

01

Einleitung

Kursübersicht > EU AI Act

In diesem Modul haben wir den EU AI Act für Sie aufbereitet – das ist die europäische Verordnung über künstliche Intelligenz, laut derer KI-Systeme künftig vier Risikogruppen zugewiesen werden sollen. Das geschieht in Abhängigkeit vom Nutzungskontext des Systems und kann schwerwiegende Folgen für Unternehmen haben, die KI-Systeme entwickeln. Hier erfahren Sie, was sich durch das Gesetz verändern wird und welche Auswirkungen das neue Gesetz auf Entwickelnde haben kann. Abschließend diskutieren unsere Experten die Chancen und Herausforderungen, die der EU AI Act für Developer und Nutzende von KI-Systemen darstellt.

1. Was ist der EU AI Act?

Nachdem Sie nun ein kurzes Einführungsvideo gesehen haben, wenden wir uns nun einer etwas detaillierteren Betrachtung des EU AI Acts zu.

Ziele des EU AI Acts

Mit dem EU AI Act haben sich die Mitgliedstaaten der EU zum Ziel gesetzt, das erste umfassende Regularium für den Umgang mit Systemen, die auf Künstlicher Intelligenz (KI) basieren, zu verfassen. Ziel ist es, rechtliche Rahmenbedingungen zu schaffen, in denen KI-Projekte in Wirtschaft, Forschung und Gesellschaft so eingesetzt und entwickelt werden können, dass ein vertrauenswürdiger Umgang mit den Systemen möglich ist. Die fundamentalen Rechte der Nutzer:innen, aber auch Aspekte wie Sicherheit und das Handeln auf Grundlage ethischer Prinzipien, sollen dabei mit einbezogen werden. Dabei soll der EU AI Act über die Grenzen der EU hinaus einen Impuls setzen und, ähnlich wie die DSGVO im Datenschutz, einen Standard stellen, der auch in Nicht-EU-Ländern wie den USA oder Japan genutzt wird.

Entwicklung des Acts

Bei der Entwicklung des EU AI Acts handelt es sich um einen komplexen bürokratischen Prozess, der sich nicht nur über viele Jahre hinweg entwickelte, sondern auch große Teile des parlamentarischen EU-Apparats durchlaufen hat.

Eine vollständige Übersicht des zeitlichen Verlaufs des Gestaltungsprozesses und der damit verbundenen Institutionen und Zwischenstände finden Sie hier:
<https://artificialintelligenceact.eu/de/entwicklungen/>.

2. Vergleich mit anderen Ländern / Regionen

insbesondere England, USA und Kanada

Betrachtet man den EU AI Act als groß angelegte Normierung innerhalb des europäischen Raums, drängt sich schnell die Frage auf, welche Auswirkungen die Gesetzgebung außerhalb seiner Mitgliedstaaten haben wird. Es kann dabei davon ausgegangen werden, dass das EU-Parlament zwar primär die Regulierung im eigenen Legislaturbereich im Blick hat, aber auch auf andere große Volkswirtschaften wie die USA, China und das Vereinigte Königreich schaut, wenn es um den Einsatz von KI geht. Wie schon bei der Datenschutz-Grundverordnung (DSGVO) scheint hier der Gedanke zu sein, einen weitreichenden "Goldstandard" zu schaffen, der auch die Gesetzgebung in den Nationen außerhalb der EU bestimmt. Wir halten es deshalb für sinnvoll, einen kurzen Blick auf den aktuellen Stand der KI-Regulierung in anderen Nationen zu werfen, um diese Vorstellung besser einordnen zu können.

Vereinigtes Königreich

Schaut man dazu beispielsweise über den Kanal ins Vereinigte Königreich, so stellt man fest, dass auch dort weitreichende Maßnahmen für die Regulierung und den ethischen Umgang mit KI bereits getroffen worden sind. Die britische Regierung setzt dabei auf bestehende sektorale Vorgaben wie bspw. die KI-Prinzipien der OECD oder die Empfehlung zum ethischen Umgang mit KI der UNESCO. Diese übergeordneten Richtlinien werden durch lokal angetriebene Maßnahmen erweitert. Von besonderer Bedeutung ist dabei zum Beispiel die Bletchley Declaration aus November 2023, bei der sich 28 Länder, darunter die Vereinigten Staaten, China und die Europäische Union, geeinigt haben, international bei der Bewältigung von Herausforderungen und Risiken im Bereich der KI zusammenzuarbeiten. Im Fokus standen dabei vor allem "frontier"-Systeme, also KI-Grundlagenmodelle, die für alle möglichen Anwendungsfälle nutzbar gemacht werden können, so wie bspw. die ChatGPT zugrunde liegenden LLMs. Es gibt also ein klares Bewusstsein für die Bedeutung des Themas KI und erste Bestrebungen für Lösungen. Die dabei getroffenen Vereinbarungen sind dabei eher Leitlinien und weniger strenges Regularium, als es der EU AI Act sein möchte.

USA

Demgegenüber steht die Regulierung von KI in den USA derzeit noch am Anfang. Zwar sind auch diese Teil der Bletchley Declaration, trotzdem fehlt ein kohärentes nationales Regelwerk. Aktuell gibt es in den USA keine umfassende föderale KI-Regulierung, sondern lediglich fragmentierte Richtlinien und Bestrebungen auf Bundesstaatenebene und in verschiedenen Sektoren. Bundesbehörden wie die Federal Trade Commission (FTC) haben zwar Leitlinien zur Vermeidung unfairer oder

irreführender KI-Anwendungen herausgegeben, aber umfassende gesetzliche Regelungen stehen noch aus.

