Foto: Adobe Stock

TITELTHEMA SERVICE SELLS

EU AI Act – Was Unternehmen jetzt wissen müssen

Der EU AI Act ist da – doch wie geht es nun weiter? Was die Regelungen der EU-Verordnung konkret für Unternehmen bedeuten, ordnet die Initiative „KI in der Praxis" des eco – Verband der Internetwirtschaft e.V. in einem praxisnahen Whitepaper ein. Ein Gastbeitrag von Dr. Jens Eckhardt, Partner bei pitc legal – Eckhardt Rechtsanwälte Partnerschaft und Vorstand bei EuroCloud, sowie Michael Hase, Manager EuroCloud bei eco.

Der EU AI Act ist seit dem 2. Februar dieses Jahres anwendbares Recht. Seitdem müssen Unternehmen in der EU die ersten Pflichten der Verordnung erfüllen. Zum einen müssen sie nun „Maßnahmen" ergreifen, mit denen sie sicherstellen, dass ihre Mitarbeitenden, wenn sie KI-Systeme betreiben oder nutzen, „über ausreichende KI-Kompetenz verfügen" (Art. 4 AI Act). Zum anderen setzt der AI Act dem Einsatz von KI-Systemen engere Grenzen, indem er Praktiken verbietet, die mit inakzeptablen Risiken verbunden sind (Art. 5 AI Act). Weitere Regelungen werden folgen, indem der AI Act sukzessive anwendbares Recht wird.

Schulungen zur Vermittlung von KI-Kompetenz

Bei den Maßnahmen, mit denen Unternehmen die KI-Kompetenz ihrer Mitarbeitenden sicherstellen, dürfte es sich meist um Schulungen oder Trainings handeln. Doch Standardkurse allein reichen dazu nicht aus: Die Unternehmen müssen bei der Weiterbildung ihrer Mitarbeitenden sowohl deren Ausbildung, technische Kenntnisse und Erfahrung berücksichtigen als auch den Kontext, in dem KI-Systeme in den Einsatz kommen sollen. So

unterscheiden sich die Anforderungen an die KI-Kompetenz in unterschiedlichen Bereichen – von Vertrieb über Personalwesen bis zu IT, Finance oder Forschung & Entwicklung. Eine Basisschulung für alle kann jedoch ein sinnvoller Ausgangspunkt sein. Zudem ist es notwendig, die Schulungsmaßnahmen zu dokumentieren, um sie gegenüber Aufsichtsbehörden nachweisen zu können.

Inakzeptable Risiken setzen Grenzen

Eine weitere Vorsichtsmaßnahme nimmt der Gesetzgeber im AI Act mit dem Verbot bestimmter KI-Praktiken vor. Dies betrifft insbesondere KI-Anwendungen, die grundlegende Rechte, die Menschenwürde, die Sicherheit oder demokratische Prozesse gefährden könnten. In diesen Fällen wird das Risiko als so gravierend angesehen, dass selbst umfassende Maßnahmen zur Risikominderung nicht ausreichen und ein vollständiges Verbot notwendig ist. Für Unternehmen und Organisationen ist es daher essenziell, die Tragweite des AI Act zu verstehen. Führungskräfte müssen sich nicht nur mit den konkreten Auswirkungen der Regulierung befassen, sondern auch die gestaffelten Inkrafttretungsfristen im Blick behalten. Aktuell besonders relevant sind einige Verbote und Pflichten – darunter das Verbot unannehmbar riskanter KI-Systeme – die bereits seit dem 2. Februar 2025 gelten. Im Whitepaper „AI Act – Worüber reden wir eigentlich?“ erläutert die Arbeitsgruppe „Rahmenbedingungen“ der eco Initiative „KI in der Praxis“, welche Aspekte das Gesetz umfasst und was Unternehmen bei der Umsetzung berücksichtigen müssen.

