



# AI Act: Der KI-Verhaltenskodex der EU

Die EU hat einen Leitfaden für KI-Anbieter veröffentlicht. Dessen Einhaltung ist zwar freiwillig. Aber sollten Anbieter von GPAI den Verhaltenskodex nicht befolgen, müssen sie nachweisen, auf welche andere Weise sie ihre Konformität mit dem AI Act erfüllen.

Von **Christina Kiefer** und **Moritz Schneider**

Die europäische KI-Verordnung (KI-VO, englisch AI Act) nimmt nicht nur verbotene und Hochrisiko-KI-Systeme in den Blick, sondern auch Anbieter sogenannter General-Purpose-AI-Modelle (GPAI). Die Pflichten für GPAI gelten seit dem 2. August 2025. Um die bislang teils vagen Vorgaben des AI Act zu GPAI zu

konkretisieren, hat die EU-Kommission pünktlich vor dem Geltungsbeginn der neuen Vorgaben des AI Act einen „General-Purpose AI Code of Practice“ veröffentlicht und ihn am 1. August genehmigt. Dieser Verhaltenskodex soll der Industrie als Orientierungshilfe dienen, um die Anforderungen des AI Act praxis-

nah umzusetzen. Der Kodex besteht aus konkretisierenden Kapiteln zu den neuen Anforderungen zu Transparenz, Urheberrecht, Sicherheit und Risikomanagement. Wir fassen die wichtigsten Punkte zusammen.

## Wie „soft“ ist der Verhaltenskodex?

Im europäischen Recht entfaltet häufig sogenanntes Soft Law, das heißt Vorgaben, die rechtlich formell nicht bindend sind, faktisch erhebliches Gewicht. Insofern ist auch dem Verhaltenskodex, obwohl grundsätzlich freiwillig, ein hoher Stellenwert bei der Umsetzung des AI Act zuzumessen. Der AI Act kennt verschiedene Instrumente, um die Befolgung der abstrakten Regelungen für Betroffene zu vereinfachen. Dazu gehören Leitlinien und harmonisierte Normen. Bei dem Verhaltenskodex handelt es sich um einen Praxisleitfaden, der ausdrücklich in Art. 56 AI Act vorgesehen ist.

Zwar begründet der AI Act keine Konformitätsvermutung bei der Befolgung eines Praxisleitfadens – anders als für künftig mögliche harmonisierte Normen. Dennoch stellt Art. 53 Abs. 4 S. 3 AI Act klar, dass Anbieter von GPAI-Modellen, die von genehmigten Praxisleitfäden oder Normen abweichen, darlegen müssen, mit welchen alternativen Maßnahmen sie die gesetzlichen Anforderungen erfüllen. Diese Abweichungen unterliegen der Bewertung durch die EU-Kommission. Mit der Genehmigung durch die EU-Kommission wird der Kodex faktisch erhebliche Relevanz erlangen.

## Die Regulierung der General-Purpose-KI-Modelle

Noch während des laufenden Gesetzgebungsverfahrens zum AI Act setzte mit der Veröffentlichung von ChatGPT durch OpenAI ein massiver Aufschwung im Bereich generativer, sprachbasierter KI-Modelle ein. Der europäische Gesetzgeber reagierte kurzfristig: In den Art. 51 ff. des AI Act wurden zusätzliche Regelungen für Anbieter von GPAI-Modellen und deren Bevollmächtigte aufgenommen. Anders als bei den übrigen Vorgaben der Verordnung, die auf das konkrete KI-System abstellen, ist bei GPAI-Anbietern das zugrunde liegende Modell der maßgebliche Anknüpfungspunkt – etwa die GPT-Modelle von OpenAI. Der darauf aufbauende Chatbot stellt ein KI-System dar. Grundsätzlich kann derselbe Akteur nach dem AI Act Anbieter eines GPAI-

### TRACT

- ▶ Der KI-Verhaltenskodex der EU soll die Anforderungen der KI-Verordnung für General-Purpose-AI-Modelle konkretisieren und so den betroffenen Unternehmen die Umsetzung einfacher machen.
- ▶ Der Kodex behandelt die drei relevantesten Themen Transparenz, Urheberrechte sowie Sicherheit und Gefahrenabwehr und liefert einige Details zur Umsetzung.
- ▶ Neben den Konkretisierungen der Anforderungen enthält die Veröffentlichung auch Hinweise für GPAI-Modelle, insbesondere zum Geltungsbereich der Vorschriften.
- ▶ Zwar liefert der Verhaltenskodex konkrete technische Hilfestellungen, in einigen wichtigen Punkten, beispielsweise der Transparenz bei Trainingsdaten, bleibt er jedoch zu vage.
- ▶ Das Thema Sanktionen bleibt vollständig ausgespart.

