

KI-Risikoklassifizierungs-Checkliste

EU-KI-Gesetz (Verordnung 2024/1689) · Schritt-für-Schritt-Entscheidungsbaum für Betreiber
· DE

Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · Bereitgestellt von ETHYX · Version 1.2 · September 2026 ·
Keine Rechtsberatung

ANLEITUNG Arbeiten Sie für jedes KI-System in Ihrem Inventar die Schritte 1–5 der Reihe nach durch. Hören Sie auf, sobald Sie ein Ergebnis erreichen – fahren Sie nicht mit dem nächsten Schritt fort. Füllen Sie für jedes KI-System eine Checkliste aus. Bewahren Sie ausgefüllte Checklisten in Ihrer KI-Dokumentationsakte auf.

**Zu
klassifizierendes
System:**

**Referenz (aus KI-
Inventar):**

Ausgefüllt von:

Datum:

Kreuzen Sie jedes zutreffende Kästchen an. Wenn eines angekreuzt ist → Ergebnis: VERBOTEN – nicht einsetzen.

SCHRITT 1 Ist das System VERBOTEN? (Art. 5 EU-KI-Gesetz)

- ☐ Unterschwellige, manipulative oder täuschende Techniken zur Verzerrung des Verhaltens auf eine Weise, die Schaden verursacht oder verursachen kann (Art. 5(1)(a)).
- ☐ Ausnutzung von Schwachstellen bestimmter Gruppen (Alter, Behinderung, soziale/wirtschaftliche Lage) zur Verhaltensverzerrung und Schadensverursachung (Art. 5(1)(b)).
- ☐ Biometrische Kategorisierung von Personen anhand sensibler Merkmale zur Ableitung von Rasse, politischen Meinungen, Gewerkschaftsmitgliedschaft, religiösen Überzeugungen, sexueller Orientierung (Art. 5(1)(g)). Ausnahmen für Strafverfolgung gelten – spezialisierte Rechtsberatung erforderlich.
- ☐ Echtzeit-Fernbiometrie (z. B. Gesichtserkennung) an öffentlich zugänglichen Orten für die Strafverfolgung (Art. 5(1)(h), mit engen Ausnahmen in (h)(i)–(iii)). Enge Ausnahmen für Strafverfolgung – spezialisierte Beratung erforderlich.
- ☐ Social Scoring durch öffentliche Stellen: Beurteilung von Personen anhand ihres Sozialverhaltens oder persönlicher Merkmale für nachteilige Behandlung (Art. 5(1)(c)).
- ☐ Individuelle Kriminalitätsrisikobewertung oder Rückfallprognose ausschließlich auf Basis von Profiling (Art. 5(1)(d)).
- ☐ Emotionserkennung an Arbeitsplätzen oder in Bildungseinrichtungen – außer für spezifische medizinische oder Sicherheitszwecke (Art. 5(1)(f)).
- ☐ Erstellung oder Erweiterung von Gesichtserkennungsdatenbanken durch ungezieltes Scraping von Gesichtsbildern aus dem Internet oder Videoüberwachung (Art. 5(1)(e)).
- ☐ KI-Systeme, die nicht einvernehmliche intime Darstellungen oder Darstellungen sexuellen Kindesmissbrauchs erzeugen oder manipulieren (Art. 5, ergänzt durch die Verordnung (EU) 2026/1744, den Digital Omnibus 2026; Umsetzung bis 2. Dezember 2026).

SCHRITT 1**Ist das System VERBOTEN? (Art. 5 EU-KI-Gesetz)**

- ☐ KEINES der oben genannten trifft zu → weiter zu Schritt 2.
- ☐ EINES ODER MEHRERE trifft zu → ERGEBNIS: VERBOTEN. Setzen Sie dieses System nicht ein. Rechtsberatung einholen.

Kreuzen Sie jedes zutreffende Kästchen an. Ein Kreuz = Ergebnis HOHES RISIKO. Beide Teilprüfungen gelten unabhängig.

