



CHEAT-SHEET · MAI 2026

EU AI Act in 10 Minuten

Was Geschäftsführer wissen müssen. Ohne Anwaltsdeutsch.

CEO-GPT · moritzmaaker.com · Mai 2026

Moritz Maaker · AI Builder & Co-Founder CEO-GPT

Der EU AI Act in einem Satz

Die EU reguliert KI nicht nach Technologie, sondern nach Risiko. Je mehr eine KI über Menschen entscheiden kann, desto strenger die Regeln.

Der EU AI Act (Verordnung (EU) 2024/1689¹) ist die erste umfassende KI-Regulierung weltweit. Sie ist seit 1. August 2024 in Kraft und rollt stufenweise bis 2027 aus³. Sie gilt für jeden, der KI in der EU anbietet, einsetzt oder importiert. Auch wenn dein Anbieter in den USA sitzt: sobald das Ergebnis in der EU wirkt, bist du in der Pflicht.

Das Gesetz arbeitet mit vier Risiko-Klassen. Verboten, hoch, begrenzt, minimal. Die meisten Systeme im Mittelstand fallen in die zwei unteren Klassen. Aber wenn du KI in HR, Bonität, Bildung oder kritischer Infrastruktur einsetzt, kann es schnell teuer werden.

Kurzfassung für eilige Leser

Du hast bis 2. August 2026 Zeit, deine Hochrisiko-Systeme konform zu machen. Eine Pflicht gilt aber schon heute: deine Mitarbeiter müssen ausreichend KI-Kompetenz haben (Art. 4, seit 2. Februar 2025)⁵. Strafen reichen bis 35 Mio. Euro oder 7 Prozent vom Konzernumsatz⁴.

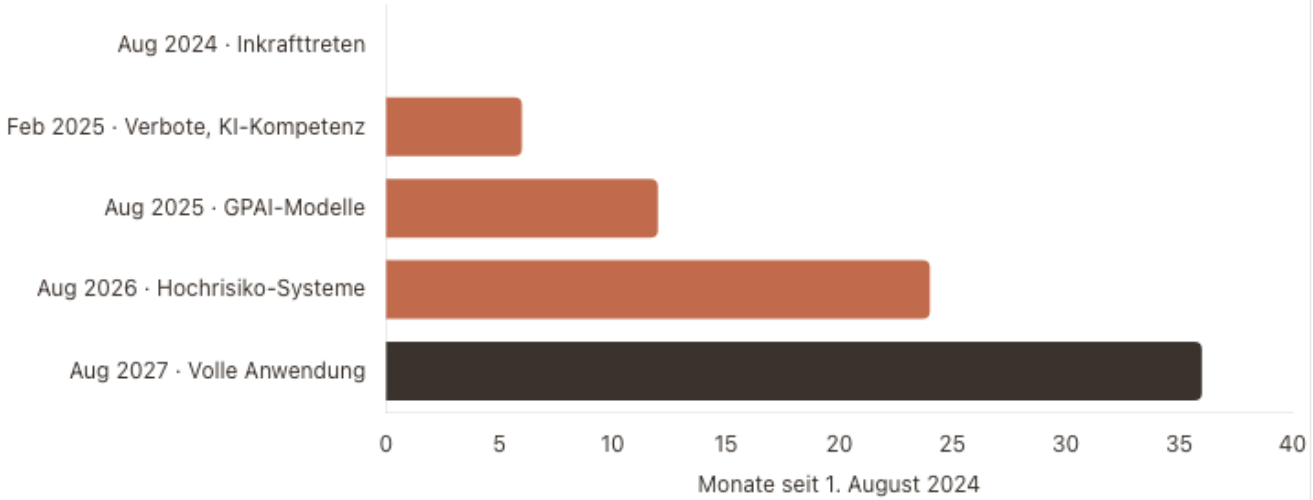
Was ab wann gilt

Vier Daten musst du kennen. Schreib sie dir an die Wand.

