EU KI-Gesetz

Verordnung (EU) 2024/1689 · AI Act

Verständliche Zusammenfassung für Unternehmen in der Schweiz, Deutschland, Österreich, das Fürstentum Liechtenstein und alle andern die KI in der EU einsetzen.

Das Original: 144 Seiten und über 83 000 Wörter. Diese Zusammenfassung bringt das Wesentliche auf knapp 2 000 Wörter, ohne dass dabei etwas Wichtiges verloren geht.

Erstellt durch

Fritz J. Bicker

BAV Trend GmbH · Zürich

www.bav.ch

Stand: April 2026 · Dient der allgemeinen Information. Ersetzt keine Rechtsberatung.

1. Einleitung: Was ist der EU AI Act?

Am 12. Juli 2024 wurde die Verordnung (EU) 2024/1689 im Amtsblatt der Europäischen Union veröffentlicht. Sie ist das erste umfassende Gesetz weltweit, das künstliche Intelligenz rechtsverbindlich reguliert.

Das Original umfasst 144 Seiten und über 83 000 Wörter juristisches EU-Deutsch. Diese Zusammenfassung bringt das Wesentliche auf knapp 2 000 Wörter, ohne dass dabei etwas Wichtiges verloren geht.

Der AI Act verfolgt zwei Hauptziele: ein hohes Schutzniveau für Grundrechte und Sicherheit, sowie die Förderung von Innovationen im europäischen Binnenmarkt.

Auch Schweizer Unternehmen sind direkt betroffen: Wer KI-Systeme in der EU einsetzt, anbietet oder deren Ausgaben dort nutzt, unterliegt dem Gesetz.

Rechtsform	EU-Verordnung – direkt anwendbar in allen EU-Mitgliedstaaten ohne nationale Umsetzungsgesetze.
Geltungsbereich	Alle Anbieter, Betreiber und Einführer von KI-Systemen in der EU sowie Unternehmen ausserhalb der EU, deren KI-Ausgaben in der EU verwendet werden.
KMU CH, D, A, FL	Direkt betroffen, wenn KI-Produkte oder -Dienste in EU-Ländern eingesetzt werden. Indirekt betroffen über Lieferanten und Kundenbeziehungen.

2. Der risikobasierte Ansatz

Der AI Act arbeitet mit einem Stufensystem: Je höher das Risiko, desto strenger die Anforderungen. Entscheidend ist nicht die Technologie selbst, sondern der Verwendungszweck.

Risikostufe	Beispiele	Rechtliche Folge
Inakzeptables Risiko	Social Scoring, Manipulation, biometrische Massenüberwachung	Vollständiges Verbot
Hohes Risiko	Personalwesen, Bildung, Kredit, Justiz, kritische Infrastruktur	Strenge Pflichten: Konformitätsbewertung, Dokumentation, Registrierung
Begrenztes Risiko	Chatbots, Deepfakes, Emotionserkennung	Transparenzpflichten und Kennzeichnung als KI
Minimales Risiko	Spamfilter, KI in Spielen, einfache Empfehlungen	Keine spezifischen Pflichten, freiwillige Kodizes empfohlen

Beispiel: Ein Gesichtserkennung-System in einem Videospiel gilt als minimales Risiko. Dasselbe System bei einer Polizeibehörde ist Hochrisiko.

3. Verbotene KI-Praktiken (Kapitel II)

Einige KI-Anwendungen sind generell verboten, weil sie als unvereinbar mit demokratischen Grundwerten gelten. Diese Verbote sind mit wenigen engen Ausnahmen absolut.

3.1 Absolute Verbote

- Unterschwellige Manipulation, die das Verhalten von Personen ohne deren Wissen wesentlich beeinflusst.
- Ausnutzen von Schwächen vulnerabler Gruppen (Kinder, ältere Menschen, Personen mit Behinderungen).
- Social Scoring durch staatliche Behörden: Bewertung von Personen nach sozialem Verhalten.
- Prädiktive Polizeiarbeit allein auf Basis von Profilbildung, ohne konkreten Verdacht.
- Erstellung biometrischer Datenbanken aus dem Internet oder Überwachungsmaterial ohne Einwilligung.
- Biometrische Kategorisierung nach Rasse, politischer Meinung, Religion oder Sexualität.
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen.

3.2 Biometrische Echtzeit-Identifizierung im öffentlichen Raum

Grundsätzlich verboten. Enge Ausnahmen für Strafverfolgungsbehörden bei terroristischen Bedrohungen, vermissten Personen oder der Verfolgung schwerer Straftaten. Jede Nutzung bedarf richterlicher Genehmigung.

4. Hochrisiko-KI-Systeme (Kapitel III)

Hochrisiko-KI-Systeme unterliegen den strengsten Anforderungen des AI Act. Anbieter und Betreiber müssen umfangreiche Pflichten erfüllen, bevor ein solches System eingesetzt werden darf.

