

Ein bedeutender Schritt in der KI-Regulierung

AI Act tritt am 2. August in Kraft: Bereits kleinere Pflichtverletzungen können sanktioniert werden – Viele Unternehmen sind unsicher

Von Susan Kempe-Müller
und Tim Wybitul *)

Börsen-Zeitung, 26.7.2025

Ein weiterer Meilenstein in der Umsetzung der europäischen KI-Verordnung tritt am 2. August 2025 in Kraft. Dann werden weitere Bestimmungen in der Europäischen Union und im Europäischen Wirtschaftsraum verbindlich, darunter: Transparenz- und Dokumentationspflichten für Anbieter von KI-Systemen, spezielle Anforderungen für Anbieter von General-Purpose AI (GPAI)-Modellen sowie Regelungen zu Governance, Marktüberwachung und erstmals auch Sanktionen.

Durchsetzung und Sanktionen

Der AI Act ist ohne Frage ein bedeutender Schritt in der Regulierung Künstlicher Intelligenz (KI) in Europa. Die EU hat ein vielschichtiges Regelwerk geschaffen, das sowohl Produktrecht als auch Grundrechtsschutz auf eine sehr komplexe Weise kombiniert. Die nun in Kraft tretenden Regeln betreffen Anbieter und Betreiber von KI-Systemen. Besonders im Fokus stehen dabei die Anbieter von KI-Systemen mit allgemeinem Verwendungszweck, sogenannten GPAI-Modellen.

Für die Kontrolle und Sanktionierung des neuen Regelwerks sind neben der EU-Kommission auch nationale Marktaufsichts- und Datenschutzbehörden zuständig. In Deutschland wird sich voraussichtlich die Bundesnetzagentur die Marktaufsicht mit sektorspezifischen Marktüberwachungsbehörden teilen.

Viele Unternehmen sind angesichts der Komplexität des AI Act unsicher, wie sie die neuen Vorschriften umsetzen sollen. Denn bereits kleinere Pflichtverletzungen, wie fehlende Schulungen für Mitarbeiter, die mit KI-Anwendungen arbeiten, können sanktioniert werden. Zudem sind einige Pflichten aus dem AI Act überraschend weitreichend: So müssen Unternehmen, die beispielsweise im Kundenservice auf ihrer Website KI-gesteuerte Chatbots einsetzen, die Nutzer spätestens bei der ersten Interaktion darüber informieren, dass es sich um ein KI-System

handelt – andernfalls riskieren sie ein Bußgeld. Die Information muss klar, direkt und innerhalb des Systems erfolgen, beispielsweise in einer gut sichtbaren Kopfzeile oder durch eine vorgeschaltete Chatbot-Nachricht. Ein bloßer Link, etwa zu einer AI Policy, genügt dagegen nicht.

Sanktionen werden grundsätzlich durch die Mitgliedstaaten bestimmt und können sowohl Bußgelder als auch andere Maßnahmen wie Verwarnungen sein. Der Bußgeldrahmen wird dabei durch den AI Act vorgegeben: Ein Unternehmen, das das Verbot bestimmter KI-Praktiken missachtet, muss mit einem maximalen Bußgeld von bis zu 7 Prozent des Jahresumsatzes oder 35 Mio. Euro rechnen. Andere Verstöße werden je nach Schwere mit bis zu 3 Prozent bzw. 15 Mio. Euro oder „nur“ 1% bzw. 7,5 Mio. Euro sanktioniert.

General-Purpose-AI-Modelle

Ab dem 2. August 2025 gelten im Rahmen der Verordnung erstmals verbindliche Governance- und Compliance-Vorgaben für Anbieter von GPAI-Modellen. Das sind KI-Modelle mit allgemeinem Verwendungszweck, wie etwa Large Language Models, also solche Modelle, die mithilfe umfangreicher Datenmengen trainiert werden, um menschenähnliche Sprache zu verstehen und zu generieren. Die EU-Kommission hat kürzlich einen Verhaltenskodex für GPAI-Modelle veröffentlicht. In den kommenden Wochen wird der Kodex nun von den Mitgliedstaaten und der Kommission bewertet und soll nun sehr bald final verabschiedet werden.

Der Kodex dient als Leitfaden für Entwickler und besteht aus den Kapiteln Transparenz, Urheberrecht und Sicherheit. Im Hinblick auf die Einhaltung des Urheberrechts konkretisiert die Kommission die Anforderungen an Anbieter von GPAI-Modellen. Dazu gehören beispielsweise Maßnahmen, die sicherstellen, dass Trainingsdaten für GPAI-Modelle im Netz rechtmäßig gesammelt und dabei Nutzungsvorbehalte erkannt und eingehalten werden. Wenn es technische Schutzmaßnahmen gibt, dann dürfen diese nicht umgangen werden. Dabei müssen KI-Anbieter

moderne Technologien einsetzen. Unterzeichnen Unternehmen den Verhaltenskodex und setzen ihn anschließend nicht um, kann darin ein bußgeldbewehrter Verstoß gegen den AI Act vorliegen.