Allerdings gibt es zunehmend Bestrebungen, eine konsistente Regulierung zu entwickeln. Präsident Joe Biden hat Anfang 2021 den "National Artificial Intelligence Initiative Act" unterzeichnet, der die Forschung und Entwicklung von KI koordiniert und fördert. Zudem hat das Weiße Haus Ende 2022 einen "Blueprint for an AI Bill of Rights" veröffentlicht, der Prinzipien zum Schutz der Bürgerrechte im Zusammenhang mit KI vorschlägt. Während die EU mit dem AI Act einen klaren und strengen Regulierungsrahmen vorgibt, arbeiten die USA daran, ihre Strategie zu entwickeln, die wahrscheinlich stärker auf Selbstregulierung und sektorale Ansätze setzt, um Innovationen nicht zu behindern (Pinsent Masons) (Skadden, Arps, Slate, Meagher & Flom LLP).

Kanada

Im Kontext des EU AI Acts hat Kanada ebenfalls Schritte unternommen, um den Einsatz von KI zu regulieren und zu fördern. Aktuell wird KI in Kanada hauptsächlich durch den Artificial Intelligence and Data Act (AIDA) reguliert, der Teil des umfassenden Digital Charter Implementation Acts ist, welcher im Juni 2022 vorgeschlagen wurde. AIDA zielt darauf ab, KI-Systeme zu regulieren, die ein erhebliches Risiko für die Sicherheit der Menschen oder ihre Grundrechte darstellen. Der Ansatz umfasst Verpflichtungen zur Transparenz, zur Risikobewertung und zur Einhaltung ethischer Standards.

Zusätzlich gibt es in Kanada Bestrebungen, die Regulierung weiter zu verfeinern und zu stärken. Die kanadische Regierung arbeitet daran, Richtlinien und Standards zu entwickeln, die sicherstellen, dass KI-Systeme sicher, fair und transparent sind. Dies beinhaltet auch die

Zusammenarbeit mit internationalen Partnern und Organisationen, um globale Standards zu fördern und die Interoperabilität von Regulierungsrahmen zu gewährleisten. Im Vergleich zum EU AI Act, der einen sehr strukturierten und strengen Rahmen vorgibt, verfolgt Kanada einen eher kooperativen und flexiblen Ansatz. Die kanadische Regulierung konzentriert sich auf die Förderung von Innovationen, während sie gleichzeitig sicherstellt, dass die Entwicklung und der Einsatz von KI ethisch und verantwortungsvoll erfolgen (Pinsent Masons) (Skadden, Arps, Slate, Meagher & Flom LLP).

Zusammengefasst kann festgehalten werden, dass zwar viele Nicht-EU-Nationen eine klare Vorstellung von KI und potenziellen unkontrollierten Auswirkungen haben, im Gegensatz zur EU allerdings teilweise noch am Anfang einer konkreten Ausformulierung von Regeln und Gesetzen stehen oder generell einen offeneren Ansatz mit Blick auf möglichst freie Innovationsentwicklung verfolgen.

3. Umsetzung des Acts in den Mitgliedstaaten

Die faktische Umsetzung des EU AI Acts in den Mitgliedstaaten erfordert sorgfältige Planung und Koordination, um die umfassenden Anforderungen des Gesetzes zu erfüllen.

Primäre Inhalte des EU AI Acts

Der EU AI Act ist ein umfassendes Regelwerk, das den Einsatz von KI innerhalb der EU reguliert. Zu den primären Inhalten gehören die Kategorisierung von KI-Systemen nach ihrem Risiko (unzulässiges, hohes, begrenztes und minimales Risiko), spezifische Anforderungen für Hochrisiko-Systeme, Transparenz- und Sicherheitsanforderungen sowie die Einrichtung eines EU-weiten Überwachungssystems für KI-Anwendungen. Einen tieferen Einblick in das Thema Risikoklassifizierung und Risikostufen finden Sie in den Kapiteln 02 und 03. Diese Maßnahmen zielen darauf ab, die Sicherheit, Transparenz und Verantwortung im Umgang mit KI zu gewährleisten und gleichzeitig Innovationen zu fördern. Darüber hinaus bilden sie eine feste rechtliche Grundlage, die Unternehmen, Forschung und Endnutzer:innen befähigt, rechtssicher mit KI umzugehen.

Anwendungsbereich und betroffene Systeme

Der Act findet Anwendung bei verschiedenen KI-Systemen, abhängig von ihrem Risiko. Hochrisiko-Systeme umfassen beispielsweise KI-Anwendungen in kritischen Infrastrukturen, wie etwa KI-gesteuerte Systeme im Gesundheitswesen. Ein konkretes Beispiel wäre ein KI-gestütztes Diagnosetool in Krankenhäusern, das strengen Auflagen hinsichtlich Datenqualität, Transparenz und menschlicher Aufsicht unterliegt. Niedrigrisiko-Systeme, wie etwa Chatbots oder KI-basierte Spiele, unterliegen weniger strengen Regelungen, müssen aber dennoch gewisse Transparenzanforderungen erfüllen.

Relevante Beteiligte

Alle Anbieter:innen und Nutzer:innen von KI-Systemen innerhalb der EU müssen sich mit den Anforderungen des Acts auseinandersetzen. Dies umfasst Entwickler:innen, Anbieter:innen und Anwender:innen von KI-Technologien. Privatpersonen, die KI-Anwendungen wie ChatGPT nutzen, sind in der Regel nicht direkt betroffen, solange sie diese nur als Endnutzer:innen einsetzen und die Anwendungen den regulatorischen Anforderungen entsprechen. Unternehmen, die solche Technologien entwickeln oder bereitstellen, müssen hingegen sicherstellen, dass ihre Produkte konform sind.

