Vertrauensbildung durch ersten KI-Rechtsrahmen

Quelle: https://commission.europa.eu/

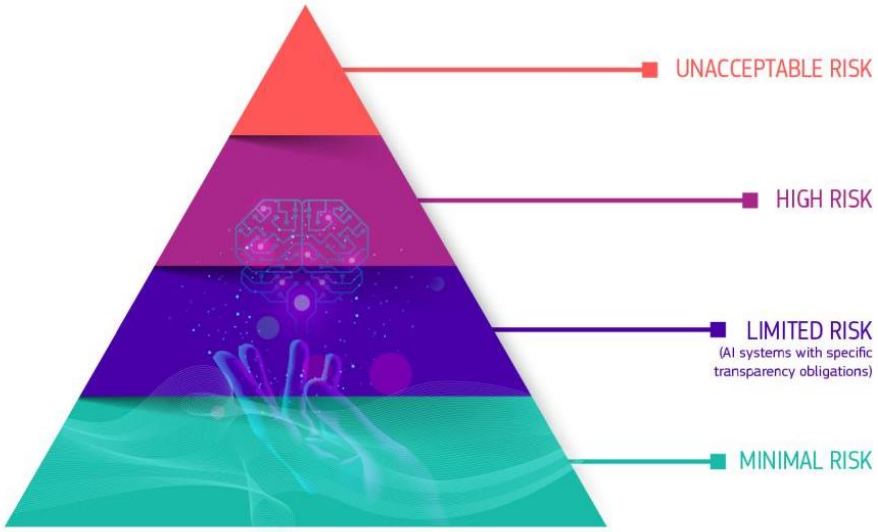
Die Europäische Kommission erstellt neue Vorschriften, um sicherzustellen, dass KI-Systeme, die in der EU verwendet werden, sicher, transparent, ethisch, unparteiisch und unter menschlicher Kontrolle sind.

Am 8.12.23 hat das Europäische Parlament und der Rat der Europäischen Union eine Einigung erzielt. Das AI Act (KI-Gesetz) wurde am 13.3.2024 beschlossen.

Beispiele für KI, die in der EU nicht Wirklichkeit werden sollen:

- Gesichtserkennung – Kameras identifizieren Personen auf öffentlichen Straßen
- Eine Software überprüft Bewerbungen und sortiert bestimmte Personen aus: Frauen, bestimmtes Alter…

KI-Systeme werden daher nach Risiko in vier Gruppen eingeteilt:



GRAFIK: EUROPÄISCHE KOMMSSION

Unzulässig

Alles, was als eindeutige Bedrohung für EU-Bürger angesehen wird, wird verboten: von der behördlichen Bewertung des sozialen Verhaltens, Manipulation von menschlichem Verhalten (Gefährdung der Grundrechte der Menschen) bis hin zu Spielzeug mit Sprachassistent, das Kinder zu riskantem Verhalten verleitet.

Hohes Risiko

- Kritische Infrastrukturen (z. B. im Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten
- Schul- oder Berufsausbildung, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z. B. Bewertung von Prüfungen)
- Sicherheitskomponenten von Produkten (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie)

- Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren)
- Zentrale private und öffentliche Dienstleistungen (z. B. Bewertung der Kreditwürdigkeit, wodurch Bürgern Darlehen verwehrt werden)
- Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (z. B. Überprüfung der Echtheit von Beweismitteln)
- Migration, Asyl und Grenzkontrolle (z. B. Überprüfung der Echtheit von Reisedokumenten)
- Rechtspflege und demokratische Prozesse (z. B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte)

Alle Systeme werden sorgfältig geprüft, bevor sie in Verkehr gebracht werden — und auch während ihres gesamten Lebenszyklus.

Begrenztes Risiko

Für KI-Systeme wie „Chatbots“ gelten minimale Transparenzverpflichtungen: Die Nutzer müssen informiert sein, ob sie mit einem Menschen oder Roboter sprechen.

