Workstream KI-Governance

Whitepaper

Autoren

Furkan Eser
Birgit Bartz
Sebastian Döll
Eric Joachim Liese

In Zusammenarbeit mit weiteren Mitgliedsunternehmen des CBA Lab sowie der HTWG Konstanz

Inhalt

1. Einleitung

1.1 Gegen den Hype

Dank der Beliebtheit von Stable Diffusion, MidJourney oder ChatGPT hat die Begeisterung für Künstliche Intelligenz (im Weiteren KI genannt) einen Höhepunkt erreicht. Nicht nur ergänzen Softwarehersteller wie Microsoft ihre Produkte um KI-Fähigkeiten wie zum Beispiel durch GitHub Copilot oder M365 Copilot, Salesforce mit Einstein KI und viele weitere erweiterten Public Cloud Anbieter ihre KI-Services, sondern ergänzen auch Unternehmen im Maschinenbau oder verarbeiten Gewerbe ihre Prozesse und Produkte mit KI-Fähigkeiten. Sie erhoffen sich dadurch Wettbewerbsvorteile zu erzielen und Effizienzsteigerungen zu realisieren. Doch der unreflektierte Einsatz[1] von KI birgt erhebliche Risiken, die oft übersehen werden.

Zu diesen Risiken gehören Reputationsschäden, negative Auswirkungen auf die Unternehmenskultur und Kommunikation, Haftungsrisiken sowie hohe Investitionskosten[2].

Um eine langfristig erfolgreiche Nutzung sicherzustellen, ist es wichtig, den tatsächlichen Mehrwert und die Notwendigkeit von KI im spezifischen Kontext eines Unternehmens sorgfältig zu prüfen. Ein Unternehmen sollte seine Prozesse und Bedürfnisse detailliert analysieren und KI gezielt dort einsetzen, wo sie echte Verbesserungen für sich und seine Kunden bringt. Anstatt einem Hype zu folgen, sollten Unternehmen eine strategische und wohlüberlegte Herangehensweise an die Implementierung von KI wählen.

Um KI erfolgreich in ein Unternehmen zu integrieren und hohe Kosten zu vermeiden, die durch unüberlegte, nicht-strategische oder nicht regulatorisch abgestimmte Planungen entstehen, ist die Einführung einer umfassenden KI-Governance von entscheidender Bedeutung. Eine solche Governance schafft einen klaren Rahmen für die Entwicklung, den Einsatz und die Überwachung von KI-Systemen und stellt sicher, dass diese im Einklang mit den ethischen Standards, den regulatorischen Anforderungen sowie den strategischen Zielen des Unternehmens stehen. Sie definiert eindeutige Verantwortlichkeiten, identifiziert Risiken frühzeitig und leitet Maßnahmen für die Risikosteuerung des Unternehmens ab.

[1] Fear of missing out (FOMO) Phänomen.
[2] https://www.blackstone.com/insights/article/the-convergence-of-data-centers-and-power-a-generational-investment-opportunity-the-connection/

1.2 Notwendigkeit einer KI-Governance

In der gemeinsamen Arbeit der Teilnehmenden wurden neben den generellen Zielen einer KI-Governance folgende spezifische Ziele definiert:

- **Effektive Bewertung und Management von Use Cases:** Ein zentrales Ziel der KI-Governance ist es, sicherzustellen, dass KI-Use Cases effektiv bewertet, umgesetzt und kontinuierlich gemanagt werden können. Dies erfordert eine detaillierte Analyse des Return-on-Investment (ROI) und eine frühzeitige, umfassende Risikoabschätzung bereits im Demand Management. Diese Bewertungsdimensionen müssen über den gesamten Lebenszyklus hinweg kontinuierlich überprüft werden, um sicherzustellen, dass der Use Case nachhaltig den Erfolg des Unternehmens unterstützt.
- **Risikomanagement bei speziellen Aspekten von KI:** Die KI-Governance muss sicherstellen, dass spezifische Risiken, die durch den Einsatz von KI entstehen, frühzeitig erkannt, effektiv gemindert und überwacht werden. Dazu gehört eine individuelle Risikoabschätzung, die bereits im Demand Management durchgeführt wird. Diese Risiken werden bereits zu Beginn des Prozesses erörtert, um fundierte Entscheidungen über die tatsächliche Investition oder auch einer Risiko-Minimierungsstrategie zu treffen. Diese initiale Risikoanalyse wird während des gesamten Lebenszyklus des Use Cases dokumentiert und überwacht.
- **Bereitstellung von Use Cases an das gesamte Unternehmen:** Ein weiteres Ziel ist es, einen klaren und effektiven Weg aufzuzeigen, wie KI-Use Cases dem gesamten Unternehmen zur Verfügung gestellt werden können. Dies erfordert, dass KI-Use Cases und ihre Parameter als Best Practice dokumentiert und veröffentlicht werden, um sicherzustellen, dass alle Stakeholder Zugang zu den relevanten Informationen haben. Zudem sollten automatisierte Prozesse, wie beispielsweise ein Monitoring, etabliert werden, um eine reibungslose und effiziente Nutzung der KI-Systeme im Unternehmensalltag zu gewährleisten.
- **Nutzung und Anpassung vorhandener Governance-Prozesse:** Schließlich sollte die KI-Governance darauf abzielen, bestehende Governance-Prozesse im Unternehmen zu nutzen und nur wo nötig, anzupassen. Funktionierende und etablierte Prozesse, wie das Datenmanagement oder der Innovationsprozess, können als Grundlage für die Implementierung von KI-Systemen dienen. Dies gewährleistet, dass die Integration von KI möglichst nahtlos in die bestehende Unternehmensstruktur eingebettet wird und die notwendigen Anpassungen in Bereichen wie Strategie, Compliance und Monitoring vorgenommen werden. (siehe auch Kap.4)

1.3 Chancen für Unternehmen durch Künstliche Intelligenz

Die Implementierung von Künstlicher Intelligenz (KI) bietet Unternehmen zahlreiche Chancen, zum Beispiel:

- **Effizienzsteigerung durch Automatisierung:** KI kann repetitive und zeitaufwändige Aufgaben automatisieren, was zu einer deutlichen Steigerung der Effizienz führt.
- **Personalisierte Kundeninteraktionen:** Durch die Analyse von Kundendaten können maßgeschneiderte Angebote und Dienstleistungen erstellt werden, die die Kundenbindung und -zufriedenheit erhöhen.
- **Optimierung der Lieferkette:** KI analysiert komplexe Daten in Echtzeit und erkennt Muster, die zur Optimierung von Lieferkettenprozessen, Bestandsmanagement und der Vorhersage von Nachfrageschwankungen beitragen.
- **Innovationsförderung:** KI schafft neue Möglichkeiten zur Entwicklung von Produkten und Dienstleistungen und eröffnet neue Geschäftsfelder.
- **Verbesserte Entscheidungsfindung:** Durch KI-gestützte Datenanalyse werden fundierte, präzisere Entscheidungen ermöglicht.
- **Risikomanagement und Betrugserkennung:** Mithilfe prädiktiver Wartung können Ausfallzeiten von Maschinen und Anlagen minimiert und Betrugsfälle frühzeitig erkannt werden.
- **Steigerung der Mitarbeiterproduktivität:** KI kann Mitarbeiter unterstützen, ihre Produktivität zu erhöhen und sich auf wertschöpfende Tätigkeiten zu konzentrieren.

Derzeitig ist nicht davon auszugehen, dass Prozesse vollständig autonom durch KI-Lösungen gesteuert werden oder dass KI ein eigenständiges Produkt darstellt. Vielmehr ist davon auszugehen, dass Prozesse und Produkte durch KI angereichert werden.

Die Potenziale von KI können nur vollständig ausgeschöpft werden, wenn der Einsatz von KI durch eine umfassende und gut durchdachte Governance begleitet wird. Diese erweitert das Spektrum der Chancen erheblich, indem neben den unmittelbaren technologischen Vorteilen auch langfristige strategische Vorteile bedacht werden.

