KI-System** ist:

„Ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Autonomiegrad arbeitet und für explizite oder implizite Ziele Vorhersagen, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen.“

Ein KI-System ist also **Software, die mit Daten arbeitet und eigenständig Ergebnisse liefert**, die wiederum Auswirkungen auf die Realität haben können. Das heißt:

- Es **lernt aus Daten oder Regeln** (z. B. durch maschinelles Lernen, Statistik, Deep Learning, aber auch regelbasierte Systeme, wenn sie komplexe Entscheidungsprozesse abbilden).
- Es **arbeitet nicht nur starr nach festen Vorgaben**, sondern kann in einem gewissen Rahmen **autonom** handeln.
- Es produziert **Ausgaben** wie:
 - eine **Vorhersage** („Wie wahrscheinlich ist es, dass Kunde X kündigt?“),
 - eine **Empfehlung** („Zeige diesem Nutzer Produkt Y an“),
 - eine **Entscheidung** („Bewerbung ablehnen/zulassen“).

Ein KI-System ist jede Software, die auf Datenbasis Ergebnisse produziert, die menschliche Entscheidungen, Prozesse oder die Umwelt beeinflussen können – egal ob es sich um Hightech-Machine-Learning oder ein einfacheres algorithmisches System handelt.

Beispiele für KI-System und kein KI-System?

KI-Systeme	Keine KI-Systeme
■ Chatbots & Sprachmodelle ■ Bilderkennungssysteme ■ Empfehlungssysteme ■ Scoring-Modelle ■ Automatisierte Bewerber- oder Mitarbeiterbewertungssysteme ■ Autonome Roboter oder Fahrzeuge	■ Taschenrechner ■ Textverarbeitung ■ Einfache Datenbanken ■ Anwendungen mit fixen Regeln (keine Intelligenz)

Systeme wie maschinelles Lernen, Deep Learning, Generative KI, Entscheidungsfindungs-Tools und Empfehlungssysteme zählen als KI-Systeme nach EU AI Act.

Ausgenommen sind reine Konfigurations-, Statistik- oder numerische Optimierungstools ohne eigenständige Schlussfolgerungsfähigkeit, rein militärische oder wissenschaftliche Forschungssysteme und Anwendungen für ausschließlich private Zwecke.

Beispiele für KI-Systeme im Sinne des AI Acts

- Chatbots & Sprachmodelle (z. B. virtuelle Assistenten, Übersetzungstools)
- Bilderkennungssysteme (z. B. zur Gesichtserkennung oder Qualitätskontrolle in der Fertigung)
- Empfehlungssysteme (z. B. Produktempfehlungen im E-Commerce, personalisierte Werbung)
- Scoring-Modelle (z. B. Kreditwürdigkeitsprüfung)
- Automatisierte Bewerber- oder Mitarbeiterbewertungssysteme
- Autonome Roboter oder Fahrzeuge

Was typischerweise nicht als KI-System gilt

- Einfache Software ohne Entscheidungslogik, z. B. Taschenrechner, klassische Datenbanken oder Textverarbeitungsprogramme.
- Systeme, die ausschließlich manuelle Regeln ohne „Intelligenz“ umsetzen (z. B. wenn eine App nur fixe Eingaben abfragt und 1:1 ausgibt).

Welche Maßnahmen sind konkret notwendig?

1. Risikobewertung und Klassifizierung
2. Dokumentation und Transparenz
3. Monitoring, Bias-Tests und Datenqualität
4. Governance und Verantwortlichkeiten
5. Technische und organisatorische Maßnahmen
6. Regelmäßige Schulungen
7. Meldung und Protokollierung von Vorfällen

Folgende Maßnahmen sind notwendig, um die Compliance mit dem EU AI Act sicherzustellen:

1. **Risikobewertung und Klassifizierung:** Alle KI-Systeme und Projekte sollten nach ihrer Risikoklasse gemäß AI Act analysiert und bewertet werden. Besonders Hochrisiko-Anwendungen erfordern strikte Kontrollen, spezielle Prüfungen und ein Risikomanagementsystem.
2. **Dokumentation und Transparenz:** Umfassende Dokumentation aller Algorithmen, Datenquellen, Systementscheidungen und Änderungen ist essenziell. Unternehmen müssen Nutzer klar über den Einsatz von KI informieren, z. B. bei automatisierten Entscheidungen oder Chatbots.
3. **Monitoring, Bias-Tests und Datenqualität:** Regelmäßige Überwachung und Tests auf Diskriminierung, Verzerrungen (Bias) und Fehler in den Daten sind notwendig, um faire Ergebnisse sicherzustellen. Etablierung interner Prozesse zur Behebung von Mängeln.
4. **Governance und Verantwortlichkeiten:** Klare Zuständigkeiten für KI-Systeme schaffen, z. B. durch AI Compliance Boards oder die Benennung von KI-Beauftragten. Aufbau eines Compliance-Frameworks anhand gesetzlicher Vorgaben und internationaler Standards (z. B. ISO / IEC 42001).
5. **Technische und organisatorische Maßnahmen:** Implementierung von Logging-, Monitoring- und Human Oversight-Maßnahmen für alle relevanten KI-Systeme. Anpassung der unternehmensweiten Sicherheits- und Qualitätsmanagementprozesse.
6. **Regelmäßige Schulungen:** MitarbeiterInnen müssen gezielt im Umgang mit KI, den Anforderungen des AI Act und ethischen Standards fortgebildet werden.
7. **Meldung und Protokollierung von Vorfällen:** Klare Abläufe für die Meldung sicherheitsrelevanter Zwischenfälle an Behörden einrichten.

1 Risikobewertung und Klassifizierung

Die 4 Risikoklassen nach EU AI Act

- Unacceptable Risk
- High Risk
- Limited Risk
- Minimal Risk

Der EU AI Act unterscheidet **vier Risikoklassen** für KI-Systeme. Die Bewertung erfolgt anhand von Anwendungsbereich und Auswirkung auf Gesundheit, Sicherheit und Grundrechte

Übersicht der Risikoklassen

- **Unacceptable Risk:** Verbotene KI-Systeme, etwa soziale Scoring-Systeme von Behörden, Manipulation vulnerabler Gruppen, oder Echtzeit-Biometrie zur Identifikation für Strafverfolgung.
- **High Risk:** KI-Systeme mit erheblichen Auswirkungen auf Sicherheit, Gesundheit oder Rechte (z.B. Medizinprodukte, HR-Software für Bewerberauswahl, Kredit- oder Versicherungsscoreing, Steuerung kritischer Infrastruktur, biometrische Identifikation).
- **Limited Risk:** KI-Anwendungen mit Transparenzpflichten, wie Chatbots oder Deepfakes, die Nutzer klar über KI-Interaktion informieren müssen.
- **Minimal Risk:** KI-Systeme ohne spürbare Risiken, etwa Spamfilter oder Spiele.

Beispiele aus Unternehmen

- Im Personalwesen: KI-gestützte Bewerbungsscreenings gelten als High Risk, da sie über Beschäftigungschancen entscheiden können.
- Im Finanzwesen: KI-basierte Kreditwürdigkeitsprüfung fällt in die High Risk Kategorie.
- Im Gesundheitswesen: KI-unterstützte Diagnosesysteme für Patienten sind als High Risk einzustufen.
- Marketing/Kommunikation: KI-gesteuerte Chatbots (Limited Risk) müssen Transparenz schaffen und Deepfakes deklarieren.
- IT-Security: Spamfilter gelten als Minimal Risk und unterliegen keinen besonderen Anforderungen.

