

Die extraterritoriale Wirkung des AI Act

Am 13. März 2024 verkündete das Europäische Parlament mit klarem Beschluss einen Meilenstein: Die Europäische Union und der Europarat gaben den Auftakt für eine umfassende Regulierung künstlicher Intelligenz (AI Act). Dies markierte den Beginn eines neuen Kapitels in der europäischen KI-Gesetzgebung. Der AI Act wird voraussichtlich bis spätestens Juli 2024 offiziell in Kraft treten. Nach dem Inkrafttreten haben Unternehmen eine Frist von 24 Monaten, um die Vorschriften zu erfüllen, bevor diese unmittelbar anwendbar werden. Da der AI Act eine extraterritoriale Wirkung hat, gehen damit auch für Unternehmen ausserhalb der EU weitreichende Folgen einher. Daher stehen auch zahlreiche Schweizer Unternehmen vor der Aufgabe, zu ermitteln, wie der AI Act sie betrifft und welche Schritte sie gegebenenfalls ergreifen müssen.

■ Von Dr. iur. Lukas Lezzi, RA, CIPP/E, CIPM, CAS Forensics

Wen betrifft der AI Act?

Der AI Act gilt für Anbieter, die KI-Systeme oder KI-Modelle mit allgemeinem Verwendungszweck in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind (Art. 2 Abs. 1 lit. a AI Act). Der Begriff «Anbieter» umfasst Personen oder Einrichtungen, die ein KI-System entwickeln und auf den Markt bringen. Folglich fallen auch Schweizer Unternehmen unter den Anwendungsbereich des AI Act.

Klassifizierung der KI-Systeme

Der AI Act basiert auf einem risikobasierten Ansatz, bei dem die Regulierung von KI-Systemen auf ihren potenziellen Risiken für die Gesellschaft und Grundrechte beruht. Die Kategorisierung erfolgt in vier Risikostufen: Es wird zwischen einem a) unannehmbaren Risiko, b) einem hohen Risiko, c) einem begrenzten Risiko und d) einem minimalen oder gar keinem Risiko unterschieden:

a) Unannehmbares Risiko

Diese Risikostufe umfasst KI-Systeme, die eine erhebliche Bedrohung für die Gesellschaft und die Grundrechte des Einzelnen darstellen. Die Nutzung dieser Systeme ist streng verboten und muss innerhalb von sechs Monaten nach Inkrafttreten des AI Act eingestellt werden. Dazu gehören beispielsweise:

- Social-Scoring-Systeme

- vorausschauende Polizeiarbeit
- biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (ausser für spezielle Strafverfolgungszwecke)
- biometrische Kategorisierungssysteme
- ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Videoüberwachungsaufnahmen zur Erstellung von Gesichtserkennungsdatenbanken
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen
- Kinderspielzeug mit Sprachassistenten, das zu gefährlichem Verhalten von Kindern führen könnte
- KI-System, das eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder ihrer körperlichen oder geistigen Behinderung ausnutzt, um das Verhalten einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann

b) KI-Systeme mit hohem Risiko

Hochrisiko-KI-Systeme sind solche, die ein erhebliches Risiko für die Gesundheit, Sicherheit oder die Grundrechte natürlicher Personen darstellen. Gemäss dem risikobasierten Ansatz sind diese Systeme auf dem europäischen Markt zulässig, sofern sie bestimmten

verbindlichen Anforderungen genügen und eine vorgängige Konformitätsbewertung durchlaufen haben. Beispiele für solche KI-Systeme sind:

- KI-Systeme gelten immer als risikoreich, wenn sie ein Profil von Personen erstellen (z. B. um die Arbeitsleistung, wirtschaftliche Lage, Bewegung, Vorlieben, Verhalten oder die Gesundheit einer Person zu bewerten)
- KI-Systeme zur Überprüfung von Bewerbern während des Einstellungsverfahrens
- KI in kritischen Infrastrukturen (z. B. Verkehr, Energie, Gas)
- KI zur Kreditwürdigkeitsprüfung oder zur Bewertung der Kreditwürdigkeit von Personen, KI in Sicherheitskomponenten von Produkten (z. B. Anwendung von KI in der robotergestützten Chirurgie)
- biometrische Identifizierungs-, Kategorisierungs- und Emotionserkennungssysteme (sofern sie nicht vollständig verboten sind) oder KI-Systeme zur Beeinflussung von Wahlen

c) Systeme mit geringem Risiko

Diese Kategorie umfasst KI-Systeme, die geringe Risiken mit sich bringen. Systeme mit geringem Risiko sind solche, bei denen eine Manipulationsgefahr besteht. Für diese Systeme müssen besondere Transparenzanforderungen erfüllt werden, damit die Nutzer fundierte Entscheidungen treffen können. Hierunter fallen z. B.:

- «Chatbots» oder «Deep fakes»
- KI-gestützte Videospiele
- KI-Systeme, die in virtuellen Assistenten eingesetzt werden
- KI-Systeme, die synthetische Audio-, Video-, Text- oder Bilddaten verwenden

Diese oben genannten Beispiele müssen so gestaltet sein, dass die Nutzer sie eindeutig als künstlich erzeugt bzw. manipuliert erkennen können.

d) Systeme mit minimalem oder gar keinem Risiko

Die Kategorie der Systeme mit minimalem oder gar keinem Risiko können unter Einhaltung des allgemein geltenden Rechts entwickelt und verwendet werden, ohne dass zusätzliche rechtliche Verpflichtungen eingeführt werden. Anbieter solcher Systeme können sich freiwillig zur Einhaltung von Verhaltenskodizes verpflichten (sog. Codes of Conduct). Beispiele für diese Kategorie sind KI-gestützte Videospiele, Spamfilter oder KI, die zum Sortieren von Dokumenten in Büros verwendet wird.