Minimales Risiko

Kostenlose Nutzung von Anwendungen wie KI-gestützten Videospielen oder Spamfiltern. Unter diese Kategorie, in der die neuen Vorschriften nicht greifen, fällt die große Mehrzahl der KI-Systeme, weil diese Systeme nur ein minimales oder kein Risiko für die Bürgerrechte oder die Sicherheit darstellen. Beispiel für ein minimales Risiko: Komponieren mit KI, https://www.google.com/doodles/celebrating-johann-sebastian-bach

Neue Vorschriften für Anbieter von KI-Systemen mit **hohem Risiko**

Schritt 1

Ein KI-System mit hohem Risiko wird entwickelt.

Schritt 2

Es muss der Konformitätsbewertung[1] unterzogen werden und den KI-Anforderungen genügen. Bei einigen Systemen wird eine notifizierte (staatlich benannte und staatlich überwachte Organisation) Stelle einbezogen.

Schritt 3

Registrierung eigenständiger KI-Systeme in einer EU-Datenbank

Schritt 4

[1] Konformitätsprüfung: Überprüfung eines Produktes auf Übereinstimmung mit den Sicherheitsanforderungen

Eine Konformitätserklärung ist notwendig. Das KI-System muss die CE-Kennzeichnung tragen. Das System kann in Verkehr gebracht werden.

Zusammengefasst (zu finden in der Pressemitteilung des Europaparlaments):

Die neuen Regeln zielen darauf ab, Grundrechte, Demokratie und Rechtsstaatlichkeit sowie ökologische Nachhaltigkeit vor Hochrisiko-KI-Systemen zu schützen…

Entwickler von KI mit ***hohem Risiko*** müssen viele Vorschriften zur Dokumentation, Risikobewertung und Transparenz einhalten.

Grundlegende Regeln:

- Garantien für künstliche Intelligenz mit allgemeinem Verwendungszweck
- Beschränkung der Nutzung von biometrischen Fernidentifizierungssystemen durch Strafverfolgungsbehörden
- Verbot des Einsatzes von KI, um soziales Verhalten zu bewerten, Menschen zu beeinflussen oder ihre Schwächen auszunutzen
- Verbraucherrecht auf Einreichen von Beschwerden und auf aussagekräftige Erklärungen

Begriffe

KI	Abkürzung für Künstliche Intelligenz
unacceptable risk	unzulässiges Risiko
high risk	hohes Risiko
limited risk	begrenztes Risiko
minimal risk	minimales Risiko
Social Scoring	Vergabe von Punkten für wünschenswertes Verhalten, bzw. der Entzug der Punkte. Bei zu geringer Punkteanzahl ist mit Konsequenzen zu rechnen: Zugang zu Beruf, Ausbildung etc. Bekanntes Beispiel: China
Spielzeug mit Sprachassistent	Das Spielzeug hat Mikrophon und Lautsprecher eingebaut. Sprachassistenten können auch Daten weiterleiten. Gefährlich: Das Spielzeug gibt Anweisungen zu riskantem Verhalten.
Kritische Infrastruktur	Dazu gehören: Verkehrswesen, Gesundheit (z. B. Krankenhäuser), Sicherheit (Polizei, Militär), Versorgung durch Energie und vieles mehr.
roboterassistierte Chirurgie	Die Roboterarme werden vom Operateur gesteuert, der eine Steuerkonsole bedient.
Migration	Abwanderung in ein anderes Land.
Spamfilter	Aus den eingehenden E-Mails werden die Spam-E-Mails herausgefiltert. Beispiel: Der Filter sucht nach bestimmten Begriffen in der E-Mail und bewertet die E-Mail entsprechend.

Chatbots	Ein *Chatbot* ist eine Anwendung, die Künstliche Intelligenz verwendet, um sich mit Menschen in natürlicher Sprache zu unterhalten. Benutzer stellen Fragen in Textform oder in Sprache, der Chatbot antwortet in natürlicher Sprache. Chatbots entlasten Kundencenter und ersetzen Telefonisten.
eigenständige KI-Systeme	Ein eigenständiges KI-System ist eine Software, die in der Lage ist, selbstständig Entscheidungen zu treffen und Aufgaben auszuführen.
interagierende Nutzer	Benutzer stellen Fragen und bekommen eine Antwort, z. B. von einem Chatbot.
Konformitätsbewertung	Das Produkt wird überprüft: Entspricht das Produkt den Sicherheitsanforderungen?

Fotografiere den QR-Code und löse das Quiz:

Erreichte Punkte: _____