Beispiele für die Risikoklassen

Unacceptable Risk (inakzeptables Risiko):

- Social Scoring durch Behörden (Bewertung von Personen basierend auf Verhalten oder Persönlichkeitsmerkmalen)
- Echtzeit-Biometrie zur Überwachung in öffentlichen Räumen (z.B. Gesichtserkennung)
- KI-Systeme, die manipulative Techniken einsetzen oder vulnerable Gruppen ausnutzen
- Deepfake-Systeme zur Täuschung ohne Kennzeichnung

High Risk (hohes Risiko):

- KI in Medizinprodukten oder robotergestützter Chirurgie
- KI-gestützte Bewerbermanagementsysteme (Screening von Bewerbern)
- Kreditwürdigkeitsprüfung mittels KI (Scoring)
- Systeme zur biometrischen Identifikation (z.B. Gesichtserkennung rückwirkend)
- KI-Anwendungen in Strafverfolgung, Justiz und Grenzkontrolle

Limited Risk (begrenztes Risiko):

- Chatbots, die Nutzerinteraktionen führen und Offenlegungspflichten unterliegen
- Deepfakes, bei denen Nutzer informiert werden müssen, dass es sich um KI-generierte Inhalte handelt
- Personalisierte Preisalgorithmen mit geringem direkten Einfluss auf Grundrechte

Minimal Risk (minimales Risiko):

- Spamfilter in E-Mail-Systemen
- Spiele mit KI-Anteilen ohne weitreichende Auswirkungen
- Empfehlungsalgorithmen ohne kritische Entscheidungen

2 Dokumentation

Die Dokumentation setzt sich zusammen aus

- Technische Dokumentation
- Risikobewertung
- Transparenz- und Erklärbarkeitsnachweise
- Qualitätssicherung
- Governance und Verantwortlichkeiten
- Prozessdokumentationen

Firmen dokumentieren ihre Compliance zum EU AI Act vor allem durch umfassende technische und organisatorische Unterlagen, die regelmäßig aktualisiert und intern vorgehalten werden.

Sie ist primär als Nachweis für Behörden und interne Kontrolle bestimmt, eine vollständige Veröffentlichung ist nicht erforderlich, wohl aber eine transparente Kommunikation gegenüber Nutzern, etwa durch Kennzeichnung KI-generierter Inhalte. Wesentliche Bestandteile sind:

- **Technische Dokumentation:** Beschreibung der KI-Systeme, ihrer Architektur, Algorithmen, Trainingsdaten, und Funktionsweise inklusive Versionskontrolle und Änderungsprotokollen.
- **Risikobewertung:** Protokollierung von Risikoanalysen, Bewertung der potenziellen Auswirkungen und Maßnahmen zum Risikomanagement.
- **Transparenz- und Erklärbarkeitsnachweise:** Darstellung, wie Nutzer über den Einsatz von KI informiert werden und wie Entscheidungen nachvollziehbar gemacht werden.
- **Qualitätssicherung:** Nachweis von Tests, Monitoring und Maßnahmen zur Vermeidung von Bias und Fehlfunktionen.
- **Governance und Verantwortlichkeiten:** Dokumentation der Zuständigkeiten, Schulungen der Mitarbeitenden und interne Kontrollmechanismen.
- **Prozessdokumentationen:** Abläufe zur Erstellung, Pflege, Überwachung und Meldung bei KI-Systemen.

Dokumente und Berichte werden typischerweise digital in Compliance- und Governance-Plattformen oder Dokumentenmanagementsystemen verwaltet. Checklisten, Audit-Berichte und Compliance-Tracker erleichtern die regelmäßige Überprüfung und Fortschrittskontrolle.

Versionierte technische Dokumentationen und Protokolle werden oft mit Software-Tools für Versionskontrolle geführt (z. B. Git), um Änderungen nachverfolgbar zu machen.

3 Monitoring – Testing - Datenqualität

Unternehmen müssen gemäß EU AI Act bei Monitoring, Bias-Tests und Datenqualität vor allem für Hochrisiko-KI-Systeme folgende konkrete Pflichten erfüllen:

- Die Systeme müssen nach Einführung und dauerhaft überwacht (“Monitoring”) werden.
- Es sind regelmäßige Bias-Tests durchzuführen, um Diskriminierung zu verhindern.
- Die verwendeten Daten müssen qualitativ hochwertig, repräsentativ und möglichst fehlerfrei sein, mit Nachweis und Kontrolle der Datenherkunft sowie automatisierten Qualitätsprüfungen.