Modells wie auch eines darauf basierenden KI-Systems sein.

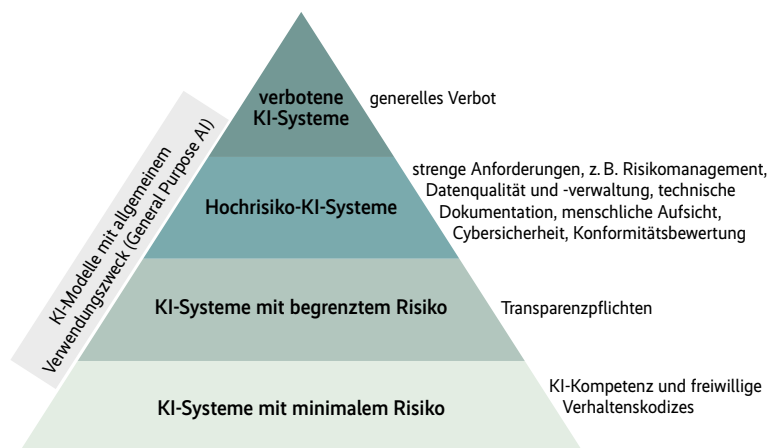
Die Regelungen für diese Modelle betreffen insbesondere Anforderungen an Transparenz, den Schutz geistigen Eigentums sowie an Sicherheit und Gefahrenabwehr. Für GPAI-Modelle mit systemischem Risiko sieht Art. 55 AI Act zudem verschärfte Vorgaben zur Modellbewertung, zu risikomindernden Maßnahmen, zur Meldung schwerwiegender Vorfälle sowie zur Cybersicherheit vor. Ein systemisches Risiko wird angenommen, wenn das betreffende Modell über besonders leistungsfähige Eigenschaften verfügt oder einen hohen Wirkungsgrad entfaltet. Die formale Einstufung als Modell mit systemischem Risiko obliegt der EU-Kommission.

## Transparenz bei wichtigen Informationen

Der erste Teil des Verhaltenskodex befasst sich mit dem Thema Transparenz. Dieses Kapitel konkretisiert die Vorgaben aus den Abschnitten a) und b) in Art. 53 Abs. 1 AI Act und legt fest, welche Informationen Anbieter von GPAI-Modellen dokumentieren und gegebenenfalls weitergeben müssen. Ziel ist es, relevante Informationen an die Anbieter von KI-Systemen (Downstream-Anbieter) weiterzugeben, die die GPAI-Modelle in ihre Systeme integrieren wollen. Ein zentrales Instrument ist das Formular „Model Documentation Form“, das detaillierte Angaben zur Modellarchitektur, zum Training, zu den verwendeten Datenquellen, zum Energieverbrauch und zu den Nutzungsmöglichkeiten verlangt.

Bei den dort aufgeführten Punkten handelt es sich um Mindestangaben, die ein GPAI-Anbieter machen muss. Während bestimmte Informationen ak-

## Risikobasierter Ansatz: Einteilung von KI in Risikogruppen



**KI-Systeme werden nach ihren Risiken eingestuft und müssen gemäß KI-Verordnung daran angepasste Anforderungen erfüllen (Abb. 1).**

tiv an Downstream-Anbieter weitergegeben werden müssen, etwa zur Integration der Modelle in eigene Systeme, bleiben zentrale Angaben wie die Herkunft und Auswahl der Trainingsdaten nur auf Anfrage für Behörden zugänglich. Eine Veröffentlichung gegenüber der breiten Öffentlichkeit ist nicht verpflichtend, sondern lediglich empfohlen. Kritiker bemängeln daher, dass die Transparenzpflichten zwar formal umfangreich sind, in der Praxis jedoch nur begrenzte Nachvollziehbarkeit und Kontrolle ermöglichen – insbesondere für Rechteinhaber, unabhängige Forschung oder die Zivilgesellschaft.

