KI-GOVERNANCE

adesso

INHALT

3 | KI-Governance – Die „EU-Verordnung über künstliche Intelligenz“ ist da!

4 | Sind alle Arten von KI-Systemen grundsätzlich zu regulieren?

5 | Für GPAI mit systemischem Risiko gelten zusätzliche Anforderungen

6 | Fristen & Sanktionen

7 | Top-10-Checkliste Anforderungen für Hoch-Risikolevel KI-Systeme

9 | Leitfaden zur Compliance

10 | Kontakt

KI-GOVERNANCE

Künstliche Intelligenz ist in der Mitte der Gesellschaft angekommen: Privatpersonen lassen via KI Texte schreiben, Rezepte heraussuchen oder ihr Smart-Home-System steuern. Auch für Organisationen wird KI zunehmend wichtiger, sei es in der Entwicklung, der Produktion oder der Verwaltung. 69 Prozent der deutschen Unternehmen sind davon überzeugt, dass Künstliche Intelligenz die wichtigste Zukunftstechnologie darstellt. Dies spiegelt sich auch in den prognostizierten Zahlen wider, die das Bundesministerium für Wirtschaft und Klimaschutz veröffentlichte: KI-basierte Lösungen sollen im produzierenden Gewerbe ein zusätzliches Wertschöpfungspotenzial von 30 Mrd. Euro eröffnen, der Einsatz von KI das deutsche Bruttoinlandsprodukt bis zum Jahr 2030 um 11,3 Prozent steigern. Kurzum: Künstliche Intelligenz ist die wichtigste Entwicklung im Bereich der Digitalisierung.

DIE „EU-VERORDNUNG ÜBER KÜNSTLICHE INTELLIGENZ“ IST AUF DEM WEG!

Für Organisationen, die KI-Systeme in ihre Prozesse, Produkte oder Dienstleistung integrieren wollen, gilt es jedoch einiges zu beachten. Allem voran die „EU-Verordnung über künstliche Intelligenz“, kurz EU KI-VO, die am 21. Mai 2024 von den 27 EU-Mitgliedsstaaten verabschiedet wurde – und die den Einsatz von KI regulieren soll. Werden KI-Systeme auf dem europäischen Markt eingesetzt, müssen diese künftig ethische und rechtliche Standards nach EU-Recht erfüllen, etwa das Antidiskriminierungsgesetz. Vorerst gilt eine Übergangsfrist von 6 bis 36 Monaten, während der die Europäische Kommission auf freiwillige Selbstbeschränkungen der Wirtschaft setzt.

Doch geht die EU KI-Verordnung mit zahlreichen Herausforderungen für Organisationen einher. Kritisiert wird die komplexe Frage der Rechtssicherheit: Was ist erlaubt, was nicht? Auch der hohe bürokratische Aufwand sorgt für Unmut.

Was ändert sich konkret für Organisationen?

Die EU KI-VO führt Produktvorschriften für KI-Systeme ein: Einige müssen mit einer CE-Kennzeichnung versehen werden, andere werden gänzlich verboten. Nicht betroffen sind Systeme, die ausschließlich privat genutzt werden, für militärische Vorhaben sowie Systeme, die für Test- und Entwicklung verwendet werden.

Wer muss seine Compliance anpassen?

Änderungen stehen allen Organisationen bevor, die KI-Systeme nutzen, anbieten oder betreiben – und die ihren Sitz in der Europäischen Union haben oder aber außerhalb der EU ansässig sind oder ihr Produkt auf dem europäischen Markt vertreiben.

SIND ALLE ARTEN VON KI-SYSTEMEN GRUNDSÄTZLICH ZU REGULIEREN?

In welchem Maße KI-Systeme von der EU KI-Verordnung reguliert werden, hängt vom Risikolevel ab, das vom jeweiligen System ausgeht. Die EU KI-Verordnung teilt die Technologien in vier Risikokategorien ein: Von den meisten KI-Systemen geht nur ein minimales Risiko aus, für sie gelten daher keinerlei Beschränkungen. Bestimmte KI-Anwendungen dagegen werden komplett verboten.