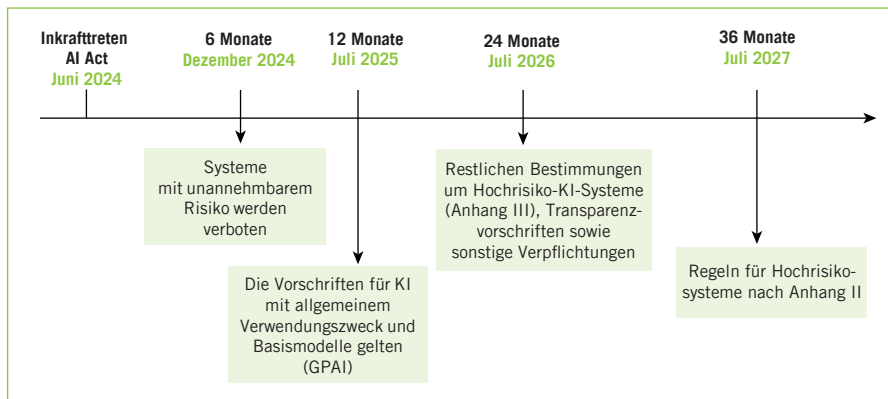
Sanktionen

Der AI Act wird hohe Geldstrafen vorsehen. Es wird eine Geldbusse bis zu EUR 35 Mio. bzw. 7% des weltweiten Jahresumsatzes für Verstösse gegen verbotene Anwendungen oder die Nichteinhaltung der Anforderung an Daten und Daten-Governance vorgesehen.

Was müssen Schweizer Unternehmen tun?

Je nach angebotenen KI-System variieren die Übergangsfristen für Schweizer Unternehmen. Schweizer Unternehmen, die an der Entwicklung eines KI-Systems arbeiten oder ein solches einsetzen, müssen die Fristen einhalten, um erhebliche Geldstrafen zu vermeiden. Bevor jedoch dieser Schritt unternommen wird, muss in erster Linie geprüft werden, ob der AI Act auf das Schweizer Unternehmen anwendbar ist.

Die Anwendbarkeit liegt dann vor, wenn Sie Ihr KI-System in der EU anbieten,



Ihr KI-System in der EU eingesetzt, importiert oder verwendet wird oder der Output Ihres KI-Systems in der EU verwendet wird. Falls dies der Fall ist, folgt im zweiten Schritt die Überprüfung, in welche Risikokategorie Ihr KI-System fällt (Art. 2 Abs. 1 lit. a AI Act).

Verwendet ein Schweizer Unternehmen KI-Systeme mit inakzeptablen Risiken, muss es deren Einsatz innerhalb von sechs Monaten nach Inkrafttreten des AI Act einstellen. Diese KI-Systeme sind nach dem AI Act streng verboten. Bei KI-Systemen mit begrenztem Risiko müssen Unternehmen bis zum Inkrafttreten des AI Act sicherstellen, dass sie die Transparenzverpflichtungen und sonstigen Verpflichtungen erfüllen. Je nach Art des begrenzten Risikos fallen unterschiedliche Übergangsfristen an.

Zeitplan des AI Act

Der AI Act tritt 20 Tage nach der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft. Die Veröffentlichung wird im Juni 2024 erwartet. Zwei Jahre nach seiner Verarbeitung und förmlichen Veröffentlichung tritt der AI Act vollständig in Kraft. Einige Bestimmungen gelten jedoch früher. Anzumerken ist, dass Hochrisiko-KI-Systeme nach Anhang II einer dreijährigen Übergangsfrist unterliegen. Den Zeitplan könnte man sich wie folgt vorstellen (siehe Grafik oben).

Um die Lücke bis zur Anwendbarkeit des AI Act zu überbrücken, wurde der AI Pact von der Kommission initiiert. Sein Ziel ist es, eine einheitliche Re-

gelung auf globaler Ebene zu unterstützen und Anbieter von KI-Systemen dazu zu ermutigen, sich freiwillig vor den gesetzlichen Fristen im Jahr 2026 zur Umsetzung der wichtigsten Anforderungen zu verpflichten.

Fazit

In Anbetracht der vielschichtigen Hürden, die mit dem AI Act verbunden sind, ist es ratsam, dass Schweizer Unternehmen die Umsetzung desselben sowie die weitere Rechtsentwicklung genau verfolgen.

Abschliessend sind die juristischen Herausforderungen in Bezug auf die Regulierung von KI jedoch keineswegs ungewöhnlich. Sie ähneln anderen regulierten Wirtschaftsbereichen, in denen auch unbestimmte Rechtsbegriffe verwendet werden, um mögliche zukünftige Entwicklungen bestmöglich zu berücksichtigen.

- Der AI Act bringt eine umfassende Regulierung von AI-Modellen mit sich
- Schweizer Unternehmen, welche AI-Modelle anbieten oder entwickeln, werden wohl in der Regel vom AI Act betroffen sein
- Es ist empfehlenswert, sich frühzeitig mit der Materie auseinanderzusetzen, um regulatorische Risiken zu begrenzen

AUTOR



Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.