Datum	Phase	Was startet
1. Aug 2024	Inkrafttreten	Gesetz tritt in Kraft, Übergangsfristen laufen ³ .
2. Feb 2025	Verbote · KI-Kompetenz	Verbotene Praktiken nach Art. 5 sind ab sofort untersagt. Pflicht zur KI-Kompetenz (Art. 4) gilt für alle Anbieter und Nutzer ⁵ .
2. Aug 2025	GPAI-Modelle	Pflichten für Anbieter von General-Purpose-AI (GPT, Claude, Gemini, Mistral) greifen. Governance-Struktur und Bussgeld-Rahmen aktiv ⁹ .
2. Aug 2026	Hochrisiko-Systeme	Volle Pflichten für Hochrisiko-Systeme nach Annex III. Hier liegt für den Mittelstand der grösste Hebel ³ .
2. Aug 2027	Volle Anwendung	Auch Hochrisiko-Systeme nach Annex I (eingebettet in regulierte Produkte) und GPAI-Modelle, die schon vor August 2025 im Markt waren, müssen voll konform sein ³ .

EU AI Act · Roll-out 2024 bis 2027

Fünf Phasen, vier Pflicht-Daten für jeden Geschäftsführer



Quelle: Future of Life Institute · AI Act Implementation Timeline³

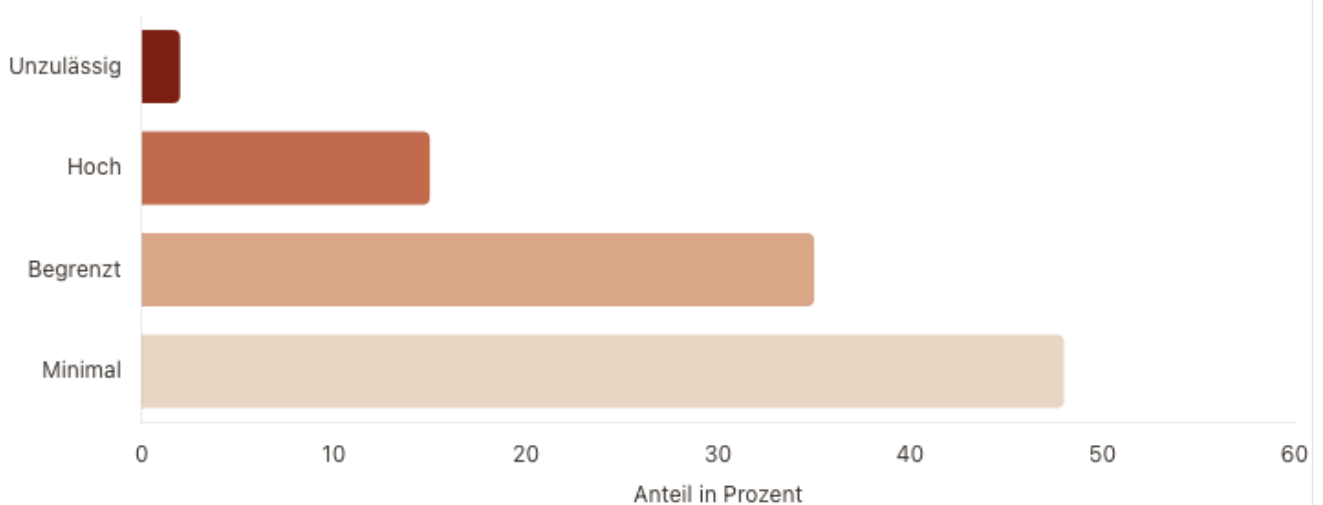
Übersetzt für deinen Kalender: wenn du heute schon KI im Recruiting, in der Bonitätsprüfung oder in der Mitarbeiter-Bewertung einsetzt, hast du noch etwa 15 Monate. Wer erst im Sommer 2026 anfängt, ist zu spät.

Die vier Klassen, in denen alles eingeordnet wird

Der AI Act schaut nicht auf die Technik, sondern auf den Einsatzzweck. Dieselbe Software kann in einem Kontext harmlos sein und in einem anderen hochreguliert.