Verbotenes System

Bedrohen KI-Systeme die Grundrechte von Betroffenen, sind sie in der Europäischen Union verboten. Dazu gehören beispielsweise KI-Systeme, die Manipulation oder Diskriminierung fördern, indem sie etwa Personen sozial bewerten. Auch eine Videoüberwachung, bei der die Bilder der erfassten Personen mit hinterlegten biometrischen Daten abgeglichen und die Personen somit identifiziert werden können, sind in der EU tabu.

Hochrisiko-System

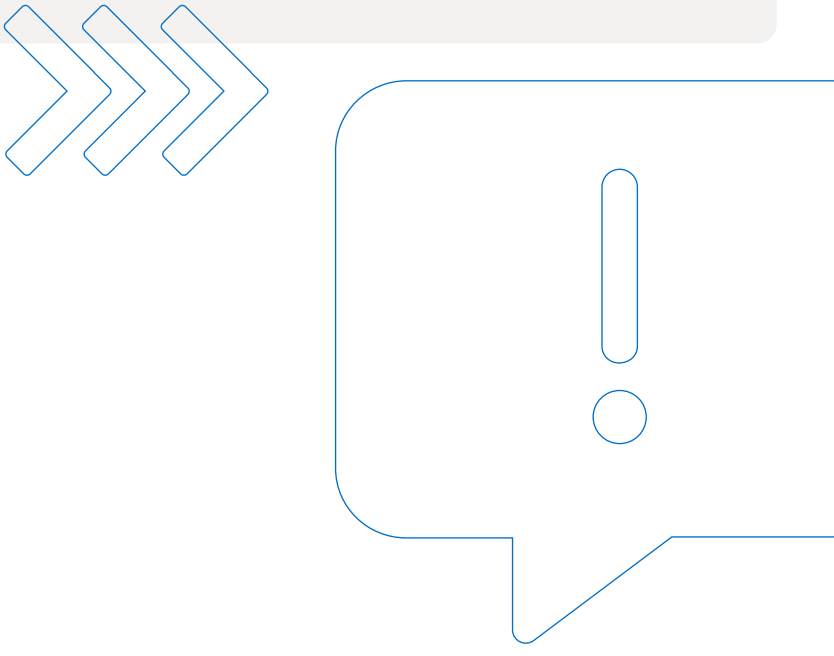
KI-Systeme, die ein hohes Risiko für die Sicherheit und Grundrechte der Bürger darstellen, müssen strenge Anforderungen erfüllen – so brauchen sie beispielsweise eine CE-Kennzeichnung. In diese Kategorie gehören unter anderem KI-Systeme, die in kritischen Infrastrukturen oder in sicherheitskritischen Bereichen wie Logistik und Verwaltung eingesetzt werden. Auch bestimmte biometrische Anwendungen, um Personen zu identifizieren, gehören dazu.

Geringes-Risiko-System

Einfacher wird es bei Systemen, von denen ein geringes Risiko ausgeht – etwa bei Chatbots, also textbasierten Dialogsystemen, mit denen Nutzende chatten können und Hilfe bei bestimmten Fragestellungen bekommen. Für solche Systeme gilt: Sie müssen lediglich bestimmte Transparenzverpflichtungen erfüllen. So muss der Nutzende klar erkennen können, dass er mit einer Maschine und nicht mit einem Menschen interagiert.

Minimales-Risiko-System

Von den meisten KI-Systemen jedoch geht nur ein minimales Risiko für Bürger und Gesellschaft aus. So etwa von Spamfiltern, Übersetzungsdiensten oder Videospielen. Für KI-Systeme dieser Kategorie gelten keine zusätzlichen Anforderungen – sie können also frei auf dem Markt genutzt werden.



FÜR GPAI MIT SYSTEMISCHEM RISIKO GELTEN ZUSÄTZLICHE ANFORDERUNGEN

Spricht man über KI, denken die meisten Menschen vor allem an generative KI wie ChatGPT – Systeme also, mit denen sich in Sekundenschnelle Texte, Bilder oder Vorträge zu bestimmten Themen und mit vorgegebener Stilrichtung erstellen lassen. Diese Systeme basieren oft auf maschinellem Lernen und werden mit großen Datenmengen trainiert, um eine breite Palette von Aufgaben kompetent zu erfüllen.

