Neue Spielregeln für künstliche Intelligenz

Der AI Act der EU ist auf der Zielgeraden – Handlungsbedarf für Unternehmen – Compliance-Verantwortung der Firmenleitung

Von Marieke Luise Merkle *)

Börsen-Zeitung, 3.2.2024

Seit einem Leak vor zwei Wochen ist die finale Einigung des AI Act bekannt. Die europäische Verordnung bringt zahlreiche Anforderungen an den Einsatz von KI mit sich. Unternehmen sollten sich frühzeitig mit den Anforderungen des Gesetzes auseinandersetzen.

Einigung in letzter Sekunde

Mit dem Ziel, die weltweit erste umfassende Regulierung künstlicher Intelligenz zu schaffen, legte die EU-Kommission am 21. April 2021 den Entwurf einer KI-Verordnung („AI Act") vor. Etwa drei Jahre nach dessen Veröffentlichung erzielten die europäischen Gesetzgebungsorgane am 8. Dezember 2023 eine Einigung im Trilogverfahren, an dem die EU-Kommission, der Rat und das Parlament beteiligt sind.

Zu den zuletzt im Gesetzgebungsverfahren heiß diskutierten Themen zählte u.a. die Regulierung von Foundation Models (auch „Basismodelle"). Charakteristisch für diese Modelle ist neben dem durchlaufenen Training anhand von großen Datenmengen ihre Anpassungsfähigkeit an unterschiedlichste Aufgaben und Einsatzzwecke. Zu den bekanntesten Foundation Models zählt GPT-4, das OpenAIs ChatGPT zugrunde liegt. Frankreich, Deutschland und Italien hatten sich im Hinblick auf derartige Foundation Models zuletzt mit Nachdruck für eine Selbstregulierung eingesetzt.

Neben der Regulierung von Foundation Models galt es etwa eine Einigung im Hinblick auf die Governance sowie das sensible Thema des Einsatzes von KI im Bereich der Strafverfolgung zu erzielen.

Aufgrund der Anzahl an bis zuletzt noch offenen Punkten im Gesetzgebungsverfahren kann zu Recht die Frage aufgeworfen werden, ob sich der europäische Gesetzgeber mehr Zeit hätte nehmen sollen, um das Gesetz zu finalisieren. Klar ist, dass hier über Parteigrenzen hinweg ein politischer Erfolg gewünscht war: Der AI Act als legislative Trophäe der ersten umfassenden Regulierung künstlicher Intelligenz. Abseits jeglicher polemischen Übertreibung kann konstatiert werden, dass die finale Einigung Anbieter und Anwender von KI-Systemen vor Herausforderungen stellt. Wesentliche Rechtsunsicherheiten – beispielsweise im Hinblick auf die Definition von KI-Systemen – konnten nicht ausgeräumt werden. Auch obliegt die oftmals nicht ganz einfache Einordnung eines KI-Systems anhand der unterschiedlichen Risikogruppen des Gesetzes vollumfänglich den Unternehmen.

Ungeachtet der Frage, ob man der Kommission in ihrer Einschätzung der Innovationsförderung durch Regulierung folgt, sind Unternehmen gehalten, sich bereits jetzt mit dem AI Act auseinanderzusetzen. Das Gesetz befindet sich auf der Zielgeraden. Nach der sich abzeichnenden Zustimmung der Mitgliedstaaten soll die formale Verabschiedung spätestens im April stattfinden. Für verbotene Anwendungen gelten die Regelungen bereits nach einer Übergangsphase von sechs Monaten nach Inkrafttreten.

Der AI Act ist als präventives Verbotsgesetz ausgestaltet: Der Einsatz von KI ist unzulässig, sofern die Anforderungen des Gesetzes nicht erfüllt werden. An dieser Stelle sei auf die Bußgelder von bis zu 35 Mill. Euro bzw. 7 % des weltweiten Umsatzes verwiesen, die im Fall eines Verstoßes gegen die Bestimmungen des AI Act verhängt werden können.

Unternehmen ist daher nahezulegen, bereits jetzt eine Einordnung von KI-Systemen anhand des AI Act vorzunehmen, um möglichst frühzeitig potenzielle Auswirkungen auf das eigene Unternehmen zu identifizieren („AI Risk Mapping").

Weiter Anwendungsbereich

Überraschend weit ist der Anwendungsbereich der Verordnung. Die Definition eines KI-Systems erfasst wesentlich mehr Softwaresysteme als dies bei Zugrundelegung einer klassischen Definition aus dem Bereich der Informatik der Fall wäre. Der Anwendungsbereich enthält daneben eine Reihe von interessanten Ausnahmen. Hierzu zählt etwa der Einsatz im Bereich der nationalen Sicherheit, militärischer Anwendungen, Forschung und Entwicklung sowie persönliche, nicht-berufliche Tätigkeiten. Unter bestimmten Voraussetzungen sind auch KI-Systeme, die unter einer Open-Source-Lizenz stehen, vom Anwendungsbereich ausgenommen.

