AI Act

Verordnung über Künstliche Intelligenz

Status:

Entwurf / Geplant | § Beschlossen

Eckdaten:

- Europäisch
- Verordnung
- Gilt seit 1. August 2024

Branchen:

Worum geht es?

Ziel der am 1. August 2024 in Kraft getretenen Verordnung über Künstliche Intelligenz (KI-Verordnung oder AI Act) ist die Festlegung eines einheitlichen Rechtsrahmens insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen Künstlicher Intelligenz (KI). Durch den AI Act soll die Einführung von menschenzentrierter und vertrauenswürdiger KI gefördert, der grenzüberschreitende freie Verkehr KI-gestützter Waren und Dienstleistungen gewährt sowie gleichzeitig die in der Charta der Europäischen Union verankerten Grundrechte eingehalten werden. Daneben ist auch die Gewährleistung des Schutzes vor schädlichen Auswirkungen von KI-Systemen ein Ziel des AI Acts. Durch die branchenoffene Verordnung werden einige Verordnungen und Richtlinien vor allem im Bereich Zivilluftfahrt und Kraftfahrzeuge geändert.

Wie wird es umgesetzt?

Um die Harmonisierung für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von auf den Menschen ausgerichteten und vertrauenswürdigen Systemen mit KI zu erreichen, werden durch den AI Act nachfolgende Maßnahmen geregelt:

Definition von KI-Systemen und Anwendungsbereich des AI Acts

Der AI Act definiert ein KI-System als *„ein maschinengeschütztes 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 und implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.“*

Anbieter, die derlei KI-Systeme in der EU in Verkehr bringen oder betreiben, unabhängig davon, ob sie in der EU ansässig sind, werden von der Verordnung umfasst. Außerdem gilt der AI Act auch für Importeure, Händler und Produkte mit integrierten KI-Systemen. Vom Anwendungsbereich ausgenommen sind militäre Anwendungen, wissenschaftliche Forschung und Systeme, die unter freier Lizenz bereitgestellt werden, wenn sie nicht als Hochrisiko-KI eingestuft werden. Der AI Act bleibt im Einklang mit anderen EU-Vorschriften, zum Beispiel zum Datenschutz und Verbraucherschutz.

Anbieter und Betreiber von KI-Systemen sind verpflichtet, Maßnahmen zu ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen. Unter KI-Kompetenz wird im Rahmen des AI Acts *„die Fähigkeit, die Kenntnis und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglicht, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“* verstanden.

Verbotene Praktiken im KI-Bereich

Durch den AI Act wird der Einsatz folgender KI-Systeme verboten:

- KI-Systeme, die unterschwellige oder manipulative Techniken anwenden, um das Verhalten von Personen zu beeinflussen und ihnen Schaden zuzufügen;
- KI-Systeme, die die Schwächen bestimmter Personen aufgrund ihres Alters, ihrer Behinderung oder sozialen Situationen ausnutzen;
- KI-Systeme, die Personen auf Basis ihres sozialen Verhaltens bewerten und dadurch benachteiligen;
- KI-Systeme, die Straftaten auf Basis von Profiling vorhersagen, ohne objektive Fakten zu berücksichtigen;
- KI-Systeme, die Gesichtserkennung aus ungezielten Internetbildern nutzen oder Emotion am Arbeitsplatz analysieren;
- KI-Systeme, die Personen biometrisch kategorisieren, um sensible Daten wie Herkunft oder politische Überzeugung abzuleiten;
- KI-Systeme, die Echtzeit-Gesichtserkennung im öffentlichen Raum zu Strafverfolgungszwecken einsetzen, außer in klar definierten Notfällen.

Besondere Anforderungen an Hochrisiko-KI-Systeme und Pflichten für Akteure in Bezug auf solche Systeme

Hochrisiko-KI-Systeme sind nach dem AI Act KI-Systeme

- die als Sicherheitsbauteil eines Produkts, das unter die EU-Harmonisierungsvorschriften fällt, verwendet werden oder selbst ein solches Produkt sind oder
- KI-Systeme selbst oder Produkte, deren Sicherheitsbauteil ein KI-Produkt ist, die einer Konformitätsbewertung durch Dritte unterzogen werden müssen.

Zusätzlich sind im Anhang III des AI Acts einige Punkte gelistet, die als Hochrisikoprodukte eingestuft werden.

