EU AI ACT

Start your compliance journey now

[at]

alexanderthamm

01 EINLEITUNG

Was ist der AI-Act und was reguliert er?

Ab wann gilt er?

02 WER IST VOM AI-ACT BETROFFEN?

03 RISIKOEINSTUFUNGEN UND ENTSPRECHENDE VERPFLICHTUNGEN

Verbotene KI-Systeme

Hochriskante KI-Systeme

KI-Systeme mit Transparenzverpflichtungen

KI-Systeme mit allgemeinem Verwendungszweck

Strafen bei Nichteinhaltung

04 GESETZESEINHALTUNG MIT [AT]

Die [at] Data Journey

- Data Strategy
- Data Lab
- Data Factory
- DataOps

Gesetzeseinhaltung mit [at]

05 SCHLUSSWORT

Verbesserungsspielraum

Beginne Deine Data Journey

Über [at]

Kontakt

EINLEITUNG

Kennen Sie die genaue Entscheidungslogik des KI-Systems, das Sie für Ihre Bewerberauswahl nutzen? Wenn Sie diese Frage nun gedanklich mit einem Nein beantwortet haben, sollten Sie unbedingt weiterlesen. Denn der von der Europäischen Union im März verabschiedete AI-Act verpflichtet Sie, relevante technische Dokumentationen bereitzustellen, die Ihre Systeme transparent, erklärbar und nachvollziehbar machen.

Doch ähnlich wie die Einführung der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 schafft auch die Einführung des AI-Acts Unsicherheiten, die die rechtskonforme Einhaltung der neuen Regelungen erschweren. Wie wirken sich die Bestimmungen speziell auf mein Unternehmen aus? Wie kann ich sicherstellen, dass die KI-Systeme, die mein Unternehmen bereits verwendet, gesetzeskonform sind – und was sollte ich bei der Einführung neuer Systeme in Zukunft beachten? In diesem Whitepaper finden Sie Antworten auf die wichtigsten Fragen rund um den AI-Act. Außerdem präsentieren wir den ganzheitlichen Ansatz von [at], mit dem wir Unternehmen dabei unterstützen, die Vorgaben des AI-Acts in der Praxis umzusetzen.

Warum sollten Sie sich jetzt damit beschäftigen? Die frühzeitige Implementierung einer ganzheitlichen Lösung wie die von [at] erleichtert die Einhaltung der Regelungen enorm und wirkt zukünftigen Strafen bei Nichteinhaltung entgegen. Bevor wir ins Detail gehen, ist es jedoch zunächst wichtig, den regulatorischen Ansatz, sowie den beabsichtigten Geltungsbereich des AI-Acts zu verstehen.

Was ist der EU AI Act und was reguliert er?

Der AI-Act wurde von der Europäischen Union erarbeitet und führt eine strenge gesetzliche Aufsicht ein, die Beteiligten am Lebenszyklus eines KI-Systems rechenschaftspflichtig macht – von der Entwicklung und Herstellung bis zur Nutzung und Verteilung eines KI-Systems. Nach drei Jahren intensiver Debatten über den genauen Geltungsbereich und Inhalt, genehmigte das Europäische Parlament den Gesetzesentwurf am 13. März 2024. Der AI-Act verfolgt einen risikobasierten Ansatz zur Klassifizierung und Regulierung von KI-Systemen und ist die erste Verordnung, die rechtlich bindende Regeln für öffentliche und private Akteure einführt.

Er ist ein alleinstehendes Gesetz, was bedeutet, dass er keine zusätzlichen nationalen Gesetze benötigt, um in Kraft zu treten. Dies wird das Risiko unterschiedlicher Auslegungen des Gesetzes aufgrund nationaler Unterschiede weitgehend mindern. Die Durchsetzung erfolgt jedoch auf lokaler Ebene und könnte zu Unterschieden führen, wie das Gesetz praktisch in den europäischen Ländern umgesetzt wird. Um die Einhaltung auf europäischer Ebene zu koordinieren, erfordert der AI-Act die Einrichtung verschiedener neuer Überwachungsorgane, wie beispielsweise das KI-Büro.

Ab wann gilt er?

Der AI-Act wird schrittweise über einen Zeitraum von drei Jahren in Kraft treten, beginnend 20 Tage nach seiner Veröffentlichung im Amtsblatt der Europäischen Union. Dies ist zwischen Mai und Juli 2024 geplant.between May and July 2024.

WER IST VOM AI-ACT BETROFFEN?

Die Bestimmungen betreffen hauptsächlich kleine und mittelständische Unternehmen (KMUs), die entweder Anbieter (z. B. der Entwickler eines Anwendungsscreening-Tools) oder Betreiber (z.B. ein Versicherungsunternehmen, das dieses Tool kauft und nutzt) von KI-Systemen innerhalb und außerhalb der EU sind. Unternehmen außerhalb der EU sind betroffen, wenn sie ein KI-System auf dem Unionsmarkt platzieren und dessen Nutzung sich direkt auf Personen innerhalb der EU auswirkt. Darüber hinaus gelten einige Regeln für Vertreiber und Importeure, die daran beteiligt sind, ein KI-System auf dem Unionsmarkt bereitzustellen.
Um missverständliche Interpretationen in Bezug auf KI-Systeme zu vermeiden, enthält der AI-Act eine entsprechende Definition, die alle KI-Systeme innerhalb ihres Geltungsbereichs identifiziert. Gemäß dieser Definition handelt es sich bei einem KI-System um ein „maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und [...] aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebung beeinflussen können“ (Artikel 3 Absatz 1). Diese Definition umfasst eine breite Auswahl an KI-Systemen, von Spamfiltern und Chatbots bis hin zu biometrischer Identifikation und Systemen, die zur Filterung von Bewerbungen genutzt werden. Je nach Art des KI-Systems und seinem angenommenen Risiko gelten unterschiedliche Verpflichtungen.

