compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

Künstliche Intelligenz in Europa: die KI-Verordnung

Ulrich Herfurth, Rechtsanwalt in Hannover und Brüssel
Sara Nesler, Mag. iur. (Torino), LL.M. (Münster)

August 2024

Mehr als 40 Prozent der befragten Unternehmen in Deutschland nutzen oder planen KI-Anwendungen (Statista Umfrage 2023). Dabei wurden 6,3 Milliarden Euro laut Digitalverband Bitkom 2023 in Deutschland für KI-Software, Dienstleistungen rund um KI sowie entsprechende Hardware ausgegeben, ein Drittel mehr als im Vorjahr. Die rasante Entwicklung zwingt viele Unternehmen, sich kontinuierlich mit den neuen Technologien und deren Regulierung auseinanderzusetzen.

Auch der europäische Gesetzgeber kann mit dem schnellen Fortschritt der Künstlichen Intelligenz kaum Schritt halten. Im Jahr 2021 haben wir uns im Compact „Künstliche Intelligenz in Europa“ mit dem ersten Entwurf der Künstliche Intelligenz Verordnung (KI-VO) beschäftigt. Ziel der Verordnung war es, den Einsatz von KI-Systemen in der EU so zu regulieren, dass die Risiken der Technologie minimiert werden. Mit der Einführung von ChatGPT im November 2022 wurde schnell klar, dass der Entwurf vom April 2021 bereits überholt war. Die endgültige Fassung der KI-VO wurde am 12. Juli 2024 veröffentlicht und trat am 1. August 2024 in Kraft.

Anwendungsbereich der KI-Verordnung

Definition des KI-Systems

Der Begriff des KI-Systems, der das zentrale Tatbestandsmerkmal der Verordnung darstellt, wurde im Gesetzgebungsverfahren intensiv diskutiert, da von vielen Seiten seine Unbestimmtheit befürchtet wurde. Letztlich wurde ein KI-System definiert als “*ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“.*

Es ist zu begrüßen, dass diese Definition fast wörtlich der OECD-Definition entspricht, die 2023 aktualisiert wurde. Was ein KI-System letztlich von einer Software unterscheidet, ist, dass KI ein gewisses Maß an Handlungsunabhängigkeit von menschlichem Eingreifen aufweist und die Fähigkeit besitzt, ohne menschliches Eingreifen zu operieren. Dieses Kriterium war bereits im Entwurf vom April 2021 enthalten. Bestehen Zweifel, ob es sich bei einem System um KI handelt, wird empfohlen, vorsorglich davon auszugehen, dass es sich um ein KI-System handelt.

Persönlicher Anwendungsbereich

Betroffen ist die gesamte Wertschöpfungskette von KI-Systemen, sowohl im privaten als auch im öffentlichen Sektor. Die Pflichten der KI-Verordnung richten sich in erster Linie an die Anbieter von KI-Systemen,

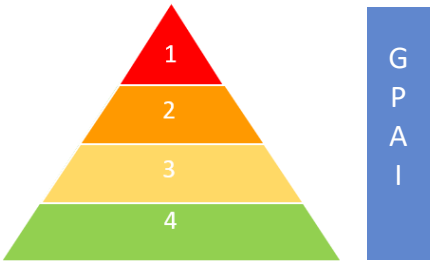
teilweise an den Betreiber und nur punktuell an den Importeur, Händler, Bevollmächtigten, die benannte Stelle (eine unabhängige Organisation, die für die Bewertung und Zertifizierung von KI-Systemen zuständig ist) oder den Endnutzer.

Räumlicher Anwendungsbereich

Um einen umfassenden Schutz zu gewährleisten, erstreckt sich der Anwendungsbereich der Verordnung auch auf Anbieter und Betreiber von KI-Systemen, die in einem Drittland niedergelassen sind oder sich in einem Drittland befinden, wenn der von dem KI-System erzeugte Output in der Union genutzt wird (Art. 2 Abs. 1 lit. c KI-VO).
Damit soll die Einfuhr verordnungswidriger KI-Systeme auch dann verhindert werden, wenn der konkrete Standort eines KI-Systems für Außenstehende nicht zuverlässig feststellbar ist oder leicht verlegt werden kann. In der Praxis ist die Durchsetzung ohne eine (grundrechtlich problematische) umfassende Überwachung jedoch sehr schwierig, so dass mit einer Umgehung der EU-Regelungen durch Anbieter aus Drittstaaten zu rechnen ist.