4.1 Was gilt als Hochrisiko?

Hochrisiko-KI liegt vor, wenn ein System als Sicherheitsbauteil eines regulierten Produkts eingesetzt wird oder in einem dieser Bereiche tätig ist:

- Kritische Infrastruktur: Strom-, Wasser-, Verkehrsnetze.
- Bildung: Entscheide über Zulassung, Prüfungen, Leistungsbewertung.
- Beschäftigung: Einstellung, Beurteilung, Entlassung, Aufgabenverteilung.
- Wesentliche Dienstleistungen: Kreditvergabe, Sozialleistungen, Krankenversicherung.
- Strafverfolgung: Risikobewertung von Personen, Beweisanalyse.
- Migration und Asyl: Antragsbearbeitung, Risikoeinschätzung.
- Justiz und demokratische Prozesse: KI-gestützte Rechtsprechung oder Wahlbeeinflussung.

4.2 Pflichten für Anbieter und Betreiber

Pflichten für Anbieter (Hersteller)

- Konformitätsbewertung vor dem Inverkehrbringen durchführen
- Umfangreiche technische Dokumentation erstellen und pflegen
- Robustes Risikomanagementsystem implementieren
- System in EU-Datenbank registrieren und CE-Kennzeichnung anbringen
- Logging-Funktion für Nachverfolgbarkeit sicherstellen
- Nutzer mit klaren Informationen und Gebrauchsanweisungen versorgen

Pflichten für Betreiber (Nutzer des Systems)

- Anweisungen des Anbieters befolgen, technische Dokumentation aufbewahren
- Menschliche Aufsicht sicherstellen: Eingriffs- und Stopp-Möglichkeit jederzeit gewährleisten
- Mitarbeitende entsprechend schulen und einweisen
- System nur für vorgesehene Zwecke einsetzen
- Schwerwiegende Vorfälle und Fehlfunktionen melden

5. Transparenzpflichten (Kapitel IV)

Auch KI-Systeme mit begrenztem Risiko unterliegen spezifischen Transparenzanforderungen. Menschen sollen immer wissen, wenn sie mit einer KI interagieren.

- Chatbots und konversationelle KI: Personen müssen darüber informiert werden, dass sie mit einer KI kommunizieren.
- Deepfakes und synthetische Inhalte (Bilder, Audio, Video, Text): Müssen als KI-generiert gekennzeichnet werden.
- Emotionserkennungssysteme: Betroffene Personen müssen informiert werden.
- Biometrische Kategorisierungssysteme: Informationspflicht gegenüber betroffenen Personen.

6. KI-Modelle mit allgemeinem Verwendungszweck (Kapitel V)

Sogenannte GPAI-Modelle (General Purpose AI) wie ChatGPT, Gemini oder Claude unterliegen eigenen Regeln. Das Gesetz unterscheidet zwischen regulären Modellen und solchen mit systemischem Risiko.

6.1 Pflichten für alle GPAI-Anbieter

- Technische Dokumentation erstellen und pflegen.
- Urheberrechte der Trainingsdaten beachten, Verwendungsrichtlinien veröffentlichen.
- Zusammenfassung des Trainings-Datensatzes bereitstellen.

6.2 GPAI mit systemischem Risiko (z.B. sehr grosse Modelle)

- Adversarielle Tests und Red-Team-Übungen durchführen.
- Schwerwiegende Vorfälle an EU-Behörden melden.
- Cybersicherheitsschutz und Energieeffizienz berichten.

7. Sanktionen und Haftung (Kapitel XII)

Der AI Act sieht erhebliche Bussgelder vor. Sie bemessen sich am weltweiten Jahresumsatz und orientieren sich am DSGVO-Modell.

Verstoss	Max. Bussgeld	Alternativ (% Umsatz)
Verletzung der Verbote (Art. 5)	**35 Mio. EUR**	7 % Jahresumsatz
Verletzung sonstiger Pflichten	**15 Mio. EUR**	3 % Jahresumsatz
Falsche Angaben gegenüber Behörden	7,5 Mio. EUR	1 % Jahresumsatz

Für KMU und Start-ups gelten in der Regel Reduktionen. Massgeblich ist stets der höhere der beiden Beträge.

8. Zeitplan und Übergangspflichten

Der AI Act tritt schrittweise in Kraft. Unternehmen haben Zeit, ihre Systeme und Prozesse anzupassen.

Datum	Phase	Was gilt ab dann?
Aug. 2024	Inkrafttreten	Verordnung tritt in Kraft. 20 Tage nach Veröffentlichung.
Feb. 2025	Phase 1	Verbotene KI-Praktiken gelten. KI-Kompetenzpflicht tritt in Kraft.
Aug. 2025	Phase 2	Regeln für GPAI-Modelle (z.B. ChatGPT, Gemini) gelten.
Aug. 2026	Phase 3	Governance und Marktüberwachung. KI-Reallabore einsatzbereit.
Aug. 2027	Phase 4	Alle Hochrisiko-KI-Pflichten vollständig anwendbar.

Für Hochrisiko-KI-Systeme, die vor August 2026 bereits in Betrieb sind, gelten Übergangsfristen bis 2030.