RISIKOEINSTUFUNGEN UND ENTSPRECHENDE VERPFLICHTUNGEN

Der AI-Act versteht unter Risiko „die Kombination aus der Wahrscheinlichkeit des Eintritts eines Schadens und der Schwere dieses Schadens“ (Artikel 3, 1a). Das bedeutet also, dass KI-Systeme je nach dem Grad und der Schwere des (potenziellen) Risikos für Gesundheit, Sicherheit und grundlegende Menschenrechte reguliert werden. Die Einschätzung des jeweiligen Risikos basiert auf drei Variablen: Erstens, ob das System auf regulierten Modellen basiert (z.B. GPAI). Zweitens, ob die beabsichtigte Anwendung reguliert ist, und Drittens, welche Rolle das Unternehmen spielt (Anbieter oder Betreiber). Daraus ergeben sich die folgenden Risikoeinstufungen und entsprechende Verpflichtungen:

Verbotene KI-Systeme

Artikel 5 des AI-Acts verbietet das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Praktiken, dessen Risiken als inakzeptable eingestuft werden.
Das betrifft unter, anderem Anwendungen, die:

- unterschwellige oder absichtlich manipulative oder täuschende Techniken einsetzen, die sich dem Bewusstsein einer Person entziehen, und somit ihre Fähigkeit zur informierten Entscheidungsfindung beeinträchtigt wird.
- biometrische Kategorisierungssystemen und / oder biometrische Echtzeit-Fernidentifizierungssysteme verwenden.
- Personen auf der Basis ihres sozialen Verhaltens oder ihrer Persönlichkeitsmerkmale bewerten oder klassifizieren.
- KI für Profiling, wie z. B. vorhersagende Polizeiarbeit, verwenden.
- Datenbanken zur Gesichtserkennung erstellen.
- Schlussfolgerungen über die Emotionen einer Person am Arbeitsplatz und in Bildungseinrichtungen ziehen.

Hochriskante KI-Systeme

Gemäß der Annexes I und III der des AI-Acts sind bestimmte KI-Systeme als hochriskant zu klassifizieren. Das sind insbesondere solche, die für die biometrische Identifikation, kritische Infrastrukturen, Bildung, Beschäftigung, private und öffentliche Dienstleistungen, Strafverfolgung, Migrations- und Grenzkontrolle sowie Verwaltung der Justiz und demokratische Prozesse verwendet werden. Ein KI-System gilt dann als hochriskant, wenn es Individuen klassifiziert, z. B. durch automatisierte Verarbeitung personenbezogener Daten, um verschiedene Aspekte des Lebens einer Person zu bewerten, wie Arbeitsleistung, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Standort oder Bewegung. Wichtig dabei ist, dass sich die Bestimmungen für hochriskante KI-Systeme in technische Anforderungen, die die Architektur und Funktionsweise des Systems betreffen, und organisatorische Verpflichtungen unterteilt sind, die die Mechanismen und Prozesse innerhalb eines Unternehmens rund um das KI-System betreffen und somit die Verwaltung der technischen Details des Systems ermöglichen.

TECHNISCHE ANFORDERUNGEN AN HOCHRISIKANTE KI-SYSTEME

ANBIETER	BETREIBER
Risikomanagementsystem: Entlang des gesamten KI-Lebenszyklus, muss die Identifizierung, Analyse du Milderung von Risiken gewährleistet sein	
Daten- und Daten Governance: Die Entwicklung von Hochrisiko KI-Systemen muss spezifischen Datenqualitätskriterien und Data-Governance Maßnahmen entsprechen	
Technische Dokumentation	
Aufzeichnungspflicht: In dem KI-System muss eine automatische Protokollierung der Systemergebnisse gewährleistet sein	
Transparenz und Bereitstellung von Informationen für Betreiber: Ergebnisse des KI-Systems müssen vom Betreiber verwendet und interpretiert werden können	
Menschliche Aufsicht: Während des gesamten Lebenszyklus müssen natürliche Personen das System beaufsichtigen	
Genauigkeit, Robustheit, Cybersicherheit: KI-Systeme müssen ihre Zuverlässigkeit, Genauigkeit und Widerstandsfähigkeit gegen Cyberangriffe nachweisen können	