Sanktionen bei Verstößen

Bei Verstößen gegen den EU AI Act drohen erhebliche Sanktionen. Die vorgeschlagenen Strafen umfassen Bußgelder von bis zu 35 Millionen Euro oder 7% des weltweiten Jahresumsatzes. Die faktische Umsetzung des EU AI Acts in den Mitgliedstaaten erfordert umfassende Maßnahmen zur Einhaltung der neuen Vorschriften, die eine sichere und transparente Nutzung von KI sicherstellen sollen.

4. Fazit

Zusammenfassend lässt sich sagen, dass der EU AI Act ein umfassendes und wegweisendes Regelwerk darstellt, das den Einsatz von KI in der EU regulieren soll. Er kategorisiert KI-Systeme nach ihrem Risikoniveau und legt spezifische Anforderungen für Hochrisiko-Systeme fest, um Sicherheit, Transparenz und Verantwortlichkeit zu gewährleisten. Der Act betrifft eine Vielzahl von KI-Anwendungen, von Gesundheitsdiagnosetools bis hin zu Chatbots, und erfordert von Anbieter:innen und Nutzer:innen die Einhaltung strenger Vorgaben. Bei Verstößen drohen erhebliche Sanktionen, einschließlich hoher Bußgelder. In den nächsten Kapiteln werden wir uns detailliert mit den Risikostufen und der Klassifizierung von KI-Systemen befassen, um ein tieferes Verständnis für die Implementierung und Einhaltung des EU AI Acts zu entwickeln.

Risikostufen - Anwendungsbei- spiele

Kursübersicht > EU AI Act

Hier werden mögliche Anwendungen beispielhaft betrachtet und welche Auswirkungen der EU AI Act auf diese hat.

1. Einteilung in Risikostufen anhand Anwendungsbeispielen

Nachdem wir zuvor einen groben Überblick über die Entwicklung und die wichtigsten Aspekte des EU AI Acts gegeben haben, möchten wir nun einen genaueren Blick auf das Herzstück des EU AI Acts werfen: die Einteilung der Risikostufen. In diesem Abschnitt wird erläutert, welche Risikostufen es gibt, welche Systeme in welche Kategorie fallen und welche Anforderungen daraus für Organisationen entstehen. Sobald Sie ein grundlegendes Verständnis der Risikostufen erlangt haben, werden wir im zweiten Schritt zwei praktische Beispiele für die Einordnung von Systemen in die verschiedenen Risikostufen betrachten und Ihnen ein Tool vorstellen, das Sie selbst zur Einstufung nutzen können.

2. Die Beispiele

Nachdem Sie sich nun mit den Grundlagen der Risikostufen vertraut machen konnten, können wir uns nun den Beispielen zuwenden, die praktischen Herausforderungen besser illustrieren.

Beispiel 1 - Antrags Assistent

Stellen Sie sich vor, Sie sind Teil einer kleinen in Berlin ansässigen Organisation, die es sich zum Ziel gesetzt hat Personen aus benachteiligten Gruppen bei der Kommunikation mit Behörden zu unterstützen, bspw. durch Hilfe beim Schreiben von Briefen oder Anträgen, kleiner Übersetzungsleistungen o.Ä.. Um Ihre Prozesse zu optimieren haben Sie vor ein Unterstützungstool einzukaufen, dass die Unterlagenprüfung für Sie übernimmt. Personen, die zu Ihnen kommen können dort ihre Dokumente digital hinterlegen, diese werden dann vom Antrags Assistenten geprüft, der Ihnen und ihren Kolleg:innen eine Auskunft darüber gibt, wie das System die Chancen auf Erfolg bei Antragsstellung bewertet. Das System kann keine Personen ablehnen und keine eigenständigen Entscheidungen treffen.

Was glauben Sie? Nehmen Sie sich einen Moment Zeit und denken Sie darüber nach wo ein solches System eingeordnet werden könnte. Wir fassen die wichtigsten Informationen hier noch mal zusammen, dabei spielen nicht nur die Dinge eine Rolle, die das System tut, sondern explizit auch was es nicht tut oder kann.

Übersicht Beispielsystem 1 - Antrags Assistent

- Unsere Organisation setzt das System nur ein.
- Wir sind mit unserem Standort in Berlin innerhalb der EU niedergelassen.
- Wir nutzen das System weder für militärische Zwecke, noch sind wir Teil einer Behörde oder Forschungseinrichtung.
- Das System wird nicht für Dinge wie Social Scoring, Emotionserkennung oder Verhaltensmanipulation genutzt.
- Da es sich um ein System handelt, dass potenziell den Zugang zu privaten und öffentlichen Leistungen beeinflusst, könnte dies besondere Auswirkungen auf die Einstufung unseres Tools haben. Wichtig ist dabei vor allem, dass kein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte einer Person darstellt.

Prüfen wir basierend auf diesen Informationen unser Assistenzsystem so bedeutet das, dass die Anwendung mit hoher Wahrscheinlichkeit der niedrigsten Risikostufe zugeordnet wird. Für Sie als Nutzende heißt das, dass Sie das System wie geplant nutzen können. Auf Anbieterseite ist dies allerdings mit einigen Pflichten verbunden. So muss das System in einer EU-Datenbank registriert werden und die getätigten Anfragen müssen beim Anbieter so gesichert werden, dass dieser Sie auf Anfrage der EU-Behörden übertragen kann.

Beispiel 2

Für unser zweites Beispiel stellen wir uns vor wir sind Teil einer in den USA und Europa agierenden auf Nachhaltigkeit und Tierwohl ausgerichtete Organisation, die in Kooperation mit einer ländlichen Kommune die Population in einem Waldstück überwachen und messen möchte. Um ein möglichst detailliertes Bild zu bekommen, sendet Ihnen ihre Hauptstelle in den Staaten durch KI-Erkennungssystem gesteuerte Kameras, die im Waldstück angebracht werden und automatisch Tiere bedrohter Arten identifizieren und die gemachten Bilder speichern sollen. Bei der genutzten Tiererkennungssoftware handelt es sich um eine etablierte Anwendung eines großen Technologiehauses, die in Kooperation mit ihrer Hauptstelle entwickelt und in den USA schon weitläufig mit Erfolg eingesetzt wird. Aufgrund der Serverinfrastruktur, auf die das System zurückgreift werden Daten, die in Deutschland aufgenommen werden in der Hauptstelle in den USA verarbeitet und aufgenommen.

