AI Act: Die EU möchte die Risiken von KI in den Griff bekommen

Am 1. August 2024 tritt der AI Act in Kraft. Er gilt als das weltweit erste Gesetz zur Regulierung künstlicher Intelligenz (KI). Der AI Act teilt KI in Risikogruppen ein. Je höher das Risiko einer Anwendung, desto höher sollen die Anforderungen und Pflichten sein.

Künstliche Intelligenz ist für viele Menschen der große Hoffnungsträger für die Wirtschaft, das Gesundheitswesen und die Wissenschaft. Doch es gibt auch eine ganze Menge Kritiker, die die Risiken der KI fürchten und nach Regeln verlangen. Mit dem AI Act (auch KI-Gesetz) will die EU künstliche Intelligenz für den europäischen Raum nun regulieren und so die größten Risiken für die Nutzerinnen und Nutzer in den Griff bekommen. Am 21. Mai 2024 hatten die EU-Mitgliedstaaten der Verordnung zugestimmt. Am 12. Juli erfolgte schließlich die Veröffentlichung im Amtsblatt der EU. Die finale Fassung der Verordnung weicht erheblich von dem Entwurf aus dem Jahr 2021 ab.

Die Idee der Verordnung: Je höher das Risiko eines KI-Systems, desto höher sind die damit verbundenen Anforderungen und Pflichten. Die KI-Regulierung soll das Vertrauen der Nutzerinnen und Nutzer in Künstliche Intelligenz innerhalb der EU stärken und so auch für Hersteller und Verwender von KI-Anwendungen bessere Voraussetzungen für Innovation schaffen.

Verstöße können Geldbußen von bis zu 35 Millionen Euro oder bis zu sieben Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres nach sich ziehen. Die Sanktionen sind damit mit denen der DSGVO zu vergleichen.

Der AI Act soll begleitet werden von einer KI-Haftungsrichtlinie. Und auch die Produkthaftungsrichtlinie möchte die EU-Kommission aktualisieren. Das Ziel: Haftungslücken beim Einsatz von KI-Systemen sollen geschlossen und Beweisschwierigkeiten bei Rechtsverletzungen im Zusammenhang mit Künstlicher Intelligenz begegnet werden.

Die Pflichten des EU AI Act treffen Hersteller, Anbieter und Händler von KI-Systemen, Produkthersteller, die KI-Systeme in ihre Produkte einbinden, sowie Nutzer von KI-Systemen, also praktisch jedes Unternehmen.

KI mit einem „unannehmbaren“ Risiko verbietet der AI Act

Der AI Act teilt Künstliche Intelligenz in drei Risikoklassen ein: „unannehmbar“, „hoch“ und „gering/minimal“.

Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die ein unannehmbares Risiko darstellen, sind verboten. Hierzu zählen insbesondere solche KI-Systeme, die dazu bestimmt sind, menschliches Verhalten unterschwellig nachteilig zu beeinflussen. Auch KI, die der Ausnutzung von Schwächen schutzbedürftiger Personen dient, ist nicht annehmbar und damit verboten. Untersagt ist auch die Nutzung von KI-Systemen durch Behörden zur Bewertung oder Klassifizierung von Vertrauenswürdigkeit natürlicher Personen („Social Scorings“). KI-Systeme dürfen ebenso grundsätzlich nicht zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eingesetzt werden.

Für KI-Systeme mit Risikoklasse „hoch“ gelten besondere Anforderungen

KI-Systeme, die ein hohes Risiko für die Gesundheit und Sicherheit oder für die Grundrechte natürlicher Personen darstellen, werden als „Hochrisiko-KI-Systeme“ bezeichnet. Darunter fallen zum Beispiel die Würde des Menschen, die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung und die Informationsfreiheit und die Versammlungs- und Vereinigungsfreiheit.

An die Gestaltung und Nutzung von Hochrisiko-KI-Systemen stellt der AI Act hohe Anforderungen, zum Beispiel an die Qualität der Datengrundlage, an die Sicherheit, die Funktionsweise, aber auch an die Dokumentation und Aufsicht durch Menschen sowie das Qualitäts- und Risikomanagement.

Die Konformität mit dem AI Act sollte mit einer CE-Kennzeichnung sichtbar gemacht werden.

Geringere Anforderungen an Systeme mit Risikoklasse „gering/minimal“

Sofern KI-Systeme nicht unannehmbar und auch nicht als Hochrisiko-KI-System einzustufen sind, fallen sie in die dritte Kategorie. Sie unterliegen dann weniger strengen Anforderungen. Anbieter solcher Systeme sollen aber dennoch Verhaltenskodizes erstellen und ermutigt werden, die Regelungen für Hochrisiko-KI-Systeme freiwillig anzuwenden. Zudem fordert der EU AI Act, dass auch KI-Systeme mit geringem Risiko sicher sein müssen, sofern sie in den Verkehr gebracht oder in Betrieb genommen werden. Sicherheit kann insbesondere dadurch gewährleistet werden, dass freiwillig die Regelungen für Hochrisiko-KI-Systeme beachtet werden.