DIE WICHTIGSTEN ORGANISATORISCHEN VERPFLICHTUNGEN FÜR ANBIETER UND BETREIBER VON HOCHRISKANTEN KI-SYSTEMEN

ANBIETER	BETREIBER
Sicherstellen, dass alle technischen Anforderungen erfüllt sind	Betrieb überwachen gemäß der vom Anbieter bereitgestellten Gebrauchsanweisung
Qualitätsmanagement-System	Menschliche Aufsicht übertragen an natürliche Personen, die über die erforderliche Kompetenz verfügen
Technische Dokumentationen für mindestens 10 Jahre aufbewahren	Sicherstellen, dass die Eingabedaten der Zweckbestimmung des Hochrisikosystems entsprechen
Protokolle für mindestens sechs Monate aufbewahren	Protokolle für mindestens sechs Monate aufbewahren
Konformitätsbewertungsverfahren vor Marketlaunch sicherstellen	Durchführung einer Datenschutz-Folgenabschätzung
Ausstellung einer EU-Konformitätserklärung	Natürliche Personen darüber informieren, dass sie Gegenstand des Einsatzes des Hochrisikosystems sind
Anbringen einer CE-Kennzeichnung	Grundrechtfolgenabschätzung für Hochrisikosysteme (*gilt nur für KI-Anwendungen im öffentlichen Dienst)
Registrierungspflicht in der EU-Datenbank Eingreifen in den Betrieb fehlerhafter Systeme	

RISIKOEINSTUFUNGEN UND ENTSPRECHENDE VERPFLICHTUNGEN

KI-Systeme mit Transparenzverpflichtungen

In diese Kategorie fallen die meisten KI-Anwendungen, die derzeit im EU-Binnenmarkt im Umlauf sind. Beispiele für solche KI-Systeme sind Systeme mit einem Risiko für Manipulation oder Täuschung, wie Chatbots oder Deepfake-Generatoren. Weitere Beispiele sind KI-gesteuerte Videospiele oder Spamfilter. Obwohl sie minimalen regulatorischen Verpflichtungen unterliegen, unterliegen sie strikten Transparenzverpflichtungen. Entsprechend müssen Anbieter und Betreiber sicherstellen, dass Endnutzer darüber informiert werden, wenn sie mit KI und KI-generiertem Output interagieren. Darüber hinaus müssen alle von KI generierten Texte, Videos, Audios und Bilder als solche gekennzeichnet werden. Zusätzliche Transparenzverpflichtungen gelten übrigens auch unabhängig davon, ob ein KI-System ein Hochrisikosystem ist oder nicht.

KI-Systeme mit allgemeinem Verwendungszweck

KI-Systeme mit allgemeinem Verwendungszweck (General-Purpose AI, GPAI) haben einen besonderen Stellenwert im AI-Act. Grundsätzlich sind Anbieter von open-source GPAI Systemen von strengeren Verpflichtungen befreit, bleiben jedoch bestimmten Transparenz- und Risikomanagementbestimmungen unterworfen. Striktere Regeln gelten erst für diejenigen GPAI-Systeme, dessen Nutzung als systemisches Risiko eingestuft werden. Gemäß des AI-Acts sind GPAI-Systeme mit systemischem Risiko solche, dessen Rechenleistung größer als 10^25 FLOPs sind (floating-point operations, ungefähr äquivalent zur Gesamtzahl der Berechnungsschritte, die zur Ausführung einer Aufgabe erforderlich sind). Tatsächlich überschreiten derzeit nur wenige vorhandene KI-Systeme diese Schwelle – darunter OpenAI‘s GPT-4 und Google DeepMind‘s Gemini. Anbieter von GPAI mit systemischem Risiko müssen zusätzliche Cybersicherheitsvorkehrungen implementieren, Modellbewertungen und Angriffstests durchführen, Risiken bewerten und mindern sowie schwerwiegende Vorfälle dokumentieren und melden. Die festgelegte Schwelle von 10^25 FLOPs wird in Zukunft angesichts technologischer Fortschritte sehr wahrscheinlich aktualisiert werden.

Strafen bei Nichteinhaltung

Bei Nichteinhaltung oder Verstoß gegen die Bestimmungen des AI-Acts drohen finanzielle Strafen:

Verstoß gegen Verbote → Bis zu 35 Mio. € oder 7% des weltweiten Gesamtjahresumsatzes des vorherigen Geschäftsjahres.

