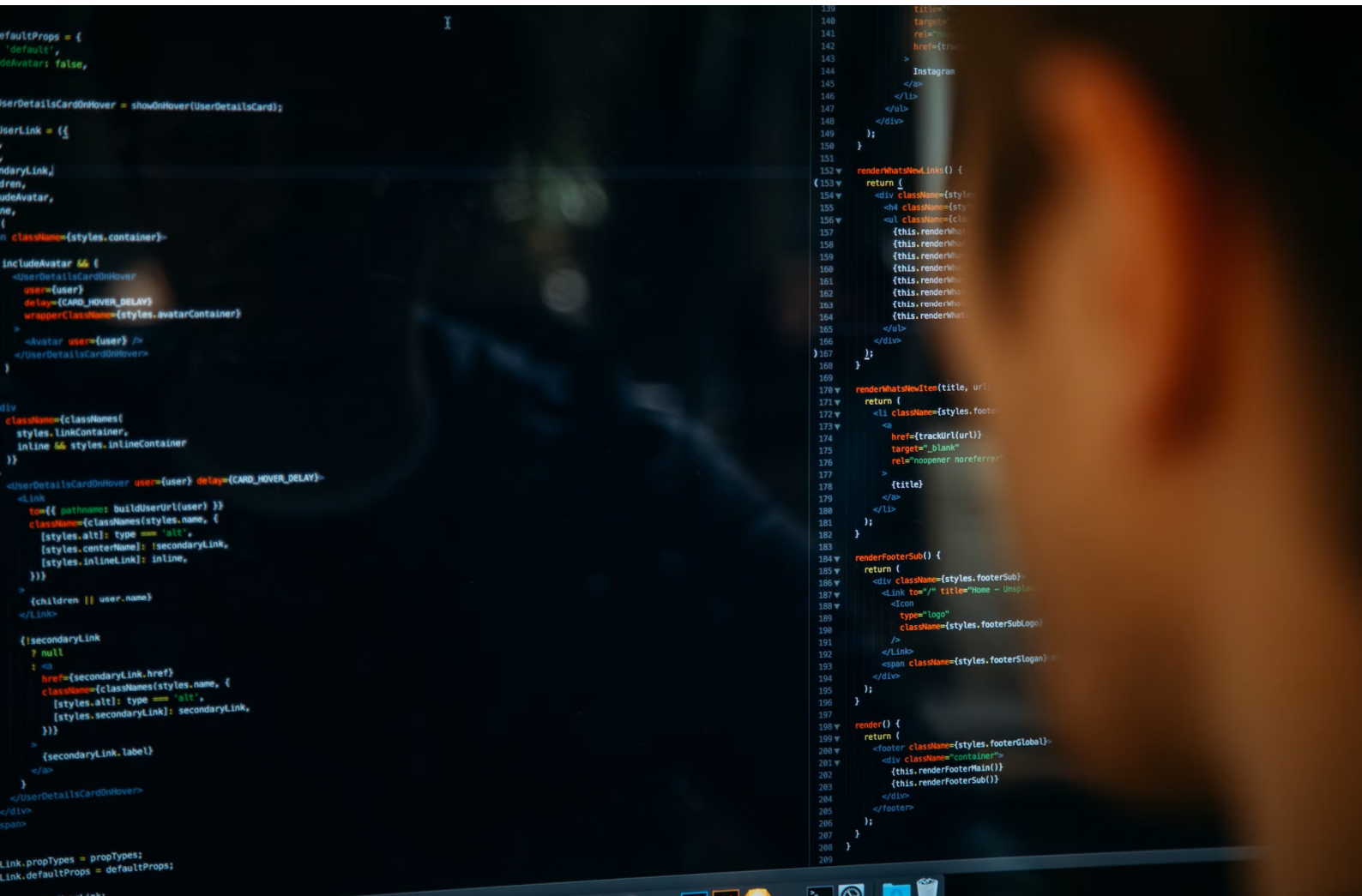
TÜV VERBAND

Juli 2023

Stellungnahme

Empfehlungen zu den AI Act-Trilogverhandlungen



Stellungnahme

Empfehlungen zu den AI Act-Trilogverhandlungen

Einführung

Mit dem Gesetz über Künstliche Intelligenz (AI Act) will die Europäische Union zum Vorreiter bei der Regulierung von Künstlicher Intelligenz werden. Ziel ist es, eine vertrauenswürdige und sichere Nutzung von KI-Systemen zu ermöglichen und die Wettbewerbsfähigkeit europäischer KI-Entwicklungen sicherzustellen. Die EU-Kommission hat ihren Vorschlag dazu im April 2021 veröffentlicht. Nach intensiven Verhandlungen haben der Rat im Dezember 2022 und das EU-Parlament im Juni 2023 ihre jeweiligen Positionen festgelegt. Die gemeinsamen Trilog-Verhandlungen haben begonnen und sollen soweit möglich unter spanischer Ratspräsidentschaft beendet werden.