- **Risikominimierung und Compliance-Sicherung:** Durch eine klare Governance-Struktur können rechtliche Risiken minimiert und regulatorische Anforderungen zuverlässig eingehalten werden.
- **Vertrauensaufbau bei Stakeholdern:** Eine erfolgreiche KI-Governance schafft Vertrauen bei Kunden, Investoren und der Öffentlichkeit, indem sichergestellt wird, dass KI verantwortungsvoll und ethisch eingesetzt wird.
- **Wettbewerbsvorteile durch Ethik und Verantwortung:** Unternehmen können sich als Vorreiter im Bereich verantwortungsvolle KI positionieren und dadurch Wettbewerbsvorteile erzielen.
- **Förderung von Innovation und Wachstum:** Eine stabile Governance bildet die Grundlage für die sichere und effiziente Nutzung von KI, was langfristig Innovation und Wachstum im Unternehmen fördert.
- **Effiziente Nutzung von Ressourcen:** Durch klare Richtlinien und Prozesse können Human- und Finanzressourcen besser eingesetzt werden, was die Gesamtleistung des Unternehmens steigert.
- **Langfristige Nachhaltigkeit und Resilienz:** Kontinuierliche Anpassungen an neue Technologien und regulatorische Anforderungen gewährleisten nachhaltigen Erfolg und Haftungsvermeidung.

Unternehmen, die auf KI ohne klare Governance setzen, riskieren vielfältige Probleme:

- **Ökonomische Dimension:** Fehlende KI-Governance kann zu ineffizienten Prozessen, finanziellen Verlusten und gescheiterten Projekten führen. Zudem besteht die Gefahr von Reputationsschäden und hohen Haftungszahlungen, die die wirtschaftliche Stabilität des Unternehmens gefährden.
- **Ethische und soziale Dimension:** Unkontrollierte KI-Systeme können diskriminierende Entscheidungen verstärken, die Privatsphäre verletzen und zu einem Vertrauensverlust bei Kunden und Mitarbeitern führen. Ohne klare ethische Leitlinien entsteht ein hohes Risiko, dass die KI-Systeme zu unethischen oder gar zu gesellschaftlich schädlichen Ergebnissen führen.
- **Strategische Dimension:** Das Fehlen einer KI-Governance kann das Unternehmen in eine strategisch nachteilige Position bringen, da es die KI-Technologien nicht effizient zur Stärkung der Wettbewerbsfähigkeit nutzen kann. Eine klare Governance schafft interne Synergien, erhöht die Effizienz und ermöglicht es dem Unternehmen, flexibel auf Marktveränderungen und neue regulatorische Anforderungen zu reagieren, wodurch es seine Innovationskraft gezielt ausbauen kann.
- **Technologische Dimension:** Ohne strukturierte Governance besteht das Risiko, dass KI-Systeme auf Basis schlechter Datenqualität operieren, unzuverlässig sind und anfällig für Angriffe. Die fehlende Integrationsfähigkeit in bestehende Systeme sowie Probleme bei der Skalierung und Wartung gefährden die langfristige technologische Leistungsfähigkeit.
- **Regulatorische Dimension:** Unternehmen riskieren, gegen gesetzliche Vorschriften zu verstoßen, was zu Problemen bei der Zertifizierung, Zulassung und Compliance führen kann. Dies kann wiederum rechtliche Konsequenzen, Sanktionen und negative Auswirkungen auf die Marktfähigkeit nach sich ziehen.

1.4 Typisierung von KI

Künstliche Intelligenz bezeichnet die Fähigkeit von Maschinen und Software, menschenähnliche Intelligenzleistungen zu erbringen. Zu diesen Leistungen gehört das Lernen, die Lösungen von komplexen mehrstufigen Problemen und die Interaktion mit der Umwelt. KI ist aber nicht nur ChatGPT, Microsoft 365 Copilot oder GitHub Copilot. Diese Lösungen gehören zum Typ der Generativen KI. Es gibt aber auch Lösungen wie AlphaFold3 für die Forscher im Jahr 2024 den Nobelpreis in Chemie erhalten, die zum Typ der Voraussagenden KI gehören. Diese Typen sind dem Bereich des Maschinellen Lernens (ML) zu zuordnen.

Die verschiedenen Typen von KI benötigen auch verschiedene Herangehensweisen und Technologien für ihre Nutzung.