Unternehmen, die KI-Systeme einsetzen, müssen konkrete Maßnahmen für Monitoring, Bias-Tests und Datenqualität ergreifen. Diese Anforderungen betreffen vor allem Hochrisiko-KI-Systeme und betreffen sowohl technische als auch organisatorische Prozesse.

Monitoring

- Unternehmen müssen ein **Post-Market Monitoring-System** etablieren, das die Leistungsfähigkeit und Konformität der KI-Systeme während ihrer gesamten Lebensdauer überwacht.
- tisch dokumentiert und analysiert, um Risiken und Schwachstellen frühzeitig zu erkennen.
- Die Monitoring-Aktivitäten müssen in einem strukturierten Monitoring-Plan festgehalten sein.

Bias-Tests

- Unternehmen sind verpflichtet, systematisch auf **Bias (Vorurteile)** zu testen.
- Die Trainings-, Validierungs- und Testdaten müssen regelmäßig darauf geprüft werden, ob bestimmte Personengruppen benachteiligt werden.
- Die Ergebnisse der Tests sowie die Maßnahmen zur Korrektur müssen dokumentiert werden.
- Organisationen müssen Methoden für faire und inklusive KI-Modelle etablieren.

Datenqualität

- Es gelten strenge Vorgaben für die Qualität aller im KI-System verwendeten Daten: Diese müssen relevant, repräsentativ, möglichst fehlerfrei und vollständig sein.
- Unternehmen müssen automatisierte Mechanismen für Qualitätschecks einrichten.
- Die Herkunft, Verarbeitung und Eigenschaften aller Datensätze sind zu dokumentieren.

4 Governance

Im Bereich Governance und Verantwortlichkeiten verlangt der EU AI Act, dass Unternehmen klare Zuständigkeiten, Kontroll- und Dokumentationsprozesse für KI-Systeme einführen. Dazu gehören:

- Aufbau eines KI-Risikomanagementsystems.
- Aufbau eines Compliance-Frameworks
- Zuweisung verantwortlicher Rollen
 - KI-Compliance-Officer
 - AI Compliance Board)
- Prüfung der Lieferkette und Einbindung von Partnern in die Compliance-Strategie.

Im Bereich Governance und Verantwortlichkeiten verlangt der EU AI Act, dass Unternehmen klare Zuständigkeiten, Kontroll- und Dokumentationsprozesse für KI-Systeme einführen. Dazu gehören:

- Aufbau eines **KI-Risikomanagementsystems** und regelmäßige Bewertung der eingesetzten Systeme, insbesondere bei Hochrisiko-Anwendungen.
- Aufbau eines Compliance-Frameworks anhand gesetzlicher Vorgaben und internationaler Standards (z. B. ISO / IEC 42001).
- Etablierung von transparenten Entscheidungswegen und Nachweis der Konformität mit technischen und rechtlichen Vorgaben – etwa durch Audits, Prüfprotokolle und umfassende Dokumentation.
- Zuweisung verantwortlicher Rollen (z. B. KI-Compliance-Officer, AI Compliance Board), die die Einhaltung der gesetzlichen Vorgaben steuern und kontrollieren.
- Prüfung und Überwachung der gesamten Lieferkette (Vendor Due Diligence) und Einbindung von Partnern in die Compliance-Strategie.

Governance und klare Verantwortlichkeiten sind zentrale Voraussetzungen für rechtskonformen und vertrauenswürdigen KI-Einsatz in Unternehmen, mit Haftung und Kontrollpflichten bis auf die Leitungsebene.