Für solche generativen KI-Systeme gelten besondere Verpflichtungen, ebenso wie für die Entwicklung von KI-System mit allgemeinem Verwendungszweck, Stichwort „General Purpose AI", kurz GPAI. Wie die Regelungen genau aussehen, unterscheidet sich für Open Source Modelle und andere Dienste.

GPAI-Modelle mit systemischem Risiko stellen besondere Herausforderungen dar, schließlich sind sie breit anwendbar und können somit eine hohe Wirkung entfalten. Sie müssen daher sorgfältig überwacht und reguliert werden, um mögliche negative Auswirkungen auf die Gesellschaft zu vermeiden. Liegt kein systemisches Risiko vor, gelten analog die Mindestanforderungen für Hochrisiko Systeme.

Dokumentation und Meldung von schweren Vorfällen

Für die Umsetzung der EU KI-Verordnung ist das Europäische Amt für KI zuständig, kurz das AI Office der EU: Es darf KI-Modelle für allgemeine Zwecke bewerten, Informationen und Maßnahmen von Modellanbietern anfordern und Sanktionen verhängen.

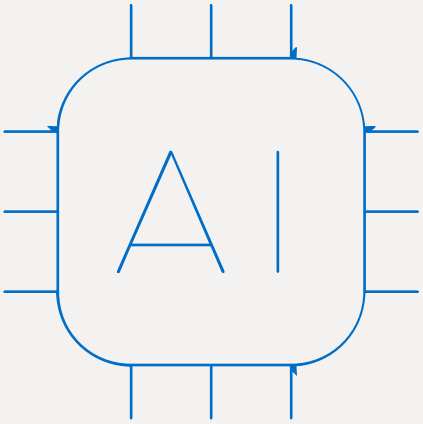
Darüber hinaus ist es die Aufgabe des AI Office, mögliche systemische Risiken auf EU-Ebene zu bewerten und zu mindern. Ebenso gehört dazu, ein angemessenes Niveau an Cybersicherheit sowie der physischen Infrastruktur sicherzustellen.

Entscheidungsprozess der Kommission

Auf Basis der europäischen EU KI-Verordnung – genauer gesagt des Anhangs 1,3 – entscheidet die Kommission darüber, ob das betroffene GPAI-Modell als solches mit systemischem Risiko eingestuft wird oder nicht. Als Grundlage für die Bewertung dienen entweder Meldungen der Anbieter oder aber das eigene Ermessen.

Besonderheiten

Für die Anbieter von GPAI-Modellen mit systemischem Risiko heißt das: Sie müssen die Kommission unverzüglich informieren, dass das Modell die benannten Anforderungen erfüllt oder erfüllen wird. Auch gilt es, zusätzliche Pflichten gemäß Art. 52d EU KI-VO einzuhalten.



FRISTEN & SANKTIONEN

Wann müssen diese Anforderungen umgesetzt sein?

Natürlich müssen die Anforderungen nicht umgehend erfüllt werden, es gelten Übergangsfristen von sechs bis zu 36 Monaten. Wie lang die Übergangszeit genau ist, hängt vom Risikolevel des jeweils verwendeten Systems ab. Bis Anfang 2025 müssen Anbieter und Betreiber nachweisen, dass ihre Mitarbeitenden eine gewisse KI-Kompetenz erlernt haben (Art. 4 EU KI-VO).

Wie hoch fallen mögliche Sanktionen aus?

Verstoßen Anbieter oder Betreiber gegen die Vorschriften der EU KI-Verordnung, müssen sie mit Sanktionen rechnen. Deren Höhe richtet sich nach der Art des Verstoßes. Werden beispielsweise verbotene Praktiken eingesetzt, stehen Strafzahlungen von 35 Mio. Euro oder sieben Prozent des Jahresumsatzes an. Wird gegen Meldungs- und Informationspflichten verstoßen, sind es immerhin 7,5 Mio. Euro oder ein Prozent des Jahresumsatzes.