Der TÜV-Verband hat sich bereits im laufenden Gesetzgebungsprozess umfassend zum AI Act positioniert. Diese Stellungnahme gibt konkrete Empfehlungen, damit ein robuster und wirksamer Regulierungsrahmen geschaffen werden kann. Prioritäre Zielsetzung des EU-Gesetzgebers sollte aus unserer Sicht sein, dass nur sichere KI-Systeme auf den Markt gebracht werden und somit das notwendige Vertrauen der Menschen in KI-basierte Produkte und Systeme gestärkt wird. Nur so kann eine schnelle Marktdurchdringung hochqualitativer KI-Systeme ermöglicht werden, und „AI Made in Europe" zum echten Qualitätsstandard und Wettbewerbsvorteil für europäische Unternehmen werden.

1. Ziel der Regulierung (Artikel 1)

- Das Ziel des AI Acts – die Einführung von menschenzentrierter und vertrauenswürdiger KI – sollte, wie vom EP vorgeschlagen, explizit als übergeordnete Zielsetzung in Artikel 1 genannt werden.
- Auch die vom EP vorgeschlagene Ausweitung der Schutzziele mit Blick auf Demokratie, Grundrechte und Umwelt ist zu begrüßen. Der AI Act muss alle von KI-Systemen ausgehenden Risiken betrachten und entsprechende Anforderungen an Anbieter und Nutzer von KI-Systemen zur Reduzierung der Risiken vorsehen.

2. Hochrisiko-Klassifizierung (Artikel 6)

- Die von Rat und EP vorgeschlagenen Klassifizierungsvorschriften für Hochrisiko-KI-Systeme sind nicht ausreichend, sowohl mit Blick auf physische Produkte, in denen KI-Systeme integriert werden (Anhang II), als auch mit Blick auf KI-Systeme, welche als Stand-Alone-Software auf den Markt gebracht werden (Anhang III).

- Bei physischen Produkten soll nach Vorstellungen der EU-Gesetzgeber eine Hochrisiko-Klassifizierung nur dann erfolgen, wenn das KI-System als Sicherheitsbauteil des Produktes verwendet wird und das Produkt schon heute einer verpflichtenden Drittprüfung unterliegt. Aus unserer Sicht ist dieser Ansatz nicht ausreichend, da sich durch die Integration eines KI-Systems in ein Produkt neue Risiken ergeben können. Vielmehr ist es notwendig, die in Anhang II gelisteten sektoralen Rechtsvorschriften einer Neubewertung mit Blick auf das Gefährdungspotential zu unterziehen. Eine entsprechende rechtliche Verpflichtung sollte im AI Act verankert werden.

- Bei Stand-Alone-KI-Systemen wurde der konkrete Anwendungsfall als zusätzliches Kriterium seitens des EP ergänzt, um entsprechende Systeme als hochriskant zu klassifizieren. Während diese Ergänzung grundsätzlich sinnvoll erscheint, ist die vom EP vorgesehene Opt-Out-Möglichkeit für Anbieter mittels einer Mitteilung an die nationale Aufsichtsbehörde bzw. das AI Office klar abzulehnen. Es besteht die Gefahr, dass KI-Anbieter diese als Hintertür zur Umgehung der verpflichtenden Anforderungen nutzen werden. Zudem ist zu erwarten, dass die vorgesehene dreimonatige Frist zur Ausstellung von begründeten Entscheidungen die nationalen Behörden vor große Herausforderungen stellen wird. Eine Opt-Out-Möglichkeit ist aus Sicht des TÜV-Verbands nicht notwendig, wenn die Kommission die kritischen Anwendungsfälle der in Anhang III aufgelisteten Bereiche mittels delegierter Rechtsakte hinreichend konkretisiert.

3. Konformitätsbewertung (Artikel 43, Anhang VII)

- Die von Rat und EP beibehaltene Nutzung einer Herstellerselbsterklärung für hochriskante Stand-Alone-KI-Systeme (Anhang III) ist abzulehnen. Sofern ein KI-System als hochriskant klassifiziert ist, sollte es einer verpflichtenden Zertifizierung durch benannte Stellen unterliegen. Nur durch eine unabhängige Prüfung können mögliche Interessenskonflikte des Anbieters ausgeschlossen werden. Zugleich wird sichergestellt, dass das KI-System alle verpflichtenden Anforderungen der Verordnung einhält. Die verpflichtende Einbindung einer benannten Stelle bei Hochrisikoprodukten ist ein Kernpfeiler der europäischen Produktegesetzgebung und des New Legislative Framework.