<u>Besondere Anforderungen an Hochrisiko-KI-Systeme</u>

Zusätzlich zu möglicherweise zu beachtenden Anforderungen im Rahmen von EU-Harmonisierungsvorschriften, legt der AI Act spezifische Anforderungen für Hochrisiko-KI-Systeme fest. Neben der Berücksichtigung der Zweckbestimmung sowie dem allgemein anerkannten Stand der Technik in Bezug auf KI und KI-bezogenen Technologien handelt es sich dabei um folgende Maßnahmen:

Risikomanagementsystem

Der AI Act schreibt vor, dass für Hochrisiko-KI-Systeme ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrecht gehalten und das über den gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant, durchgeführt, überprüft und aktualisiert werden muss. Der iterative Prozess umfasst nachfolgende Schritte:

- Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die bei zweckmäßiger Verwendung des Hochrisiko-KI-Systems entstehen können,
- Abschätzung und Bewertung der möglichen Risiken,
- Bewertung anderer möglicherweise auftretender Risiken und
- Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der ermittelten Risiken.

Die ergriffenen Risikomanagementmaßnahmen müssen die Risiken wirksam minimieren und gleichzeitig ein angemessenes Gleichgewicht bei der Durchführung der Maßnahmen zur Erfüllung der Anforderungen an ein Risikomanagementsystem sicherstellen. Dabei ist darauf zu achten, dass das Gesamtrestrisiko sowie jedes mit einer Gefahr verbundene relevante Restrisiko als vertretbar beurteilt wird.

Um geeignete Risikomanagementmaßnahmen zu identifizieren, schreibt der AI Act die Testung der Hochrisiko-KI-Systeme zu geeigneten Zeitpunkten während des gesamten Entwicklungsprozesses sowie vor dem Inverkehrbringen und der Inbetriebnahme vor.

Daten und Daten-Governance

Hochrisiko-KI-Systeme, die mit KI-Modellen arbeiten, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden. Diese Datensätze müssen spezifischen Qualitätskriterien entsprechen. So müssen diese im Hinblick auf die Zweckbestimmung eines Hochrisiko-KI-Systems relevant, repräsentativ und möglichst fehlerfrei sein. Zudem müssen Daten-Governance- und Datenverwaltungsverfahren eingehalten werden, um Verzerrungen zu erkennen und zu korrigieren. Hierzu dürfen in Ausnahmefällen und unter Einhaltung strenger Sicherheits- und Datenschutzmaßnahmen auch besondere Kategorien personenbezogener Daten verarbeitet werden. Personenbezogene Daten müssen nach der Verwendung gelöscht werden.

Technische Dokumentation

Um nachzuweisen, wie und dass die Anforderungen an Hochrisiko-KI-Systeme erfüllt sind, wird eine Technische Dokumentation erstellt, die vom Anbieter auf dem aktuellen Stand zu halten ist. Die Technische Dokumentation muss mindestens die folgenden Informationen enthalten:

- Allgemeine Beschreibung des KI-Systems;
- Detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses;
- Detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems;
- Darlegung zur Eignung der Leistungskennzahlen für das spezifische KI-System;
- Detaillierte Beschreibung des Risikomanagementsystems;
- Beschreibung einschlägiger Änderungen, die der Anbieter während des Lebenszyklus an dem System vorgenommen hat;
- Aufstellung der vollständigen oder teilweise angewandten harmonisierten Normen;
- Kopie der EU-Konformitätserklärung;
- Detaillierte Beschreibung des Systems zur Bewertung der Leistung des KI-Systems in der Phase nach dem Inverkehrbringen sowie einem Plan für die Beobachtung nach dem Inverkehrbringen.

Aufzeichnungspflichten

Anbieter von Hochrisiko-KI-Systemen sind verpflichtet, während des gesamten Lebenszyklus der Systeme automatisierte Protokollierungen von relevanten Ereignissen zu ermöglichen. Dadurch soll sichergestellt werden, dass das System rückverfolgbar ist und potenzielle Risiken identifiziert werden können.

Hierfür ist der Nutzungszeitraum, die Referenzdatenbank, die Eingabedaten sowie die Identität der an der Überprüfung beteiligten Person zu protokollieren.

Weitere Anforderungen an Hochrisiko-KI-Systeme

Des Weiteren stellt der AI Act Anforderungen an die Transparenz, die Bereitstellung von Informationen für die Betreiber, die menschliche Aufsicht sowie an die Genauigkeit, Robustheit und Cybersicherheit von Hochrisiko-KI-Systemen.

