NKF Client News / CLDS News

31. Juli 2024

Der EU AI Act tritt in Kraft: Auswirkungen auf Schweizer Unternehmen

1. Überblick und Zeitplan

Am 12. Juli 2024 erfolgte der letzte Schritt zur Inkraftsetzung des **AI Act**,[1] des weltweit ersten Rahmenerlasses zur Regulierung von Künstlicher Intelligenz (KI). Mit der Veröffentlichung des AI Act im Amtsblatt der Europäischen Union wurden folgende **Übergangsfristen** ausgelöst:

2. August 2024	**Inkrafttreten des AI Act**
2. Februar 2025	Verbot von KI-Praktiken mit inakzeptablen Risiken (Kapitel II) und Inkrafttreten der Verpflichtung für Anbieter und Betreiber von KI-Systemen, Massnahmen zur Sicherstellung der KI-Kompetenz zu ergreifen (Kapitel I)
2. Mai 2025	Code of Conduct muss vorliegen (andernfalls können Regeln durch das Büro für KI erlassen werden)
2. August 2025	Anwendbarkeit der Governance-Regeln und -Verpflichtungen für KI-Systeme mit allgemeinem Verwendungszweck (General Purpose AI, GPAI)
2. August 2026	**Allgemeines Inkrafttreten des AI Act**, Regulierung der KI-Systeme (einschliesslich Hochrisiko-KI-Systeme gemäss Anhang III), Transparenzvorschriften und nationale Sandboxes
2. August 2027	Anwendung des gesamten AI Act auf alle Hochrisiko-KI-Systeme (einschliesslich eingebettete Hochrisiko-Systeme gemäss Art. 6 Abs. 1 AI Act)

Der AI Act **bezweckt**, **einheitliche Regelungen** auf dem Binnenmarkt und ein **hohes Schutzniveau** in Bezug auf Gesundheit, Sicherheit und die in der EU-Charta der Grundrechte verankerten Grundrechte zu schaffen und dabei gleichzeitig die **Innovation** zu fördern. Die EU möchte bei der Förderung vertrauenswürdiger KI auf internationaler Ebene eine Führungsrolle übernehmen.

Beim AI Act handelt es sich um eine **Technikregulierung** in Form eines **Rahmengesetzes**, welches anknüpft an den **Begriff "KI-System"**, welcher in Art. 3 Ziff. 1 AI Act definiert wird als ein "*maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb*

[1] Verordnung (EU) 2024/1689 Des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (link).

ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können". Zudem enthält der AI Act eine eigenständige Definition für das sog. "KI-System mit allgemeinem Verwendungszweck", welches auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen.

Der AI Act folgt einem **risikobasierten Ansatz** mit vier Risikostufen:

Risikostufe	Beispiele	Regulierungsansatz
Inakzeptables Risiko (Art. 5 AI Act)	KI-Systeme mit Social Scoring für öffentliche oder private Zwecke, Ausnutzung der Schwachstellen von Personen oder mit Einsatz unterschwelliger Techniken	Verbot mit eng gefassten Ausnahmen
Hohes Risiko (Art. 6 ff., Anhang II und III AI Act)	KI-Systeme mit Anwendung in kritischen Infrastrukturen, allgemeine oder berufliche Bildung, Personalmanagement oder eingebettete KI-Systeme, die als Sicherheitsbauteile von Produkten nach den Produktsicherheitsvorschriften der EU zum Einsatz kommen	Erfordernis einer Konformitäts-bewertung und Einhaltung restriktiver Anforderungen (u.a. Risikomanagementsystem, Anforderungen an Daten und Daten-Governance, technische Dokumentation, Aufzeichnungspflichten, Transparenz, menschliche Aufsicht)
Limitiertes Risiko (Art. 50 AI Act)	Chatbots oder KI-Systeme, welche synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen	Transparenz und Offenlegungsanforderungen, Code of Conduct
Minimales Risiko	Alle anderen KI-Systeme, vorbehältlich KI-Systeme mit Risiken im Einzelfall (Art. 82 AI Act)	Keine zusätzlichen rechtlichen Verpflichtungen unter dem AI Act, Code of Conduct für die freiwillige Anwendung bestimmter Anforderungen