Maßnahmen nach Risikostufe

Um unterschiedliche KI-Systeme und Anwendungen umfassend zu regulieren, ohne unnötige Hürden für die Entwicklung und Verwendung der neuen Technologien zu setzen, folgt die Verordnung einem risikobasierten Ansatz. Unabhängig von den vier Risikostufen hat der neue Entwurf nun die Kategorie der „KI-Modell mit allgemeinem Verwendungszweck“ (GPAI) eigeführt.



(1) Verbotene KI-Systeme (Art.5 KI-VO)

KI-Systeme, die ein unannehmbares Risiko darstellen, sind verboten. Darunter fallen u.a. Systeme, die das Verhalten von Menschen manipulieren oder physische oder psychische Schwächen ausnutzen, um Menschen zu schädlichem Verhalten zu verleiten, z.B. Spielzeug, das kleine Kinder zu gefährlichem Verhalten verleitet. Inwieweit auch KI-gesteuerte Social Media Feeds und personalisierte Werbung erfasst werden, ist noch unklar. Verboten sind auch Systeme zur sozialen Bewertung (Social Scoring) sowie Systeme zur biometrischen Identifizierung (Ausnahmen sind u.a. für die Identifizierung und Verfolgung von Tätern oder Verdächtigen einer Straftat vorgesehen).

(2) KI-Systeme mit hohem Risiko (Art. 6-49 KI-VO)

Diese Risikostufe umfasst zwei Hauptgruppen von Anwendungen: zum einen Sicherheitssysteme und -komponenten, z. B. Anwendungen in der robotergestützten Chirurgie oder Sicherheitskomponenten in Kraftfahrzeugen oder Spielzeug, zum anderen Systeme, die in sensiblen Bereichen eingesetzt werden und zu Grundrechtsverletzungen führen können. Dazu gehören unter anderem kritische Infrastrukturen, der Zugang zu Schule und Berufsausbildung, Einstellungsverfahren, die Strafverfolgung, die Rechtspflege sowie wichtige private und öffentliche Dienstleistungen wie die Bewertung der Kreditwürdigkeit.
KI-Systeme, die kein signifikantes Risiko für bestimmte Rechtsgüter darstellen und keinen wesentlichen Einfluss auf Entscheidungsprozesse haben, werden nicht als Hochrisikosysteme eingestuft. Dies gilt insbesondere für KI-Anwendungen, die lediglich vorbereitende Aufgaben übernehmen, die anschließend durch eine menschliche Entscheidung ergänzt werden. In der Praxis wird dieser Ausnahmetatbestand und seine (schwierige) Abgrenzung von großer Bedeutung sein.
Die hohen Anforderungen, die bereits im ersten Entwurf an Hochrisiko-KI-Systeme gestellt wurden, haben sich im Laufe des Gesetzgebungsverfahrens kaum verändert. Die strengen Anforderungen betreffen unter anderem die Risikobewertung von Systemen, die

Qualität von Datensätzen, die Nachvollziehbarkeit von Vorgängen und eine angemessene menschliche Aufsicht. Um die Einhaltung der Vorschriften zu gewährleisten, ist für das Inverkehrbringen eines Hochrisiko-KI-Systems eine positive (interne oder externe) Konformitätsbewertung, die Registrierung in einer dafür eingerichteten europäischen Datenbank und die Anbringung einer CE-Kennzeichnung erforderlich. Neu ist die in Art. 27 KI-VO vorgesehene Grundrechtsverträglichkeitsprüfung.

(3) KI-Systeme mit begrenztem Risiko (Art. 50 KI-VO)

KI-Systeme mit begrenztem Risiko unterliegen nur geringen Transparenzanforderungen. Diese sind je nach Anwendung unterschiedlich. So müssen künftig der Einsatz von Chatbots und die Exposition gegenüber Deep Fakes (manipulierte oder generierte Inhalte, die als authentische Personen, Sachverhalte oder Gegenstände wahrgenommen werden) offengelegt werden. Gleiches gilt für Systeme, die Emotionen erkennen oder biometrische Kategorisierungen vornehmen.

(4) Minimales Risiko

Die Mehrheit der KI-Systeme, wie KI-gestützte Empfehlungssysteme oder Spam-Filter, werden von keiner der dargestellten Risikokategorien erfasst und unterliegen keine Regulierung.
Die KI-VO sieht für solche Systeme lediglich die Erstellung von Verhaltenskodizes vor, deren Einhaltung freiwillig ist.