5 Technische Maßnahmen

Unternehmen müssen laut EU AI Act für ihre relevanten KI-Systeme folgende technische und organisatorische Maßnahmen umsetzen:

- Logging & Monitoring
- Human Oversight
- Sicherheits- und Qualitätsmanagement
- Technische Dokumentation
- Schulungen

Unternehmen müssen laut EU AI Act für ihre relevanten KI-Systeme folgende technische und organisatorische Maßnahmen umsetzen:

- **Logging & Monitoring:** Alle relevanten Aktivitäten und Entscheidungen der KI müssen automatisch protokolliert werden. Monitoring-Systeme sind erforderlich, um jederzeit die Funktionsweise zu überwachen und Vorfälle frühzeitig zu erkennen.
- **Human Oversight:** Hochrisiko-KI-Systeme dürfen nicht unbegrenzt autonom laufen. Unternehmen müssen klare Prozesse schaffen, damit autorisierte Mitarbeitende jederzeit prüfen, intervenieren oder stoppen können (“Human-in-the-Loop” oder “-on-the-Loop”).
- **Sicherheits- und Qualitätsmanagement:** Bestehende Sicherheits- und Qualitätsmanagementprozesse sind um KI-spezifische Anforderungen zu ergänzen – hierzu zählen Risikomanagement, Change-Management, Versionierung, Audits und laufende Überprüfung.
- **Technische Dokumentation:** Alle Maßnahmen, Protokolle und Entscheidungswege müssen nachvollziehbar dokumentiert und regelmäßig geprüft werden, um die Compliance nachweisen zu können.
- **Schulungen:** Mitarbeitende sind in den neuen Prozessen und der sicheren Anwendung von KI-Systemen zu schulen.

Ziel ist es, die Sicherheit, Qualität und Transparenz von KI-Systemen durchgängig zu gewährleisten und bei Bedarf schnell eingreifen zu können.

6 Schulungen

Bis **Februar 2025** Konzepte für regelmäßige, dokumentierte Schulungen entwickeln und umsetzen.

- Vermittlung von KI-Grundwissen, technischen sowie rechtlichen und ethischen Aspekten, Risiken und Anwendungsgrenzen.
- Spezifische Trainings für Entwickler, Führungskräfte, Anwender und Compliance-Beauftragte
- Anleitung zur sicheren, rechtmäßigen und transparenten Nutzung von KI inkl.
- Dokumentation aller Schulungen.

Unternehmen müssen bis spätestens Februar 2025 Konzepte für regelmäßige, dokumentierte Schulungen entwickeln und umsetzen, auch wenn weitere Teile der Verordnung erst später komplett wirksam werden. Die Pflicht gilt für Anbieter und Betreiber **aller KI-Systeme** und umfasst technische, rechtliche und ethische Inhalte zur KI-Nutzung und Risiken. Die Schulungen sollen folgende Inhalte abdecken:

- Vermittlung von KI-Grundwissen, technischen sowie rechtlichen und ethischen Aspekten, Risiken und Anwendungsgrenzen.
- Spezifische Trainings für Entwickler, Führungskräfte, Anwender und Compliance-Beauftragte – angepasst an die Risikoklasse des eingesetzten KI-Systems.
- Anleitung zur sicheren, rechtmäßigen und transparenten Nutzung von KI inkl. Sensibilisierung für Bias, Datenschutz und Qualität.
- Dokumentation aller Schulungen als Nachweis für Behörden.

Kontinuierliche Weiterbildung ist Pflicht, denn nur so stellen Unternehmen sicher, dass der Umgang mit KI gesetzeskonform, sicher und verantwortungsvoll bleibt.

7 Meldungen

Betrifft vor allem **Anbieter von Hochrisiko-KI-Systemen**.

- Meldung schwerwiegender Vorfälle an die zuständigen Behörden.
- Die Meldung muss spätestens 15 Tage nach Kenntnis erfolgen, bei besonders schweren.
- Sofort Untersuchungen zum Vorfall, Risikobewertungen und Abhilfemaßnahmen einleiten.
- Umfangreiche Dokumentations- und Berichtspflichten sind einzuhalten.

Der Bereich Meldungen im EU AI Act betrifft **vor allem Anbieter von Hochrisiko-KI-Systemen**. Diese Unternehmen müssen jeden schwerwiegenden Vorfall, bei dem ein Zusammenhang zwischen dem KI-System und dem Ereignis besteht oder vermutet wird, **unverzüglich melden**.