Voraussagende KI

Dieser Typ von KI wird eingesetzt, um nicht-lineare Zusammenhänge in Daten zu analysieren und daraus Vorhersagen über zukünftige Ereignisse oder Verhaltensweisen abzuleiten. Ein typisches Beispiel ist die Vorhersage von Wartungsarbeiten oder von Angriffsmustern im Internetverkehr. Aber auch bei Finanzanalysen, Kundenverhalten oder Risikomanagement kommt dieser Typ von KI zum Einsatz, um Produkte oder Geschäftsprozesse zu verbessern. Sie ist darauf ausgelegt, Entscheidungen zu unterstützen und strategische

[3] https://alphafold.ebi.ac.uk/

Einblicke zu liefern.

Generative KI

Dieser Typ ist darauf spezialisiert, neue Inhalte zu erstellen, wie Texte, Bilder oder Musik. Sie nutzt Techniken wie neuronale Netzwerke, um kreative Ergebnisse für eine große Breite von Anwendungsfällen zu erstellen. Generative KI findet inzwischen in vielen Bereichen Anwendung, zum Beispiel in der Programmierung, in dem Programmtext erzeugt wird, bei Geschäftsprozessen in denen E-Mails zusammengefasst oder Präsentationen erstellt werden. Es wird häufig zwischen Multimodalen und Monomodalen Modellen für KI unterschieden. Ein multimodales Modell ist ein ML-Modell, das Informationen aus verschiedenen Modalitäten verarbeiten kann, darunter Bilder, Video und Text. Wobei Monomodale Modelle meist nur aus Text Informationen verarbeiten können. KI ist nicht gleich KI. Es gibt unterschiedliche Typen, die sich für unterschiedliche Anwendungen nutzen lassen. Der Hype um KI der mit der Einführung von GPT-3 durch OpenAI entstanden ist fokussiert sich insbesondere darauf, dass Maschinen auch die komplexesten vorher unbekannte Aufgaben lösen können. Aber auch wenn diese Generative KI immer leistungsfähiger geworden ist, so fehlt ihr immer noch die Fähigkeit völlig autonom zu agieren.

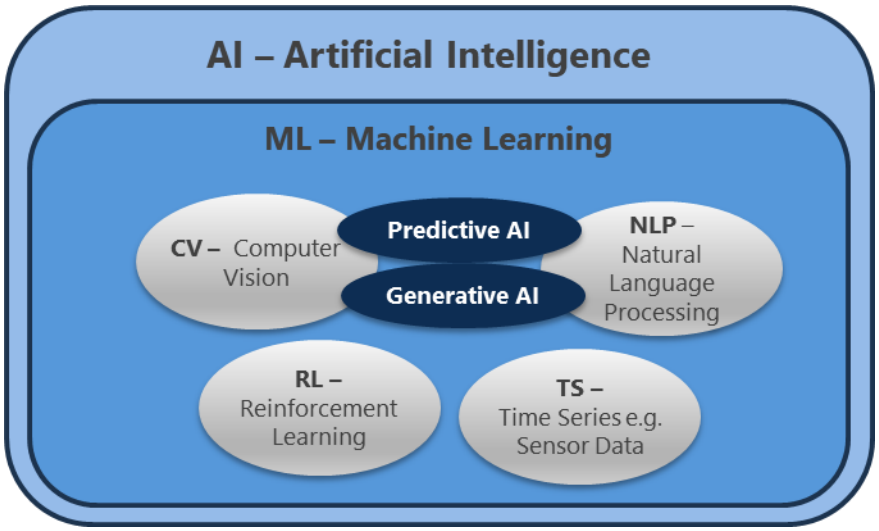

Abbildung 1: Künstliche Intelligenz (AI) und Maschinelles Lernen (ML)

2. Methodik zum Aufbau einer KI-Governance

Der Aufbau einer KI-Governance bildet das Fundament für eine verantwortungsvolle und effiziente Nutzung von Künstlicher Intelligenz im Unternehmen. Hierzu müssen die verschiedenen Anforderungen und Bedingungen im Unternehmen betrachtet und die relevanten Aspekte herausgearbeitet werden. Dieses unternehmensspezifische Governance Ecosystem bildet dann den Rahmen für die Spezifizierung and Ausprägung einer KI-Governance-Practice. Die einzelnen Dimensionen des Ecosystems, die Kernelemente und Attribute einer KI-Governance sowie deren Abhängigkeiten wurden in einem KI-Governance Modell zusammengetragen und methodisch dargestellt.

