d-fine

Der European Artificial Intelligence Act

Herausforderungen erkennen und erfolgreich begegnen

analytisch. technologisch. quantitativ.

August 2021

1. Der Artificial Intelligence Act

Die Europäische Union (EU) hat mit dem Artificial Intelligence Act (AIA) den weltweit ersten Entwurf für eine umfassende Regulierung von KI-Systemen vorgelegt. Der AIA regelt, unter welchen Bedingungen KI-Systeme – entweder als eigenständige Einheit oder als Produktkomponente – innerhalb der EU angeboten bzw. eingesetzt werden können. Der AIA lässt sich also nicht dadurch umgehen, dass ein Anbieter seinen Standort außerhalb der EU hat. Nach Aussage der Europäischen Kommission könnte der AIA bereits in der zweiten Jahreshälfte 2024 als in der gesamten EU geltendes Recht in Kraft treten.

2. Hochrisiko KI-Systeme stehen im Fokus

Der AIA folgt einem risikobasierten und verbraucherschutzorientierten Ansatz, der Use Cases für KI-Systeme in unterschiedliche Gruppen einordnet:[1] Viele Anwendungen, die wir im Alltag verwenden, fallen in die Gruppe von KI-Systemen mit geringem Risiko und werden nicht direkt reguliert. Darauf folgt die Gruppe von KI-Systemen mit beschränktem Risiko, für welche gewisse Transparenzregeln gelten. Diese umfasst vor allem KI-Systeme, die mit natürlichen Personen interagieren.

Ein besonderes Augenmerk legt die EU-Kommission auf die Gruppe von Hochrisiko-Systemen, die sich potentiell negativ auf die Sicherheit und die Grundrechte von natürlichen Personen auswirken können. Betroffen sind Sicherheitskomponenten von bereits regulierten Produkten, etwa aus der Medizintechnik, sowie eigenständige KI-Systeme in folgenden Einsatzgebieten:[2]

- Biometrische Identifizierung und Kategorisierung natürlicher Personen
- Verwaltung und Betrieb kritischer Infrastrukturen
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Allgemeine und berufliche Bildung
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

Eine kleine Gruppe von Use Cases mit einem unannehmbaren Risiko für die Sicherheit und die Grundrechte natürlicher Personen wird generell verboten.

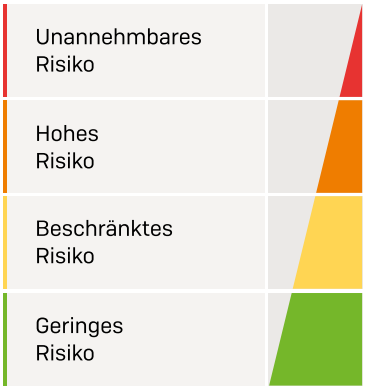

Abbildung 1: Risikobasierte Kategorisierung von KI-Systemen

1 Bei Bedarf können Use Cases angepasst oder neue Use Cases hinzugefügt werden.

2 Siehe Anhang II des AIA für eine Liste an Harmonisierungsrechtsvorschriften für bereits regulierte Produkte und Anhang III für eine Liste an Use Cases für eigenständige KI-Systeme in den genannten Bereichen.

3. Was ist KI?

Die Definition von KI umfasst im AIA prinzipiell alle Techniken des maschinellen Lernens, statistische Verfahren sowie logik- und wissensgestützte Konzepte. Der AIA strebt hier eine technologieneutrale Definition von KI an, die in der Zukunft erweitert werden kann.

Abbildung 2: KI-Techniken und Konzepte. Die Auflistung ist nicht abschließend und kann zukünftig um weitere Punkte ergänzt werden.

Diese sehr generelle Definition von KI wird durch die Definition von KI-Systemen im Speziellen eingeschränkt, siehe Infobox 1.

Demnach ist zunächst zu prüfen, ob eine Anwendung ein KI-System im Sinne des AIA darstellt. Im Anschluss ist die Risikoeinwertung anhand des Use Cases vorzunehmen.

KI-Systeme

Der AIA bezeichnet solche Software als KI-System, die mit KI-Techniken und -Konzepten entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflusst, mit dem sie interagiert.

Infobox 1: Definition KI-Systeme

4. Was Anbieter und Nutzer von Hochrisiko-KI-Systemen beachten müssen

Für Anbieter, bzw. Nutzer bei Eigenentwicklungen, gilt es ein geeignetes Risiko- und Qualitätsmanagementsystem aufzubauen.[3] Insgesamt sind verschiedene Grundsätze einzuhalten, die sich grob wie folgt zusammenfassen lassen:

- Datensätze, welche für das Training, Testen und Validieren von KI-Systemen genutzt werden, müssen relevant, repräsentativ, fehlerfrei und vollständig sein
- KI-Systeme müssen nachvollziehbar und überprüfbar sein, dies beinhaltet umfangreiche Dokumentation und automatisierte Generierung von Logs
- KI-Systeme und Modellergebnisse müssen für Nutzer möglichst transparent sein
- Eine menschliche Aufsicht muss technisch ermöglicht werden
- KI-Systeme müssen über ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit verfügen

Der AIA formalisiert und vereinheitlicht somit Prinzipien der verantwortungsvollen Entwicklung von KI-Systemen. Anbieter von KI-Systemen werden vor die Aufgabe gestellt ein umfängliches Risikomanagementsystem vorzulegen, das einerseits auf die Anforderungen der gegebenen KI-Systeme zugeschnitten ist und andererseits auch neue Entwicklungen im Bereich KI miteinbeziehen kann.

