EU AI Act — Self-Assessment Checkliste 2026

Für KMU und Mittelstand mit KI-Einsatz · Stand: Q3 2026

BRAINMAZE
brain-maze.de

Für wen? Unternehmen, die KI-Systeme einsetzen oder entwickeln und prüfen wollen, ob und welche Anforderungen des EU AI Act gelten. Ersetzt keine Rechtsberatung — schafft aber die Grundlage für ein strukturiertes Gespräch mit Juristen oder einem KI-Compliance-Beauftragten.
Felder mit Stern (*) sind Pflichtanforderungen für Hochrisiko-KI-Systeme (Annex III).

T Zeitplan — was gilt wann

AUG 2024	FEB 2025	AUG 2025	AUG 2026 ←
In Kraft getreten	Verbotene Praktiken (Art. 5) — bereits anwendbar	Governance & GPAI-Modelle (Kap. III, V)	Hochrisiko-KI (Annex III) vollständig anwendbar

Aug 2027: Hochrisiko-KI in bestehenden regulierten Produkten (Medizinprodukte, Fahrzeuge)

1 Bin ich betroffen?

- [ ] Mein Unternehmen entwickelt, vertreibt oder betreibt Systeme auf Basis von maschinellem Lernen, statistischen Methoden oder regelbasierter KI — *Weite Definition*
- [ ] Diese Systeme werden in der EU genutzt oder sind für EU-Nutzer bestimmt (Marktortprinzip gilt auch für Non-EU-Anbieter)
- [ ] Rolle geklärt: Bin ich **Anbieter** (entwickelt / in Verkehr bringt) oder **Deployer** (setzt im eigenen Betrieb ein) — oder beides? — *Pflichten unterscheiden sich*
- [ ] Ausnahmen geprüft: militärische/nationale Sicherheit, rein private Nutzung ohne Inverkehrbringen, reine Forschung & Entwicklung ohne Echtbetrieb — *Ggf. nicht betroffen*

2 Verbotene Praktiken — sofortige Prüfung (seit Feb 2025 in Kraft)

- [ ] Kein System, das Personen durch unterschwellige oder täuschende Techniken beeinflusst *
- [ ] Kein System, das Schutzbedürftigkeit von Personen ausnutzt (Alter, Behinderung, wirtschaftliche Lage) *
- [ ] Kein Social-Scoring-System, das Verhalten im Privatbereich bewertet und zu nachteiligen Konsequenzen führt *
- [ ] Keine Echtzeit-Biometrie zur Massenidentifikation im öffentlichen Raum (eng begrenzte Ausnahmen für Strafverfolgung) *
- [ ] Keine Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen — außer aus medizinischen oder Sicherheitsgründen *
- [ ] Keine biometrischen Kategorisierungssysteme auf Basis sensibler Merkmale (Rasse, politische Meinung, Religion, Gewerkschaft) *

3 Risikoklassifizierung — welche Kategorie trifft auf meine Systeme zu?

Kategorie	Typische Anwendungen	Konsequenz
Verboten	Social Scoring, Subliminal Manipulation, biometrische Massenüberwachung	Sofortige Einstellung. Bußgeld bis 35 Mio. € / 7 % Jahresumsatz
Hochrisiko (Annex III)	Bewerberselektion, Kreditwürdigkeitsprüfung, medizinische Diagnose, kritische Infrastruktur, biometrische Identifikation	Vollständige Compliance-Dokumentation, CE-Kennzeichnung, Registrierung in EU-Datenbank
Geringes Risiko	Chatbots, KI-generierte Texte/Bilder/Videos, Deepfake	Transparenzpflicht: Nutzer muss wissen, dass er mit KI interagiert
Minimales Risiko	Spam-Filter, KI-Produktempfehlungen, einfache Prozessautomatisierung	Keine Pflichtanforderungen — freiwillige Kodizes empfohlen