Nehmen Sie sich auch hier wieder einen Moment Zeit und denken Sie darüber nach welcher Risikostufe so ein System zugeordnet werden könnte. Hier noch einmal die wichtigsten Informationen:

Übersicht Beispielsystem 2

- Das System wird von unserer Organisation hergestellt und eingesetzt.
- Wir sind eine amerikanische Organisation mit einem Standort in Deutschland.
- Wir nutzen das System weder für militärische Zwecke, noch sind wir Teil einer Behörde oder Forschungseinrichtung.
- Das System wird nicht für Dinge wie Social Scoring, Emotionserkennung oder Verhaltensmanipulation genutzt.
- Das System wird nicht in einem Hochrisikobereich eingesetzt bspw. bei der Strafverfolgung oder zum Grenzkontrollmanagement.

Prüfen wir basierend auf diesen Informationen unser Assistenzsystem so bedeutet das, dass auch diese Anwendung mit hoher Wahrscheinlichkeit der niedrigsten Risikostufe zugeordnet wird. Trotz der Verarbeitung der Daten im Nicht-Eu-Ausland und dem Einsatzgebiet bei der Überwachung handelt es sich mit hoher Wahrscheinlichkeit um ein System, dass auf Nutzendenseite keine weiteren Pflichten mit sich bringt. Unsere Dachorganisation bzw. der Technologiekonzern unterliegen dabei trotz ihres Standortes in den USA den gleichen Transparenzpflichten wie in Beispiel 1, wenn sie ihr System innerhalb der EU einsetzen wollen.

Die genaue Einschätzung in welche Risikostufe ein gegebenes KI-System fällt, kann durchaus komplex sein und hängt von mehr Faktoren ab als wofür es inhaltlich genutzt wird bspw. ob ich als Hersteller und Nutzender auftrete. Wo ich das System einsetzen will? Ob ich Teil der EU bin etc.

3. EU AI Act Compliance Checker

Um sich einen Überblick über die verschiedenen Möglichkeiten zu verschaffen, gibt es den EU-Compliance-Checker. Das Tool bietet die Möglichkeit verschiedene Varianten durchzuspielen, um herauszufinden welche Regelungen für das eigene System gelten. Wir empfehlen daher es einmal selbst auszuprobieren und die oben genannten Beispiele oder eigene Idee einfach mal auf <https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/> oder mit einem Klick auf die unten befindliche Einbindung zu testen.

EU AI Act Compliance Checker

Das EU-Gesetz über künstliche Intelligenz führt neue Verpflichtungen für Unternehmen innerhalb und außerhalb der EU ein. Nutzen Sie unser interaktives Tool, um festzustellen, ob Ihr KI-System davon betroffen ist oder nicht.

Wenn Sie über Ihre Verpflichtungen im Rahmen des EU AI Act auf dem Laufenden bleiben möchten, empfehlen wir Ihnen, den EU AI Act Newsletter zu abonnieren.

Um mehr Klarheit zu schaffen, empfehlen wir Ihnen, sich rechtlich beraten zu lassen und die nationalen Richtlinien zu befolgen. Weitere Informationen über die Durchsetzung des EU-AI-Gesetzes in Ihrem Land werden voraussichtlich im Jahr 2024 zur Verfügung gestellt.

Feedback - Wir arbeiten an der Verbesserung dieses Tools. Bitte senden Sie Ihr Feedback an Taylor Jones unter taylor@futureoffice.org

Sehen Sie sich den offiziellen Text an, oder durchsuchen Sie ihn online mit unserem AI Act Explorer. Der in diesem Tool verwendete Text ist das "Gesetz über künstliche Intelligenz (Verordnung (EU) 2024/1689, Fassung des Amtsblatts vom 13. Juni 2024". Interinstitutionelle Akte: 2021/0106(COD)

Wie wirkt sich das EU-KI-Gesetz auf mein KI-System aus?
Bitte füllen Sie dieses Formular für jedes einzelne in Ihrer Organisation verwendete AI-System aus.

Ist mein System ein "KI-System" im Sinne des EU-KI-Gesetzes?

Ein System der künstlichen Intelligenz (KI-System) ist definiert als: Ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können.

Quelle: Artikel 3, Punkt 1

Entitätstyp
Welche Art von Einrichtung ist Ihre Organisation?

Hinweis: Wenn Sie die Definition mehrerer Entitätstypen erfüllen, müssen Sie das Formular mehrfach ausfüllen, einmal für jeden Entitätstyp.

Anbieter
 Einsetzer
 Verteiler
 Importeur
 Hersteller des Produkts
 Bevollmächtigter

Siehe Definitionen
Definitionen für diese Begriffe anzeigen.

Quelle: Artikel 3 Nummern 2-8, Erwägungsgrund 87

Im nächsten Abschnitt gehen wir dann noch mal konkret auf die Auswirkungen der Risikostufen auf mögliche Entwicklungsprozesse ein.

Risikostufen - Auswirkungen

Kursübersicht > EU AI Act

In diesem Kapitel werden einzelne Artikel des Acts näher betrachtet und welche Auswirkungen sie auf verschiedene System haben können.

