Info zum EU AI Act:

Der EU AI Act, offiziell bekannt als ***Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz***, ist ein neues Gesetz der Europäischen Union, das am 1. August 2024 in Kraft getreten ist. Dieses Gesetz legt klare und einheitliche Regeln für den Einsatz von Künstlicher Intelligenz (KI) fest und zielt darauf ab, KI-Systeme in der EU sicherer und transparenter zu machen, während es gleichzeitig die Innovation fördert.

Diese abgestufte Herangehensweise sorgt für eine Balance zwischen der **Förderung von Innovation** und dem **Schutz der Bürger** vor potenziellen Risiken, die von KI ausgehen könnten. Der EU AI Act zielt somit darauf ab, KI-Anwendungen so zu regulieren, dass die **Grundrechte und die Sicherheit der Menschen gewahrt werden** und gleichzeitig Europa als Innovationsstandort für vertrauenswürdige und **ethische KI** gestärkt wird.

Der AI-Act stellt einen **einheitlichen Rechtsrahmen**; dadurch **Rechtssicherheit** für alle im Europäischen Wirtschaftsraum.

Der AI-Act stärkt das **Vertrauen** in die KI und fördert die **Akzeptanz**.

Der AI-Act zeigt Anbietern, Betreibern & Usern ihre **Handlungsfelder**.

Der EU AI Act regelt den Einsatz von KI in Unternehmen. Er definiert drei Hauptrollen: ***Anbieter***, ***Betreiber*** und ***Anwender***. Jede Nutzung von KI im Unternehmenskontext unterliegt diesen Vorschriften.

1. Anbieter (Provider)
Entwickeln oder lassen KI-Systeme entwickeln
Bringen KI-Systeme unter eigenem Namen/Marke auf den Markt
Tragen die umfangreichsten Verpflichtungen

2. Betreiber (Deployer)
Setzen KI-Systeme eigenverantwortlich im beruflichen Kontext ein
Integrieren KI in interne Prozesse
Haben weniger Pflichten als Anbieter, müssen aber Transparenz- und Sicherheitsregeln einhalten

3. Anwender (User)
Nutzen KI-Systeme ohne eigene Verantwortung
Haben die geringsten Pflichten
Private Nutzung fällt nicht unter den Geltungsbereich

Diese Rollendefinition bestimmt den Umfang der Verpflichtungen für Unternehmen im Umgang mit KI-Systemen.

Der EU AI Act arbeitet mit einem risikobasierten Ansatz und teilt KI-Anwendungen in vier Risikokategorien ein, die unterschiedlich reguliert werden:

1. Unannehmbares Risiko: KI-Systeme, die Menschen manipulieren, überwachen oder diskriminieren könnten, sind komplett verboten, da sie europäische Werte oder Grundrechte verletzen. Beispiele hierfür sind soziale Bewertungssysteme, wie sie teilweise in anderen Ländern (z.B. China) genutzt werden.

2. Hohes Risiko: KI-Systeme in diesem Bereich könnten die Gesundheit, Sicherheit oder Grundrechte beeinflussen. Sie unterliegen strengen Sicherheits- und Transparenzanforderungen. Dies betrifft z.B. KI in der medizinischen Diagnostik, biometrische Identifikationssysteme, oder bei der Auswahl von Bewerbern.

3. Begrenztes Risiko: Systeme, die direkt mit Menschen interagieren, wie Chatbots, müssen klar erkennbar machen, dass sie **KI** sind. Hier sollen die Nutzer informiert werden, dass sie es mit einer KI-Anwendung zu tun haben. Hierunter fällt auch der Einsatz von LLM-basierten Systemen (ChatGPT).

4. Minimales Risiko: Systeme, die kaum Risiken bergen, wie KI-gestützte Spiele oder Filter in Social Media, unterliegen keinen weiteren Auflagen.

Empfehlung: Unternehmen sollten immer eine **KI-Strategie** für sich entwickeln, Aus der KI-Strategie leiten sich die wesentlichen Handlungsfelder des AI-Acts ab. Ein interdisziplinäres Team (z.B. IT, Recht, Datenschutzbeauftragte, Compliance) sollte die Umsetzung überwachen. Falls nötig, ziehen Sie externe Beratung hinzu.