Die wichtigsten Anforderungen sind:

- Meldung schwerwiegender Vorfälle an die zuständigen Marktüberwachungsbehörden im Mitgliedstaat, in dem der Vorfall aufgetreten ist.
- Die Meldung muss spätestens 15 Tage nach Kenntnis erfolgen, bei besonders schweren Vorfällen (z. B. Todesfälle) aber innerhalb von 2 bis 10 Tagen.
- Anbieter müssen nach Meldung unverzüglich Untersuchungen zum Vorfall durchführen, Risikobewertung erstellen und Abhilfemaßnahmen einleiten.
- Die Meldungen dienen der Überwachung und Einhaltung der Sicherheit und Qualität der KI-Systeme auf dem Markt.
- Umfangreiche Dokumentations- und Berichtspflichten sind einzuhalten, um die Nachvollziehbarkeit zu gewährleisten.

Diese Meldepflichten sind zentral für das Risikomanagement und die Compliance von Unternehmen, die KI-Systeme mit hohem Risiko einsetzen oder anbieten.

Mögliche Strafen für Verstöße

- **Schwerwiegende Verstöße**, etwa Einsatz verbotener KI-Anwendungen (z.B. Manipulation, Grundrechtsverletzungen): bis zu 35 Mio. Euro oder 7% des globalen Jahresumsatzes.
- **Verstöße gegen Pflichten bei Hochrisiko-KI**, fehlende Transparenz, mangelhafte Dokumentation: bis zu 15 Mio. Euro oder 3% des Umsatzes.
- **Falsche**, irreführende oder unvollständige **Angaben** gegenüber Behörden: bis zu 7,5 Mio. Euro oder 1,5% des Umsatzes.

Die Strafen des EU AI Act können deutlich höher ausfallen als etwa nach DSGVO. Unternehmen, die gegen Vorschriften des EU AI Act verstoßen, müssen mit extrem hohen Geldbußen rechnen – bis zu 35 Millionen Euro oder 7% des weltweiten Jahresumsatzes, abhängig davon, welcher Betrag höher ist.

Höhe der Sanktionen

- **Schwerwiegende Verstöße**, etwa Einsatz verbotener KI-Anwendungen (z.B. Manipulation, Grundrechtsverletzungen): bis zu **35 Mio. Euro** oder **7% des globalen Jahresumsatzes**.
- Verstöße gegen Pflichten bei Hochrisiko-KI, fehlende Transparenz, mangelhafte Dokumentation: bis zu **15 Mio. Euro** oder **3% des Umsatzes**.
- Falsche, irreführende oder unvollständige Angaben gegenüber Behörden: bis zu **7,5 Mio. Euro** oder **1,5% des Umsatzes**.

Weitere mögliche Sanktionen

- Wiederholte oder vorsätzliche Verstöße können neben Bußgeldern auch Marktverbote und den Rückzug nicht konformer KI-Produkte zur Folge haben.
- Reputationsschäden, Verwarnungen und weitere aufsichtsrechtliche Maßnahmen bis hin zum EU-weiten Verkaufsverbot ganzer KI-Systeme sind möglich.

Besonderheiten für KMU und Start-ups

- Für kleinere Unternehmen und Start-ups gelten in einigen Fällen reduzierte Bußgelder und Schwellenwerte entsprechend den Bestimmungen des Gesetzes.

Vorgehensplan

Vorgehen und Projektorganisation

- Bildung eines organisationsübergreifenden Projektteams
- Bestandsaufnahme und Risikoklassifizierung aller eingesetzten Systeme
- Aufbau eines risikobasierten Compliance-Frameworks
- Einrichtung von Governance-Strukturen
- Durchführung von Schulungen und Sensibilisierung

Typisches Vorgehen und Projektorganisation:

- Bildung eines **organisationsübergreifenden Projektteams** mit Vertretern aus den Bereichen Recht, Compliance, Entwicklung, IT, Qualitätsmanagement und Management.
- Zunächst wird eine **Bestandsaufnahme** aller eingesetzten KI-Systeme durchgeführt, einschließlich deren Risikoklassifizierung nach dem EU AI Act.
- Aufbau eines **risikobasierten Compliance-Frameworks**, das gesetzliche Anforderungen mit Unternehmensprozessen verbindet (z.B. technische und organisatorische Maßnahmen, Audits und Monitoring).
- Einrichtung von **Governance-Strukturen** wie AI Compliance Boards zur Steuerung und Überwachung der KI-Regelkonformität.
- Durchführung von **Schulungen und Sensibilisierung** der Mitarbeitenden, um Verständnis für Pflichten und Chancen zu schaffen.
- Erstellung und Pflege der erforderlichen **Dokumentation** und der technischen Unterlagen für die Compliance.

Aus Fallstudien und Beispielen lassen sich wiederkehrende Best Practices ableiten:

- Frühzeitige Risikoanalysen und systematische Klassifizierung aller KI-Systeme.
- Zentrale Governance-Strukturen mit klar definierten Verantwortlichkeiten.
- Integration in bestehende Prozesse statt separater Compliance-Systeme.
- Kontinuierliche Mitarbeiterschulung und Kompetenzaufbau.
- Proaktive Zusammenarbeit mit Regulierungsbehörden und Branchenkollegen.

Softwaretools - Beispiele

Kostenlose Einstiegstools

- AuditOne EU AI Compliance Checker
- EU AI Act Compliance Checker

Kommerzielle Angebote

- Validaitor - All-in-One Trustworthy AI Platform
- caralegal - AI Governance & Compliance Software
- Thetis - Deutsche AI-Compliance-Lösung

- **EU AI Act Compliance Checker:** Offizielle EU-Bewertungstool für KMU. Kostenlos.
- **AuditOne EU AI Compliance Checker:** Kostenloses Self-Assessment mit STARED-Framework
- **Validaitor** - All-in-One Trustworthy AI Platform:
 - Automatisierte AI-System-Inventarisierung mit zentraler, unveränderlicher Dokumentation
 - Integrierte Risikobewertung und -management mit umfangreicher Template-Bibliothek
 - Automatisierte Testing-Suites mit vordefinierten Benchmarks für verschiedene KI-Typen
 - Compliance-Management mit maßgeschneiderter Anleitung und anpassbaren Vorlagen
 - Unterstützung für ISO 42001 und NIST AI RMF zusätzlich zum AI Act
- **caralegal** - AI Governance & Compliance Software:
 - Zentrales AI-System-Register mit automatischer Klassifizierung
 - AI Flow-Workflow der systematisch durch alle Regulierungsanforderungen führt
 - Cross-funktionale Zusammenarbeit zwischen IT-Sicherheit, Datenschutz und KI-Entwicklung
 - Umfassendes Risikomanagement über den gesamten KI-Lebenszyklus
 - Automatisierte Compliance-Audits und Dashboard-Übersichten
- **Thetis** - Deutsche AI-Compliance-Lösung:
 - Vollautomatische Prüfungen der technischen AI Act-Anforderungen
 - Revisionssichere Dokumentation gemäß Artikel 11, 15 und Annex IV
 - Integrierte Risikoanalyse für Performance, Fairness, Robustheit und Datenqualität
 - Kollaborative Arbeitsumgebung für Entwickler, Juristen und Entscheider
 - Made in Germany mit DSGVO-Konformität

Die 900 Milliarden Chance!

Vorgehen und Projektorganisation

- Bildung eines organisationsübergreifenden Projektteams
- Bestandsaufnahme und Risikoklassifizierung aller eingesetzten Systeme
- **Systematische Identifikation von AI Potenzialen**
 - **Start von AI Potenzial-Projekten**
- Aufbau eines risikobasierten Compliance-Frameworks
- Einrichtung von Governance-Strukturen
- Durchführung von Schulungen und Sensibilisierung



Der EU AI Act wird von vielen Unternehmen in der EU zunächst als lästige Pflicht wahrgenommen. Unter Androhung hoher Strafen von bis zu 7 % des Umsatzes sind Unternehmen verpflichtet, sämtliche KI-Anwendungen im Betrieb zu erfassen und zu klassifizieren. Hinzu kommen Anforderungen in den Bereichen Organisation, Compliance und Schulungen. Doch warum diese Pflicht nicht als Chance begreifen?