- Zur ordnungsgemäßen Durchführung einer Konformitätsbewertung durch benannte Stellen benötigen diese in der Regel umfassenden Zugriff auf alle notwendigen Daten (z. B. den

Quellcode, die Trainings- und/oder Validierungsdaten). Nur so kann überprüft werden, ob das KI-System den Anforderungen des AI Acts entspricht. Sowohl die Rats- als auch die EP-Position schränken diesen Zugang jedoch stark ein. Diese Einschränkung erscheint aus unserer Sicht nicht gerechtfertigt, insbesondere da schon heute hohe Anforderungen an Konformitätsbewertungsstellen mit Blick auf den Schutz des geistigen Eigentums und die Wahrung von Geschäftsgeheimnissen gestellt werden.

- Zur Reduzierung der Compliance-Kosten, insbesondere für KMUs und Start-ups, sollte der EU-Gesetzgeber geeignete finanzielle Förderungsinstrumente in Erwägung ziehen.

4. Zusammenspiel mit sektoraler Gesetzgebung (Artikel 8)

- Aufgrund der Tatsache, dass in einzelnen sektoralen Rechtsakten bereits KI-spezifische Anforderungen enthalten sind, muss sichergestellt werden, dass es zu keinen überlappenden oder sich widersprechenden Anforderungen kommt (zum Beispiel der Medizinprodukte-Verordnung MDR). Die vom EP ergänzte Kollisionsregel ist daher grundsätzlich zu begrüßen. Ziel muss es sein, Rechtssicherheit für Hersteller und benannte Stellen zu schaffen.

5. Anforderungen an Hochrisiko-KI-Systeme (Artikel 9, 12)

- Die Nutzung von bereits bestehenden Qualitätsmanagementsystemen im Rahmen der Konformitätsbewertung sollte, wie vom EP vorgeschlagen, ermöglicht werden. Insbesondere bei KI-Systemen, welche in Produkten integriert werden, können die Vorgaben aus dem AI Act in die bestehenden Qualitätsmanagementsysteme integriert und somit unnötiger Mehraufwand vermieden werden. Ziel muss es sein, dass die europäische Gesetzgebung so harmonisiert ist, dass für ein Produkt ein Qualitätsmanagementsystem ausreicht.

- Die vom EP vorgeschlagene verpflichtende Messung und Aufzeichnung des Energie- und Ressourcenverbrauchs von KI-Systemen ist ebenfalls zu begrüßen. In einem nächsten Schritt sollten auf EU-Ebene verpflichtende Energieeinsparziele formuliert werden.

6. Anforderungen an benannte Stellen und benennende Behörden (Artikel 30, 38, 44)

- Mit Blick auf die Benennung von Konformitätsbewertungsstellen durch die zuständigen nationalen Behörden sind einheitliche Vorgaben und Bewertungsverfahren erforderlich, um ein durchgängig hohes Kompetenzniveau der benannten Stellen sicherzustellen. Nur dadurch kann ein einheitliches Level-Playing-Field zwischen den benannten Stellen erreicht werden. Die vom EP vorgesehenen Kooperations- und Austauschformate zwischen den benennenden Behörden sind zu unterstützen, ebenso die für behördliche Auditoren vorgeschriebenen

Qualifikationsstandards.

- Aufgrund der fortlaufenden Entwicklung von KI-Systemen sollte die Gültigkeit der von benannten Stellen ausgestellten Zertifikate begrenzt werden. Die vom EP vorgeschlagene Gültigkeitsdauer von vier Jahren ist vor dem Hintergrund der kürzeren Produktlebenszyklen und der kontinuierlichen Veränderungen der KI-Systeme (Lernen) sinnvoll.

7. KI-Reallabore (Artikel 53)

- Die Einrichtung von KI-Reallaboren ist eine gute Möglichkeit, um die Entwicklung und Erprobung von KI-Systemen zu erleichtern. Auch unabhängige Prüforganisationen sollten als wichtiger Partner bei der Entwicklung und Nutzung von Reallaboren mit einbezogen werden. Zudem sollte wie vom EP vorgesehen deren Einrichtung perspektivisch innerhalb eines oder zwischen mehreren Mitgliedsstaaten verbindlich gemacht werden.

