By PwC Deutschland | 18. Januar 2024

Update KI-Verordnung (EU AI Act)

EU-Parlament und Rat einigen sich auf umfassende Regeln für vertrauenswürdige KI

Content

Verfasst von Matthias Bleidiesel

Nachdem die EU-Kommission im April 2021 den ersten Vorschlag zu einer KI-Verordnung vorlegte, wurde kontrovers über KI-Systeme, deren potenziellen Risiken und Auswirkungen debattiert. Nun konnten sich im Dezember 2023 die Unterhändler des Europaparlaments und der EU-Mitgliedsstaaten auf eine vorläufige Fassung geeinigt.

Damit ist der Weg frei für den wohl weltweit ersten umfassenden Rechtsrahmen für Künstliche Intelligenz. Mit den schnellen Entwicklungsintervallen künstlicher Intelligenzsysteme erscheint dies nötig, um sicherzustellen, dass die Rechtsstaatlichkeit, Grundrechte und die ökologische Nachhaltigkeit vor risikoreicher KI geschützt werden. Gleichzeitig soll der europäische Regelungsvorstoß Innovationen fördern und Europa zu einem Vorreiter in diesem Bereich machen.

Die Eckpunkte der jetzigen Einigung sind:

- Einführung von**Schutzmaßnahmen**für künstliche Intelligenzsysteme mit allgemeiner Ausrichtung (general purpose artificial intelligence, GPAI)
- Beschränkung der Nutzung**biometrischer Identifizierungssysteme**durch Strafverfolgungsbehörden
- Verbot von**Social Scoring**und KI-Systemen, die zur**Manipulation**oder**Ausnutzung von Schwachstellen**der Nutzer eingesetzt werden
- **Recht der Verbraucher**, Beschwerden einzureichen und aussagekräftige Erklärungen zu erhalten
- **Bußgelder**in Höhe von bis zu 35 Millionen Euro oder 7% des weltweiten Umsatzes

Von besonderem Interesse dürfte der Konsens bei den**verbotenen Anwendungen**sein. In Anbetracht der potenziellen Bedrohung der Bürgerrechte und der Demokratie durch bestimmte Anwendungen der KI sollen folgende Anwendungen bzw. Verfahren verboten werden:

- **biometrische Kategorisierungssysteme**, die sensible Merkmale verwenden, wie beispielsweise politische, religiöse, philosophische Überzeugungen oder sexuelle Orientierung
- das ungezielte**Auslesen von Gesichtsbildern**aus dem Internet oder aus Überwachungsaufnahmen, um Datenbanken zur Gesichtserkennung zu erstellen
- **Emotionserkennung**am Arbeitsplatz und in Bildungseinrichtungen
- **Soziales Scoring**auf der Grundlage von sozialem Verhalten oder persönlichen Merkmalen
- KI-Systeme, die das**Verhalten von Menschen manipulieren**, um ihren freien Willen zu umgehen
- KI-Systeme, die eingesetzt wird, um die**Schwächen von Menschen auszunutzen**, beispielsweise aufgrund ihres Alters, einer Behinderung, ihrer sozialen oder wirtschaftlichen Situation.

Schutzmaßnahmen für künstliche Intelligenzsysteme mit allgemeiner Ausrichtung

(GPAI)

KI-Systeme mit allgemeiner Ausrichtung und die Modelle, auf denen sie basieren, müssen weitreichende Transparenzanforderungen erfüllen. Dazu gehört die Erstellung einer technischen Dokumentation, die Einhaltung des EU-Urheberrechts und die Verbreitung detaillierter Zusammenfassungen über die für das Training verwendeten Inhalte. Für Modelle mit hohem systemischem Risiko sind zusätzliche Maßnahmen erforderlich. Dies umfasst beispielsweise die Durchführung von Modellevaluierungen, die neben der Analyse und Bewertung systemischer Risiken auch die Durchführung von Gegentests vorsehen. Bei schwerwiegenden Vorfällen wird ein Bericht an die EU-Kommission verpflichtend.

Grundrechte-Folgenabschätzung für Hochrisikosysteme

Für KI-Systeme, die als hochriskant eingestuft werden – beispielsweise aufgrund ihres erheblichen Schadenspotenzials für Gesundheit, Sicherheit oder Rechtsstaatlichkeit – wurde ein Katalog von Verpflichtungen festgezurrt. Unter anderem wurde eine verpflichtende Folgenabschätzung zur Bewertung etwaiger Grundrechtsbeeinträchtigung eingeführt. Diese Risikobewertung ist bereits aus dem Versicherungs- und Bankensektor bekannt. Betroffene haben daneben das Recht, sich über KI-Systeme zu beschweren und Erklärungen zu Entscheidungen zu erhalten, die auf KI-Systemen mit hohem Risiko basieren und ihre Rechte beeinträchtigen.

Enge Rahmenbedingungen für Strafverfolgungsbehörden

Für Strafverfolgungsbehörden sollen biometrische Identifizierungssysteme (RBI) in öffentlich zugänglichen Räumen zwar nicht gänzlich verboten werden. Sie sollen RBI aber nur für klar definierte Ausnahmefälle einsetzen können. Voraussetzung ist u.a., dass eine Straftat einer streng definierten Liste betroffen ist, eine vorherige richterliche Genehmigung vorliegt und, dass spezielle Sicherheitsvorkehrungen umgesetzt wurden.

Maßnahmen zur Unterstützung von KMU und Innovationen

Zur Verbesserung der Situation für kleine und mittlere Unternehmen (KMU) sollen sogenannte regulatorische Sandkästen und Praxistests von nationalen Behörden eingerichtet werden. Dies soll KMU befähigen, innovative KI-Lösungen ohne unangemessenen Druck von Branchenriesen, die die Wertschöpfungskette kontrollieren, entwickeln und trainieren zu können, bevor sie auf den Markt gebracht werden.

Viele Änderungen im**Vergleich zum ursprünglichen Verordnungsentwurf von 2021**sind begrüßenswert.

Die Anlehnung an die etwas enger gefasste Definition von KI der OECD ist aus Sicht der Praxis grundsätzlich positiv, wenngleich auch diese Definition keine Rechtsklarheit versprüht. Da eine rechtsklare Definition von KI vermutlich ohnehin nicht gelingen wird, werden sich die einzelnen Grenzfälle in der Praxis

zurechtrütteln müssen.

Auch die Einführung der Anforderungen für GPAI, wie beispielsweise durch Verhaltenskodizes, und die hohen Bußgelder sind angesichts des Schadenspotenzials nachvollziehbar.

Im Blick behalten sollten Unternehmen die verschiedenen Geltungszeiträume. Zwar gilt weiterhin ein genereller Geltungszeitrahmen von 2 Jahren nach In-Kraft-Treten der Verordnung. Allerdings ist nun ein gestaffelter Geltungsbeginn für einzelne Regelungen vorgesehen, wie beispielsweise für verbotene KI-Systeme (bereits nach 6 Monaten), für GPAI (nach 1 Jahr) oder für hoch risikoreiche KI-Systeme (nach 3 Jahren).

Ausblick

Obwohl der Gesetzgebungsprozess noch nicht abgeschlossen ist, sind höchstens noch vereinzelte Änderungen zu erwarten. Der vereinbarte Text muss nun sowohl vom Parlament als auch vom Rat formell angenommen werden.

Schlagwörter

EU-Recht