Blogartikel vom 02.05.2024
Rechtsgebiet: IT-Recht
Autor: Rechtsanwalt Christian Geißler

Der AI ACT – Was hat die Europäische Union vor und was müssen Unternehmen beachten?

Das Thema Künstliche Intelligenz beschäftigt bereits seit Jahren unser privates und berufliches Leben. Seit Markteinführung von ChatGPT im Jahr 2022 hat das Thema aber eine ganz neue Dimension erreicht. Seitdem beschäftigen sich auch Behörden und Regierungen verstärkt damit, wie mit dem Thema Künstliche Intelligenz umzugehen ist und ob eine Regulierung möglich ist.

So auch die Europäische Union, die im März den sog. Artificial Intelligence Act (AI Act) im EU-Parlament verabschiedet hat und damit den ersten Versuch einer umfassenden Regulierung des Einsatzes von künstlicher Intelligenz geschaffen hat.

Doch was genau regelt der AI Act und was hat die neue Verordnung für Unternehmen in der EU zu bedeuten?

Ab wann gilt der AI Act?

Der AI Act wurde am 13. März 2024 durch das Europäische Parlament verabschiedet. Sobald dieser auch vom Europäischen Rat verabschiedet worden ist, wird er 20 Tage nach seiner Veröffentlichung im Amtsblatt in Kraft treten. Die meisten Regelungen des AI Acts sind aber erst nach zwei Jahren anwendbar, nur ein paar wenige schon vorher.

Insbesondere die Regelungen zu verbotenen Systemen werden schon nach 6 Monaten wirksam. Auch die Verpflichtungen für Anwendungen mit Künstlicher Intelligenz mit einem allgemeinen Verwendungszweck werden schon nach einem Jahr wirksam.

Diese Fristen sollen Wirtschaft und Behörden die Möglichkeit geben die Verordnung umsetzen zu können.

Für wen oder was gilt der AI Act?

Der AI Act soll Systeme unter Verwendung Künstlicher Intelligenz regulieren. Zur Abgrenzung welche Systeme darunterfallen, übernimmt der AI Act die Definition der OECD zur Künstlichen Intelligenz (die deutsche Übersetzung der Definition steht noch aus):

> *„‘AI system‘ is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.“*

Es muss sich also um ein maschinengestütztes System handeln, welches für einen wechselnden autonomen Betrieb ausgelegt ist, anpassungsfähig ist und aufgrund verschiedener Eingaben eigene Ausgaben in Form von Ergebnissen wie Vorhersagen, Inhalten, Empfehlungen oder Entscheidungen generieren kann, die eine physische oder virtuelle Umgebung beeinflussen können.

Die Regelungen

Der AI Act verfolgt einen risikobasierten Ansatz, mit welchem vor allem diejenigen Systeme reguliert werden sollen, die ein hohes Risiko darstellen.

Im Detail unterscheidet der AI Act zwischen verbotenen KI-Praktiken, Hochrisiko-Systemen, Systemen mit begrenzten Risiken und Systemen mit minimalem oder keinem Risiko.

Unter verbotene Praktiken fallen z.B. Systeme zur Beeinflussung von Verhalten, Soziale Bewertungssysteme, Prädikative Polizeisysteme, biometrische Echtzeitfernidentifizierungssysteme oder Systeme zur Erkennung von Emotionen.

Hochrisiko Systeme sind z.B. autonome Fahrzeuge oder Systeme mit welchen die Kreditwürdigkeit einer natürlichen Person bewertet werden kann.

Die Hersteller, Einführer aber auch die Händler von KI-Systemen unterliegen also bestimmten Verpflichtungen aus dem AI Act.

Die Hersteller müssen vorab prüfen unter welche Kategorie das betreffende System fällt und ob vor Inbetriebnahme weitere Maßnahmen wie z.B. noch notwendige Anpassungen des Systems, die Überwachung des Betriebs oder bestimmte Dokumentationspflichten erfüllt werden müssen, damit die Vorgaben des AI Acts eingehalten werden.

Der Einführer eines KI Systems muss unter anderem prüfen, ob das betreffende System die notwendigen Dokumentationspflichten aus dem AI Act eingehalten hat. Falls er sogar Grund zur Annahme hat, dass ein System den AI Act nicht einhält, so darf er dieses erst dann in Verkehr bringen, wenn Konformität hergestellt werden konnte.

Der Händler muss dagegen nicht nur prüfen, ob das System mit der erforderlichen CE-Konformitätskennzeichnung versehen ist, sondern auch, ob dem System die erforderliche Dokumentation und Gebrauchsanweisung beigefügt sind und ob der Anbieter bzw. gegebenenfalls der Einführer des Systems die im AI Act festgelegten Pflichten erfüllt hat.

Zudem gibt es Transparenzpflichten für Systeme die mit natürlichen Personen interagieren. Den natürlichen Personen muss offenbart werden, dass sie mit einem KI-System interagieren. Ebenso müssen künstlich erstellte Audio-, Bild- oder Textinhalte als solche gekennzeichnet werden.

Daneben müssen auch die Vorgaben aus der Europäischen Datenschutzgrundverordnung (DS-GVO) eingehalten werden, wenn in den Systemen personenbezogene Daten verarbeitet werden.

Weiterhin sollen in allen EU-Mitgliedsstaaten Aufsichtsbehörden geschaffen werden, deren Aufgabe die Überwachung und Einhaltung des AI Acts ist.

Zuletzt gibt es, wie auch bei der seit dem Jahr 2018 geltenden DS-GVO Sanktionsmöglichkeiten bei Verstößen gegen die Verordnung. Die Bußgelder sind dabei sogar noch höher als die der DS-GVO und können bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes eines Unternehmens betragen. Unternehmen, die Systeme mit Künstlicher Intelligenz herstellen, in den Verkehr bringen oder selbst nutzen, haben also einen noch größeren Anreiz die Vorgaben des AI Acts zu erfüllen.