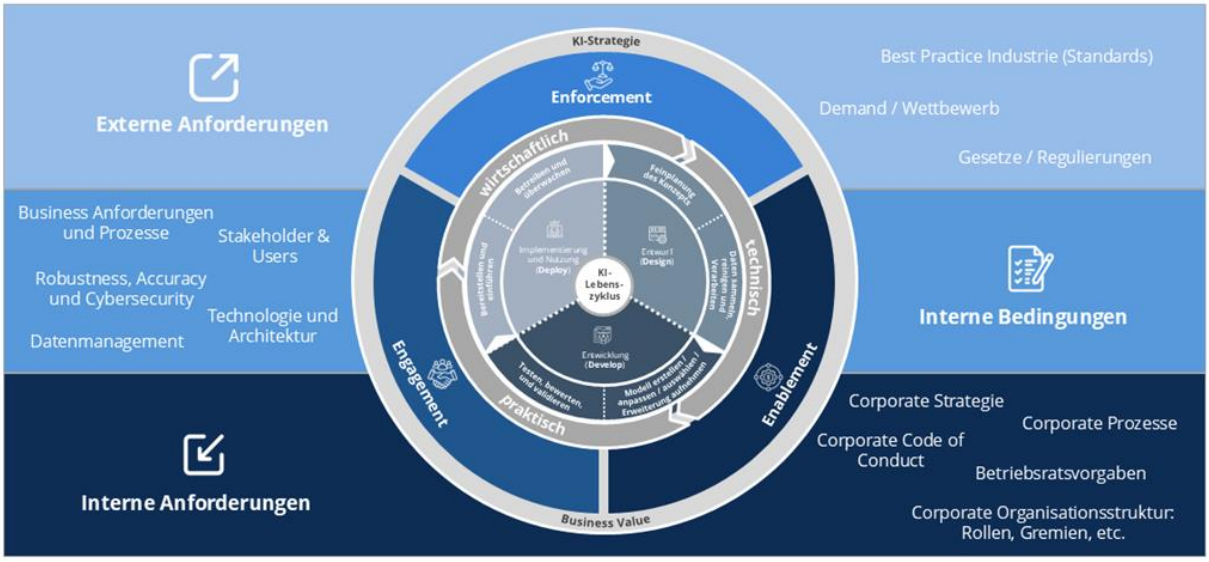

Abbildung 2: KI Governance Ecosystem

2.1 Das KI-Governance-Ecosystem

Das KI-Governance-Ecosystem bildet das Fundament für eine verantwortungsvolle und effiziente Nutzung von Künstlicher Intelligenz im Unternehmen. Es setzt sich aus verschiedenen Anforderungen zusammen, die nahtlos in die Strategie, Struktur und Prozesse des Unternehmens integriert werden müssen.

Diese Anforderungen gliedern sich in drei zentrale Dimensionen: **Externe Anforderungen**, **Interne Anforderungen** und **Interne Bedingungen**.

Externe Anforderungen im KI-Governance-Ecosystem umfassen die Rahmenbedingungen, die Unternehmen beachten müssen, um rechtliche Vorgaben zu erfüllen um den Wettbewerb sowie die Marktanforderungen zu bewältigen. Dazu gehören Best Practices der Industrie, Marktnachfrage und Wettbewerb sowie Gesetze und Regulierungen.

- **Best Practices der Industrie:** Industriestandards und bewährte Verfahren bieten Orientierung, um sichere, ethische und effektive KI-Systeme zu entwickeln.
- **Marktnachfrage und Wettbewerb:** Der Druck, innovative und marktfähige KI-Lösungen zu schaffen, treibt Unternehmen dazu, KI-Systeme vertrauenswürdig, effizient und nutzerfreundlich zu gestalten.