Von der Risiko-Kategorisierung bis zur kontinuierlichen Überprüfung

Angefangen beim Ziel des AI Acts: Während die Datenschutz-Grundverordnung (DSGVO) den Schutz personenbezogener Daten zum Gegenstand hat, zielt der EU AI Act darauf ab, potenzielle Schäden, die KI-Systeme verursachen können, zu verhindern. Darüber hinaus will die Verordnung EU-weite Rechtssicherheit für den Einsatz und die Entwicklung von KI auf dem europäischen Markt schaffen. Denn der AI Act fällt in die Kategorie des Produktsicherheitsrechts. Das heißt, er regelt die Verkehrsfähigkeit und Sicherheit der Produkte, die der Markt bereitstellt, und ist keine Art „Datenschutz 2.0“-Gesetz. Dazu gehört auch die Bewertung von KI-Algorithmen, die in Anwendungen zum Filtern problematischer Inhalte, in Plattformen für zielgerichtete Werbung und in Chatbots für den Kundendienst eingesetzt werden. Der AI Act kategorisiert KI-Systeme nach ihrem Risikoniveau und teilt sie in vier Klassen ein: Systeme mit unannehmbarem, hohem, begrenztem und minimalem Risiko.

Bei Systemen mit inakzeptablem Risiko ist es durch den AI Act grundsätzlich untersagt, sie in Verkehr zu bringen, in Betrieb zu nehmen oder zu verwenden. Zu den verbotenen Praktiken zählen unter anderem:

- **Manipulative KI:** Systeme, die unterschwellige oder manipulative Techniken einsetzen, um das Verhalten von Menschen zu beeinflussen und ihnen Schaden zuzufügen, und Systeme, die Schwachstellen bestimmter Personengruppen (z. B. aufgrund von Alter oder Behinderung) ausnutzen
- **Social Scoring:** KI-Systeme, die Menschen aufgrund ihres Sozialverhaltens bewerten und dadurch benachteiligen
- **Risikobewertung bei Straftaten:** KI-Systeme, die das Risiko einer Straftat allein aufgrund von Persönlichkeitsprofilen vorhersagen (Ausnahmen gelten für Systeme, die bei der Bewertung von Straftaten auf Basis objektiver Fakten unterstützen)
- **Biometrische Systeme:** Datenbanken zur Gesichtserkennung, KI-Systeme, die Emotionen von Menschen am Arbeitsplatz oder in Bildungseinrichtungen erkennen und identifizieren, Systeme, die Menschen

/ 5 TAKE-AWAYS ZUM AI ACT

Im Whitepaper „AI Act – Worüber reden wir eigentlich?“ finden Unternehmen praktische Erläuterungen zu den Regelungen der EU-Verordnung. Zudem beinhaltet es ein Glossar, das die Zuordnung zwischen den Begriffen aus dem technologischen Kontext mit der Begriffswelt des AI Act erleichtert. Auf ihrer Website will sich die Initiative KI in der Praxis der weiteren Ausarbeitung widmen.

1. Seit dem 2. Februar 2025 gelten eine KI-Schulungspflicht für Mitarbeitende, die KI-Systeme nutzen, sowie ein Verbot für KI-Systeme mit inakzeptablem Risiko.
2. Als Teil einer umfassenden Datenstrategie ist der EU-AI Act darauf ausgelegt, die Risiken von KI zu bewältigen, aber auch Innovationen zu fördern – gleichzeitig sollen personenbezogene Daten geschützt sein.
3. KI-Systeme werden auf der Grundlage von Risiken kategorisiert, wobei für verschiedene Anwendungen unterschiedliche Konformitätsniveaus erforderlich sind. Zum Beispiel: KI-Modelle für allgemeine Zwecke wie Claude, Gemini und GPT stellen aufgrund ihrer breiten Anwendbarkeit systemische Risiken dar, die besondere Vorsicht und die Berücksichtigung ihrer gesellschaftlichen Auswirkungen erfordern.
4. Unternehmen können zu KI-Anbietern mit größeren rechtlichen Verpflichtungen werden, indem sie bereits trainierte Modelle modifizieren oder ihren Verwendungszweck ändern.
5. Die Zusammenarbeit von Unternehmen mit politischen Entscheidungsträgern ist gefragt, um zukünftig ein Gleichgewicht zwischen dem Schutz der Gesellschaft und der Förderung von Innovationen zu gewährleisten. Dabei können Unternehmen, die ethischen KI-Praktiken Priorität einräumen, bei den Nutzern Vertrauen aufbauen und sich einen Wettbewerbsvorteil auf dem Markt verschaffen.

