get started by bitkom

Get Started Guide: AI Act

April 2024

Am 02. Februar haben die Mitgliedstaaten der EU im Ausschuss der Ständigen Vertreter den AI Act einstimmig gebilligt. Am 13. März folgte das Parlament. Es gilt damit als gesichert, dass die KI-Regulierung nach finaler Abstimmung durch den Rat in Kraft tritt und Übergangsfristen zeitlich wirken. Was das für dein Startup bedeutet, fassen wir im Folgenden zusammen.

Was ist der AI Act?

Der AI Act ist der weltweit erste umfassende Rechtsrahmen zur Regulierung Künstlicher Intelligenz.[1] Durch die Verordnung will die EU sicherstellen, dass KI-Systeme, die in Mitgliedsstaaten vertrieben werden, sicher und fair sind und weder europäische Grundwerte noch -rechte verletzen. Von einer klaren gesetzlichen Regelung verspricht sich die EU, das Vertrauen in die Technologie zu stärken und Innovation zu fördern. Erreicht werden soll dies durch einen risikobasierten Ansatz zur Klassifizierung von KI-Systemen, mit spezifischen Anforderungen an Systeme, die als hochriskant eingestuft werden.

Bitkom-Bewertung:

Wir begrüßen den AI Act der EU grundsätzlich, sehen jedoch entscheidenden Bedarf an einer rechtssicheren und innovationsfreundlichen Umsetzung auf europäischer und nationaler Ebene. Obwohl der AI Act wesentliche Entscheidungsbefugnisse dem neu geschaffenen AI Office der EU sowie den Mitgliedstaaten überträgt, mangelt es ihm in seiner aktuellen Fassung an der notwendigen Klarheit zur Schaffung von Rechtssicherheit, die für die Entwicklung und Nutzung von KI-Technologien essenziell ist. Es ist zwingend notwendig, dass die Bundesregierung die Potenziale Künstlicher Intelligenz priorisiert und die Fehler der DSGVO vermeidet. Wir kritisieren, dass der AI Act Anforderungen formuliert, die mit bestehenden Regularien, wie der Medizinprodukt- oder Maschinenrichtlinie, kollidieren oder diese gar konterkarieren und mahnen, unnötige bürokratische Lasten zu vermeiden. Die Art und Weise der Implementierung des AI Acts wird darüber entscheiden, ob europäische Startups mit den global führenden Innovatoren der KI-Branche Schritt halten können.

[1] Der AI Act definiert KI als ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können.

Wir warnen zudem vor der Gefahr divergierender Interpretationen des AI Acts innerhalb der EU, die insbesondere Startups vor erhebliche Herausforderungen stellen könnten, und fordern, dass Deutschland Innovationen nicht durch übermäßig strenge Regulation erstickt. Die Bundesregierung ist aufgerufen, die Unterstützungsmaßnahmen für Startups signifikant zu erweitern.

Wie funktioniert der risikobasierte Ansatz?

Die rechtlichen Anforderungen an Hersteller sogenannter Fixed-Purpose-Systeme[2] richten sich nach dem Risiko, das von einer Anwendung ausgeht. Hierfür wurden vier Kategorien definiert. Im Folgenden stellen wir die jeweiligen Risikogruppen anhand fiktiver Beispiele dar.

Kategorie 1: Nicht annehmbares Risiko

Das Herstellen, Inverkehrbringen und Nutzen von Anwendungen mit nicht annehmbarem Risiko ist in der EU verboten. Hierzu zählen unter anderem Systeme, die der Verhaltensmanipulation dienen, Emotionserkennung in Arbeits- und Bildungseinrichtungen (außer aus Sicherheitsgründen wie bspw. Vorbeugung von Unfällen oder zur therapeutischen Nutzung), prädiktive Polizeiarbeit in Bezug auf Einzelpersonen, Sozialkreditsysteme, biometrische Echtzeit-Fernidentifizierung (Ausnahmen gelten hierbei für schwere Verbrechen und Terrorismus).

