Dr. Hans Markus Wulf, Hamburg

Die KI-Verordnung kommt noch vor der Sommerpause – Hat der Zeitdruck wertvolle Qualität gekostet?

Der Autor
ist Rechtsanwalt und Fachanwalt für IT-Recht, Datenschutz- sowie ISO 27001 Auditor (TÜV) und Partner bei der Wirtschaftskanzlei HEUKING.

Der neue AI Act sollte eigentlich im Juni im Amtsblatt veröffentlicht werden, nachdem er schon Mitte Mai final vom Rat gebilligt worden war, und wäre dann nach 20 Tagen in Kraft getreten. Verzögerung in Brüssel haben nun dazu geführt, dass die Veröffentlichung auf Mitte Juli verschoben wurde. Es ist daher mit einem Inkrafttreten Anfang August zu rechnen.

Ab diesem Zeitpunkt greifen die Umsetzungsfristen: Zunächst 6 Monate bis Februar 2025 für das Verbot bestimmter KI-Systeme, etwa solche zur unterschwelligen Verhaltensmanipulation oder zum gezielten Auslesen von Gesichtsbildern aus dem Internet. Nach 12 Monaten (also ab August 2025) greifen dann u. a. die neuen Vorgaben für KI-Modelle wie ChatGPT (OpenAI), Gemini (Google) oder Llama (Meta), während Anbieter und Nutzer von KI-Systemen 24 Monate (also bis August 2026) Zeit haben werden, die neuen, regulativen Vorgaben umzusetzen.

Vom Anwendungsbereich gelten die Grundsätze des Marktortprinzips, das aus der Datenschutz-Grundverordnung bekannt ist: Die KI-Verordnung findet u. a. Anwendung, sobald das KI-System bestimmungsgemäß auf dem EU-Markt in Verkehr gebracht oder in Betrieb genommen wird, selbst wenn der Anbieter aus einem Drittland stammt.

Aber was sind nun die neuen Pflichten für Unternehmen, die KI-Systeme einsetzen? Das hängt davon ab, ob es sich um Hochrisiko-KI oder reguläre KI handelt. Die Nutzung regulärer KI (etwa Spamfilter oder Chatbots) hat nur wenig Konsequenzen: Hier muss lediglich informiert werden, wenn etwa eine Emotionserkennung bzw. biometrische Kategorisierung erfolgt, das KI-System Bild-, Ton- oder Videoinhalte als „Deepfake" erzeugt bzw. manipuliert oder die KI einen Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheit von öffentlichem Interesse zu informieren. Hochrisiko-KI dagegen ist zunächst etwa solche, die im Bereich der kritischen Infrastruktur, Grenzkontrolle, Migration eingesetzt wird, oder zur Risikobewertung bei Abschluss von Versicherungsverträgen. In der Praxis relevanter dürften dagegen die Sektoren Bildung und Beschäftigung sein, denn auch diese werden als Hochrisiko-Bereiche qualifiziert. Lässt ein Bildungsinstitut daher zukünftig eine KI entscheiden, ob ein Teilnehmer in den betreffenden Lehrgang aufgenommen wird oder lässt ein Unternehmen die eingegangenen Bewerbungen zukünftig von einer KI sichten oder filtern, so befinden wir uns bereits im Bereich der Hochrisiko-KI. Das wiederum bedeutet umfassende, regulative Vorgaben: Es sind u. a. die notwendigen technischen und organisatorischen Maßnahmen zur Einhaltung der Gebrauchsanweisung umzusetzen, eine menschliche Aufsicht zu bestellen, eine Daten-Compliance sicherzustellen (die Eingabedaten müssen relevant und repräsentativ sein), interne Überwachungs- und Meldeprozesse zu installieren, Betriebsprotokolle aufzubewahren, Mitarbeiter zu schulen, eine Datenschutz-Folgenabschätzung durchführen und sich als Nutzer von Hochrisiko-KI in der diesbezüglichen EU-Datenbank registrieren. Zuwiderhandlungen können mit Bußgeldern bis zu 15 Mio. EUR (bzw. 3 % des Jahresumsatzes) sanktioniert werden, der Einsatz verbotener KI sogar bis zu 35 Mio. EUR (bzw. 7 %).

Im Bereich der verbotenen KI-Systeme gab es zuletzt zwischen EU-Parlament, EU-Kommission und Europäischem Rat erhebliche Differenzen, insbesondere zum Einsatz biometrischer, KI-gestützter Echtzeitüberwachungssysteme im öffentlichen Raum. Die Mitgliedstaaten hatten großes Interesse, diese Form des Ermittlungswerkzeuges einzusetzen, weshalb die Verhandlungen nicht wirklich vorankamen. Ab Mai 2024 standen jedoch die EU-Wahlen an, weshalb alle Abstimmungsprozesse bis März 2024 abgeschlossen sein mussten. In teilweise 38-stündigen Verhandlungsrunden wurden daher im Dezember 2023 innerhalb des Triloges Kompromisse gefunden, die zuletzt mit „heißer Nadel" gestrickt waren. Das Verbot der biometrischen Echtzeitüberwachung etwa wurde schlussendlich bis zur Unkenntlichkeit verwässert, ist nun etwa zulässig bei der Fahndung nach vermissten Kindern oder dem Verdacht auf einen Terroranschlag. Auch die geplante, strenge Regulierung von KI-Modellen wurde (auch dank erheblicher Lobbyarbeit der relevanten Anbieter aus den USA, jedoch auch Frankreich und Deutschland) später deutlich aufgeweicht. Am 12. 2. 2024 stimmte schließlich der Rat der aktuellen Version zu, am 13. 3. folgte das EU-Parlament. Obwohl die EU-Kommission bereits im April 2021 den ersten Entwurf der KI-Verordnung vorlegte, der Abstimmungsprozess daher nahezu drei Jahre dauerte, wurden maßgebliche Textfassungen der Verordnung auf die Schnelle im November und Dezember 2023 in hitzigen Debatten und langen Nächten hinzugefügt. Es dürfte zu erwarten sein, dass sich dies später in der Praxis zeigen wird.

> *Die ersten Verbote aus der KI-Verordnung greifen schon Anfang 2025*

Sicherheit dürfte sich jedoch nun zumindest in Deutschland im Hinblick auf die zuständige Aufsichtsbehörde einstellen. Diese ist nach Art. 70 der KI-Verordnung vom jeweiligen Mitgliedstaat zu benennen. Während sich zuletzt noch sehr aktiv die Landesdatenschutzbehörden um diese Funktion der KI-Marktüberwachung beworben hatten, ist die Entscheidung nun offenbar (Stand Juli 2024) in Berlin zugunsten der Bundesnetzagentur gefallen. Aus Sicht des Verfassers ist dies zu begrüßen, denn die einheitliche Anwendung von Regeln und Standards zur KI-Nutzung setzt bestenfalls auch eine zentrale Koordination der Marktüberwachung voraus. Zudem können hierdurch wichtige Ressourcen und Kompetenzen gebündelt werden und müssen nicht in den unterschiedlichen Landesbehörden neu aufgebaut werden.