1. Was muss je nach Risikostufe beachtet werden?

Dieser Text zielt darauf ab, ein tieferes Verständnis der verschiedenen Risikokategorien zu vermitteln, die in der KI-Verordnung (KIVO) definiert sind, die Anforderungen für jede Kategorie zu erläutern, mit besonderem Fokus auf Hochrisiko-KI-Systeme, und das Konzept eines KI-Managementsystems gemäß der KIVO und DIN 42001:2023 zu erklären.

Risikostufen im AI-Gesetz

Das AI-Gesetz klassifiziert KI-Systeme in mehrere Risikostufen, von denen jede spezifische Anforderungen zur Gewährleistung von Sicherheit, Transparenz und Compliance hat. Diese Kategorien sind darauf

ausgelegt, öffentliche Interessen wie Gesundheit, Sicherheit und grundlegende Rechte zu schützen und gleichzeitig Innovation zu fördern. Zur Einstufung finden sich mehr Infos unter X.

Verbotene KI-Praktiken

Die KIVO identifiziert bestimmte KI-Praktiken, die als untragbare Risiken angesehen werden und daher vollständig verboten sind. Diese Praktiken stehen in grundlegendem Widerspruch zu den in der EU-Gesetzgebung verankerten Werten und Rechten. Beispielsweise sind KI-Systeme, die darauf abzielen, menschliches Verhalten in einer Weise zu manipulieren, die Schaden verursacht, streng verboten. Dies könnte Nudging-Techniken umfassen, die Personen ohne deren bewusste Wahrnehmung beeinflussen sollen. Darüber hinaus sind Systeme, die eine soziale Bewertung durch Regierungen ermöglichen und zu ungerechter oder diskriminierender Behandlung basierend auf sozialem Verhalten oder Merkmalen führen, nicht erlaubt. Auch die Nutzung von KI-Systemen zur biometrischen Erkennung in öffentlichen Räumen durch Strafverfolgungsbehörden ist weitestgehend verboten.

Was ist zu tun? In Fällen, in denen KI-Systeme als verboten gelten, ist die sofortige Einstellung jeglicher laufender Nutzung erforderlich. Rechtliche Durchsetzungsmaßnahmen müssen ergriffen werden, um sicherzustellen, dass diese Systeme weder entwickelt noch innerhalb der Europäischen Union eingesetzt werden.

Hochrisiko-KI-Systeme

Hochrisiko-KI-Systeme sind solche, die erhebliche Risiken für Gesundheit, Sicherheit und grundlegende Rechte darstellen. Diese Systeme unterliegen strengen regulatorischen Anforderungen, um sicherzustellen, dass sie sicher und ethisch betrieben werden (wird auch im vorherigen Abschnitt erklärt). Beispiele für Hochrisiko-KI-Systeme sind solche, die in kritischen Infrastrukturen verwendet werden, wie etwa KI-Systeme zur Verwaltung von essenziellen Dienstleistungen wie Wasser, Energie und Transport. Im Bereich Bildung und berufliche Ausbildung bestimmen Hochrisiko-KI-Systeme den Zugang zu Bildungs- und Ausbildungsmöglichkeiten und beeinflussen damit wesentliche Lebensentscheidungen für Einzelpersonen. Ähnlich verhält es sich im Beschäftigungsbereich, wo KI-Systeme in Rekrutierungsprozessen, Leistungsbewertungen und Entscheidungsfindungen als Hochrisiko gelten, da sie tiefgreifende Auswirkungen auf die Lebensgrundlagen der Menschen haben.

Hochrisiko-KI-Systeme erstrecken sich auch auf essenzielle private und öffentliche Dienstleistungen, bei denen sie den Zugang zu Finanzdienstleistungen, Sozialleistungen und Versorgungsleistungen bestimmen. Im Kontext der Strafverfolgung und Migration spielen biometrische Identifikationssysteme und KI-Systeme zur Risikobewertung eine entscheidende Rolle und werden daher als Hochrisiko eingestuft.

Was ist zu tun? Die Anforderungen an Hochrisiko-KI-Systeme sind in den Artikeln 8 bis 15 der KIVO ausführlich dargelegt. Diese Artikel beschreiben die strengen Standards und Prozesse, die eingehalten werden müssen, um sicherzustellen, dass die Systeme verantwortungsbewusst entwickelt, eingesetzt und betrieben werden.

Artikel 8

Gemäß Artikel 8 müssen Hochrisiko-KI-Systeme strengen Standards entsprechen, die den beabsichtigten Zweck des Systems und den Stand der Technik berücksichtigen. Die Einhaltung umfasst umfassende Tests, Dokumentations- und Überwachungsprozesse, um sicherzustellen, dass das System sicher und effektiv ist.

Artikel 9

Artikel 9 schreibt vor, dass Anbieter ein umfassendes Risikomanagementsystem implementieren. Dieses System muss kontinuierlich und iterativ sein, wobei Risiken während des gesamten Lebenszyklus des Systems identifiziert, analysiert, bewertet und gemindert werden. Anbieter müssen gezielte Risikomanagementmaßnahmen ergreifen und umfassende Tests durchführen, um die fortlaufende Einhaltung und Leistung des Systems zu gewährleisten. Darauf wird am Ende dieses Abschnitts nochmal eingegangen.

Artikel 10

Artikel 10 betont die Bedeutung der Datenqualität für Hochrisiko-KI-Systeme. Anbieter müssen Datensätze verwenden, die relevant, repräsentativ, fehlerfrei und vollständig sind. Eine ordnungsgemäße Datenverwaltung ist entscheidend, um die Zuverlässigkeit und Fairness des KI-Systems zu gewährleisten.

Artikel 11

Umfassende technische Dokumentation, wie in Artikel 11 gefordert, ist unerlässlich, um die Einhaltung zu demonstrieren. Dies umfasst detaillierte Informationen zum Design des Systems, zu den Entwicklungsprozessen und zu den durchgeführten Tests, um Transparenz und Verantwortlichkeit zu gewährleisten.