Wie sich typische Business-KI verteilt

Grobe Schätzung. Im Mittelstand liegt die große Mehrheit in den unteren zwei Klassen.



Eigene Einordnung auf Basis von Annex III und Art. 5 AI Act¹⁰

1 · Unzulässig (Art. 5)

Komplett verboten. Egal in welchem Kontext. Wer das einsetzt, riskiert das volle Bussgeld.

- Social Scoring durch Behörden oder Unternehmen (Bürger nach Verhalten bewerten)
- Emotionserkennung am Arbeitsplatz oder in Schulen (ausser medizinisch oder Sicherheit)²
- Biometrische Kategorisierung nach Religion, politischer Meinung, sexueller Orientierung
- Predictive Policing rein anhand von Persönlichkeitsmerkmalen
- Untargeted Scraping von Gesichtsbildern für Erkennungs-Datenbanken
- Subliminale Manipulation, die Personen schadet

BUSINESS-BEISPIEL

Du baust ein Recruiting-Tool, das aus Stimme oder Mimik im Bewerbungsgespräch die Emotionen ableitet. Verboten. Auch ein Mitarbeiter-Monitoring-Tool, das per Webcam Stress oder Müdigkeit misst, fällt darunter.

2 · Hoch (Annex III)

Erlaubt, aber stark reguliert. Hier liegt die Hauptarbeit für viele Mittelständler. Acht Bereiche nennt Annex III¹⁰:

- **Biometrie:** Fernidentifikation, Emotionserkennung in nicht verbotenen Kontexten
- **Kritische Infrastruktur:** Strom, Wasser, Verkehr, digitale Infrastruktur
- **Bildung:** Zulassungs-Algorithmen, Prüfungs-Bewertung, Test-Überwachung
- **Beschäftigung:** CV-Screening, Beförderungs-Entscheidungen, Performance-Monitoring, Aufgabenzuweisung
- **Wesentliche Dienste:** Bonitätsprüfung, Kranken- und Lebensversicherungs-Pricing, Notruf-Priorisierung, Sozialleistungs-Vergabe
- **Strafverfolgung:** Opfer-Risiko-Einschätzung, Beweismittel-Bewertung
- **Migration und Grenzen:** Visum-Bearbeitung, Asyl-Prüfung
- **Justiz und Demokratie:** Recherche-Tools für Richter, KI mit Einfluss auf Wahlverhalten

BUSINESS-BEISPIELE

Eine HR-Software, die Bewerber-Lebensläufe sortiert und in Reihenfolge bringt. Ein Algorithmus, der Kredit-Anträge automatisch ablehnt. Eine KI, die im Recruiting-Funnel entscheidet, wer ins Vorstellungsgespräch kommt. Alles Hochrisiko, alles Pflicht zu Konformitäts-Bewertung, Risiko-Management, Logging, menschlicher Aufsicht und CE-Kennzeichnung.

3 · Begrenzt

Transparenz-Pflicht. Die Nutzer müssen wissen, dass sie mit einer KI interagieren.

- Chatbots im Kundenservice
- KI-generierte Inhalte (Bilder, Videos, Audio) müssen kennzeichenbar sein, vor allem Deepfakes
- Emotionserkennung in erlaubten Kontexten (z.B. UX-Research mit Einwilligung)

BUSINESS-BEISPIEL

Du hast einen Voice-Bot, der eingehende Anrufe annimmt und vorqualifiziert. Pflicht: am Anfang klar machen, dass es eine KI ist. Wer das verschleiert, ist im Verstoß.

4 • Minimal

Keine speziellen Pflichten aus dem AI Act. Hier liegt vermutlich der Grossteil deiner KI-Tools.

- Spam-Filter
- KI in Videospielen
- Empfehlungs-Systeme für Produkte
- Standard-Office-KI (Texterstellung, Übersetzung, Zusammenfassung)

Achtung Kontext-Falle

Dasselbe Sprachmodell kann minimal, begrenzt oder hoch sein. ChatGPT als Brainstorming-Tool ist minimal. ChatGPT als Bewerber-Filter ist hoch. Es kommt auf den Einsatz an, nicht auf das Modell.

