AI ACT: VERORDNUNG (EU) 2024/1689

des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Der EU-AI Act 2024/1689[1] ist am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union am 12. Juli 2024 in Kraft getreten und gilt in mehreren Stufen. Der AI Act gilt unmittelbar in jedem EU-Mitgliedstaat.

Ab 2. Februar 2025 gilt **Kapitel I** (Allgemeine Bestimmungen) mit vier Artikeln. Das sind Artikel 1 (Gegenstand), Artikel 2 (Anwendungsbereich), Artikel 3 (Begriffsbestimmung) und Artikel 4 (KI-Kompetenz). Des Weiteren gilt ab dann auch **Kapitel II** mit Artikel 5 (Verbotene Praktiken im KI-Bereich).

Artikel 1 befasst sich mit dem Zweck und den Festlegungen des AI Acts. Dabei werden die harmonisierten Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union sowie die Verbote bestimmter Praktiken im KI-Bereich, die besonderen Anforderungen an Hochrisiko-KI-Systeme und Pflichten für Akteure in Bezug auf solche Systeme festgelegt. Darüber hinaus werden Maßnahmen zur Innovationsförderung mit besonderem Augenmerk auf KMU, einschließlich Start-up-Unternehmen festgelegt.

Artikel 2 befasst sich mit dem Anwendungsbereich des AI Acts und legt die Personen sowie die Bereiche fest, die unter den Geltungsbereich fallen.

Artikel 3 adressiert die Begriffsbestimmungen, die innerhalb des AI Acts zum Ausdruck gebracht werden und die Bedeutung der Bezeichnungen.

Artikel 4 bestimmt, dass die Anbieter und Anbieterinnen sowie Betreiber und Betreiberinnen von KI-Systemen über ein ausreichendes Maß an KI-Kompetenz verfügen müssen, um Maßnahmen für ihr Personal zu ergreifen, die sich in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befassen.

Artikel 5 befasst sich mit den verbotenen Praktiken im KI-Bereich und unterliegt dem Kapitel II. Zu den Verboten gehört das Inverkehrbringen und die Inbetriebnahme sowie die Verwendung von KI-Systemen, die absichtlich manipulative oder täuschende Techniken bei Personen oder Gruppen einsetzen, um das Verhalten von Personen zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, beeinträchtigt wird. Darüber hinaus ist es verboten, KI Systeme zu verwenden, die Profiling vornehmen sowie schutzbedürftige Personen ausnutzen, um ihr Verhalten zu ändern, dass dieser Person oder einer anderen Person erheblichen Schaden zufügen kann.

Auch Systeme, die biometrische Kategorisierung in Verkehr bringen, um Personen mit dem Ziel individuell zu kategorisieren, sensible Informationen abzuleiten, wie ihre politische Einstellung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugungen, Sexualleben oder sexuelle Orientierung. Ausnahme hierbei ist der Einsatz biometrischer Echtzeit-Fernidentifizierung in öffentlichen Räumen, welche nur unter strengen Bedingungen zur Strafverfolgung erlaubt ist, wie z. B. bei Terrorgefahr oder Vermisstenfällen. Das gilt auch nur mit vorheriger Genehmigung, Berichterstattung sowie angemessenen Schutzvorkehrungen.

Ab 2. August 2025 gilt **Kapitel III Abschnitt 4**, die Festlegung der notifizierenden Behörden und notifizierte Stellen. Jeder Mitgliedstaat sorgt für die Benennung oder Schaffung mindestens einer notifizierenden Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

HISOLUTIONS

AUTOREN

Rozerin Karaterzi
Manuel Atug

zur Bewertung, Benennung und Notifizierung der Konformitätsbewertung und für deren Überwachung zuständig ist. Diese Verfahren werden in Zusammenarbeit zwischen den notifizierenden Behörden aller Mitgliedstaaten entwickelt. Das ebenfalls ab dann geltende **Kapitel V** bestimmt die Einstufungsvorschrift der KI-Modelle mit allgemeinem Verwendungszweck und **Kapitel VII** bestimmt die Governance. **Kapitel XII** bestimmt ab dann Sanktionen, die beim Verstoßen des AI Acts Anwendung finden. Dabei müssen die Sanktionen wirksam, verhältnismäßig und abschreckend sein. Des Weiteren gilt ab dann **Artikel 78**, der die Vertraulichkeit der Informationen und Daten bestimmt, die von der Kommission, der notifizierten Stellen sowie von den Marktüberwachungsbehörden gewahrt werden soll.