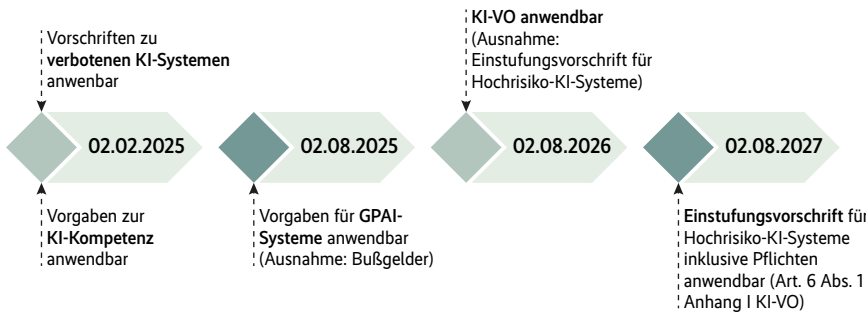
## Urheberrecht muss gewährleistet sein

Ein zentraler Aspekt der öffentlichen und juristischen Diskussion rund um große Sprachmodelle (LLMs) ist der Schutz des Urheberrechts, vor allem im Kontext des Trainings solcher Systeme.

Nach den Abschnitten c) und d) in Art. 53 Abs. 1 AI Act sind Anbieter von GPAI-Modellen verpflichtet, eine Strategie zur Einhaltung des Urheberrechts zu entwickeln und eine detaillierte Zusammenfassung der zum Training verwendeten Inhalte zu veröffentlichen. Diese Vorgabe ist sehr abstrakt und für die praktische Umsetzung kaum geeignet. Daher ist es zu begrüßen, dass der Verhaltenskodex diese Anforderungen konkretisiert.

Ausdrücklich enthält der Verhaltenskodex Vorgaben zum Einsatz von Webcrawlern beim Training von KI-Modellen. Diese dürfen keine technischen Schutzmaßnahmen wie Paywalls umgehen, um Webinhalte zum Training der Algorithmen zu verwenden. Auch müssen Seiten vom Webcrawling ausgenommen werden, die dauerhaft und wiederholt Rechte Dritter verletzen. Des Weiteren gibt es konkrete technische Vorgaben für den Einsatz von Webcrawlern: Diese sollen Vorgaben der Datei robots.txt beachten, in denen Websitebetreiber dar-

## Übergangsfristen nach der KI-VO



### Pünktlich zur Anwendbarkeit des AI Act auf GPAI veröffentlichte die Kommission den Verhaltenskodex mit einigen Konkretisierungen der Vorgaben (Abb. 2).

legen, welche Inhalte ausgelesen oder ignoriert werden sollen.

Neben diesen konkreten Vorgaben bleiben die Angaben zur Transparenz bezüglich genutzter Trainingsdaten vage. Statt konkreter Offenlegungspflichten verweist der Kodex lediglich auf ein noch zu entwickelndes Template des europäischen AI Office. Rechteinhaber kritisieren dies als unzureichend. Auch fehlt es an einem verbindlichen Mechanismus zur Sanktionierung bei Nichteinhaltung. Immerhin sollen Beschwerdewege für Rechteinhaber geschaffen werden – allerdings ohne klare Vorgaben zur rechtlichen Verbindlichkeit oder Reaktionsfrist.

### Sicherheit und Gefahrenabwehr

Weitere Vorgaben existieren für GPAI-Modelle mit systemischen Risiken. Für diese Modelle gelten nach Art. 55 AI Act strikte Regularien, insbesondere zum Risikomanagement. Beispielsweise muss eine Bewertung erfolgen, zu der auch gehört, Angriffstests auf das Modell durchzuführen und zu dokumentieren, um systemische Risiken zu ermitteln und zu mindern. Daneben steht eine allgemeine Anforderung, mögliche systemische Risiken, die sich auch aus der Verwendung des KI-Modells ergeben können, zu bewerten und zu mindern. Zudem sollen einschlägige Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen erfasst, dokumentiert und gemeldet und ein angemessenes Maß an Cybersicherheit des Modells gewährleistet werden.