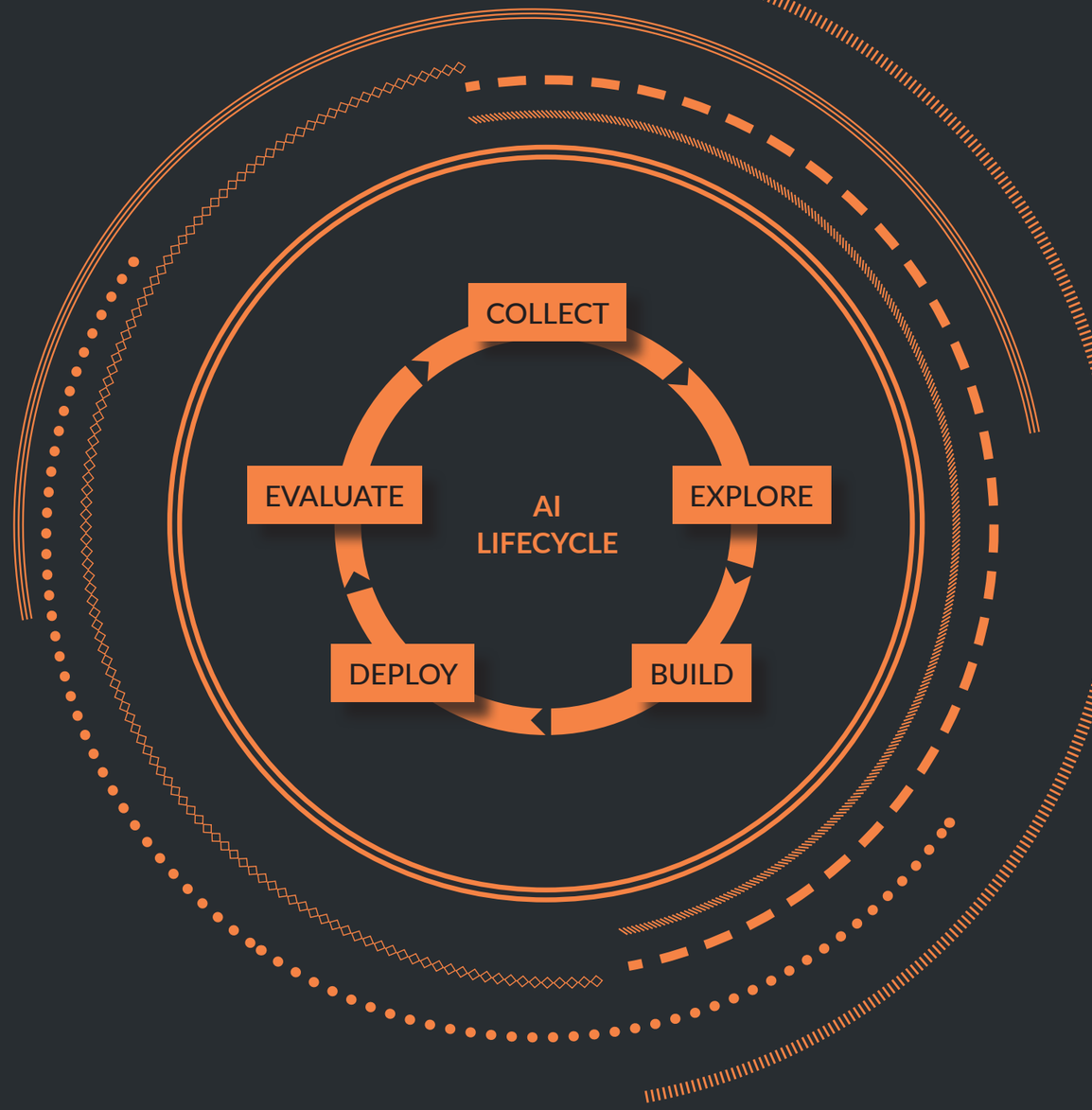
Nichteinhaltung anderer Verpflichtungen, einschließlich derjenigen für GPAI → Bis zu 15 Mio. € oder 3% des weltweiten Gesamtjahresumsatzes des vorherigen Geschäftsjahres.

Bereitstellung falscher, unvollständiger oder irreführender Informationen auf Anfrage einer nationalen Behörde → Bis zu 7,5 Mio. € oder 1,5% des weltweiten Gesamtjahresumsatzes des vorherigen Geschäftsjahres.

GESETZESEINHALTUNG MIT [at]

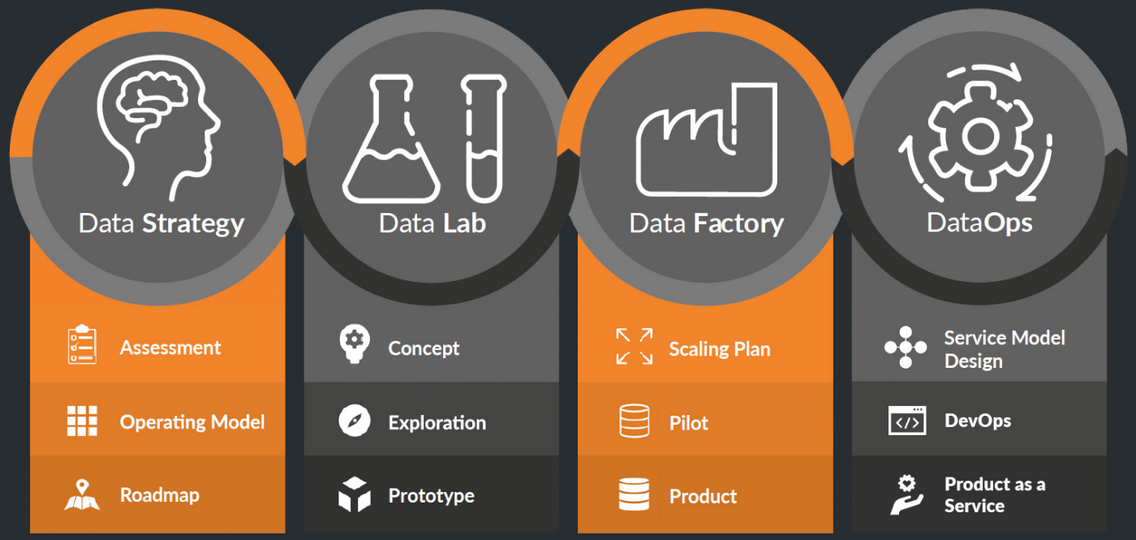
Die technischen Anforderungen an hochriskante KI-Systeme und die damit verbundenen organisatorischen Verpflichtungen sind bereits etablierte Branchenstandards und somit nichts Neues. Der AI-Act bringt diese Branchenstandards lediglich in einen umfassenden rechtlichen Rahmen. „Idealerweise haben Sie bereits Prozesse implementiert, die die Genauigkeit und Robustheit Ihrer Systeme, die technische Dokumentation und Protokollierungsfunktionen sicherstellen. Sind diese Funktionen jedoch fehlerhaft integriert, ist es teilweise sogar unmöglich, die Architektur des betroffenen KI-Systems entsprechend zu korrigieren und die Anforderungen des AI-Acts zu erfüllen – zum Beispiel, wenn aufgrund fehlender Dokumentation unklar ist, welche Daten für das Training des Systems verwendet wurden. Daher empfehle ich Kunden immer, die Themen AI-Governance und Konformität früh zu priorisieren, um so das Risiko zu minimieren, das System in Zukunft nicht mehr verwenden zu können“, erklärt Patrick Zimmermann, Principal Data & AI Project Lead bei [at].