Die 10-Punkte-Checkliste

Diese Liste deckt das Pflichtprogramm. Mehr ist erlaubt, weniger ist riskant.

1 · KI-Inventar erstellen

Liste alle KI-Systeme, die in deinem Unternehmen laufen. Auch die, die deine Mitarbeiter „heimlich“ nutzen. ChatGPT, Claude, Copilot, Midjourney, alles. Ohne Inventar keine Risiko-Einschätzung.

2 · Pro System Risiko-Klasse bestimmen

Frag pro Tool: was tut es konkret in welchem Geschäftsprozess? Daraus folgt die Klasse. Halte das schriftlich fest. Die Begründung zählt im Zweifel mehr als das Ergebnis.

3 · KI-Kompetenz für dein Team sicherstellen

Pflicht seit 2. Februar 2025 nach Art. 4⁵. Kein bestimmtes Format vorgeschrieben, aber dokumentationspflichtig. Eine Schulung pro Jahr, ein internes Playbook, eine kurze Onboarding-Sektion. Wer keinen Nachweis hat, dass die Leute geschult sind, hat ein Problem⁶.

4 · Verbotene Praktiken aktiv ausschliessen

Geh die Liste aus Art. 5 durch. Setzt jemand bei dir Emotionserkennung in Recruiting oder Mitarbeiter-Monitoring ein? Sofort stoppen. Diese Kategorie kostet die volle Strafe.

5 · Hochrisiko-Systeme identifizieren und kennzeichnen

Wenn du in HR, Bonität, Bildung, kritischer Infrastruktur, Versicherung oder Sozialleistungen unterwegs bist: sehr wahrscheinlich Hochrisiko. Für jedes solche System brauchst du bis August 2026 ein Konformitäts-Verfahren.

6 · Anbieter-Verträge prüfen

Der AI Act unterscheidet zwischen Provider (entwickelt das System) und Deployer (setzt es ein). Wer du bist, hängt davon ab, wie stark du das System anpasst. Wenn du ein Foundation Model nutzt, bist du Deployer. Wenn du eigene Features draufbaust und verkaufst, kannst du zum Provider werden mit viel mehr Pflichten⁸.

7 · DSGVO und AI Act zusammen denken

Beide Gesetze gelten parallel. Eine DSGVO-konforme Bonitätsprüfung kann trotzdem gegen den AI Act verstossen. Eine AI-Act-konforme Lösung kann trotzdem DSGVO-Probleme haben¹². Dein Datenschutzbeauftragter und dein KI-Verantwortlicher müssen sprechen.

8 · Datenschutzfolgenabschätzung (DSFA) erweitern

Wenn du eine DSFA nach Art. 35 DSGVO machst, ergänze die AI-Act-Aspekte. Datenqualität, Bias-Risiken, menschliche Aufsicht, Logging. Das spart später eine Doppel-Prüfung.

9 · Dokumentation aufbauen

Trainingsnachweise, Risiko-Bewertungen pro System, technische Dokumentation, Logs der Hochrisiko-Systeme, Beschwerde-Prozess. Im Zweifel ist die Dokumentation das, was dich rettet. Behörden prüfen nicht primär dein System, sondern deine Akten.

10 · Verantwortung im Unternehmen klären

Wer ist intern für KI-Compliance verantwortlich? Ein KI-Officer ist nicht vorgeschrieben⁶, aber jemand sollte den Hut aufhaben. In kleineren Firmen oft der Datenschutzbeauftragte mit Erweiterung. In grösseren ein eigenes Mandat.

Die ehrliche Reihenfolge

Wenn du nur drei Sachen in diesem Monat machst: Inventar (Punkt 1), Klassifizierung (Punkt 2), KI-Kompetenz dokumentieren (Punkt 3). Damit hast du 70 Prozent deines Compliance-Risikos abgedeckt.