Diese Vorgaben konkretisiert das Kapitel „Sicherheit und Gefahrenabwehr“, das im Verhaltenskodex das umfangreichste ist. Es legt detailliert fest, wie Anbieter von GPAI-Modellen mit systemischem Risiko ihrer Verantwortung nachkommen müssen. So verlangt der Kodex nicht nur

die Durchführung von Angriffstests, sondern auch die kontinuierliche Bewertung der Effektivität aller eingesetzten Sicherheitsmaßnahmen entlang des gesamten Modelllebenszyklus. Die Modellbewertung selbst ist breit angelegt: Sie umfasst neben klassischen Benchmarks auch Adversarial Tests – also Tests mit manipulierten Eingangsdaten –, offene Evaluationen und externe Red-Teaming-Verfahren. Hinzu kommt eine systematische Risikoanalyse, die sowohl technische Aspekte als auch mögliche gesellschaftliche Auswirkungen der Modellverwendung einbezieht.

Das Kapitel liefert außerdem Details zur Einrichtung von Prozessen zur Erkennung und Meldung schwerwiegender Vorfälle, inklusive Fristen, Berichtsinhalten und Anforderungen an die Nachvollziehbarkeit. Darüber hinaus fordert der Kodex von Anbietern die Definition eines konkreten Cybersicherheitsziels, das unter anderem Schutzmaßnahmen gegen Insider-Bedrohungen, Modelldiebstahl und unerlaubte Modellverbreitung umfassen soll. Dabei gilt stets: Die eingesetzten Schutzmaßnahmen müssen dem Stand der Technik entsprechen und fortlaufend an die Entwicklung der Modellfähigkeiten angepasst werden.

Viel Kritik, etwa vonseiten des Branchenverbands Bitkom, erntete die Forderung nach „open-ended risk identification“. Der Verhaltenskodex sieht vor, dass Unternehmen kontinuierlich nach Risiken suchen müssen. Gerade vor dem Hintergrund, dass die Risiken nach AI Act teils vage unter Verweis auf Grundrechte und gesellschaftliche Risiken bestimmt werden, sorgt dies für weitere Rechtsunsicherheit.

### Wie geht es weiter?

Die Ausarbeitung des Verhaltenskodex wurde vom AI Office der EU-Kommis-

sion unter Einbindung zahlreicher Stakeholder angestoßen. Die am 10. Juli 2025 veröffentlichte aktuelle Fassung hat die EU-Kommission am 1. August 2025 im Wege eines Angemessenheitsbeschlusses genehmigt. Damit hat der Kodex in der Union allgemeine Gültigkeit erlangt. Insbesondere solange keine harmonisierten Normen bestehen, ist die Veröffentlichung des Verhaltenskodex ein wichtiger Schritt, um der Industrie klare Vorgaben an die Hand zu geben.

### Hilfreiche GPAI-Ergänzung

Zu begrüßen ist ebenfalls, dass die EU-Kommission den Verhaltenskodex um Leitlinien für GPAI-Modelle ergänzt, die klarstellen sollen, wer in den Anwendungsbereich dieser Vorschriften fällt. Der AI Act ist in vielen Anforderungen zu abstrakt, um handhabbare Maßnahmen abzuleiten. Dass einzelne Vorgaben, insbesondere in Bezug auf den Schutz von Rechten Dritter, umstritten sind, liegt in der Natur der Sache. Aufseiten sowohl der Digitalbranche als auch der Rechteinhaber stehen nachvollziehbare und weitreichende wirtschaftliche Interessen. Daran, den AI Act für die europäische Wirtschaft handhabbar zu machen, sollten alle Akteure ein Interesse haben. (ur@ix.de)

### Quellen

Den Originaltext des Verhaltenskodex inklusive FAQ und einige Veröffentlichungen dazu sind über [ix.de/zx5z](https://ix.de/zx5z) zu finden.

#### CHRISTINA KIEFER



ist Rechtsanwältin und Senior Associate in der Digital Business Unit bei reuschlaw. Dort berät sie Unternehmen und öffentliche Einrichtungen zu Datenschutz, Cybersicherheit sowie IT- und Vertragsrecht.

#### MORITZ SCHNEIDER



ist Rechtsanwalt und Associate bei reuschlaw in Saarbrücken. Dort berät er in der Digital Business Unit Unternehmen zu Datenschutz, Cybersicherheit und IT-Recht.