Aus diesem Gedanken heraus haben wir ein ganzheitliches System für Daten- und KI-Projekte entwickelt – die [at] Data Journey. Von der Konzeption über das Design und die Entwicklung bis hin zur Implementierung und Wartung von KI-Systemen unterstützt unsere Data Journey Ihr Datenprojekt und berücksichtigt dabei die Gesetzeskonformität in jeder Phase. Wie die folgende Abbildung zeigt, umfassen die Bestimmungen des AI-Acts umfassen den gesamten KI-Lebenszyklus, wie er von unserer Data Journey abdeckt wird. Folglich sind viele der technischen und organisatorischen Anforderungen des AI-Acts in unserer Data Journey verankert und werden automatisch mit unserem AI-Governance-Framework erfüllt.



- Risk Management System
- Data & AI Governance
- Technical Documentation
- Accuracy, Robustness & Cybersecurity
- Record Keeping
- Transparency
- Human Oversight

GESETZESEINHALTUNG MIT [at]



Unsere Data Journey umfasst vier zusammenhängende Bereiche – Data Strategy, Data Lab, Data Factory, DataOps. Dieser ganzheitliche Ansatz für die Planung und Umsetzung von Datenprojekten ermöglicht es uns, einen kontinuierlichen Überblick über modernste Technologien und Trends zu behalten.

Darüber hinaus bietet diese Struktur unseren Kunden Zugang zu einem qualifizierten Expertenteam, das verschiedene Probleme in jedem Stadium der Reise ansprechen und unterstützen kann. So können wir echten Mehrwehrt aus Daten generieren.

Data Strategy

„Der Fokus der Data Strategy liegt darauf, einen Plan zu erstellen, der den nachfolgenden Prozess der Konzeption, Entwicklung und Implementierung eines Datenprojekts ganzheitlich leitet“, beschreibt Patrick Zimmermann. Unsere Experten in der Data Stratgey unterstützen unsere Kunden dabei, zu definieren, wie bestimmte Datenbestände einen Mehrwert für eine Organisation bieten können. Dies legt den Grundstein und die langfristige Vision für ein Datenprojekt fest. Gemeinsam mit unserem Kunden führen wir eine erste Bewertung ihres Status quo durch, um ihren aktuellen (Daten-)Servicereifegrad zu identifizieren. Anschließend entwickeln und stellen wir einen Fahrplan für jeden individuellen Anwendungsfall vor.

GESETZESEINHALTUNG MIT [at]

Data Lab

Nach der Identifizierung eines strategischen Fahrplans zur Umsetzung eines Anwendungsfalls konzentriert sich unser Data Lab darauf, eine technische Lösung für diesen Anwendungsfall zu testen und einen Prototyp zu bauen. Zunächst erstellen wir ein Konzept für den Anwendungsfall, in dem wir Hypothesen für den Anwendungsfall generieren und die erforderlichen Daten identifizieren und testen. In einer anschließenden Explorationsphase führen wir ein Proof-of-Concept durch und richten eine Testumgebung ein. Dies ist entscheidend, um die Machbarkeit des Anwendungsfalls zu bewerten, aufgrund derer der erste Prototyp entwickelt wird. Ein großer Teil der Arbeit des Lab-Tracks konzentriert sich auf die Integration von Erklärbarer KI (Explainable AI, XAI) in den Entwicklungslebenszyklus von KI-basierten Lösungen. „XAI ist eine Reihe von Prozessen und Methoden, die die Entscheidungen und Funktionsweisen von KI-Systemen für verschiedene Interessengruppen verständlich machen, vor allem für Anbieter, Behörden und letztendlich Endbenutzer. Daher ist ihre Einbettung in den Entwicklungslebenszyklus eine wesentliche Konvergenz, die sicherstellt, dass das System zugänglich, verantwortlich und überprüfbar ist“, erklärt Dina Krayzler, Data Scientist bei [at]. Letzteres ist besonders wichtig im Hinblick auf die regulatorischen Verpflichtungen, denen