2A – Sicherheitskomponente eines Annex-I-regulierten Produkts (Art. 6(1)):

SCHRITT 2**Ist das System HOCHRISIKO? (Art. 6, Anhang I & III)**

- ☐ Maschinen, Spielzeug, Freizeitboote, Aufzüge, Geräte für explosionsgefährdete Bereiche, Funkanlagen, Druckgeräte, Medizinprodukte (inkl. In-vitro-Diagnostika), Zivilluftfahrt, Eisenbahnsysteme, Kraftfahrzeuge, landwirtschaftliche Maschinen.
- ☐ 2B – In Anhang III aufgeführt (Art. 6(2)) – acht Hochrisikokategorien:
 - ☐ Biometrische Identifizierung und Kategorisierung natürlicher Personen. Ausgen.: Verifikation, Barrierefreiheit, Sicherheit.
 - ☐ Verwaltung und Betrieb kritischer Infrastruktur (Strom, Wasser, Gas, Verkehr, Digital).
 - ☐ Allgemeine und berufliche Bildung: KI, die den Zugang, Zulassung, Beurteilung oder Qualifikation entscheidet oder beeinflusst.
 - ☐ Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit: Einstellung, Auswahl, Leistungsbeurteilung, Beförderung, Kündigung, Aufgabenverteilung, Überwachung. Häufigster Auslöser für KMU – z. B. Lebenslauf-Screening, Anwesenheitsüberwachung.
 - ☐ Zugang zu und Inanspruchnahme von wesentlichen Privatdienstleistungen und öffentlichen Leistungen: Kreditbewertung, Versicherungsrisikobewertung, Notfallentsendung, Sozialleistungen.
 - ☐ Strafverfolgung: individuelle Risikobeurteilungen, Polygraphen, Beweiswürdigung, Kriminalitätsanalyse, Profiling.
 - ☐ Migration, Asyl und Grenzkontrolle.
 - ☐ Justizverwaltung und demokratische Prozesse.
- ☐ KEINES der oben genannten trifft zu → weiter zu Schritt 3.
- ☐ EINES ODER MEHRERE trifft zu → ERGEBNIS: HOHES RISIKO. Betreiberpflichten gemäß Art. 26 EU-KI-Gesetz gelten. Betreiberdokumentationspaket ausfüllen. Grundrechte-Folgenabschätzung (Art. 27) kann erforderlich sein. Bußgeld: bis zu 15 Millionen Euro oder 3 % des globalen Jahresumsatzes. Für KMU und Start-ups gilt nach Art. 99(6) der jeweils niedrigere der beiden Werte statt des höheren.

KMU ist hier die Definition der Verordnung selbst: weniger als 250 Beschäftigte und bis zu 50 Mio. € Jahresumsatz oder bis zu 43 Mio. € Bilanzsumme (Empfehlung 2003/361/EG). Die DSGVO kennt keine solche Regel – beide Stufen gelten unabhängig von der Unternehmensgröße.

KI-Mehrzweckmodelle werden auf großen Datenmengen trainiert und können viele Aufgaben erfüllen (z. B. GPT-4, Claude, Gemini, Llama). Als Betreiber sind Sie nicht der Anbieter des GPAI-Modells – Ihre Pflichten hängen davon ab, wie Sie es nutzen.

SCHRITT 3

Ist dies ein KI-Mehrzwecksystem (GPAI)? (Art. 51)

- ☐ Sie verwenden ein GPAI-Modell oder ein darauf aufgebautes Produkt (z. B. ein LLM-gestützter Chatbot, Copilot, eine Empfehlungsmaschine).
- ☐ Das von Ihnen genutzte GPAI-Modell wurde vom EU-KI-Büro als Modell mit 'systemischem Risiko' eingestuft (typischerweise: $>10^{25}$ FLOPs Trainingsrechnen).

Wenn Sie das erste Kästchen angekreuzt haben: Klassifizieren Sie den <i>Anwendungsfall</i> anhand der Schritte 1–2 und 4. Ein für internes Verfassen verwendetes GPAI-Modell = minimales Risiko. Dasselbe Modell für HR-Screening = wahrscheinlich hohes Risiko. Wenn Sie das zweite Kästchen angekreuzt haben: Zusätzliche Pflichten können gelten – konsultieren Sie die Dokumentation Ihres Anbieters.

Kreuzen Sie jedes zutreffende Kästchen an. Ein Kreuz = Transparenzpflicht, kein Verbot oder vollständige Compliance-Last.