Beispiel:

Ein System, das in Schulen eingesetzt wird, um die Aufmerksamkeit von Schülerinnen und Schülern zu überwachen und zu bewerten, wäre unter dem AI Act verboten. Dementsprechend hätte eine solche Anwendung **keine Chance auf einen Marktgang in der EU**.

Kategorie 2: Hohes Risiko Hochrisiko-KI-Systeme müssen strenge Anforderungen erfüllen, um zugelassen zu werden. In diese Kategorie fallen vor allem Dienste, die das Leben der Bürgerinnen und Bürger direkt betreffen wie z.B. die Bewertung der Kreditwürdigkeit oder Bildungschancen sowie Anwendungen, die auf kritische Infrastrukturen angewendet werden.[3] Auf nationaler Ebene müssen Sandboxes eingerichtet und für KMU und Startups prioritär zugänglich gemacht werden, um Systeme testen zu können, bevor sie auf den Markt kommen - allerdings ohne

[2] Fixed-Purpose-Systeme dienen einem definierten und begrenztem Zweck wie bspw. der Personalvermittlung.
[3] Startups mit Hochrisiko-KI-Systemen müssen ein Konformitätsbewertungsverfahren durchlaufen. Die Kosten dafür werden verhältnismäßig an deren Größe und Leistungsfähigkeit angesetzt. Die EU-Kommission plant, das Verfahren für die Einreichung technischer Dokumentationen für Startups, die Hochrisiko-KI-Systeme anbieten, erheblich zu vereinfachen. Zu diesem Zweck wird ein standardisiertes Formular entwickelt, das von den betreffenden Unternehmen ausgefüllt werden muss. Durch das Ausfüllen dieses Formblatts soll die Anforderung an die Bereitstellung technischer Dokumentationen als erfüllt angesehen werden.

Konformitätsvermutung. Das bedeutet, das Startup hat auch nach Durchlaufen dieser Sandboxes keine 100-prozentige Garantie auf einen Marktgang. Abgesehen von speziellen Ausnahmefällen, in denen Kosten entstehen könnten, ist die Nutzung dieser KI-Reallabore für KMUs und Startups grundsätzlich kostenlos. Eine falsche Einstufung kann Strafen nach sich ziehen. Die Regelungen zu Bußgeldern im Rahmen der KI-Verordnung enthalten spezifische Erleichterungen für Startups. Artikel 71 Absatz 5a der KI-Verordnung legt eine generelle Begrenzung der Bußgelder für KMUs und Startups fest. Im Falle von zwei möglichen Bußgeldern für ein Unternehmen muss stets das niedrigere ausgewählt werden.

Beispiel:

Ein HR-Dienstleister möchte eine Anwendung bauen, die auf Grundlage von persönlichen Daten, Bewerbungen rankt. Hierfür werden unter anderem Lebensläufe genutzt. Die Anwendung wird als risikoreich eingestuft, da sie die Gefahr der Diskriminierung birgt. Das System muss eine Konformitätsbewertung durchlaufen und Anforderungen in folgenden Bereichen erfüllen:

- Risikomanagementsystem
- Daten und Datenverwaltung
- Technische Dokumentation
- Aufzeichnungen
- Transparenz und Bereitstellung von Informationen für den Nutzer
- Menschliche Aufsicht
- Genauigkeit, Robustheit und Cybersicherheit
- Qualitätsmanagementsystem
- Bewertung der Auswirkungen auf die Grundrechte

Kategorie 3: Begrenztes Risiko

Es werden drei Gruppen von Systemen mit begrenztem Risiko definiert:

1. KI-Systemen, die zur Interaktion mit natürlichen Personen konzipiert sind.
2. KI-Systeme, die zur Emotionserkennung oder biometrischen Kategorisierung fähig sind.
3. KI-Systeme, die Bild-, Audio- oder Videoinhalte generieren oder manipulieren, um Deepfakes zu erstellen.

Für diese Systeme sind Transparenzanforderungen zu erfüllen. Das bedeutet vor allem, dass User darüber informiert werden müssen, mit einem KI-System zu interagieren bzw., dass KI-generierter Content als solcher gekennzeichnet werden muss.