Wenn ohnehin eine Inventur der bestehenden KI-Systeme notwendig ist, lässt sich dieser Schritt ideal mit der Aufdeckung von **profitablen KI-Potenziale** verbinden. Verschiedene Studien schätzen den Mehrwert durch den Einsatz von KI in Unternehmen in der EU auf mehrere Billionen Euro.

- **Effizienzsteigerung:** Der Einsatz von KI kann durchschnittlich 5 – 20 % Kostenersparnis ermöglichen.
- **Neuer Umsatz:** Noch größer ist das Potenzial durch zusätzliche Leistungen und innovative Geschäftsmodelle auf Basis von KI.

Bei **oetti-ds** haben wir eine Methode entwickelt, die die verpflichtenden Vorbereitungen auf den EU AI Act mit einem **AI-Growth-Projekt** im Unternehmen verbindet. Konkret bedeutet das:

Auf den Projektschritt „Bestandsaufnahme und Risikoklassifizierung“ im Rahmen des AI-Act-Projekts folgt eine systematische Identifizierung von KI-Potenzialen – in zwei Dimensionen:

- **Effizienz:** Analyse entlang der gesamten Wertschöpfungskette nach Einspar- und Optimierungsmöglichkeiten.
- **Growth:** Analyse mithilfe der von **oetti-ds** entwickelten „**Customer Journey Kette**“ zur Identifizierung neuer Produkte und Dienstleistungen.

Wer hat den Leitfaden erstellt?

Der Leitfaden **Fit für den EU AI Act** wurde erstellt von der **oetti-ds GmbH**, einer unabhängigen Beratungsboutique mit Fokus auf Organisationsberatung, Data Science, Machine Learning und Künstliche Intelligenz. Das Unternehmen ist herstellerneutral und produktunabhängig und verfügt über breite Umsetzungserfahrung in den Bereichen KI, Generative AI, AI-Agenten, MCP-Server, lokale LLM-Installationen, RAG-Integrationen, Fraud Detection, Marketing-Automatisierung, Kampagnenmanagement, Churn Prevention, Root Cause Analysis, Sprach- und Bilderkennung, Prozessautomatisierung, Datenstrategie, AI-Implementierung, Analytics-Plattformen sowie organisatorische Change Management-Projekte.

Zu den Kunden zählen namhafte Unternehmen wie Mercedes-Benz, Deutsche Bank, EnBW, REWE digital, GfK, arvato, TÜV Rheinland und Schwäbisch Hall.

Autor der Studie



Michael Oettinger ist Gründer und Geschäftsführer der **oetti-ds GmbH** und ausgewiesener Experte für Künstliche Intelligenz mit über 20 Jahren Projekterfahrung in den Bereichen Künstliche Intelligenz, Machine-Learning, Datenanalyse und Organisations.

Er hat zahlreiche erfolgreiche Projekte für führende Unternehmen umgesetzt und verfügt über fundierte Expertise in relevanten Technologien und Tools (u. a. SQL, Python, Generative AI, AI-Agenten, RAG, MCP-Server und Cloud-Plattformen).

Er ist Autor des Fachbuchs *Data Science & AI* (3. Auflage, 2023) und unterrichtet als Dozent für Künstliche Intelligenz an der Hochschule der Medien in Stuttgart.

 Bitte folgen sie mir auf LinkedIn: linkedin.com/in/michael-oettinger/

Wenn Sie Unterstützung bei der Vorbereitung auf den EU AI Act wünschen und mehr über unsere Methode der Kombination mit einem **AI-Growth-Projekt** erfahren möchten, freue ich mich über Ihre Kontaktaufnahme.



oetti-ds GmbH
Römerschanzenstr. 1
D - 82110 Germering
michael.oettinger@oetti-ds.de