KI-Modelle mit allgemeinem Verwendungszweck (GPAI-Modelle)

Die Regulierung von GPAI-Modellen in der KI-VO erfolgte als Reaktion auf die Einführung von Chat-GPT. Es wurde erkannt, dass solche Allzwecktools durch das Raster des Risikoansatzes der KI-VO fallen würden.

Definition

Ein KI-Modell mit allgemeinem Verwendungszweck (General Purpose Artificial Intelligence Model –GPAI) wird definiert als *„ein KI-Modell, dass eine erhebliche allgemeine Verwendbarkeit aufweist, und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und dass in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann“*.
Die KI-VO enthält keine Definition des KI-Modells. Fragt man ChatGPT nach dem Unterschied zwischen einem KI-System, einem KI-Modell und einer KI-Anwendung und was davon ChatGPT ist, erfährt man: ChatGPT sei eine KI-Anwendung, die ein spezifisches Modell (Generative Pre-trained Transformer) verwendet und als Teil eines umfassenden Systems betrieben wird, um seine Funktionalität bereitzustellen.

Auch hier ist entsprechend dem allgemeinen risikobasierten Ansatz der Verordnung zwischen "GPAI-Modellen" und „GPAI-Modellen mit systemischem Risiko" zu unterscheiden: Ein systemisches Risiko im Sinne des Art. 51 Abs. 1 KI-VO liegt vor, wenn ein GPAI-Modell über Fähigkeiten mit hohem Wirkungsgrad verfügt oder von der Kommission als gleichwertig eingestuft wird. Ein hoher Wirkungsgrad wird vermutet, wenn der Trainingsaufwand mehr als 10^25 FLOPS beträgt.

Verpflichtungen

Alle in Verkehr gebrachten GPAI-Modelle unterliegen grundsätzlich Dokumentations- und Designanforderungen sowie Anforderungen zur Einhaltung des EU-Urheberrechts, insbesondere in Bezug auf Text- und Data Mining. Davon ausgenommen sind GPAI-Modelle, die unter einer Open-Source-Lizenz veröffentlicht werden und keine GPAI-Modelle mit systemischen Risiken sind.
Anbieter von GPAI-Modellen mit systemischem Risiko müssen zusätzliche Anforderungen erfüllen. Dazu gehören die Durchführung einer Modellbewertung, die

Nachverfolgung, Dokumentation und Meldung von schwerwiegenden Vorfällen und Abhilfemaßnahmen an das (neu geschaffene) AI-Office sowie die Gewährleistung eines angemessenen Niveaus an Cybersicherheit und physischer Infrastruktur. Darüber hinaus müssen potenzielle „systemische Risiken auf Unionsebene“ bewertet und gemindert werden.

Ausblick

Die Umsetzungsfristen der Verordnung laufen schrittweise zwischen Februar 2025 und August 2027 ab. Unternehmen, die von der Verordnung betroffen sind, sollten sich daher umgehend und detailliert mit den neuen Regelungen auseinandersetzen. Dabei werden sie schnell feststellen, dass die Verordnung unter großem Zeit- und Ergebnisdruck verabschiedet wurde. Dies spiegelt sich in einer Vielzahl von unbestimmten Begriffen wider, die zu erheblicher Rechtsunsicherheit führen und die Umsetzung erschweren.

Die Kommission muss nun innerhalb von 12 Monaten Leitlinien für die praktische Umsetzung der Verordnung erarbeiten (Art. 95 KI-VO). Die Umsetzungsfristen laufen jedoch unabhängig davon, so dass die Gefahr besteht, dass einige Anforderungen umgesetzt werden müssen, bevor sie hinreichend konkretisiert sind und die Produktentwicklung nicht rechtzeitig gesteuert werden kann.

Den Bedürfnissen von KMU einschließlich Start-ups muss die Kommission besondere Aufmerksamkeit widmen (Art. 95 KI-VO). Dies wurde jedoch im Verordnungstext kaum berücksichtigt, vielmehr belastet die EU kleine Unternehmen durch die Gleichbehandlung mit den Tech-Giganten erneut mit unverhältnismäßig hohem personellen und finanziellen Aufwand.

+ + +

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-307 56-0 Fax 0511-307 56-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Günter Stuff; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Konstantin Kuhle, Rechtsanwalt; Antonia Herfurth, Rechtsanwältin, LL.M. (Göttingen); Sara Nesler, Mag. iur. (Torino), LL.M. (Münster).

KORRESPONDENTEN

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511-307 56-50 Fax 0511-307 56-60
Mail info@caston.info; Web www.caston.info