TOP-10-CHECKLISTE ANFORDERUNGEN FÜR HOCH-RISIKOLEVEL KI-SYSTEME

1. Risikomanagement eingeführt?

> Implementierung eines umfassenden Risikomanagementsystems zur Identifizierung, Bewertung und Steuerung der Risiken im Zusammenhang mit dem KI-System.
> Regelmäßige Überprüfung und Aktualisierung des Risikomanagementsystems.

2. Daten-Governance eingeführt?

> Einhaltung der in der EU KI-Verordnung festgelegten Anforderungen an die Datenverarbeitung und Daten-Governance.
> Implementierung von Maßnahmen zur Sicherstellung der Qualität, Sicherheit und Integrität der Daten.
> Etablierung eines transparenten Systems für die Datenzugriffsrechte.

3. Technische Dokumentation eingeführt?

> Erstellung einer detaillierten technischen Dokumentation des KI-Systems,
> einschließlich seiner Architektur, Algorithmen, Datensätze und Modellparameter.
> Verwendung standardisierter Formate und Schnittstellen für die technische Dokumentation.

4. Menschliche Überwachung und Feedback eingeführt?

> Implementierung von Mechanismen zur menschlichen Überwachung und Kontrolle des KI-Systems.
> Sicherstellen, dass Menschen die Möglichkeit haben, in kritischen Situationen einzugreifen und Entscheidungen zu treffen.

5. Auditierung bzw. Qualitätsmanagementsystem eingeführt?

> Einführung eines Systems zur Nachverfolgung aller Aktivitäten des KI-Systems, einschließlich der Eingabedaten, der Entscheidungen und der Outputs.
> Sicherstellen, dass die Auditierung für die Aufsichtsbehörden zugänglich ist.

6. Transparenz und Kommunikation eingeführt?

> Bereitstellung von transparenten Informationen über das KI-System und seine Nutzung an alle interessierten Parteien.
> Entwicklung eines Kommunikationsplans zur Information der Öffentlichkeit über das KI-System und seine potenziellen Auswirkungen.

7. Genauigkeit, Robustheit und Cybersicherheitsmaßnahmen

> Während des gesamten Lebenszyklus der KI-Systeme sind Präzisionsmetriken, Maßnahmen zur Widerstandsfähigkeit gegen Fehler und Maßnahmen zur Beseitigung möglicher Verzerrungen eingeführt worden.

8. EU-Konformitätserklärung erstellt?

> Für jedes KI-System mit hohem Risiko ist eine eindeutige und unterzeichnete Konformitätserklärung nach Kapitel 2 erstellt.