SCHRITT 4

Gilt eine BEGRENZTE RISIKO-Transparenzpflicht? (Art. 50)

- ☐ KI-Chatbot oder virtueller Assistent im Umgang mit Menschen (außer wenn offensichtlich, dass es sich um KI handelt).
- ☐ KI-System, das synthetische Audio-, Bild-, Video- oder Textinhalte erzeugt, die für echt gehalten werden könnten (Deepfake oder synthetische Inhalte).
- ☐ Emotionserkennungssystem oder biometrisches Kategorisierungssystem (noch nicht als Hochrisiko in Schritt 2 eingestuft).
- ☐ KI-generierte Inhalte: Text, Bilder, Audio, Video, die von KI produziert und anderen präsentiert werden (Kennzeichnung erforderlich).
- ☐ KEINES trifft zu → weiter zu Schritt 5.
- ☐ → ERGEBNIS: BEGRENZTES RISIKO. Transparenzoffenlegung implementieren und dokumentieren. Bußgeld bei Nichtkonformität: bis zu 15 Millionen Euro oder 3 % des globalen Jahresumsatzes (Art. 99(4)). Für KMU und Start-ups gilt nach Art. 99(6) der jeweils niedrigere der beiden Werte statt des höheren.

Art. 50 verlangt, dass Sie Personen klar darüber informieren, dass sie mit KI oder KI-generierten Inhalten interagieren. Implementieren Sie ein Offenlegungsbanner, eine Gesprächseröffnung oder ein Label. Verwenden Sie die Art. 50-Vorlage im Betreiberdokumentationspaket.

Wenn Sie Schritt 5 erreicht haben, fällt das System in keine höhere Risikokategorie. Es gibt keine Pflichten gemäß EU-KI-Gesetz – aber verantwortungsvolle Nutzungspraktiken gelten.

SCHRITT 5

MINIMALES RISIKO (Standard für alle verbleibenden Systeme)

- ☐ Dokumentieren Sie das System in Ihrem KI-System-Inventar mit Risikoeinstufung = Minimales Risiko.
- ☐ Bestätigen Sie, dass die beabsichtigte Nutzung mit der Nutzungsrichtlinie des Anbieters übereinstimmt.
- ☐ Informieren Sie Mitarbeitende über Fähigkeiten und Grenzen des Tools (Art. 4 KI-Kompetenz).

- ☐ Überprüfen Sie die Einstufung jährlich oder bei wesentlichen Änderungen des Anwendungsfalls.
- ☐ → ERGEBNIS: MINIMALES RISIKO. Dokumentieren und fortfahren. Keine Pflichten gemäß EU-KI-Gesetz über gute Praxis hinaus.
- ☐ ERGEBNISZUSAMMENFASSUNG – Klassifizierung hier festhalten
- ☐ Klassifizierungsergebnis: ☐ Verboten ☐ Hohes Risiko ☐ Begrenztes Risiko ☐ Minimales Risiko ☐ In Prüfung
- ☐ Begründung (Zusammenfassung):

- ☐ Erforderliche nächste Schritte:

- ☐ Geprüft und freigegeben von: _____ (Name) _____ (Datum)

Keine EU-KI-Gesetz-Bußgeldstufe für Systeme mit minimalem Risiko – aber die DSGVO kann dennoch gelten, wenn personenbezogene Daten verarbeitet werden. Prüfen Sie Ihr KI-System-Inventar auf etwaige DSGVO-Pflichten (AVV, VVT-Eintrag usw.).

Diese Checkliste dient nur als Orientierung und stellt keine Rechtsberatung dar. Sie basiert auf der Verordnung (EU) 2024/1689 (EU-KI-Gesetz) in der durch die Verordnung (EU) 2026/1744 (Digital Omnibus 2026) geänderten Fassung (beschlossen Juni 2026; danach gelten die Pflichten für eigenständige Hochrisiko-Systeme nach Anhang III, einschließlich der Betreiberpflichten aus Art. 26/27, ab dem 2. Dezember 2027, Anhang I ab dem 2. August 2028; Art. 4 AI Literacy und Art. 50 Transparenz bleiben unverändert). Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E).
Bereitgestellt von ETHYX – ethyx.eu. DSGVO-Höchststrafe: 20 Mio. € / 4 % Umsatz. EU-KI-Gesetz-Höchststrafe: 35 Mio. € / 7 % Umsatz. Für KMU und Start-ups – weniger als 250 Beschäftigte und bis zu 50 Mio. € Jahresumsatz oder bis zu 43 Mio. € Bilanzsumme (Empfehlung 2003/361/EG) – gilt nach Art. 99(6) der jeweils niedrigere der beiden Werte statt des höheren. Version 1.2 · September 2026.