Darüber hinaus enthalten Art. 51 ff. AI Act **spezifische Regelungen** (inkl. Risikoklassifizierung) **für "KI-Modelle mit allgemeinem Verwendungszweck" (GPAI)**, womit die EU insbesondere die Regulierung von breit angewandten Large Language Models (LLM) bezweckt. GPAI-Modelle werden zu Transparenz verpflichtet. Strengere Anforderungen gelten für GPAI-Modelle mit systemischem Risiko.

Die wohl grösste Herausforderung unter dem AI Act besteht in der **Risikoklassifizierung**. Von besonderer Bedeutung ist dabei **die Unterscheidung zwischen KI-Systemen mit hohem Risiko** (zu denen der AI Act den Grossteil seiner Regelungen enthält) **und solchen mit limitiertem Risiko**. Die EU-Kommission wird spätestens bis zum 2. Februar 2026 – d.h. sechs Monate vor Inkrafttreten der Regelungen zu Hochrisiko-KI-Systemen – Leitlinien zu den Einstufungsvorschriften für Hochrisiko-KI-

Systeme (inkl. eine umfassende Liste praktischer Anwendungsfälle) zur Verfügung stellen. Dieser Vorlauf ist äusserst knapp bemessen und die Anbieter und Betreiber werden kaum umherkommen, bis dahin eine Einstufung der KI-Systeme zu tätigen und mit der Umsetzung der Anforderungen zu beginnen.

Die **Einstufung der KI-Systeme** hat durch die Anbieter zu erfolgen. In Art. 80 AI Act ist ein **Abklärungsverfahren der Marktüberwachungsbehörde** vorgesehen, sollte diese einen hinreichenden Grund zur Annahme haben, dass ein vom Anbieter als nicht hochriskant eingestuftes KI-System tatsächlich hochriskant ist. Sollte die Marktüberwachungsbehörde zum Schluss kommen, dass das betreffende KI-System hochriskant ist, fordert sie den Anbieter auf, innert Frist Massnahmen zu ergreifen und die Anforderungen und Pflichten gemäss AI Act sicherzustellen. Kommt der Anbieter dieser Aufforderung nicht innert Frist nach, so werden Geldbussen gemäss Art. 99 AI Act verhängt (siehe sogleich).

Verstösse gegen den AI Act unterstehen den Strafandrohungen von Art. 99 AI Act, welcher **Bussen von bis zu EUR 35 Mio. oder 7% des gesamten weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres vorsieht.

2. Anwendung des AI Act auf Schweizer Unternehmen

Hauptadressaten des AI Act sind **Anbieter**[2] und **Betreiber**[3] von KI-Systemen.[4] **Anbieter** sind **von den Pflichten des AI Act erfasst, wenn sie in der EU KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck (GPAI) in Verkehr bringen**, unabhängig davon, ob diese Anbieter in der EU oder in einem Drittland niedergelassen sind (Art. 2 Abs. 1 lit. a AI Act). Beim Tatbestand des Inverkehrbringens stellt sich die Frage, ob ein Vertrieb an Adressaten innerhalt der EU stattfindet. Schwieriger ist die Frage des Betriebs. Insbesondere stellt sich die Frage, ob der AI Act bereits Anwendung findet, wenn die Verarbeitung von Daten durch Nutzer oder Geräte mit Aufenthalt innerhalb der EU stattfindet.