Neue Regelungen für General Purpose AI Models (GPAI)

Der AI Act enthält zusätzlich konkrete Regelungen für KI-Modelle mit allgemeinem Verwendungszweck, auch General Purpose AI (GPAI) genannt. Diese KI-Modelle können unterschiedlichen Zwecken dienen und als selbständiges System oder als integrativer Bestandteil anderer Systeme auftreten. Sie stellen grundsätzlich KI-Systeme mit begrenztem Risiko dar und unterfallen damit den Transparenzpflichten aus Art. 52. Zusätzlich wurde jedoch im neuen Art. 52a die Kategorie der „GPAI-Modelle mit systemischem Risiko“ eingeführt. Darunter fallen GPAI-Modelle mit einer „hohen Wirkungsmöglichkeit“. Die Wirkungsmöglichkeit ist hoch, wenn die Fähigkeiten des Modells den Fähigkeiten der fortschrittlichsten GPAI-Modelle entsprechen oder diese übertreffen. Dies soll anhand von Benchmarks oder auf Grund von Feststellungen der EU-Kommission ermittelt werden. Wenn der Rechenaufwand für das Training, gemessen in „floating point operations“, 10^25 übersteigt, wird es vermutet. Für GPAI-Modelle gibt es einige Pflichten, zum Beispiel: die Bereitstellung technischer Unterlagen und Gebrauchsanweisungen, die Beachtung des Urheberrechts und die Zusammenfassung der für das Training verwendeten Inhalte. Für GPAI-Modelle mit systemischem Risiko treten weitere Verpflichtungen bezüglich der Risikosteuerung und der Gewährleistung der Cybersicherheit hinzu.

Ab wann gilt der AI Act?

Die Anwendung der Regelungen des AI Acts ist zeitlich gestaffelt: Regelungen zu verbotener KI gelten nach sechs Monaten, bestimmte Regelungen für Hochrisiko-KI und GPAI nach einem Jahr und die restlichen Regelungen gelten zwei Jahre nach dem Inkrafttreten. Für KI-Systeme, die einer in Annex II des AI Acts aufgezählten Regulierung unterfallen, ist derzeit sogar eine Umsetzungsfrist von 36 Monaten vorgesehen.

Mit einer KI-Governance können Unternehmen Risiken absichern

Unternehmen sollten aktiv jede einzelne Anwendung evaluieren und in eine Governance-Struktur einbinden.

Auch alle KI-basierten Lösungen sollten betrachtet werden. Anwendungsfälle und die damit verbundenen Risiken sollten Unternehmen kennen. Hersteller eines Endprodukts müssen die im AI Act festgelegten Anbieterpflichten erfüllen und sicherstellen, dass das in das Endprodukt eingebettete KI-System den Anforderungen entspricht. Zu den Risiken gehört auch das Haftungsrisiko aus dem KI-Gesetz.

Beim Aufbau einer KI-Governance ist entscheidend, wer die Einstufung der Risiken verantwortet. Damit die Einschätzung möglich objektiv wird, sollte das Team interdisziplinär sein.

Wie ein KI-Risikomanagement gelingen kann

Für ein effektives Risikomanagement sollten Unternehmen Guidelines, Prozesse und Monitoring-Lösungen etablieren. Verschiedene Institutionen und Organisationen wie BSI, IDW oder DIN erarbeiten bereits Standards hierfür.

Es ist empfehlenswert, Compliance und Performance nicht voneinander zu trennen. Das Management und die IT sollten daher eng mit den Rechts- und Compliance-Funktionen zusammenarbeiten. Nur wenn sichergestellt ist, dass Rechtsvorschriften eingehalten sind und Haftungsrisiken minimiert werden, kann das Potenzial von Künstlicher Intelligenz tatsächlich ausgeschöpft werden.

Nachdem der AI Act jetzt final verabschiedet ist, sollten Unternehmen mit der Risikoeinschätzung beginnen und eine entsprechende Governance etablieren.

Erfahren Sie mehr zum Thema „KI-Risiken im Blick“: Unser Whitepaper gibt Empfehlungen für eine KI-Governance, die eine verantwortungsvolle Nutzung der neuen Technologie sicherstellt. Jetzt herunterladen.

Autoren:
KPMG AG Wirtschaftsprüfungsgesellschaft: Dr. Justus H. Marquardt, Oleg Brodski
KPMG Law Rechtsanwaltsgesellschaft mbH: Francois Heynike

Ansprechpartner:

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com