Unternehmen gemäß des AI-Acts nachkommen müssen: „Die Berücksichtigung von XAI während des Entwicklungslebenszyklus wird voraussichtlich zu einer Standardpraxis werden. Der AI-Act verlangt ausdrücklich, dass dass Benutzer die Logik hinter ihrem Entscheidungsprozess verstehen können: Insbesondere die Integration automatisierter Aufzeichnungsfunktionen in diese Systeme ist eine spezifische technische Anforderung des AI-Acts, die darauf abzielt, eine solche Transparenz zu etablieren und zu standardisieren“, beschreibt Dina im Weiteren. Daher ist die Berücksichtigung von XAI-Praktiken während des Entwicklungslebenszyklus eine entscheidende Voraussetzung dafür, dass Ihre KI-Lösung mit standardisierten Praktiken übereinstimmt.

Data Factory

In der Data Factory bauen wir den getesteten Anwendungsfall zu einem fertigen Datenprodukt aus. Der Schwerpunkt liegt hier auf der Skalierung und Mehrwertgenerierung – daher stehen hier der Betreiber und/oder Endnutzer des Datenprodukts im Mittelpunkt. Zunächst entwickeln wir einen umfassenden Skalierungsplan, in dem Merkmale, Märkte und Marken priorisiert werden. Basierend auf den spezifischen Aspekten des Skalierungsplans erstellen wir dann ein Minimal Viable Product (MVP), das durch kontinuierliche Tests im Entwicklungsprozess zu einem marktfähigen Produkt verfeinert werden kann.

DataOps

Die Entwicklung und Inbetriebnahme eines Datenprodukts enden nicht mit seiner erstmaligen Einführung. Es ist die kontinuierliche Optimierung und Verbesserung, die es langfristig wirklich wertvoll und effizient macht. Hier setzt unsere DataOps-Praxis an: Sie gewährleistet die Skalierbarkeit des Produkts und stärkt dessen Leistung, Sicherheit und Robustheit. Dies umfasst unter anderem die Aktualisierung seiner Funktionen und die Sicherstellung, dass das Produkt neuen technischen und regulatorischen Anforderungen entspricht. „DataOps hat daher viele Berührungspunkte mit anderen Disziplinen wie Governance, Sicherheit oder DevOps“, betont Kai Sahling, Principal MLOPs Engineer bei [at]. In Bezug auf Governance fordert der AI-Act, dass beim „Aufbau von KI-basierten Produkten bewährte Verfahren eingehalten werden. Und die bewährten Verfahren, die in der AI-Actfestgelegt sind, stimmen eng mit den besten Praktiken von MLOP und DataOps überein. Daher ist die Einhaltung dieser bewährten Verfahren entscheidend für den Aufbau von KI-Produkten, die mit der AI-Actkonform sind“, so Kai.

AI ACT

GESETZESEINHALTUNG MIT [at]

Obwohl die bevorstehende Übergangsphase zeitlichen Spielraum zur Umsetzung der neuen Bestimmungen lässt, lohnt es sich, jetzt zu handeln. „Für Unternehmen ist es äußerst vorteilhaft, Prozesse von Anfang an zu definieren und durchzusetzen, da ihnen dies die unglaublich mühsame Aufgabe erspart, veraltete oder ineffektive Praktiken später einzufangen“, betont Patrick Zimmermann.

In Zusammenarbeit mit Lausen Rechtsanwälte, unseren rechtlichen Partnern und Spezialisten für KI-Governance und Richtlinien, Datenschutz und Urheberrecht, unterstützen Sie unsere Experten auf Ihrem Weg zur Einhaltung des AI-Acts mit folgenden Dienstleistungen:

Vorbereitung

Einen umfassenden Überblick über alle aktiven KI-Systeme in Ihrem Unternehmen zu gewinnen, ist der erste Schritt zur Einhaltung des AI-Acts. Während dieser ersten Vorbereitungsphase helfen wir Ihnen, ein Inventar Ihrer KI-Systeme zu erstellen und unterstützen Sie dabei, diese zu klassifizieren und die damit verbundenen Risiken zu identifizieren.

Implementierung

Hier geht es darum, die technischen Anforderungen und organisatorischen Verpflichtungen des AI-Acts umzusetzen, um sowohl Ihre Organisation und KI-Systeme auditierbar zu machen. Wie bereits erwähnt, verfügt [at] über umfangreiche Erfahrung bei der Einrichtung relevanter Prozesse und technischer Maßnahmen, wie sie der AI-Act erfordert. Die Beratung zur effektiven Implementierung eines Risikomanagementsystems, technischer Dokumentationen oder Aufzeichnungsfunktionen in KI-Systeme ist seit vielen Jahren ein fester Bestandteil unserer Beratungsdienstleistungen.

Upskill

Neben der Bereitstellung praktischer Anleitung und Beratungsdienste zur Einhaltung des AI-Acts legen wir großen Wert darauf, theoretische Unterstützung anzubieten. Daher haben wir AI-Act-spezifische Bildungs- und Schulungsprogramme entwickelt, in denen unsere Experten Sie durch die Besonderheiten des AI-Acts führen und das Verständnis Ihres Teams für den Gesetzestext stärken. Beispielsweise haben wir Schulungen entwickelt, die gezielt auf die Bedürfnisse und Trends von Unternehmen in verschiedenen Branchen, Führungskräfte oder bestimmte Abteilungen innerhalb von Unternehmen abzielen.