Zudem können KI-Systeme, selbst wenn sie in der EU weder in Verkehr gebracht noch in Betrieb genommen oder verwendet werden, in den Anwendungsbereich des AI Act fallen. So findet der AI Act auf **Anbieter und Betreiber** von KI-Systemen Anwendung, die ihren Sitz in einem Drittland (z.B. in der Schweiz) haben oder sich in einem Drittland befinden, **wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird** (Art. 2 Abs. 1 lit. c AI Act). Erwägung 22 des AI Act hält hierzu fest:

> "Dies ist beispielsweise der Fall, wenn ein in der Union niedergelassener Akteur bestimmte Dienstleistungen an einen in einem Drittland niedergelassenen Akteur im Zusammenhang mit einer Tätigkeit vergibt, die von einem KI-System ausgeübt werden soll, das als hochriskant einzustufen wäre. Unter diesen Umständen könnte das von dem Akteur in einem Drittland betriebene KI-System Daten verarbeiten, die rechtmäßig in der Union erhoben und aus der Union übertragen wurden, und dem vertraglichen Akteur in der Union die aus dieser Verarbeitung resultierende Ausgabe dieses KI-Systems liefern, ohne dass dieses KI-System dabei in der Union in Verkehr

---

2 Als **Anbieter** gilt gemäss Art. 3 Ziff. 3 AI Act "*eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.*"

3 Zu den **Betreibern** zählt gemäss Art. 3 Ziff. 4 AI Act "*eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.*"

4 Darüber hinaus enthält der AI Act Regeln für weitere Adressaten, insb. Produkthersteller, Bevollmächtigte, Importeure und Händler. Ergänzend ist zu erwähnen, dass gemäss Art. 2 Ziff. 8 AI Act die Verordnung keine Anwendung findet auf Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden (ausgenommen von diesem Ausschluss sind Tests unter Realbedingungen).

> gebracht, in Betrieb genommen oder verwendet würde. Um die Umgehung dieser Verordnung zu verhindern und einen wirksamen Schutz in der Union ansässiger natürlicher Personen zu gewährleisten, sollte diese Verordnung auch für Anbieter und Betreiber von KI-Systemen gelten, die in einem Drittland niedergelassen sind, soweit beabsichtigt wird, die von diesem System erzeugte Ausgabe in der Union zu verwenden."

Angesichts des weit gefassten **Wortlauts ist es möglich, dass der AI Act auf KI-Systeme in Drittländern (wie der Schweiz) Anwendung findet, unabhängig davon, ob die Daten in der EU erhoben wurden.** Aufgrund des weiten Wortlauts muss davon ausgegangen werden, dass einzig **entscheidend ist, ob eine Verwendung resp. Verwertung eines Ergebnisses eines KI-Systems in der EU stattfindet.**

Es muss entsprechend damit gerechnet werden, **dass ein erheblicher Teil von Schweizer Anbietern und Betreibern von KI-Systemen unter die neue Regulierung des AI Act fallen wird**, zum Beispiel weil die Ergebnisse eines KI-Systems für Leistungen an Kunden mit Niederlassung oder Aufenthalt in der EU verwendet werden. Erhebliche Auswirkungen könnte dies insbesondere für **Anbieter von Schweizer Hochrisiko-KI-Systemen** haben, welche gemäss Art. 22 AI Act verpflichtet wären, einen in der EU niedergelassenen Bevollmächtigten zu bestimmen. Auch auf Schweizer **Betreiber von KI-Systemen**, deren Ergebnisse in der EU verwendet werden, werden eine Reihe von Pflichten zukommen. Sie werden insbesondere die Anforderungen an die KI-Kompetenz, die Transparenzpflichten und einen Code of Conduct umzusetzen haben.

3. Bedeutung für Data Science Projekte

Im Rahmen von Data Science Projekten finden KI-Systeme zunehmend Anwendung, z.B. zur Klassifizierung und Interpretation von Daten. Es stellt sich daher die Frage, inwieweit sich der AI Act auf Data Science Projekte auswirken könnte. Insoweit der AI Act zur Anwendung gelangt, gilt das Obenstehende hinsichtlich Anwendbarkeit, Risikoeinstufung und Regulierungsansatz.