Handlungsbedarf für Unternehmen: (Details siehe Rückseite)

Kurzfristig (nächste 6–12 Monate)

1. Bestandsaufnahme:
   - Welche KI-Systeme werden eingesetzt?
   - In welche Risikokategorien fallen diese?
2. Konformitätsanalyse:
   - Prüfen Sie, ob bestehende Systeme die Anforderungen erfüllen.
   - Gegebenenfalls Zusammenarbeit mit Zertifizierungsstellen.
3. Mitarbeiterschulungen:
   - Aufklärung über den AI-Act und dessen Anforderungen.

Mittel- und langfristig (12–36 Monate)

4. Systemanpassung:
   - Upgrades oder Änderungen bei nicht-konformen Systemen.
5. Dokumentation:
   - Aufbau eines Compliance-Management-Systems.
6. Fortlaufende Überwachung:
   - Etablieren Sie Prozesse zur kontinuierlichen Bewertung der Systeme.

Anforderungen je Risikoklasse

a) Anbieter ***[Unternehmen, die KI-Systeme entwickeln oder bereitstellen]:***

- **Hohes Risiko**:
  - Durchführung einer **Risikobewertung**.
  - Einhaltung von **technischen und organisatorischen Maßnahmen** (z. B. robuste Datensicherheit, Nichtdiskriminierung).
  - **CE**-Kennzeichnung nach erfolgreicher Konformitätsbewertung.
  - Bereitstellung von **technischer Dokumentation** und **Nutzungsrichtlinien**.
- **Begrenztes Risiko**:
  - Offenlegung, dass Nutzer mit einer KI interagieren.
  - Sicherstellung der **Nachvollziehbarkeit** der KI-Funktion.
- **Minimales Risiko**:
  - Keine spezifischen regulatorischen Anforderungen.

b) Betreiber ***[Unternehmen, die KI-Systeme einsetzen]:***

- **Hohes Risiko**:
  - Überprüfung der **Konformität** der eingesetzten Systeme.
  - Durchführung von **Schulungen** für Nutzer und Personal.
  - Regelmäßige **Überwachung** und **Meldung von Vorfällen**.
- **Begrenztes Risiko**:
  - Transparente Kommunikation mit Kunden/Nutzern über die KI-Anwendung.
- **Minimales Risiko**:
  - Freie Nutzung, jedoch freiwillige Berücksichtigung ethischer Leitlinien empfohlen.

c) Anwender ***[Unternehmen, die KI in der Wertschöpfungskette nutzen]:***

- Sicherstellen, dass die genutzten KI-Systeme den regulatorischen Anforderungen entsprechen.
- Bewusstsein für die **rechtlichen und ethischen Auswirkungen** der genutzten Systeme.
- **Schulungen** der Mitarbeiter zur Nutzung und zum Umgang mit der KI.

GPAI: "**G**eneral **P**urpose **A**rtificial **I**ntelligence". GPAI-Systeme sind darauf ausgelegt, eine Vielzahl verschiedener Aufgaben zu lösen
Sie können in unterschiedlichsten Kontexten eingesetzt werden
Ihre Anwendungsmöglichkeiten sind nicht von vornherein festgelegt.

Wichtiger Hinweis: Die hier bereitgestellten Informationen dienen ausschließlich zur Orientierung und erheben nicht den Anspruch auf Vollständigkeit. Unternehmen sollten ihre KI-Produkte gründlich überprüfen, notwendige Maßnahmen, zur Einhaltung der geltenden EU-Vorschriften ergreifen und bei Bedarf rechtliche Beratung in Anspruch nehmen.

Hier ist eine detaillierte Übersicht der allgemeinen und bedingten Verpflichtungen, die alle Unternehmen im Europäischen Wirtschaftsraum (EWR) nach Inkrafttreten des EU AI Act einhalten müssen. Die Übersicht enthält Anforderungen für alle Unternehmen sowie spezifische Pflichten für solche, die KI-Systeme entwickeln, bereitstellen oder einsetzen.