Was es kostet, wenn du nichts tust

Drei Stufen. Verglichen mit der DSGVO ist der AI Act teurer.

Vergehen	Max. Bussgeld	oder max. Umsatzanteil
Verbotene KI-Praktiken (Art. 5)	35 Mio. Euro	7 Prozent vom weltweiten Jahresumsatz ⁴
Verstoss gegen Hochrisiko-Pflichten oder andere Vorschriften	15 Mio. Euro	3 Prozent vom weltweiten Jahresumsatz ⁴
Falsche oder unvollständige Angaben gegenüber Behörden	7,5 Mio. Euro	1,5 Prozent vom weltweiten Jahresumsatz ⁴

Zur Einordnung: die DSGVO hat 20 Mio. Euro oder 4 Prozent als Höchststrafe. Der AI Act schraubt die Spitze auf 35 Mio. Euro oder 7 Prozent. Das ist eine bewusste Aussage des Gesetzgebers.

ERLEICHTERUNG FÜR KMU

Für kleine und mittlere Unternehmen sowie Start-ups gilt jeweils der niedrigere Betrag aus den genannten Prozentsätzen oder Summen¹¹. Heisst: bei 35 Mio. vs. 7 Prozent zahlt das KMU 7 Prozent, wenn das weniger ist. Trotzdem kann das existenzbedrohend werden.

Wer setzt das durch?

In Deutschland ist die Marktüberwachung noch nicht final geklärt. Wahrscheinlich werden mehrere Behörden zuständig sein: die Bundesnetzagentur als zentrale Koordinationsstelle, sektorspezifische Behörden wie BaFin (Finanz), BfArM (Medizin), Datenschutz-Aufsichten (DSGVO-Schnittstelle). Bis spätestens 2. August 2026 muss jeder Mitgliedstaat seine Aufsichts-Struktur stehen haben⁹.

Was Strafen mildert

Wer einen Verstoss selbst meldet, schnell Abhilfe schafft und transparent kooperiert, kann mit niedrigerer Strafe rechnen¹¹. Wer Informationen zurückhält oder die Aufklärung behindert, bekommt das volle Programm. Diese Logik kennst du aus dem Steuer- und Kartellrecht.

AI Act und DSGVO · zwei Gesetze, ein Risiko

Der AI Act ersetzt die DSGVO nicht. Er kommt obendrauf. Wer nur eines im Blick hat, übersieht die Hälfte¹².

Frage	DSGVO	AI Act
Darf ich personenbezogene Daten verarbeiten?	Ja, mit Rechtsgrundlage (Art. 6)	Indirekt: ja, wenn Datenqualität stimmt (Art. 10)
Wer ist verantwortlich?	Verantwortlicher · Auftragsverarbeiter	Provider · Deployer · Distributor · Importer
Welche Daten darf ich für Training nutzen?	Zweckbindung · Minimierung	Repräsentativ · frei von Bias · dokumentiert
Pflicht zur Folgenabschätzung?	DSFA bei hohem Risiko	FRIA (Grundrechte-Folgenabschätzung) bei Hochrisiko-Systemen
Max. Strafe	20 Mio. Euro oder 4 Prozent	35 Mio. Euro oder 7 Prozent

Wo es konkret zusammenläuft

- **Automatisierte Einzelentscheidung:** Art. 22 DSGVO erlaubt sie nur in engen Grenzen. Hochrisiko-KI in HR oder Kredit fällt fast immer auch unter Art. 22. Beide Pflichten gleichzeitig prüfen.
- **Datenqualität:** DSGVO will Richtigkeit, AI Act will zusätzlich Repräsentativität und Bias-Freiheit. Im Trainings-Datensatz heisst das: nicht nur sauber, sondern auch ausgewogen.
- **Transparenz:** DSGVO verlangt Informationspflicht (Art. 13, 14). AI Act verlangt zusätzlich Kennzeichnung bei begrenztem Risiko. Doppelte Hinweis-Pflicht.
- **Aufsicht:** DSGVO hat den Datenschutzbeauftragten. AI Act hat keinen Pflicht-Officer, aber Menschen-Aufsicht bei Hochrisiko-Systemen.