Art. 2 Abs. 6 AI Act enthält eine Ausnahme für KI-Systeme oder KI-Modelle, einschliesslich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden. Diese Ausnahme wurde auf Vorschlag der tschechischen Ratspräsidentschaft eingefügt, um Einschränkungen der Wissenschaftsfreiheit zu vermeiden. Erwägung 25 des AI Act hält hierzu fest:

> "Diese Verordnung sollte die Innovation fördern, die Freiheit der Wissenschaft achten und Forschungs- und Entwicklungstätigkeiten nicht untergraben. Daher müssen KI-Systeme und -Modelle, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, vom Anwendungsbereich der Verordnung ausgenommen werden. Ferner muss sichergestellt werden, dass sich die Verordnung nicht anderweitig auf Forschungs- und Entwicklungstätigkeiten zu KI-Systemen und -Modellen auswirkt, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. [...] Darüber hinaus sollte unbeschadet der Ausnahme in Bezug auf KI-Systeme, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, jedes andere KI-System, das für die Durchführung von Forschungs- und Entwicklungstätigkeiten verwendet werden könnte, den Bestimmungen dieser Verordnung unterliegen. In jedem Fall sollten jegliche Forschungs- und Entwicklungstätigkeiten gemäß anerkannten ethischen und professionellen Grundsätzen für die wissenschaftliche Forschung und unter Wahrung des geltenden Unionsrechts ausgeführt werden."

Damit ist die Ausnahmebestimmung beschränkt auf KI-Systeme und -Modelle, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden. Wird demgegenüber zu Forschungs- und Entwicklungszwecken ein anderes KI-System verwendet, so kommt der AI Act zur Anwendung. Angesichts der enormen Entwicklungskosten von KI-Systemen wird dies die grosse Mehrheit der Fälle sein. Damit wird es auch aus Sicht der AI Regulierung zentral, ob das verwendete KI-System rein wissenschaftlichen oder auch anderen Zwecken dient. Angesichts der grossen Bedeutung von KI-Systemen, welche nicht zum alleinigen Zweck der wirtschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen wurden, ist damit zu rechnen, dass der AI Act auf die Mehrheit der Data Science Projekte, welche KI verwenden, zur Anwendung kommen wird.

4. Nachvollzug des AI Act in der Schweiz?

Die Schweiz evaluiert derzeit Regulierungsansätze zu KI-Systemen. Hierfür hat der Bundesrat im November 2023 beim Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) eine Übersicht möglicher Regulierungsansätze in Auftrag gegeben, welche bis Ende 2024 vorliegen soll. Angesichts der Entwicklungen in der EU halten wir es für wahrscheinlich, dass die Schweiz ein Rahmengesetz ähnlich dem AI Act im ordentlichen Gesetzgebungsverfahren erlassen wird, wobei der Zeitrahmen noch nicht absehbar ist.

Aufgrund der weitreichenden extraterritorialen Regelung des AI Act stellt sich die Frage, ob eine Koordination der Regulierung möglich ist. Der AI Act enthält in Art. 39 AI Act die Möglichkeit, dass Konformitätsbewertungsstellen in Drittländern anerkannt werden. Voraussetzung ist jedoch ein bilaterales Abkommen zwischen der Schweiz und der EU, welches aus politischen Gründen und Erfahrungen in anderen Bereichen derzeit unwahrscheinlich erscheint. Es muss daher damit gerechnet werden, dass der AI Act und eine (noch zu erlassende) schweizerische Regulierung für KI-Systeme parallel zur Anwendung kommen werden.

Autoren /Kontakte

Prof. Dr. Tilmann Altwicker
Chair CLDS
tilmann.altwicker@ius.uzh.ch

Juerg Bloch
Partner, Compliance & Investigations
Mitglied Advisory Board CLDS
juerg.bloch@nkf.ch

Simon Bühler
Partner, Regulatory
simon.buehler@nkf.ch

Clara-Ann Gordon
Partner, Data Protection
clara-ann.gordon@nkf.ch

Janine Reudt-Demont
Partner, Data Protection
janine.reudt-demont@nkf.ch