Pflichten für Akteure in Bezug auf Hochrisiko-KI-Systeme

Neben den Anforderungen an Hochrisiko-KI-Systeme schreibt der AI Act auch Pflichten vor, denen Anbieter und Betreiber derlei Systemen sowie andere Beteiligte nachkommen müssen. Es handelt sich dabei unter anderem um folgende Pflichten:

Qualitätsmanagementsystem

Um die Einhaltung des AI Acts zu gewährleisten, müssen Anbieter von Hochrisiko-KI-Systemen ein Qualitätsmanagementsystem einrichten, das schriftlich dokumentiert sein muss. Außerdem muss es verschiedene Aspekte wie Regulierungscompliance, Entwurfskontrollen, Qualitätskontrollen, Risikomanagement, Datenmanagement und Kommunikation mit Behörden abdecken.

Aufbewahrung der Dokumentation

Anbieter von Hochrisiko-KI-Systemen sind verpflichtet unter anderem die Technische Dokumentation, die Dokumentation des Qualitätsmanagementsystems, die Dokumentation über etwaige von notifizierten Stellen genehmigte Änderungen und die EU-Konformitätserklärung für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems aufzubewahren.

Weitere Pflichten der Anbieter von Hochrisiko-KI-Systemen

- Sicherstellung, dass die Hochrisiko-KI-Systeme alle festgelegten Anforderungen erfüllen;
- Aufbewahrung automatisch erzeugter Protokolle;
- Sicherstellung, dass die Hochrisiko-KI-Systeme einem Konformitätsbewertungsverfahren unterzogen werden;
- Ausstellung einer EU-Konformitätserklärung;
- Anbringen der CE-Kennzeichnung auf dem Produkt, der Verpackung oder in der beigefügten Dokumentation;
- Einhaltung der Registrierungspflichten;
- Ergreifen von erforderlichen Korrekturmaßnahmen;
- Sicherstellung, dass das Hochrisiko-KI-System die vorgeschriebenen Barrierefreiheitsanforderungen erfüllt.

Konformitätsbewertung

Anbieter von Hochrisiko-KI-Systemen müssen ein Konformitätsbewertungsverfahren anwenden, um sicherzustellen, dass ihre Systeme den festgelegten Anforderungen entsprechen. Hierbei gibt es zwei Möglichkeiten:

- die Anforderungen an Hochrisiko-KI-Systeme sind erfüllt und harmonisierte Normen und/oder gemeinsame Spezifikationen werden angewandt: Der Anbieter entscheidet zwischen einer internen Kontrolle oder der Bewertung des Qualitätsmanagementsystems und der Bewertung der Technischen Dokumentation durch eine Notifizierte Stelle oder

- es liegen keine harmonisierten Normen und/oder gemeinsame Spezifikationen vor oder diese werden nicht beziehungsweise nur teilweise angewandt: In diesem Fall hat die Konformitätsbewertung durch eine Notifizierte Stelle zu erfolgen.

Es gilt bei der Konformitätsbewertung auch noch einige Ausnahmeregelungen für im AI Act aufgeführte Hochrisiko-KI-Systeme zu beachten.

Eine erneute Konformitätsbewertung ist erforderlich, wenn bei einem Hochrisiko-KI-System, das bereits Gegenstand eines Konformitätsbewertungsverfahrens gewesen ist, eine wesentliche Änderung durchgeführt wurde.

EU-Konformitätserklärung

Der AI Act schreibt vor, dass Anbieter für jedes Hochrisiko-KI-System eine EU-Konformitätserklärung ausstellen müssen. Diese muss für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme bereitgehalten werden, sowie als Kopie den zuständigen nationalen Behörden übermittelt werden. Aus der EU-Konformitätserklärung muss hervorgehen, für welches Hochrisiko-KI-System diese ausgestellt wurde und dass die festgelegten Anforderungen erfüllt werden. Unterliegt das Hochrisiko-KI-System anderen Rechtsvorschriften, die wiederum eine EU-Konformitätserklärung erfordern, so ist es ausreichend, wenn eine einheitliche Erklärung erstellt wird.

Weiterhin finden sich im AI Act unter anderem Informationen zu folgenden Punkten:

- Notifizierende Behörden und notifizierte Stellen sowie zuständige nationale Behörden
- Normen, Bescheinigungen und Registrierung
- Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme
- Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck
- Praxisleitfäden
- Maßnahmen zur Innovationsförderung
- EU-Datenbank für Hochrisiko-KI-Systeme
- Beobachtung nach dem Inverkehrbringen, Informationsaustausch und Marktüberwachung
- Sanktionen

BIOPRO Baden-Württemberg GmbH | Alexanderstraße 5 | 70184 Stuttgart
Zentrale Anlaufstelle Regulatorik Gesundheitswirtschaft BW | E-Mail: regulatorik-gesundheitswirtschaft@bio-pro.de | Web: regulatorik-gesundheitswirtschaft.bio-pro.de