Praktischer Move

Erweitere deinen bestehenden DSGVO-Prozess um die AI-Act-Felder. Wenn dein Verfahrens-Verzeichnis nach Art. 30 DSGVO sauber ist, ergänze pro KI-System die Risiko-Klasse, die Provider/Deployer-Rolle und den Compliance-Status. Doppelarbeit vermieden.

Der 30-Tage-Plan für Geschäftsführer

Wenn du heute anfängst, bist du spätestens im Juli 2026 sauber. Hier die ehrliche Reihenfolge.

Woche 1 · Bestandsaufnahme

Schick eine Mail ins Team: „Welche KI-Tools nutzt ihr in der Arbeit?“ Sammle die Antworten. Du wirst überrascht sein.

Woche 2 · Klassifizierung

Geh jede Antwort durch und klassifiziere. Die meisten Tools landen in minimal oder begrenzt. Markier die, bei denen du unsicher bist. Hol dir bei Hochrisiko-Kandidaten eine zweite Meinung.

Woche 3 · KI-Kompetenz

Plane eine 60-90-Min-Schulung. Was ist der AI Act, was sind die vier Klassen, was sind verbotene Praktiken, wie meldet ihr neue Tools. Dokumentiere Teilnahme und Inhalte⁵.

Woche 4 · Verantwortung

Bestimme einen KI-Verantwortlichen. Pflegt das Inventar weiter, prüft neue Tools vor Einführung, baut den Pflicht-Prozess für Hochrisiko bis 2026 aus. Halte das schriftlich fest.

Wann du externe Hilfe brauchst

Drei Konstellationen rechtfertigen einen Anwalt oder spezialisierten Berater. Wenn du KI in HR-Entscheidungen oder Bonitäts-Prüfungen einsetzt. Wenn du selbst KI-Produkte für andere Unternehmen baust und verkaufst. Wenn du in einer regulierten Branche bist (Finanz, Medizin, Energie). In allen anderen Fällen reicht eine saubere Eigenarbeit.

Quellen

1. EU AI Act · Verordnung (EU) 2024/1689 · Volltext · EUR-Lex · eur-lex.europa.eu/eli/reg/2024/1689/oj
2. AI Act High-Level Summary · Future of Life Institute · artificialintelligenceact.eu/high-level-summary
3. Implementation Timeline · Future of Life Institute · artificialintelligenceact.eu/implementation-timeline
4. Artikel 99 · Sanktionen · artificialintelligenceact.eu/article/99
5. Article 4 · AI literacy · artificialintelligenceact.eu/article/4
6. AI Literacy Q&A · Europäische Kommission · digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
7. Wettbewerbsfähige AI-Act-Normen schaffen · Bitkom Positionspapier 2025 · bitkom.org/...AI-Act-Normen-schaffen
8. EU AI Act Unpacked · Freshfields Bruckhaus Deringer · freshfields.com/...artificial-intelligence-act
9. AI Act Service Desk · Implementation Timeline · Europäische Kommission · ai-act-service-desk.ec.europa.eu/...timelines
10. Annex III · High-Risk AI Systems · artificialintelligenceact.eu/annex/3
11. EU AI Act · Wie werden Bussgelder berechnet · secjur · secjur.com/...bussgeld-sanktionen-berechnung
12. DSGVO und AI Act im Zusammenspiel · Law-Blog · law-blog.de/...dsgvo-ai-act

Dieses PDF ist kein Rechtsrat. Es soll dir helfen, die richtigen Fragen zu stellen. Für den konkreten Fall hol dir einen Anwalt.

MEHR DAVON? DIENSTAGS PER MAIL.

Mehr davon? Dienstags per Mail.

Jede Woche eine kurze Mail: was bei meinen Kunden funktioniert, welche neuen Skills dazukommen, ohne Bullshit.

moritzmaaker.com

Trag dich einmal ein, kriegst direkten Zugang zu allen Skills. Kein Spam, jederzeit abmelden.