Übersicht der Obliegenheiten für Unternehmen nach Inkrafttreten des EU AI Act

Obliegenheit	Gilt für alle Unternehmen?	Beschreibung	Bedingte Anforderungen / Details	Umsetzungsfrist
1. Prüfung und Kategorisierung der KI-Systeme	Ja	Unternehmen müssen alle KI-Systeme prüfen und entsprechend dem Risikolevel (gering, begrenzt, hoch, inakzeptabel) kategorisieren.	Besonders wichtig für Unternehmen mit potenziell risikoreichen Systemen.	Unverzüglich nach Inkrafttreten 01.08.2024
2. Vermeidung verbotener KI-Praktiken	Ja	Sicherstellen, dass verbotene KI-Praktiken, z.B. Echtzeit-Biometrie-überwachung oder emotionale Analyse am Arbeitsplatz, nicht genutzt werden.	**Nur wenn** solche Technologien zum Einsatz kommen oder entwickelt werden.	6 Monate nach Inkrafttreten 01.02.2025
3. Transparenz-anforderungen	Ja, bei Nutzung gewisser KI-Systeme	Unternehmen müssen Informationen bereitstellen, wenn ihre KI-Systeme Interaktionen mit Menschen haben.	**Beispiel**: Chatbots müssen die Benutzer darauf hinweisen, dass sie mit einem KI-System interagieren.	12 Monate nach Inkrafttreten 01.08.2025
4. Dokumentationspflicht	Nur bei Hochrisiko- und **GPAI**-Systemen	Technische Dokumentationen und Datenaufzeichnungen sind für alle Hochrisiko-KI-Systeme und General Purpose AI (GPAI) erforderlich.	Dokumentation sollte technische Details, Funktionsweise und Risikobewertungen enthalten.	12 Monate für GPAI; 36 Monate für Hochrisiko-KI 01.08.2025
5. Risikomanagement-Systeme für Hochrisiko-KI	Nur für Hochrisiko-KI-Systeme	Implementierung und regelmäßige Aktualisierung eines Risikomanagement-Systems, das die möglichen negativen Auswirkungen auf Gesundheit, Sicherheit und Grundrechte bewertet und minimiert.	**Erforderlich für** alle Unternehmen, die Hochrisiko-KI einsetzen.	36 Monate nach Inkrafttreten 01.08.2027
6. Konformitätsbewertung und Zertifizierung	Nur für Hochrisiko-KI-Systeme	Sicherstellen, dass alle Hochrisiko-KI-Systeme den festgelegten Konformitätsbewertungsprozessen unterzogen werden.	**Interne Überprüfung** möglich, aber bei manchen Systemen durch Dritte erforderlich.	36 Monate nach Inkrafttreten 02.08.2027
7. Meldung schwerwiegender Vorfälle und Fehlfunktionen	Ja, bei Hochrisiko-KI-Systemen	Unternehmen müssen ernsthafte Vorfälle oder Fehlfunktionen an die zuständigen Behörden melden und dokumentieren.	**Erforderlich, wenn** Hochrisiko-KI genutzt wird, z.B. bei Unfällen im Zusammenhang mit dem System.	Sofort nach Inkrafttreten 01.08.2024
8. Sicherheits- und Datenschutzmaßnahmen	Ja	Alle Unternehmen müssen die Sicherheit und den Datenschutz im Einklang mit DSGVO und ergänzenden Anforderungen des AI-Act gewährleisten.	**Bedingt auf Art der Daten**, z.B. biometrische Daten sind strenger reguliert.	Sofort nach Inkrafttreten 01.08.2024
9. Bereitstellung und Aktualisierung technischer Dokumentation für GPAI	Ja, bei **GPAI**-Anbietern	Unternehmen, die General Purpose AI (GPAI) Modelle bereitstellen, müssen technische Unterlagen erstellen und bereitstellen.	**Erforderlich** auch bei Updates oder wesentlichen Veränderungen des GPAI-Modells.	12 Monate nach Inkrafttreten 01.08.2025
10. Compliance durch Dritte (Outsourcing)	Nur bei externem Dienstleistereinsatz	Unternehmen, die externe Anbieter für ihre KI-Systeme beauftragen, müssen sicherstellen, dass diese den AI-Act einhalten.	**Zusatzpflicht**, wenn der Drittanbieter außerhalb der EU/EWR ansässig ist.	Sofort nach Inkrafttreten 01.08.2024
11. Schulung und Bewusstseinsschaffung im Unternehmen (AI Literacy)	Ja	Sensibilisierung der Mitarbeitenden für die Vorschriften des AI-Act und die spezifischen Anforderungen an den Umgang mit KI.	**Erforderlich für** alle Mitarbeiter, die KI einsetzen oder überwachen.	12 Monate nach Inkrafttreten 01.08.2025
12. Berichtspflichten und Zusammenarbeit mit Behörden	Nur für Hochrisiko-KI-Systeme und **GPAI**	Zusammenarbeit mit den Aufsichtsbehörden durch Berichte und Bereitstellung von Informationen bei Nachfragen.	**Erforderlich bei** relevanten Anfragen oder Prüfungen durch Behörden.	Sofort nach Inkrafttreten 01.08.2024