Casebase

De AI-Act ist ein auf Anwendungsfällen basierendes Gesetz. Das bedeutet, dass die Konformitätsanforderungen für jeden implementierten Anwendungsfall in Ihrem Unternehmen variieren. Daher ist es essenziell zu ermitteln, ob und in welchem Umfang sie unter die Bestimmungen des Acts fallen. Dies bildet die Grundlage für anschließende Bemühungen zur Gesetzeseinhaltung, da dies die wesentlichen Einhaltungsverpflichtungen bestimmt, die erfüllt werden müssen, um Anwendungsfälle zu entwickeln, bereitzustellen und zu überwachen. Ein umfassendes Tool zur Verwaltung und Steuerung von KI-Anwendungsfällen ist Casebase, das von der Alexander Thamm GmbH entwickelt wurde und die oben skizzierten Vorbereitungs- und Implementierungsphasen erleichtert.

„Casebase unterstützt jede Phase des KI-Anwendungsfalls-Lebenszyklus – von der ersten Idee bis zur effektiven Implementierung einer KI-Anwendung“, erklärt Lucia Karch, Principal Venture Building & Director of Casebase. Es zeigt den Reifegrad jedes Anwendungsfalls an, gibt Verantwortlichkeiten an und zeigt, welche Technologien und Datenbestände für die einzelnen Anwendungsfälle verwendet werden. „Dies ermöglicht es Ihrem Team, strategisch wertvolle Entscheidungen über Projektinvestitionen in Zeit, Geld und Ressourcen zu treffen“, ergänzt Lucia. Während diese Funktionen notwendig sind, um die Projektladung zu bewältigen, ermöglicht die integrierte Funktion für den KI-Risiko-Check, die jeweilige Risikokategorie gemäß des AI-Acts zu identifizieren. „Um die Risikokategorie zu identifizieren, wird der Benutzer durch einen vereinfachten Fragebogen geführt, der darauf abzielt, die Risikokategorie anhand von vier Leitfragen zu bestimmen: 1) Handelt es sich um ein KI-System?; 2) Welche Marktrolle hat es?; 3) Fällt das KI-System in den Anwendungsbereich der EU-KI-Verordnung?; 4) Welcher Risikokategorie gehört das KI-System an?“, erklärt Lucia weiter. Auf diese Weise ermöglicht es Casebase Ihnen, Daten- und KI-Projekte basierend auf dem Reifegrad jedes Datenprodukts zu bewerten, was wiederum eine solide Grundlage für die effiziente Planung der erforderlichen Maßnahmen zur Einhaltung der AI-Act bietet.

*Bitte beachten Sie, dass der Fragebogen zur Bestimmung der Risikokategorie eines Datenprodukts mit der aktuellen Version des AI-Acts entworfen ist. Er wird kontinuierlich aktualisiert, um etwaige Entwicklungen oder Änderungen im Gesetz widerzuspiegeln.

SCHLUSSWORT

Verbesserungsspielraum

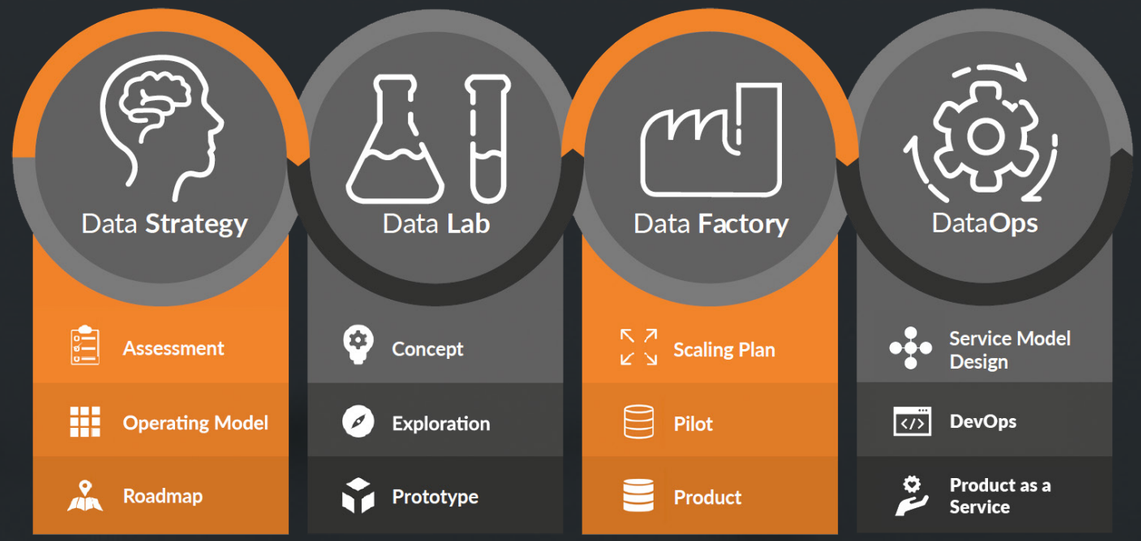
Obwohl der AI-Act ein großer Fortschritt in der KI-Regulierung ist, weist die aktuelle Version noch potenzielle Mängel auf.
Zum einen geriet den vorgeschlagenen Grenzwert für GPAI-Systeme mit systemischem Risiko in Kritik. Wie bereits erwähnt, überschreiten diesen nur wenige vorhandene Modelle. Trotzdem haben andere, kleinere bereits erhebliche Sicherheits- und Cybersicherheitsrisiken bewiesen. Hinzu kommt, dass aktuelle Trends die Entwicklung kleineren, spezialisierteren Modellen mit Rechenleistungen weit unterhalb des vorgeschlagenen Grenzwertes vorsehen, was langfristig in riskanten regulatorischen Schlupflöchern resultieren könnte
Zum anderen könnten die Unklarheit und die mangelnde Spezifität bestimmter Definitionen zu falscher oder fehlerhafter Klassifizierung führen. Zum Beispiel verbietet der AI-Act den Einsatz von KI-Systemen, die durch „unterschwellige Techniken, die sich dem Bewusstsein einer Person entziehen [...], das Verhalten einer Person oder einer Personengruppe wesentlich beeinflussen und [...] erheblichen Schaden zufügt“ (Artikel 5, 1a). Dabei bleibt unklar, wie Manipulation und Schaden definiert sind.