Artikel 12

Artikel 12 beschreibt die Pflichten zur Aufbewahrung von Aufzeichnungen und verlangt, dass Betreiber detaillierte Aufzeichnungen über den Betrieb und die Leistung des Systems führen. Dies ist entscheidend für die Prüfungsfähigkeit und Verantwortlichkeit, um sicherzustellen, dass die Funktion des Systems überprüft werden kann und eventuelle Probleme umgehend behoben werden können.

Artikel 13

Die Transparenz und Bereitstellung von Informationen für Benutzer, wie in Artikel 13 beschrieben, erfordert, dass Benutzer klare und verständliche Informationen über das KI-System erhalten. Dies umfasst detaillierte Nutzungshinweise und Informationen zu den Fähigkeiten und Einschränkungen des Systems, sodass Benutzer fundierte Entscheidungen treffen können. Hier kann auch an der Vereinfachung von z.B. Interfaces gearbeitet werden, um Artikel 13 besser zu erfüllen.

Artikel 14

Artikel 14 unterstreicht die Bedeutung von menschlicher Aufsicht, auch human oversight im Englischen. Eine angemessene menschliche Überwachung stellt sicher, dass die Leistung des KI-Systems kontinuierlich gemonitored wird und dass menschliche Bediener eingreifen können, wenn dies erforderlich ist, um Schäden zu verhindern oder Risiken zu mindern. Diese müssen aber auch angemessen in die Lage versetzt werden, Systeme zu überwachen.

Artikel 15

Schließlich schreibt Artikel 15 vor, dass Hochrisiko-KI-Systeme hohe Genauigkeit, Robustheit und Cybersicherheit gewährleisten müssen. Dies umfasst die Gestaltung des Systems, um genau zu funktionieren, robust gegenüber Fehlern zu sein und gegen Cyber-Bedrohungen geschützt zu sein, um die Integrität und Sicherheit des Systems während seines gesamten Lebenszyklus zu gewährleisten.

Begrenzte Risikostufe

Begrenzte Risikostufe-KI-Systeme unterliegen spezifischen Transparenzverpflichtungen, insbesondere in Situationen, in denen es für Benutzer nicht offensichtlich ist, dass sie mit einem KI-System interagieren. Transparenz ist entscheidend, um sicherzustellen, dass Benutzer sich bewusst sind und fundierte Entscheidungen über ihre Interaktionen mit solchen Systemen treffen können.

Was ist zu tun? Im Kontext von begrenzten Risikostufe-KI-Systemen müssen Anbieter Benutzer klar darüber informieren, wenn sie mit einem KI-System interagieren, es sei denn, dies ist aus dem Kontext offensichtlich. Die Sicherstellung der Transparenz und Erklärbarkeit der Funktionsweise des Systems ist der Schlüssel zum Aufbau von Vertrauen und zur Ermöglichung der Benutzer, das Betrieb und die Entscheidungen des KI-Systems zu verstehen.

Minimale Risikostufe

Minimale Risikostufe-KI-Systeme umfassen Anwendungen wie Spamfilter oder KI-gestützte Videospiele, die nur geringe Risiken für Benutzer darstellen. Diese Systeme erfordern keine zusätzlichen spezifischen Verpflichtungen gemäß der KIVO, müssen jedoch die bestehenden Gesetze und Vorschriften einhalten.

Was ist zu tun? Für minimale Risikostufe-KI-Systeme ist es entscheidend, die allgemeinen gesetzlichen Anforderungen einzuhalten, um sicherzustellen, dass die Systeme im Rahmen der bestehenden Gesetze betrieben werden und keine unangemessenen Risiken für Benutzer darstellen.

3. KI-Managementsystem laut KIVO und DIN 42001:2023

Ein KI-Managementsystem, wie in der KIVO definiert, umfasst umfassende Prozesse und Verfahren, um sicherzustellen, dass KI-Systeme die regulatorischen Anforderungen erfüllen, Risiken managen und hohe Leistungsstandards aufrechterhalten. Dieses System sollte in die allgemeinen Managementprozesse der Organisation integriert werden.

Das KI-Managementsystem muss einen systematischen Ansatz zur Verwaltung aller KI-bezogenen Aktivitäten annehmen, um kontinuierliche Verbesserungen und Aktualisierungen der KI-Prozesse zu gewährleisten und sich an neue Entwicklungen anzupassen, um fortlaufende Compliance sicherzustellen. Es ist entscheidend, Rollen und Verantwortlichkeiten innerhalb der Organisation klar zu definieren, um eine Kultur der Verantwortung und Rechenschaftspflicht zu fördern.

Der DIN 42001:2023-Standard bietet Leitlinien zur Implementierung eines KI-Managementsystems und betont die Notwendigkeit eines systematischen und kontinuierlichen Ansatzes zur Verwaltung von KI-Technologien. Der Fokus liegt darauf, das KI-Managementsystem in die bestehenden Managementprozesse der Organisation zu integrieren, um sicherzustellen, dass KI-Systeme ethisch und verantwortungsvoll entwickelt, eingesetzt und genutzt werden.

Zusammenfassend lässt sich sagen, dass die KIVO einen umfassenden Rahmen für die Entwicklung, den Einsatz und die Nutzung von KI-Systemen schafft, diese in verschiedene Risikostufen einteilt und spezifische Anforderungen für jede Kategorie festlegt. Insbesondere Hochrisiko-KI-Systeme unterliegen strengen regulatorischen Anforderungen, um ihre Sicherheit und ethische Nutzung zu gewährleisten. Durch die Implementierung eines KI-Managementsystems gemäß der KIVO und DIN 42001:2023 können Organisationen effektiv KI-bezogene Aktivitäten verwalten, Compliance sicherstellen, verantwortungsvollen Einsatz fördern und Innovation in KI-Technologien vorantreiben.

