# EU AC Act Cheat Sheet

Noch nicht in Kraft getreten. Politische Einigung erzielt am 8. Dezember 2023.

## GRUNDLAGEN

- Die Definition von KI entspricht der kürzlich aktualisierten Definition der OECD
- Wirkt Extraterritorial: gilt für Organisationen außerhalb der EU
- Ausnahmen: nationale Sicherheit, Militär und Verteidigung; F&E; Open Source (teilweise)
- Übergangsfristen für die Einhaltung von 6 bis 24 Monaten

- Risikobasierter Ansatz: Verbotene KI, Hochrisiko-KI, KI mit begrenztem Risiko, KI mit minimalem Risiko
- Umfangreiche Anforderungen für Anbieter und Nutzer von Hochrisiko-KI
- Generative KI: Spezifische Transparenz- und Offenlegungsanforderungen

## VERBOTENE AI

- Systeme zur sozialen Kreditbewertung
- Emotionserkennungssysteme am Arbeitsplatz und in der Bildung
- KI, die genutzt wird, um die Schwächen von Menschen auszunutzen (z.B. Alter, Behinderung)
- Verhaltensmanipulation und Umgehung des freien Willens
- Zielloses Sammeln von Gesichtsbildern für die Gesichtserkennung
- Biometrische Kategorisierungssysteme unter Verwendung sensibler Merkmale
- Spezifische Anwendungen zur vorhersagenden Polizeiarbeit
- Einsatz von Echtzeit-Biometrieerkennung durch Strafverfolgungsbehörden in der Öffentlichkeit (außer in begrenzten, vorab genehmigten Situationen)

## HOCHRISIKO-KI

- Medizinische Geräte
- Fahrzeuge
- Personalbeschaffung, Personalwesen und Arbeitsmanagement
- Bildung und berufliche Ausbildung
- Beeinflussung von Wahlen und Wählern
- Zugang zu Dienstleistungen (z. B. Versicherungen, Bankwesen, Kredite, Sozialleistungen usw.)
- Verwaltung kritischer Infrastrukturen (z. B. Wasser, Gas, Strom usw.)
- Emotionserkennungssysteme
- Biometrische Identifikation
- Strafverfolgung, Grenzkontrolle, Migration und Asyl
- Verwaltung der Justiz
- Spezifische Produkte und/oder Sicherheitskomponenten spezifischer Produkte

## WICHTIGE ANFORDERUNGEN AN HOCHRISIKO-KI

- Einschätzung der Einflüsse auf die Grundrechte und Bewertung der Konformität
- Obligatorische Registrierung in öffentlicher EU-Datenbank für Hochrisiko-KI-Systeme ist vorgesehen
- Implementierung eines Risikomanagements und Qualitätsmanagementsystems ist obligatorisch
- Datenverwaltung (z.B. Verringerung von Verzerrungen, repräsentative Trainingsdaten usw.) als wichtige Anforderung
- Transparenzanforderungen (z. B. Gebrauchsanweisungen, technische Dokumentation, Prozessbeschreibungen usw.)
- Menschliche Aufsicht (z.B. Erklärbarkeit, überprüfbare Protokolle, Mensch-im-Regelkreis usw.)
- Genauigkeit, Robustheit und Cybersicherheit (z. B. Tests und Audits)

## GENERAL PURPOSE AI

- Spezifische Anforderungen für Allgemeinzweck-KI (GPAI) und Grundmodelle
- Transparenz für alle GPAI (z.B. technische Dokumentation, Zusammenfassungen der Trainingsdaten, Urheberrechts- und IP-Schutzmaßnahmen usw.)
- Zusätzliche Anforderungen für hochwirksame Modelle mit systemischem Risiko: Modellbewertungen, Risikobewertungen, gegnerische Tests, Berichterstattung über Vorfälle usw.
- Generative KI: Individuen müssen informiert werden, wenn sie mit KI interagieren (z. B. Chatbots); KI-Inhalte müssen gekennzeichnet und erkennbar sein (z. B. Deepfakes)

## SANKTIONEN UND RECHTSDURCHSETZUNG

- Bis zu 7 % des weltweiten Jahresumsatzes oder 35 Millionen Euro für Verstöße gegen verbotene KI
- Bis zu 3 % des weltweiten Jahresumsatzes oder 15 Millionen Euro für die meisten anderen Verstöße
- Bis zu 1,5 % des weltweiten Jahresumsatzes oder 7,5 Millionen Euro für die Bereitstellung falscher Informationen
- Begrenzungen der Strafen für KMU und Start-ups
- Europäisches KI-Büro und KI-Ausschuss werden zentral auf EU-Ebene eingerichtet
- Überwachungsbehörden werdem in den EU-Ländern zur Durchsetzung eingerichtet
- Jede Person kann Beschwerden über Nichteinhaltung einreichen

Michael Mrak

Übersetzung einer Zusammenfassung von Oliver Patel