Beispiel:

Eine Bildungsplattform verwendet KI, um Lehrvideos mit generierten Abbildungen historischer Persönlichkeiten zu erstellen, die komplexe wissenschaftliche und historische Themen verständlich erklären. Das Unternehmen ist laut AI Act verpflichtet, User darüber aufzuklären, dass sie mit einem KI generierten Avatar kommunizieren.

Kategorie 4: Minimales Risiko

Hierzu zählen Anwendungen, von denen ein geringes Risiko ausgeht, beispielsweise Anti-Spam-Filter oder Künstliche Intelligenz in Videospielen. Es bestehen keine Anforderungen nach dem AI Act. Eine freiwillige Verpflichtung zu Compliance-Richtlinien kann erfolgen.

Beispiel:

Ein Startup hat einen fortschrittlichen Mail-Filter entwickelt. Dieser nutzt KI, um Spam basierend auf einer Vielzahl von Kriterien, wie Keywords, Absender oder Öffnungs-Verhalten des Nutzers zu klassifizieren. Da von dem Filter ein geringes Risiko ausgeht, fallen keine spezifischen Anforderungen an. Das Unternehmen beschließt jedoch freiwillig Compliance-Verpflichtungen zu implementieren. Diese umfassen:

- Transparenz
- Datenschutz
- Nutzerkontrolle
- Feedbackmöglichkeit

Wie werden sogenannte *General-Purpose-Systeme* klassifiziert?

Für generative KI weicht der AI Act vom zuvor dargestellten risikobasierten Ansatz ab. Generative KI wird im AI Act unter dem Begriff General-Purpose-AI-Modelle (GPAI) reguliert. Unter GPAI versteht man leistungsstarke KI-Systeme, die eine Bandbreite an Aufgaben übernehmen können und nicht auf ein Anwendungsgebiet spezialisiert sind (wie beispielsweise GPT-4). Neben “normalen” GPAI-Modellen gibt es eine zweite Stufe von GPAI-Modellen mit systemischen Risiken, die zusätzlichen Anforderungen unterliegen. Die Definition als systemisch riskant basiert aktuell lediglich auf der Rechenleistung des jeweiligen Modells. Ab 10^{25} FLOPS gelten GPAI-Modelle als systemisch riskant.

Das EU AI Office, welches die alleinige Aufsicht über GPAI-Modelle übernehmen wird, behält sich jedoch die Einführung weiterer Kriterien vor. Dies könnte beispielsweise die Anzahl der Nutzerinnen und Nutzer betreffen, um eine differenzierte Bewertung zu ermöglichen. Die rechtlichen Anforderungen hängen stark davon ab, ob ein Modell als Open Source gilt oder nicht (siehe unten).

Rechenleistung > 10^{25} Flops

Open Source	Erfordert Einhaltung der Urheberrechtsrichtlinie und detaillierte Dokumentation zu Trainingsdaten.
Nicht Open Source	Zudem technische Dokumentation erforderlich, neben anderen Verpflichtungen wie u.a. Pflichten gegenüber Downstream-Anbietern, Strategien zur Einhaltung des EU-Urheberrechts sowie eine Zusammenfassung der Trainingsdaten.

Rechenleistung < 10^{25} Flops

Open Source	Erfordert Einhaltung der Urheberrechtsrichtlinie und detaillierte Dokumentation zu Trainingsdaten.
Nicht Open Source	Gleiche Anforderungen wie Open Source, jedoch mit zusätzlichen Verpflichtungen etwa Adversarial Testing und Modellevaluierung oder Cybersicherheitsvorkehrungen.

Noch Fragen oder Unklarheiten? Nutze jetzt unser AI Act - Risk Classification Tool. Beantworte einfach einige kurze Fragen und erhalte unmittelbar eine personalisierte Übersicht über relevante Aspekte des AI Act.

Link zum Tool: https://www.bitkom.org/Startup-Risk-Classification-Tool-AI-Act

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in

Christofer Bingener | Referent Startups

T 030 27576-220 | c.bingener@bitkom.org

Verantwortliches Bitkom-Gremium

Get Started Deeptech Network