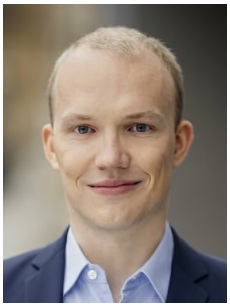
- Die erfolgreiche Nutzung eines Reallabors durch ein KI-System allein kann jedoch keine Konformitätsvermutung auslösen. Bevor ein KI-System auf den Markt gebracht wird, muss es in jedem Fall ein vollständiges Konformitätsbewertungsverfahren durchlaufen, ggf. unter Einbindung einer benannten Stelle. Diese kann im Rahmen der Zertifizierung z. B. auf bestimmte gesammelte Daten aus dem Reallabor zurückgreifen, muss jedoch eine gesamtheitliche Betrachtung der Erfüllung aller gesetzlichen und normativen Anforderungen vornehmen. Zwecks rechtlicher Klarheit sollte deshalb der Begriff der Konformitätsvermutung aus der EP-Position gestrichen werden.

8. Generative KI/Basismodelle (ErwG 60h, Artikel 28b)

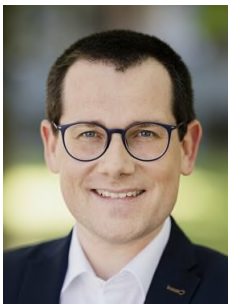
- Die letzten Monate haben deutlich gemacht, wie schnell sich Basismodelle (foundational models) bzw. generative KI-Systeme entwickeln und welche Risiken von ihnen ausgehen können. Es ist daher notwendig, auch diese Technologie direkt im AI Act mit zu regulieren, um den rechtlichen Rahmen zukunftssicher zu gestalten. Der EP-Ansatz einer direkten Regulierung ist daher gegenüber dem Ratsansatz vorzuziehen.
- Aufgrund des großen Einsatzspektrums von Basismodellen erscheint es auch grundsätzlich zielführend, bei der Klassifizierung einen risikobasierten Ansatz zu wählen. Gleichwohl muss sichergestellt werden, dass dabei alle von den jeweiligen Einsatzbereichen ausgehenden Risiken vollumfänglich betrachtet werden. In einem ersten Schritt sollten entsprechend der EP-Position bestimmte Grundanforderungen für alle Anbieter eines Basismodells bzw. eines generativen KI-Modells festgelegt werden. In einem zweiten Schritt sollte anschließend sichergestellt werden, dass auch besonders risikobehaftete Basismodelle bzw. generative KI-Systeme als Hochrisikosysteme klassifiziert werden und damit allen Anforderungen des AI Acts unterliegen.

- Mit Blick auf die Überprüfung von Basismodellen sieht die EP-Position eine interne Bewertung seitens der Anbieter vor. Begründet wird dies mit der fehlenden Expertise von Konformitätsbewertungsstellen bei der Bewertung von Basismodellen. Mangels konkreter gesetzlicher und normativer Anforderungen bestehen derzeit jedoch noch keine umfassenden Prüftools für Basismodelle. Dies stellt jedoch aktuell noch ein Problem für jedwede Form der Bewertung von Basismodellen dar. Dieser Umstand bildet jedoch keine hinreichende Begründung für die Beschränkung auf eine rein interne Bewertung durch den Anbieter selbst. Vielmehr sollte sich auch bei Basismodellen das anzuwendende Bewertungsverfahren ausschließlich nach deren Risikopotential richten. Sofern der EU-Gesetzgeber zu der Einschätzung gelangt, dass bestimmte Basismodelle als hochkritisch einzustufen sind, sollten auch diese einer unabhängigen Drittprüfung durch benannte Stellen unterliegen. Entsprechende Übergangsfristen erlauben europäischen Normungsorganisationen und Konformitätsbewertungsstellen, entsprechende Normen und Prüfstandards hierfür zu erarbeiten.

Autoren und Ansprechpartner



Johannes Kröhnert
Leiter Büro Brüssel
E-Mail: johannes.kroehnert@tuev-verband.de
Tel.: +49 30 760095 500
www.tuev-verband.de



Dr. Patrick Gilroy
Referent Künstliche Intelligenz & Bildung
E-Mail: patrick.gilroy@tuev-verband.de
Tel.: +49 30 760095-360
www.tuev-verband.de

Der TÜV-Verband vertritt die politischen und fachlichen Interessen seiner Mitglieder gegenüber Politik, Verwaltung, Wirtschaft und Öffentlichkeit. Der Verband setzt sich für technische und digitale Sicherheit bei Produkten, Anlagen und Dienstleistungen durch unabhängige Prüfungen und qualifizierte Weiterbildung ein. Mit seinen Mitgliedern verfolgt der TÜV-Verband das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und Vertrauen für die digitale Welt zu schaffen.

Herausgeber
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de