High-Level Expert Group

Kursübersicht > EU AI Act

Es wird die HLEG betrachtet, was deren Ziele sind und welchen Einfluss sie haben.

1. Die Rolle der High-Level Expert Group für Trustworthy AI

Die High-Level Expert Group on Artificial Intelligence und ihre Ziele

Die High-Level Expert Group on Artificial Intelligence (HLEG) wurde im Juni 2018 von der Europäischen Kommission ins Leben gerufen. Diese unabhängige Expertengruppe besteht aus einer vielfältigen Auswahl von Fachleuten aus Wissenschaft, Industrie und Zivilgesellschaft. Ihr Hauptziel ist es, die Entwicklung und Implementierung von Künstlicher Intelligenz (KI) in Europa zu fördern und sicherzustellen, dass diese

Technologien im Einklang mit europäischen Werten und Grundrechten stehen (European Commission, 2020a).

Die HLEG verfolgt mehrere wesentliche Ziele. Erstens soll durch die Definition von Anforderungen für vertrauenswürdige KI das Vertrauen in diese Technologien gestärkt werden. Dies ist besonders wichtig, da die Akzeptanz von KI in der Gesellschaft davon abhängt, dass die Menschen den Systemen vertrauen und sich sicher fühlen. Zweitens sollen ethische Prinzipien und Grundrechte geschützt werden. Dies bedeutet, dass KI-Systeme nicht nur technisch einwandfrei sein müssen, sondern auch moralische und ethische Standards einhalten müssen. Drittens soll die technische Exzellenz gefördert werden. KI-Systeme müssen robust und sicher sein, um Risiken und potenzielle Schäden zu minimieren. Viertens soll die Wettbewerbsfähigkeit europäischer Unternehmen gestärkt werden. Durch die Entwicklung innovativer und vertrauenswürdiger KI-Lösungen können sich europäische Unternehmen im globalen Wettbewerb behaupten (European Commission, 2020b).

Ein zentrales Dokument der HLEG sind die „Ethics Guidelines for Trustworthy AI“, die im April 2019 veröffentlicht wurden. Diese Leitlinien definieren, was vertrauenswürdige KI ausmacht und welche Anforderungen an solche Systeme gestellt werden sollten. Vertrauenswürdige KI basiert auf drei Hauptkomponenten: Gesetzeskonformität, Ethik und Robustheit. Gesetzeskonformität bedeutet, dass KI-Systeme alle relevanten Gesetze und Vorschriften einhalten müssen. Ethik umfasst die Respektierung ethischer Prinzipien und Werte, während Robustheit sicherstellt, dass die Systeme technisch und sozial robust sind, um unabsichtliche Schäden zu vermeiden (High-Level Expert Group on Artificial Intelligence, 2019).

2. Die sieben Anforderungen der HLEG

Um diese Ziele zu erreichen, hat die HLEG sieben zentrale Anforderungen definiert:

1. Menschliche Autonomie und Aufsicht

KI-Systeme sollten die Entscheidungsfreiheit und -kompetenz der Menschen unterstützen und nicht untergraben. Dies bedeutet, dass KI als Unterstützung für menschliche Entscheidungen dienen sollte und Mechanismen zur menschlichen Aufsicht und Kontrolle der Systeme implementiert werden müssen. Beispielsweise könnten Systeme entwickelt werden, die klare Hinweise geben, wann eine menschliche Überprüfung erforderlich ist, oder die es den Nutzern ermöglichen, Entscheidungen der KI-Systeme zu hinterfragen und zu überstimmen.

2. Technische Robustheit und Sicherheit

Zuverlässigkeit, Sicherheit und Robustheit der KI-Systeme sind entscheidend, um die Integrität und Vertrauenswürdigkeit der Technologien zu gewährleisten. Technische Robustheit erfordert die Fähigkeit der Systeme, in verschiedenen Situationen und unter unterschiedlichen Bedingungen zuverlässig zu funktionieren. Sicherheit bedeutet, dass Systeme vor Angriffen geschützt und Ausfälle minimiert werden müssen. Dies schließt auch die Notwendigkeit ein, dass KI-Systeme regelmäßig getestet und aktualisiert werden, um sicherzustellen, dass sie sicher und effektiv bleiben (European Commission, 2020a; High-Level Expert Group on Artificial Intelligence, 2019).

3. Privatsphäre und Datenmanagement

Der Schutz der Privatsphäre und eine verantwortungsbewusste Datenverwaltung sind essenziell. KI-Systeme müssen so gestaltet sein, dass sie die Privatsphäre der Nutzer respektieren und schützen. Dies umfasst Maßnahmen zum Datenschutz, zur Qualität und Integrität der Daten sowie zu transparenten Zugriffs- und Verarbeitungsprotokollen. Beispielsweise sollten Daten, die von KI-Systemen gesammelt werden, anonymisiert oder pseudonymisiert werden, um die Privatsphäre der Nutzer zu schützen (European Commission, 2020a).

4. Transparenz

Nachvollziehbarkeit, Erklärbarkeit und klare Kommunikation der KI-Systeme sind entscheidend, um Vertrauen in diese Technologien zu schaffen. Transparenz bedeutet, dass die Entscheidungen und Funktionsweisen der KI-Systeme verständlich und zugänglich erklärt werden müssen. Dies ermöglicht es den Nutzern, die Funktionsweise der Systeme zu verstehen und ihre Entscheidungen zu hinterfragen. Erklärbarkeit bezieht sich darauf, dass die Prozesse, die zu einer bestimmten Entscheidung führen, klar und nachvollziehbar sind (High-Level Expert Group on Artificial Intelligence, 2019).