Ähnliche unklare oder mangelnde Definitionen zeigen sich auch hinsichtlich der der Anforderungen an XAI und MLOPs. „Der aktuellen Fassung des Gesetzestextes fehlt es an klaren Definitionen, inwiefern und in welchem Umfang ein KI-System erklärbar sein soll. Das macht es herausfordernd, entsprechende gesetzeskonforme Systeme zu entwickeln. Wir raten daher, bewährte Verfahren und Branchenstandards einzuhalten und auf weitere Vorgaben zu warten“, sagt Dina Krayzler. Ähnliches beobachtet Kai Sahling im Bereich MLOPs: „Was Daten und MLOPs betrifft, so sind die Anforderungen des AI-Acts erforderlichen sehr allgemein gehalten und lassen viel Raum für Interpretation. In den nächsten Jahren müssen sowohl die gesamte Branche als auch verantwortliche Aufsichtsbehörden festlegen, welches Niveau in MLOPs ausreichend ist.“

Tatsächlich ist die Kommission verpflichtet, innerhalb von 12 Monaten nach Inkrafttreten des AI-Acts weitere Richtlinien zu veröffentlichen. Ob diese Richtlinien das Erfüllen und Einhalten des KI-Gesetzes erleichtern, bleibt jedoch abzuwarten.

Starten Sie jetzt Ihre Data Journey!
Trotz ihrer Kritikpunkte ist der AI-Act bereits sehr fortschrittlich und dient für viele Länder als Orientierungspunkt. Daher ist zu erwarten, dass in den kommenden Monaten und Jahren weltweit ähnliche Gesetze entstehen. Ebenso wird sich der AI-Act selbst an zukünftige technologische Fortschritte anpassen und im Laufe der Zeit reifen.

Die frühzeitige Etablierung relevanter Governance-Prozesse stärkt die strategische Wettbewerbsfähigkeit Ihres Unternehmens somit erheblich. Allerdings gewährleistet die bloße Umsetzung der entsprechenden Bestimmungen nicht automatisch die erfolgreiche Gesetzeseinhaltung – ähnlich wie das bloße Installieren eines Airbags in einem Auto keine Sicherheit garantiert. Vielmehr kommt es darauf an, wie diese Regeln umgesetzt werden. Mit anderen Worten: Eine robuste und gut umgesetzte AI-Governance ist entscheidend für die langfristige Konformität mit dem AI-Act. [at] hilft Ihnen gerne.



Über [at]

Die Alexander Thamm GmbH – kurz [at] – ist eine auf Daten und Künstliche Intelligenz spezialisierte Beratung. [at] wurde 2012 von Alexander Thamm gegründet und zählt heute mit mehr als 500 Mitarbeitenden zu den Top-Adressen in Europa. [at] versteht sich als Partner, der kompetente Beratung mit konkreter Umsetzung in Einklang bringt. So konnte [at] bisher mehr als 2.000 Daten und KI-Projekte realisieren. Die Beratung begleitet zahlreiche DAX-Konzerne und Mittelständler auf ihrer Data Journey und unterhält Standorte in München, Berlin, Köln, Frankfurt, Stuttgart, Leipzig, Nürnberg, Essen, Innsbruck, Wien und Gossau.

Theresa Adamietz // Content & Editorial
Communication Manager
+49 172 1386 475
theresa.adamietz@alexanderthamm.com

Philipp Beitlich // Layout & Design
Head of Brand, Communication & Digital
+49 173 1845 262
philipp.beitlich@alexanderthamm.com

Ihre Ansprechpartner

Matthias Lein
Chief Technology Officer
Tel: +49 172 1362 253

E-Mail:
Matthias.Lein@alexanderthamm.com

Patrick Zimmermann
Principal Data Strategist
Tel: +49 173 1854 724

E-Mail:
Patrick.Zimmermann@alexanderthamm.com

[at]
alexanderthamm

Alexander Thamm GmbH
Sapporobogen 6-8
80637 München
www.alexanderthamm.com