EU AI Act

Five Questions Every CTO Should Answer Before August 2026

Penalties up to €35M or 7% of global turnover go live on 2 August 2026.

1 HAVE YOU CLASSIFIED ALL YOUR AI SYSTEMS BY RISK TIER?

The EU AI Act (Regulation 2024/1689) categorises AI systems into four risk tiers: prohibited, high-risk, limited, and minimal. Your entire compliance obligation depends on this classification. If you deploy AI in hiring, credit scoring, law enforcement support, or critical infrastructure, you are likely operating high-risk systems — whether you have labelled them as such or not.

2 DO YOU KNOW WHETHER YOU ARE A PROVIDER OR A DEPLOYER?

It matters significantly. Providers (those who develop or place AI systems on the market) face the heaviest obligations: technical documentation, conformity assessment, quality management, post-market monitoring. Deployers have fewer but still substantial duties: human oversight, transparency to affected persons, data governance. If you fine-tune a foundation model for your own use case, you may have crossed the line from deployer to provider without realising it.

3 ARE ANY OF YOUR AI SYSTEMS SUBJECT TO PROHIBITED PRACTICES?

Since February 2025, certain AI practices are already banned: social scoring, real-time biometric identification in public spaces (with narrow exceptions), manipulation of vulnerable groups, and emotion recognition in workplaces and educational institutions. Non-compliance carries the highest penalties: up to €35 million or 7% of worldwide turnover.

4 WHAT IS YOUR GPAI EXPOSURE?

If you use general-purpose AI models (GPT-4, Claude, Gemini, Llama, etc.), your providers must meet transparency obligations under the Act. If a GPAI model is classified as presenting systemic risk, additional requirements apply: adversarial testing, incident reporting to the AI Office, cybersecurity measures, and energy consumption documentation. As a deployer, you need to understand what your provider's obligations are — and what they pass through to you contractually.

5 HAVE YOU STARTED YOUR CONFORMITY ASSESSMENT?

For high-risk AI systems, conformity assessment must be completed before deployment — not after. This includes: technical documentation, a quality management system, human oversight measures, data governance documentation, and registration in the EU database. The Commission missed its own deadline for publishing detailed guidelines. Standardisation bodies are behind schedule. But the enforcement date has not moved. Waiting for perfect guidance is not a compliance strategy.

These questions are a starting point — not a substitute for proper compliance assessment.

If you need clarity on your AI Act obligations, contact Friedrich Kurz:

fk@rechtkreativ.de · +49 30 2388 9840 · smartcontracts.berlin

EU AI Act

Fünf Fragen, die jeder CTO vor August 2026 beantworten sollte

Bußgelder bis zu 35 Mio. € oder 7 % des weltweiten Umsatzes greifen ab dem 2. August 2026.

1 HABEN SIE ALLE IHRE KI-SYSTEME NACH RISIKOSTUFE KLASSIFIZIERT?

Die EU AI Act (Verordnung 2024/1689) unterteilt KI-Systeme in vier Risikostufen: verboten, hochrisiko, begrenzt und minimal. Ihre gesamte Compliance-Verpflichtung hängt von dieser Klassifizierung ab. Wenn Sie KI bei Einstellungen, Kreditvergabe, Unterstützung der Strafverfolgung oder kritischer Infrastruktur einsetzen, betreiben Sie wahrscheinlich hochrisiko-Systeme — unabhängig davon, ob Sie diese als solche gekennzeichnet haben oder nicht.

2 WISSEN SIE, OB SIE ANBIETER ODER NUTZER SIND — UND IST DAS WICHTIG?

Ja, es ist sehr wichtig. Anbieter (diejenigen, die KI-Systeme entwickeln oder auf den Markt bringen) haben die schwersten Verpflichtungen: technische Dokumentation, Konformitätsbewertung, Qualitätsmanagementsystem, Überwachung nach dem Inverkehrbringen. Nutzer haben weniger, aber immer noch erhebliche Pflichten: menschliche Aufsicht, Transparenz für betroffene Personen, Datenverwaltung. Wenn Sie ein Fundament-Sprachmodell für Ihren eigenen Anwendungsfall anpassen, haben Sie möglicherweise die Grenze vom Nutzer zum Anbieter überschritten, ohne es zu bemerken.

3 UNTERLIEGEN EINIGE IHRER KI-SYSTEME VERBOTENEN PRAKTIKEN?

Seit Februar 2025 sind bestimmte KI-Praktiken bereits verboten: Social Scoring, Echtzeit-Gesichtserkennung im öffentlichen Raum (mit engen Ausnahmen), Manipulation von gefährdeten Gruppen und Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen. Nichtbefolgung führt zu den höchsten Strafen: bis zu 35 Millionen Euro oder 7 % des weltweiten Umsatzes.

4 WELCHES IST IHRE GPAI-EXPOSITION?

Wenn Sie allgemeine KI-Modelle verwenden (GPT-4, Claude, Gemini, Llama usw.), müssen Ihre Anbieter Transparenzverpflichtungen gemäß dem Gesetz erfüllen. Wenn ein GPAI-Modell als systemisches Risiko eingestuft wird, gelten zusätzliche Anforderungen: adversarielle Tests, Meldung von Zwischenfällen an die KI-Behörde, Cybersicherheitsmaßnahmen und Energieverbrauchsdokumentation. Als Nutzer müssen Sie verstehen, welche Verpflichtungen Ihre Anbieter haben — und welche sie vertraglich an Sie weitergeben.

5 HABEN SIE IHRE KONFORMITÄTSBEWERTUNG GESTARTET?

Für hochrisiko-KI-Systeme muss die Konformitätsbewertung vor der Bereitstellung abgeschlossen sein — nicht danach. Dies umfasst: technische Dokumentation, ein Qualitätsmanagementsystem, Maßnahmen zur menschlichen Aufsicht, Dokumentation der Datenverwaltung und Registrierung in der EU-Datenbank. Die Kommission hat ihre eigenen Fristen für die Veröffentlichung detaillierter Richtlinien überschritten. Normungsorganisationen sind im Verzug. Aber das Durchsetzungsdatum hat sich nicht verschoben. Auf perfekte Leitlinien zu warten ist keine Compliance-Strategie.

Diese Fragen sind ein Ausgangspunkt — kein Ersatz für eine fundierte Compliance-Bewertung.

Wenn Sie Klarheit über Ihre AI-Act-Pflichten benötigen, wenden Sie sich an Friedrich Kurz:
fk@rechtkreativ.de · +49 30 2388 9840 · smartcontracts.berlin