Download des Whitepapers unter bit.ly/ecoKIPraxis

Dr. Jens Eckhardt, Partner bei pitc legal – Eckhardt Rechtsanwälte Partnerschaft und Vorstand bei EuroCloud

Michael Hase, Manager EuroCloud bei eco.

nach sensiblen Merkmalen wie ethnischer Zugehörigkeit oder sexueller Orientierung kategorisieren, sowie Systeme zur Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (Ausnahmen gelten, wenn eine akute Bedrohung vorliegt)

Zu den Systemen mit hohem Risiko, die mit erheblichen Anforderungen verbunden sind, gehören KI-Systeme, die unter anderem in kritischen Infrastrukturen, im Gesundheitswesen, im Personalwesen und bei der Kreditvergabe eingesetzt werden. Für diese Systeme müssen Unternehmen ein robustes Risikomanagement einführen, die Entwicklungsprozesse dokumentieren, die Konformität der Systeme bewerten und sie in einer EU-Datenbank registrieren. Die Einhaltung des AI Act ist kein einmaliges Ereignis, sondern erfordert eine laufende Überwachung, Berichterstattung und die Beseitigung potenzieller Verzerrungen z. B. durch diskriminierende Trainingsdaten.
Der AI Act regelt auch die Verwendung von KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI, GPAI), wenn sie aufgrund ihres Umfangs und ihrer potenziellen Auswirkungen als systemisches Risiko durch den AI Act eingeordnet werden. Dazu zählen Modelle wie Claude, Gemini oder GPT. Die Anbieter dieser leistungsstarken Werkzeuge müssen über die Bewertung des Risikos ihrer spezifischen Anwendung hinausgehen und die breiteren gesellschaftlichen Auswirkungen des Modells selbst berücksichtigen.

Unterschiedliche Pflichten je Rolle und Zeitpunkt

Zudem unterscheidet der AI Act zwischen verschiedenen Rollen mit unterschiedlichen Pflichten und betrachtet dabei die Akteure der gesamten Wertschöpfungskette. Im Zentrum stehen die Anbieter und die Betreiber. Der Anbieter ist – vereinfacht gesagt – derjenige, der das KI-System bereitstellt, während der Betreiber der Verwender ist. Dabei kann ein Betreiber von KI-Systemen zum Anbieter werden, wenn er wesentliche Änderungen an einem vortrainierten Modell vornimmt oder es nicht bestimmungsgemäß nutzt. In diesem Fall unterliegt er anderen regulatorischen Verpflichtungen.

Die Auslegung des AI Act ist noch in der Entwicklung. Es ist daher außerdem entscheidend, zu berücksichtigen, wann welche Regelungen zur Anwendung kommen. So lässt sich beobachten, wie sich die Auslegung entwickelt und zur richtigen Zeit in die Umsetzung einsteigen. Sowohl zu früh als auch zu spät kann dies zu erhöhten Aufwänden führen. Eine Übersicht über den Anwendungsbeginn der kommenden Regelungen ist im Whitepaper „AI Act – Worüber reden wir eigentlich?“ zu finden.
Mehr Einblicke in das Thema gibt auch die Roadshow zum AI Act, organisiert von der eco Initiative KI in der Praxis: Start in Berlin, 21. März 2025.

/ ÜBER ECO

Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.

/ ÜBER EUROCLOUD

EuroCloud Deutschland_eco e. V. ist der Verband der Cloud-Computing-Wirtschaft. Er setzt sich für Akzeptanz und bedarfsgerechte Bereitstellung von Cloud Services am deutschen Markt ein. Dabei steht der Verein in ständigem Dialog mit den Partnern des europäischen EuroCloud-Netzwerks. EuroCloud Deutschland_eco e. V. wurde im Dezember 2009 gegründet und ist dem eco – Verband der Internetwirtschaft e. V. angegliedert. Zusammen erschließen die Verbände größtmögliche Synergien, um bei den relevanten Themen maximale Reichweite zu schaffen.