Adressaten der Pflichten

Für welche Unternehmen gelten nun die Anforderungen nach dem AI Act? Diejenigen, die sich in Sicherheit wägen, weil sie selbst keine KI-Systeme entwickeln, sollten aufhorchen. Der AI Act enthält nicht nur Anforderungen an Softwarehersteller, sondern auch an weitere an der Wertschöpfungskette Beteiligte. So können bestimmte für Hersteller geltende Pflichten auf Anbieter, Importeure, Händler etc. übergehen. Ein Beispiel hierfür könnte etwa die Anpassung eines Foundation Models an einen bestimmten Einsatzzweck sein.

Neben einigen – mehr oder weniger konsequent ausgestalteten Verboten (z.B. Social Scoring, biometrische Fernidentifikation im öffentlichen Raum) – betrifft der Großteil der Regelungen und damit auch Pflichten des AI Act die Betreiber sogenannter Hochrisiko-KI. Als Hochrisiko-KI-Systeme werden zunächst Sicherheitskomponenten von Produkten und Produkte eingestuft, die bereits jetzt produktsicherheitsrechtlichen Anforderungen unterliegen. Daneben kann sich eine Einstufung als Hochrisiko-KI anhand besonders sensibler Einsatzbereiche ergeben, etwa im Bereich kritischer Infrastrukturen oder der Berufsausbildung.

Zu den von Anbietern von Hochrisiko-KI einzuhaltenden Anforderungen gehören die Einrichtung eines Risikomanagementsystems, Dokumentations-, Aufsichts- und Transparenzpflichten sowie strenge Anforderungen an die Daten, mit welchen das betreffende System trainiert, validiert und angewendet wird. Daneben ist ein Qualitätsmanagementsystem zu unterhalten. Das Berufsbild des KI-Beauftragten ist vor diesem Hintergrund gesichert. Die Kontrolle der Einhaltung der Anforderungen unterliegt dabei einem Konformitätsbewertungsverfahren und geht damit mit einer CE-Kennzeichnung einher.

Hervorzuheben an der nunmehr getroffenen Regelung ist, dass diese bereits unabhängig von einem etwaig mit dem Einsatzzweck verbundenen Risiko bestimmte Pflichten für Anbieter von Foundation Models (oder nach dem Wording der EU „General Purpose AI", „GPAI") vorsieht. Der europäische Gesetzgeber scheint mithin davon auszugehen, dass von GPAI – unabhängig von ihrem Anwendungsbereich – ein gewisses immanentes Risiko ausgeht. Anbieter von GPAI wie generativer KI müssen u.a. bestimmte Transparenzpflichten einhalten. Hierzu gehört die Offenlegung von Informationen über die Daten, mit welchen das Modell trainiert wurde. Eine Befriedung auf Seiten von Kunstschaffenden im Hinblick auf ihre urheberrechtlich geschützten Inhalte ist angesichts der geringen Detailtiefe der Information nicht zu erwarten. Im Fall generativer KI ist weiterhin offenzulegen, dass der Output des Systems (z.B. im Fall von Deepfakes) nicht authentisch ist.

Weitergehende Anforderungen gelten für GPAI, die mit systematischen Risiken verbunden ist. Hierzu zählen nach der Definition des Gesetzes besonders leistungsstarke Modelle, deren Rechenleistung im Rahmen des Trainings 10 hoch 25 Gleitkommaoperationen („FLOPS") übersteigt. Nur wenige der derzeit führenden Modelle erreichen bzw. überstiegen diesen Schwellenwert. Für GPAI, von denen systematische Risiken ausgehen, müssen Unternehmen u.a. ein Risikomanagementsystem einrichten und schwerwiegende Sicherheitsvorfälle gegenüber der zuständigen Behörde melden.

AI-Compliance ist Chefsache

Ungeachtet der noch verbleibenden kurzen Vorbereitungszeit auf den AI Act haben Unternehmen im Bereich der AI Compliance bereits jetzt zahlreiche Anforderungen rechtlicher Art zu beachten. Diese reichen vom Urheberrecht – man denke an die sich häufenden Klagen zu Urheberrechtsverletzungen wie etwa der Fall New York Times gegen Microsoft – über den Schutz personenbezogener Daten und die Wahrung von Geschäftsgeheimnissen. Je nach Sektor oder Einsatzzweck können sich weitere Anforderungen ergeben. Die Einhaltung der rechtlichen Rahmenbedingungen ist Teil der Führungsverantwortung der Unternehmensleitung.

Nichtsdestotrotz dürfen sich Unternehmen des Einsatzes von AI nicht verschließen. Ein rechtskonformer Einsatz kann i.d.R. durch verschiedene Maßnahmen wie AI Policies und entsprechende Compliance-Strukturen gewährleistet werden. Die Frage des „Ob" des Einsatzes stellt sich nicht; es geht mithin allein um das „Wie".

*) Marieke Luise Merkle ist Associated Partner der Kanzlei Noerr.