Artikel 101 mit den Geldbußen i. H. v. bis zu 3 % ihres gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr oder 15 Millionen Euro für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck ist eine Ausnahme und gilt dann allerdings noch nicht.

Ab 2. August 2027 gelten die Artikel 6 Absatz 1 (Einstufungsvorschriften für Hochrisiko-KI-Systeme) und die entsprechenden Pflichten gemäß dieser EU-Verordnung.

Damit es einen vereinheitlichten Rechtsrahmen in Bezug auf die Anwendung von KI-Systemen gibt, und der Binnenmarkt funktioniert, wurde der AI Act etabliert. Zukünftig soll KI aktiv gefördert und ein hohes Schutzniveau in Bezug auf Sicherheit, Gesundheit und die Grundrechte der EU gewährleistet werden. Die Einführung des AI Acts soll darüber hinaus vor schädlichen Folgen von KI-Systemen bewahren.

Die in der Charta der Grundrechte der Europäischen Union 2016/C 202/02[2] verankerten Werte der EU wurden im AI Act im Einklang adressiert. Der AI Act sorgt daher für den Schutz von natürlichen Personen, Unternehmen, Demokratie und Rechtsstaatlichkeit. Innovation soll gefördert werden und die EU soll eine Führungsrolle bei der Einführung von vertrauenswürdiger KI einnehmen.

FESTLEGUNGEN IM AI ACT

Der Anforderungsbereich des AI Acts beinhaltet die Regelung einer abgestimmten Vorschrift, die zuständig ist für das Inverkehrbringen, die Inbetriebnahme und die Anwendung von KI-Systemen in der EU. Das betrifft sowohl Vorschriften für die Transparenz als auch für das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck. Die Marktbeobachtung, als auch die Governance und Durchsetzung der Marktüberwachung sind als weitere Vorschriften zu beachten. Gleichzeitig ist bedeutend, dass Verbote bei bestimmten Praktiken im KI-Bereich bestehen und besondere Anforderungen an Hochrisiko-KI-Systeme und Pflichten für Akteure geregelt werden. Zuletzt sollen Maßnahmen in Bezug auf Innovationsförderung mit Schwerpunkt auf kleine und mittlere Unternehmen (KMU), einschließlich Start-up Unternehmen, festgelegt werden.

ANWENDUNGSBEREICH DES AI ACTS

Der AI Act-Anwendungsbereich gilt für:

- Anbieter, die in der EU KI-Systeme in Verkehr bringen,
- Anbieter, die KI Modelle mit allgemeinem Verwendungszweck in Verkehr bringen,
- Anbieter und Betreiber, die ihren Sitz in einem Drittland haben,
- Betreiber von KI-Systemen, die ihren Sitz in der EU haben
- Einführer und Händler von KI-Systemen,
- Produkthersteller, die zusammen mit ihrem Produkt die KI-Systeme in Verkehr bringen,
- Bevollmächtigte von Anbietern, die nicht in der EU etabliert sind und
- betroffene Personen, die sich in der EU befinden.

Die in Unionsrecht fallenden Bereiche sind von dem Anwendungsbereich betroffen und berühren nicht die Zuständigkeiten der Mitgliedstaaten oder die Vorschriften anderer Rechtsakte der EU zum Verbraucherschutz und zur Produktsicherheit.

Die EU als auch die Mitgliedstaaten sind dabei frei, Rechts- oder Verwaltungsvorschriften beizubehalten oder entsprechend einzuführen. Gleichzeitig werden dabei KI-Systeme abgedeckt, die als Hochrisiko KI-Systeme gemäß Artikel 6 Absatz 1 eingestuft sind.

Ausgeschlossen vom Anwendungsbereich des AI Acts sind:

- KI-Systeme, die ausschließlich für militärische Zwecke der nationalen Sicherheit in Verkehr gebracht werden,
- Behörden in Drittländern sowie Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen,
- Betreiber, die natürliche Personen sind und KI-Systeme im Rahmen von persönlichen und nicht beruflichen Tätigkeiten verwenden und

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12016P/TXT

HISOLUTIONS

- KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden.