9. CE-Konformitätsbewertung eingeführt?

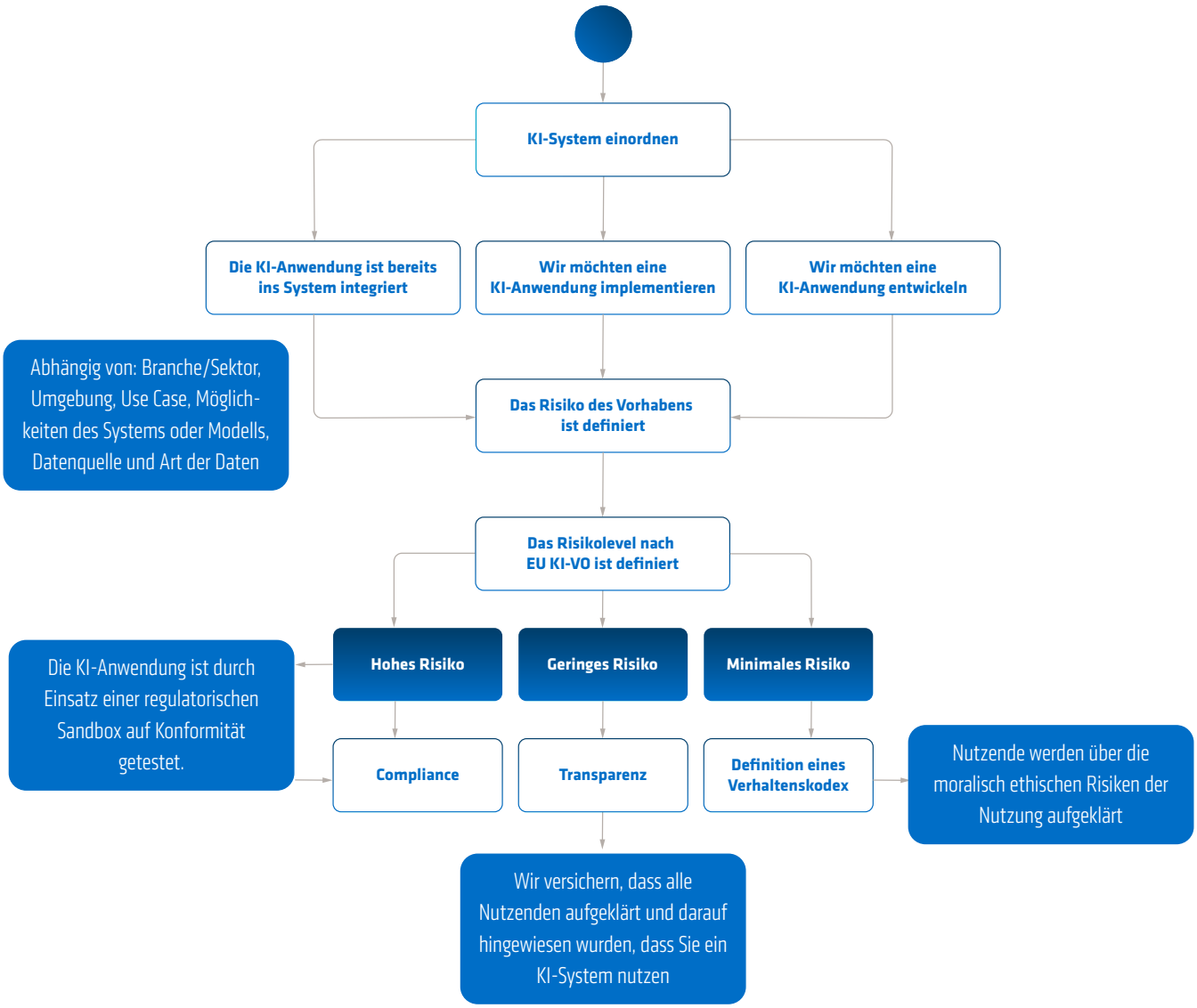
> Durchführung einer CE-Konformitätsbewertung durch eine benannte Stelle, um die Konformität des KI-System mit den Anforderungen des EU KI Acts zu bestätigen.

10. Eintrag in EU-Datenbank erledigt?

> Das KI-System ist in der EU-Datenbank nach Artikel 60 angelegt worden.

LEITFADEN ZUR COMPLIANCE

Die EU KI-VO gilt sowohl für existierende Systeme als auch für neue Produkte. Im Folgenden finden Sie einen Leitfaden, der einen groben Weg zur Erfüllung der Compliance Vorschriften skizziert.



KONTAKT

Haben wir Ihr Interesse geweckt? Kommen Sie gerne direkt auf uns zu, um mit unseren Experten einen Termin für ein Erstgespräch über unser Angebot im Kontext KI-Governance zu vereinbaren. Für einen Überblick empfehlen wir einen Besuch unserer Landingpage.

Martin Krisch
Team Lead Manager

+49 152 38856791
Martin.Krisch@adesso.de

Martin Wanke
Managing Consultant

+49 152 38856791
Martin.Wanke@adesso.de

Laurenz Eckert
Consultant

+49 152 38856791
Laurenz-Paul.Eckert@adesso.de

Quellen:

KI-basierte Lösungen sollen im produzierenden Gewerbe ein zusätzliches Wertschöpfungspotenzial von 30 Mrd. Euro eröffnen, der Einsatz von KI das deutsche Bruttoinlandsprodukt bis zum Jahr 2030 um 11,3 Prozent steigern.

www.digitale-technologien.de

eur-lex.europa.eu

adesso SE
Adessoplatz 1
44269 Dortmund
Deutschland
T +49 231 7000-7000
F +49 231 7000-1000
E info@adesso.de
www.adesso.de

adesso