Der Kodex soll dabei helfen, die Anforderungen des AI Acts zu erfüllen. Anbieter von GPAI-Modellen können ihn nutzen, um die Einhaltung ihrer rechtlichen Pflichten nachzuweisen. Die Europäische Kommission hat angekündigt, am 1. August 2025 eine erste Liste von Unternehmen zu veröffentlichen, die den Verhaltenskodex bis dahin unterzeichnet haben. Der Kodex ist zwar grundsätzlich freiwillig. Falls sich Unternehmen zum Nachweis der Einhaltung der Pflichten nach dem AI Act aber nicht oder nur teilweise auf den Kodex stützen wollen, müssen sie geeignete alternative Verfahren der Einhaltung aufzeigen. Diese alternativen Verfahren sind dann von der Kommission gesondert zu bewerten. Es bleibt abzuwarten, wie viele Anbieter von GPAI-Modellen sich für eine solche Sonderprüfung durch die EU-Kommission entscheiden.

Neue GPAI-Modelle, die ab dem 2. August 2025 in Verkehr gebracht werden, müssen die Anforderungen des AI Acts

grundsätzlich sofort erfüllen. Bußgelder für Verstöße gegen GPAI-spezifische Vorgaben werden aber erst ab dem 2. August 2026 verhängt. Ältere Modelle müssen erst bis zum 2. August 2027 mit dem AI Act konform sein. Bußgelder werden hier nicht durch die Mitgliedstaaten, sondern direkt durch die Kommission verhängt und können bis zu 3% des Jahresumsatzes oder 15 Mio. Euro erreichen.

Transparenz und Dokumentation

Anbieter bestimmter KI-Systeme müssen ab dem 2. August 2025 neue Transparenzpflichten einhalten. Dies gilt unabhängig davon, ob diese KI-Systeme GPAI-Modelle integrieren oder nicht. Die Pflichten gelten vor allem für solche KI-Systeme, bei denen der Nutzer nicht unbedingt weiß, dass er mit KI interagiert. Beispielsweise müssen KI-Systeme, die Deepfakes – also KI-generierte, aber täuschend echt wirkende Bilder oder Videos von echten Personen – erstellen können, gegenüber dem Nutzer offenlegen, dass die Inhalte künstlich erzeugt bzw. manipuliert wurden. Anbieter von GPAI-Modellen müssen zudem eine technische Dokumentation nach den Vorgaben des AI Act erstellen sowie eine detaillierte Zusammenfassung der Trainingsdaten des jeweiligen Modells veröffentlichen.

Rolle der Datenschutzbehörden

Das neue Kapitel der KI-Verordnung führt zu einem komplexen Zusammenspiel mit anderen EU Digitalrechtsakten wie dem Data Act und der Datenschutzgrundverordnung (DSGVO). Europäische Datenschutzbehörden haben bereits klargestellt, dass sie den Einsatz von KI vor allem auch über den Datenschutz regulieren wollen. Sie betrachten überraschend viele Daten als personenbezogen im Sinne der DSGVO. Auf dieser Basis gehen sie von einer sehr weiten Geltung der Anforderungen des Datenschutzes beim Einsatz von KI aus. Verstöße gegen andere EU-Rechtsakte bewerten sie ebenfalls als Datenschutzverstöße, da die DSGVO die Verarbeitung personenbezogener Daten

nur für legitime Zwecke erlaubt. Und ein Zweck, der gegen ein anderes EU-Gesetz oder ein Gesetz eines Mitgliedstaats verstößt, könne nicht legitim im Sinne der DSGVO sein. Auch die beim Einsatz von KI häufig herangezogene Rechtsgrundlage des berechtigten Interesses könne keine Anwendung finden. Denn wenn eine Datenverarbeitung mittels KI beispielsweise gegen die KI-Verordnung verstößt, könne sie nicht einem berechtigten Interesse dienen. Im Ergebnis sehen sich die EU-Datenschutzbehörden damit derzeit wohl als primärer Kontrolleur des rechtskonformen Einsatzes von KI in der Europäischen Union.

Die Neuregelungen stehen zudem vor der Herausforderung, sich mit anderen EU-Digitalrechtsakten wie dem Digital Markets Act, dem Digital Services Act und dem Cybersecurity Resilience Act zu koordinieren. Rechtsanwender sind gefordert, die Anforderungen des Datenschutzes und der KI-Verordnung in Einklang zu bringen. Dies kann zu Fragen der Auslegung und Klarheit führen, die von den betroffenen Parteien sorgfältig berücksichtigt werden müssen.

Praxisorientierte Umsetzung

Unternehmen sind gut beraten, die umfassenden Dokumentationspflichten des AI Acts und der DSGVO sorgfältig umzusetzen. Sie sollten in der Lage sein, ihre Strukturen und Prozesse zu begründen und darzulegen, wie sie den Anforderungen entsprechen. Sie müssen sich intensiv mit den neuen Regelungen beschäftigen, um rechtskonform zu agieren und mögliche Sanktionen und aufwändige behördliche und zivilrechtliche Verfahren zu vermeiden. Am 2. August 2026 werden (fast) alle übrigen Regelungen des AI Acts in Kraft treten. Bis dahin bleibt abzuwarten, wie die EU-Kommission und die nationalen Aufsichtsbehörden die Umsetzung des AI Acts in der Praxis gestalten.

*) Dr. Susan Kempe-Müller ist Partnerin für Geistiges Eigentum und Informationstechnologie, Tim Wybitul ist Partner im Datenschutz bei der Kanzlei Latham & Watkins.