5. Von der Entwicklung zur CE-Kennzeichnung

Ist ein KI-System eine Sicherheitskomponente eines bereits regulierten Produkts, wird die Prüfung des Systems in die bestehende Konformitätsprüfung dieses Produkts integriert. Ähnlich sieht es bei der Prüfung von KI-Systemen für die Kreditwürdigkeitsprüfungen und das Kreditscoring natürlicher Personen aus, bei denen sich die Überprüfung der Modelle in die bereits bestehenden aufsichtlichen Anforderungen und etablierten Prozesse zur Überprüfung von Kreditinstituten einfügen soll.

Bei eigenständigen KI-Systemen ist eine Überprüfung durch Dritte nur für KI-Systeme notwendig, die der biometrischen Identifikation von Personen dienen. Anbieter aller anderen Hochrisiko-Systeme nehmen die Konformitätsprüfung selbst vor und müssen darlegen, dass die Vorgaben des AIA erfüllt sind.

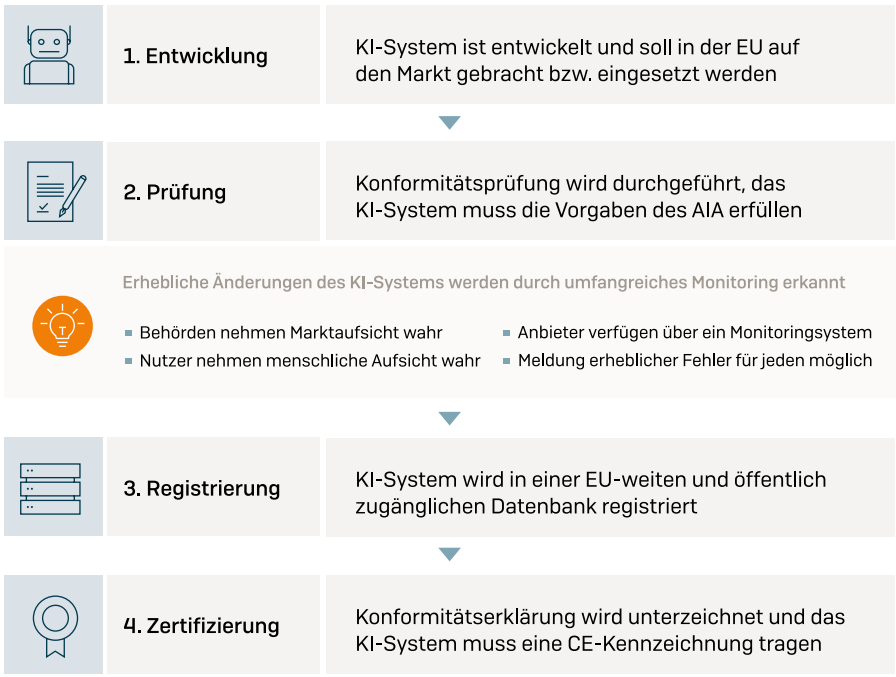

Abbildung 3: Schritte zum konformen eigenständigen KI-System

3 Kreditinstitute nehmen hier eine gesonderte Rolle ein, da für diese u.a. die Vorgaben des AIA in Verbindung mit Artikel 74 der Richtlinie 2013/36/EU gelten.

6.

Konzeption und Umsetzung aus einer Hand

Wir begleiten Unternehmen entlang des gesamten Lebenszyklus von KI-Systemen – von der Konzeption und Entwicklung über die ex-ante Konformitätsprüfung bis zum Monitoring. Basierend auf der regulatorischen Roadmap und daraus abgeleiteter Implikationen für KI-Systeme können wir eine technologisch nachhaltige Produktivlösung umsetzen, die konform zu allen regulatorischen Anforderungen ist – inklusive denen des AIA.

Weitere Informationen finden Sie auf www.d-fine.com oder kontaktieren Sie uns telefonisch unter +49 (0)69 90 737 0.

Autoren

Todor Dobrikov
Head of AI, d-fine GmbH, Frankfurt
Todor.Dobrikov@d-fine.de

Dr. Ulf Menzler
MLOps Expert, d-fine GmbH, Düsseldorf
Ulf.Menzler@d-fine.de

Dr. Sebastian Pfaff
AI Expert, d-fine GmbH, Frankfurt
Sebastian.Pfaff@d-fine.de

d-fine

Berlin
d-fine GmbH
Friedrichstraße 68
10117 Berlin
Deutschland
berlin@d-fine.de

Düsseldorf
d-fine GmbH
Dreischeibenhaus 1
40211 Düsseldorf
duesseldorf@d-fine.de

Frankfurt
d-fine GmbH
An der Hauptwache 7
60313 Frankfurt
Deutschland
frankfurt@d-fine.de

München
d-fine GmbH
Bavariafilmplatz 8
82031 Grünwald
Deutschland
muenchen@d-fine.de

London
d-fine Ltd
6-7 Queen Street
London, EC4N 1SP
United Kingdom
london@d-fine.co.uk

Wien
d-fine Austria GmbH
Riemergasse 14 Top 12
1010 Wien
Österreich
wien@d-fine.at

Zürich
d-fine AG
Brandschenkestrasse 150
8002 Zürich
Schweiz
zuerich@d-fine.ch