9. GO und NO-GO: Was ist erlaubt, was verboten?

Die wichtigsten praktischen Handlungsanweisungen für Unternehmen auf einen Blick:

GO Erlaubt und empfohlen	NO-GO Verboten oder stark eingeschränkt
✓ KI-Systeme mit Transparenz und menschlicher Aufsicht einsetzen	✗ KI einsetzen, um Menschen unterschwellig zu manipulieren
✓ KI-Ausgaben als solche kennzeichnen (Chatbots, Deepfakes, synthetische Texte)	✗ Soziale Bewertungssysteme (Social Scoring) für Bürger betreiben
✓ Für Hochrisiko-KI: technische Dokumentation führen und aktuell halten	✗ Biometrische Echtzeit-Überwachung im öffentlichen Raum (ausser enge Ausnahmen)
✓ Mitarbeitende über KI-Grundlagen schulen (Kompetenzpflicht ab Feb. 2025)	✗ KI nutzen, um Schwächen vulnerabler Gruppen auszunutzen
✓ KI-Systeme vor dem Einsatz auf Risikostufe prüfen	✗ Hochrisiko-KI ohne menschliche Aufsicht einsetzen
✓ Für Hochrisiko-KI: Register in EU-Datenbank anlegen	✗ KI für Entscheide in Bildung oder Personalwesen ohne Transparenz verwenden
✓ Datensätze für KI-Training dokumentieren und auf Qualität prüfen	✗ Emotionserkennung am Arbeitsplatz oder in Schulen ohne Einwilligung
✓ Logging und Protokollierung für kritische KI-Entscheide sicherstellen	✗ Prädiktive Polizeiarbeit auf Personenebene ohne konkreten Verdacht
✓ KI-Lieferanten auf AI-Act-Konformität prüfen	✗ Synthetische Inhalte (Deepfakes) ohne Kennzeichnung verbreiten
✓ Interne KI-Governance aufbauen (Verantwortlichkeiten, Prozesse)	✗ Hochrisiko-KI ohne Konformitätsbewertung und CE-Kennzeichnung einsetzen

10. Kurzübersicht: Der AI Act in 10 Sätzen

Das EU KI-Gesetz auf einen Blick

1. KI ist nützlich, kann aber schaden. Das Gesetz schützt Menschen und fördert gleichzeitig Innovation.
2. Je gefährlicher eine KI-Anwendung, desto strenger die Regeln. Es gibt vier Risikostufen.
3. Einige KI-Anwendungen sind absolut verboten: Manipulation, Social Scoring, Massenüberwachung.
4. Hochrisiko-KI in Personalwesen, Bildung oder Kredit braucht strenge Prüfungen und Dokumentation.
5. Wer mit einem Chatbot spricht, muss wissen, dass es kein Mensch ist.
6. Deepfakes und KI-generierte Inhalte müssen als solche gekennzeichnet werden.
7. KI darf nie ganz allein entscheiden: Menschliche Kontrolle bleibt immer Pflicht.
8. Auch Schweizer Unternehmen sind betroffen, sobald ihre KI in der EU genutzt wird.
9. Verstösse kosten bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.
10. **Jetzt handeln: Die ersten Regeln gelten bereits seit Februar 2025.**

11. Handlungsempfehlungen Unternehmen

Auch wenn die Schweiz nicht EU-Mitglied ist: Wer KI-Systeme in EU-Ländern einsetzt, vermarktet oder EU-Kunden hat, ist direkt betroffen.

Kurzfristig (bis Ende 2025)

- KI-Inventar erstellen: Welche KI-Systeme setzen wir ein? Wofür?
- Risikoeinstufung vornehmen: Fällt eines unserer Systeme in die Hochrisikokategorie?
- Verbotene Praktiken eliminieren: Sofortige Compliance mit Kapitel II.
- Transparenzpflichten umsetzen: Kennzeichnung bei Chatbots und KI-generierten Inhalten.
- KI-Kompetenz aufbauen: Mitarbeitende schulen.

Mittelfristig (2025–2027)

- Governance-Struktur entwickeln: Wer ist intern verantwortlich für KI-Compliance?
- Lieferantenmanagement: Verträge mit KI-Anbietern auf AI-Act-Konformität prüfen.
- Dokumentation aufbauen: Technische Unterlagen und Risikoabschätzungen für Hochrisiko-KI.
- Meldeprozesse etablieren: Wie melden wir schwerwiegende KI-Vorfälle?

BAV Trend GmbH begleitet Sie

Wir unterstützen Unternehmen bei der strukturierten Einführung von KI: von der Risikobewertung über die Entwicklung interner Governance bis zur praxisnahen Schulung Ihrer Teams. Unser Ansatz: Human-Centered AI, bei dem der Mensch immer die Kontrolle behält. Darüber hinaus arbeiten wir in allen Bereichen der Unternehmensorganisation um für Sie das Optimum herauszuholen.

Diese Zusammenfassung dient der allgemeinen Orientierung und ersetzt keine rechtliche oder fachliche Beratung. Sie basiert auf der Verordnung (EU) 2024/1689 vom 12. Juli 2024.

BAV Trend GmbH
Hohensteinweg 22
8055 Zuerich
Switzerland

www.bav.ch
info@bav.ch

Stand: April 2026