4 Hochrisiko-Pflichten — gilt nur bei Annex III-Systemen

- [ ] Risikomanagement-System dokumentiert: laufender Prozess zur Identifikation, Bewertung und Minderung von Risiken *
- [ ] Data Governance: Trainingsdaten dokumentiert — Herkunft, Qualität, bekannte Biases, Vorverarbeitungsschritte *
- [ ] Technische Dokumentation erstellt (Annex IV): Systemarchitektur, Trainingsprozess, Validierung, Leistungsmetriken *
- [ ] Automatisches Logging aktiviert: relevante Ereignisse werden während des Normalbetriebs automatisch protokolliert *
- [ ] Transparenz gegenüber Deployern: Gebrauchsanweisung mit Zweck, Einschränkungen, Leistungskennzahlen, Wartungshinweisen *
- [ ] Human Oversight sichergestellt: Menschen können das System überwachen, pausieren oder außer Kraft setzen — technisch implementiert *
- [ ] Genauigkeit, Robustheit und Cybersicherheit nach Stand der Technik — definierte Metriken und Testergebnisse dokumentiert *
- [ ] Konformitätsbewertung abgeschlossen (Selbst- oder Drittpartei) und EU-Konformitätserklärung ausgestellt *
- [ ] Registrierung in der EU-KI-Datenbank vor Inverkehrbringen abgeschlossen *

* Primär Pflicht für Anbieter. Deployer haben abgestufte eigene Pflichten (Art. 26 EU AI Act).

5 Schnittstelle DSGVO — wo sich die Regelwerke überschneiden

- [ ] Datenschutz-Folgenabschätzung (DSFA, Art. 35 DSGVO) wurde für alle KI-Systeme mit personenbezogenen Daten durchgeführt — *Oft Pflicht bei Hochrisiko-KI*
- [ ] Automatisierte Entscheidungen mit erheblicher Wirkung (Art. 22 DSGVO): Betroffene werden informiert, Widerspruchsrecht ist implementiert — *Kreditvergabe, HR-Screening*
- [ ] Auftragsverarbeitungsvertrag (AVV) mit allen KI-Dienstleistern abgeschlossen, die personenbezogene Daten verarbeiten
- [ ] Drittlandtransfer geprüft: Werden personenbezogene Daten zur KI-Verarbeitung an US-Anbieter übermittelt? Standard-Vertragsklauseln (SCC) vorhanden? — *US Cloud Act — kritischer Punkt*
- [ ] Datenschutzerklärung aktualisiert: alle KI-gestützten Verarbeitungen sind transparent und vollständig benannt
- [ ] Besondere Kategorien (Art. 9 DSGVO) geprüft: Werden Gesundheits-, biometrische oder politische Daten im KI-System verarbeitet? — *Verschärfte Anforderungen*

6 Sofortmaßnahmen — strukturierter Einstieg

KI-Inventar erstellen	SOFORT	Vollständige Liste aller im Unternehmen genutzten oder entwickelten KI-Systeme mit Beschreibung, Anbieter, Zweck und verarbeiteten Daten.
Risikoklasse bestimmen	SOFORT	Für jedes System aus dem Inventar: Verboten / Hochrisiko (Annex III) / Geringes Risiko / Minimal? Annex III als Prüfmaßstab verwenden.
Anbieter- oder Deployer-Rolle	SOFORT	Wer hat das System entwickelt — Sie selbst oder ein Dritter? Bestimmt Ihre gesetzlichen Pflichten grundlegend.
KI-Verantwortlichen benennen	KURZFRISTIG	Interne Koordinationsrolle analog zum Datenschutzbeauftragten. Muss kein Jurist sein — aber strukturiert den Prozess.
Dokumentationslücken schließen	KURZFRISTIG	Fehlende technische Dokumentation für bestehende Hochrisiko-Systeme vor August 2026 nachholen.
Drittanbieter-Verträge prüfen	KURZFRISTIG	KI-Tools von OpenAI, Microsoft, Google etc.: Welche AI-Act-Konformität sichert der Anbieter vertraglich zu?
Mitarbeitende schulen	MITTELFRISTIG	Alle Mitarbeitenden, die Hochrisiko-KI einsetzen, müssen gemäß Art. 26(6) EU AI Act nachweislich geschult sein.

Bußgeldrahmen EU AI Act

Verbotene Praktiken (Art. 5)	**bis 35 Mio. € oder 7 %**
Sonstige Verstöße	bis 15 Mio. € oder 3 %
Falsche Angaben ggü. Behörden	bis 7,5 Mio. € oder 1 %

Basis: globaler Jahresumsatz, der jeweils höhere Wert gilt. KMU-Deckelung vorgesehen.

Auswertung dieser Checkliste

Blöcke 1–2 vollständig	Grundpflichten erfüllt
Block 3: nur Minimal/Gering	Kein Hochrisiko-Audit nötig
Block 4 unvollständig	Handlungsbedarf vor Aug 2026
Block 5 mit Lücken	DSGVO + AI-Act-Risiko

BrainMaze Limited · Larnaca, Zypern
EU-USt-ID: CY 601 267 54E

Stand: Q3 2026 · Aktuelle Version unter brain-maze.de