HOCHRISIKO-KI-SYSTEME

Die Einstufungsvorschrift definiert, ab wann man von einem Hochrisiko-KI-System spricht. Es gibt insgesamt zwei Bedingungen, die dabei erfüllt sein müssen. Erstens muss das KI-System als Sicherheitsbauteil eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften (20 Punkte Liste) in der EU fallenden Produkts verwendet werden oder selbst ein solches Produkt sein. Zweitens muss das Sicherheitsbauteil des Produkts nach Anhang XI Technische Dokumentation gemäß Artikel 53 Absatz 1 Buchstabe a das KI-System sein, oder das KI-System selbst wird als Produkt durch eine Konformitätsbewertung durch Dritte gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der EU unterzogen.

Ein erhebliches Risiko wird dann als hochriskant eingestuft, wenn es eine Gefahr für die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen darstellt. Das heißt, dass ein KI-System genau dann hochriskant ist, wenn es ein Profiling natürlicher Personen vornimmt.

Das KI-System ist dazu bestimmt, dass eine Verfahrensaufgabe durchgeführt wird und die Ergebnisse der abgeschlossenen menschlichen Tätigkeiten verbessert werden. Gleichzeitig soll sie Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkennen. Die zuvor abgeschlossene menschliche Bewertung ohne eine menschliche Überprüfung soll aber nicht ersetzt oder beeinflusst werden.

RISIKOMANAGEMENTSYSTEM

Für Hochrisiko-KI-Systeme soll ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten werden. Das Risikomanagementsystem wird als ein sogenannter kontinuierlicher iterativer Prozess bezeichnet, der während des gesamten Lebenszyklus des Hochrisiko-KI-Systems geplant und durchgeführt wird. Gefordert wird daher eine konstante systematische Überprüfung und Aktualisierung.

Dabei müssen bestimmte Schritte berücksichtigt werden, wie beispielsweise die Ermittlung und Analyse von vorhersehbaren Risiken, die vom Hochrisiko-KI-System ausgehen könnten, wie z. B. für die Gesundheit, für die Sicherheit und für die Grundrechte. Darüber hinaus ist eine Abschätzung und Bewertung der Risiken vorzunehmen, wenn das Hochrisiko-KI-System als Fehlanwendung verwendet wird. Zu dieser Bewertung gehören dabei auch mögliche andere Risiken aus den im Artikel 72 genannten Systemen. Artikel 72 beinhaltet sowohl die Beobachtung nach dem Inverkehrbringen durch die Anbieter als auch die Pläne für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme. Zur Bewältigung der ermittelten Risiken wird eine Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen benötigt.

Die bestmögliche Risikomanagementmaßnahme für Hochrisiko-KI-Systeme ist die Beseitigung oder Verringerung der ermittelten Risiken durch die entsprechende Konzeption und Entwicklung. Für die Anwendung von nicht ausschließbaren Risiken kann es gegebenenfalls Minderungs- und Kontrollmaßnahmen geben. Des Weiteren sollte eine Bereitstellung der gemäß Artikel 13 erforderlichen Informationen und Schulungen der Betreiber vorgesehen werden. Die Transparenz und Bereitstellung von Informationen für die Betreiber wird in Artikel 13 adressiert.

Das Testen der Hochrisiko-KI-Systeme ist vorgegeben, um die bestmöglichen Risikomanagementmaßnahmen zu ermitteln. Dadurch kann festgestellt werden, ob Hochrisiko-KI-Systeme gemäß ihrer zweckgemäßen Bestimmung funktionieren. Dieser Prozess ist im gesamten Entwicklungsprozess und vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme vorzunehmen.

ANFORDERUNGEN AN HOCHRISIKO-KI-SYSTEME

Festgelegte Anforderungen sind insbesondere durch Hochrisiko-KI-Systeme zu erfüllen. Die im EU-AI Act Artikel 9 genannten Anforderungen zum Risikomanagementsystem sind mit abzudecken. Die Anbieter sind in der Verantwortung, dass ihr Produkt die geltenden Anforderungen der Harmonisierungsvorschrift der EU einhaltet. Dabei besteht die Möglichkeit, dass die erforderlichen Test- und Berichterstattungsverfahren, Informationen und Dokumentationen in bereits bestehende Verfahren integriert werden.