5. Vielfalt, Nichtdiskriminierung und Fairness

KI-Systeme sollen inklusiv gestaltet sein und dürfen keine diskriminierenden Auswirkungen haben. Dies erfordert die Beseitigung von Verzerrungen in den Daten und Modellen sowie die Berücksichtigung aller Nutzergruppen. Beispielsweise sollten KI-Systeme so entwickelt werden, dass sie alle Nutzer unabhängig von deren ethnischer Herkunft, Geschlecht, Alter oder anderen persönlichen Merkmalen gleich behandeln. Dies könnte durch die Implementierung von Mechanismen zur

Überprüfung und Korrektur von Verzerrungen in den Daten und Algorithmen erreicht werden (European Commission, 2020a).

6. Gesellschaftliches und ökologisches Wohlergehen

Die Auswirkungen von KI auf Gesellschaft und Umwelt müssen berücksichtigt werden. Dazu gehört die Förderung des gesellschaftlichen Wohlergehens und die Minimierung negativer Umweltauswirkungen. KI-Systeme sollten so gestaltet sein, dass sie positive soziale und ökologische Auswirkungen haben. Beispielsweise könnten KI-Systeme entwickelt werden, die Energieeffizienz verbessern oder zur Lösung sozialer Probleme beitragen (High-Level Expert Group on Artificial Intelligence, 2019).

7. Rechenschaftspflicht

Es muss klare Verantwortlichkeiten und Mechanismen zur Überprüfung und Rechenschaftspflicht geben. Dies umfasst die Möglichkeit zur Überprüfung der Systeme durch unabhängige Dritte sowie die Implementierung von Mechanismen zur Korrektur von Fehlern und zur Rechenschaftspflicht derjenigen, die die Systeme entwickeln und einsetzen. Rechenschaftspflicht bedeutet auch, dass klare Verfahren und Standards zur Überprüfung und Bewertung der KI-Systeme etabliert werden müssen (European Commission, 2020a; High-Level Expert Group on Artificial Intelligence, 2019).

3. Unterschiede zwischen dem AI Act und den Anforderungen der HLEG

Die Arbeit der High-Level Expert Group on AI und der EU AI Act stellen wesentliche Schritte dar, um sicherzustellen, dass KI-Systeme im Einklang mit europäischen Werten und Grundrechten entwickelt und eingesetzt werden. Während die HLEG einen breiteren, ethisch orientierten Ansatz verfolgt, legt der EU AI Act einen stärkeren Fokus auf die Regulierung basierend auf dem Risiko, das KI-Systeme darstellen.

Ein wesentlicher Unterschied liegt in der Herangehensweise: Der EU AI Act kategorisiert KI-Systeme basierend auf dem Risiko, das sie darstellen. Es gibt verbotene Praktiken, Hochrisiko-Systeme, Systeme mit eingeschränktem Risiko und Systeme mit minimalem Risiko. Diese risikobasierte Herangehensweise bestimmt, welche Anforderungen an die jeweiligen KI-Systeme gestellt werden. Im Gegensatz dazu definiert die HLEG allgemeine Anforderungen, die für alle KI-Systeme gelten sollten, unabhängig von ihrem spezifischen Risikopotenzial (European Commission, 2020b).

Besonders hervorzuheben sind die Themen Vielfalt und ökologische Wirkung, die von der HLEG stärker betont werden als vom EU AI Act. Die HLEG legt großen Wert auf die Inklusion aller Nutzergruppen und die Vermeidung von Diskriminierung. Dies erfordert Maßnahmen zur Beseitigung von Verzerrungen in den Daten und Modellen sowie die Berücksichtigung aller demografischen Gruppen. Der EU AI Act hingegen fokussiert sich stärker auf rechtliche und technische Anforderungen und behandelt die Vielfalt weniger ausführlich (European Commission, 2020a).

Ebenso legt die HLEG besonderen Wert auf das gesellschaftliche und ökologische Wohlergehen. KI-Systeme sollten nicht nur technisch robust sein, sondern auch positive soziale und ökologische Auswirkungen haben. Dies schließt die Förderung von Energieeffizienz und die Minimierung negativer Umweltauswirkungen ein. Der EU AI Act hingegen betont stärker die Einhaltung rechtlicher Standards und die technische Sicherheit, während die ökologischen Aspekte weniger prominent behandelt werden (High-Level Expert Group on Artificial Intelligence, 2019).

4. Zusammenfassung der Kriterien und Ziele der HLEG

- Menschliche Autonomie und Aufsicht
- Technische Robustheit und Sicherheit
- Privatsphäre und Datenmanagement
- Transparenz
- Vielfalt, Nichtdiskriminierung und Fairness
- Gesellschaftliches und ökologisches Wohlergehen
- Rechenschaftspflicht

Die Arbeit der High-Level Expert Group on AI stellt einen wichtigen Schritt dar, um sicherzustellen, dass KI-Systeme im Einklang mit europäischen Werten und Grundrechten entwickelt und eingesetzt werden. Definierte Kriterien und Leitlinien dienen dabei als Grundlage für die Entwicklung und Implementierung vertrauenswürdiger und ethisch verantwortungsvoller KI-Systeme. Die umfassende Betrachtung technischer, ethischer und sozialer Aspekte trägt dazu bei, dass KI nicht

nur technologisch fortschrittlich, sondern auch sozial und ethisch verantwortungsvoll ist.

06

Quellen

Kursübersicht > [EU AI Act](#)

Literaturverzeichnis

- European Commission. (2020a). *The Ethics Guidelines for Trustworthy AI*. Abgerufen von <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- European Commission. (2020b). *The EU AI Act: Regulatory framework proposal for Artificial Intelligence*. Abgerufen von <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>