- **Gesetze und Regulierungen:** Nationale und internationale Vorschriften stellen sicher, dass KI-Systeme Mindestanforderungen erfüllen

Interne Bedingungen umfassen die technischen und organisatorischen Voraussetzungen, die Unternehmen schaffen müssen, um am Markt zu funktionieren. Dazu gehören:

- **Business-Anforderungen und -Prozesse:** Diese definieren, welche geschäftlichen Ziele durch KI-Systeme erreicht werden sollen und wie Prozesse entsprechend angepasst werden.
- **Stakeholder und Nutzer:** Die Bedürfnisse und Erwartungen der Stakeholder sowie Endnutzer müssen berücksichtigt werden, um nutzerzentrierte und akzeptierte KI-Lösungen bereitzustellen.
- **Robustheit, Genauigkeit und Cybersicherheit:** KI-Systeme müssen widerstandsfähig gegen Angriffe sein, verlässliche Ergebnisse liefern und hohe Sicherheitsstandards erfüllen.
- **Technologie und Architektur:** Eine solide technologische Infrastruktur und klare Systemarchitektur sind notwendig, um KI-Lösungen effizient und skalierbar umzusetzen.
- **Datenmanagement:** Eine effektive Datenverwaltung ist entscheidend, um qualitativ hochwertige, sichere und relevante Daten für den KI-Einsatz bereitzustellen.

Interne Anforderungen betreffen die organisatorischen, strategischen und ethischen Rahmenbedingungen, die Unternehmen intern festgelegt haben, wonach die KI-Governance ausgerichtet werden muss. Dazu gehören:

1. **Corporate-Strategie:** Die übergeordnete Unternehmensstrategie bestimmt die Ausrichtung der KI-Strategie und der KI-Governance-Strategie.
2. **Corporate Code of Conduct:** Ethische Richtlinien, bzw. gemeinsame Werte legen fest, wie KI-Systeme verantwortungsvoll und im Einklang mit den Werten des Unternehmens entwickelt und eingesetzt werden.
3. **Corporate-Prozesse:** Geschäftsprozesse müssen einerseits so gestaltet werden, dass sie den Einsatz von KI unterstützen und effizient auf die Integration neuer Technologien reagieren und anderseits sollten Prozesse der KI-Governance schon etablierte Prozesse nutzen und darauf aufbauen.
4. **Betriebsratsvorgaben:** Vorgaben des Betriebsrats stellen sicher, dass der Einsatz von KI auch arbeitsrechtliche und mitbestimmungsrechtliche Aspekte berücksichtigt.
5. **Corporate-Organisationsstruktur:** Klare Rollen, Zuständigkeiten und Gremien sorgen für eine effektive Steuerung und Kontrolle des KI-Einsatzes im Unternehmen.

Die internen und externen Anforderungen legen fest, wie Unternehmen den Einsatz von KI planen, umsetzen und steuern müssen. Diese Anforderungen müssen klar in die Strategie, in die Entwicklung von Fähigkeiten, in Rollen und Verantwortlichkeiten, in Compliance-Strukturen, in Tools, Technologie und Prozesse sowie in Policies, Dokumente und Richtlinien übersetzt werden. Wichtig ist, dass Unternehmen diese Anforderungen individuell und unternehmensspezifisch anpassen und entwickeln müssen.

Für die Übersetzung ist es wichtig, dass die Anforderungen nicht isoliert oder nur in bestimmten Abteilungen bearbeitet werden. Stattdessen sollten Experten aus den verschiedenen Dimensionen – wie Recht, Technologie, Compliance, Personalwesen und Strategie – eng zusammenarbeiten. Durch diese interdisziplinäre Zusammenarbeit

wird sichergestellt, dass die Anforderungen ganzheitlich verstanden und umgesetzt werden. Eine enge Zusammenarbeit stellt sicher, dass die Anforderungen reibungslos und effizient in die Praxis umgesetzt werden, ohne für die Entwicklungsteams unnötige Verzögerungen durch komplexe bürokratische Prozesse zu riskieren. So können sowohl strategische als auch operative Aspekte optimal aufeinander abgestimmt werden und ebnen den Weg, Innovationen mit möglichst wenigen Hürden entwickelt, geprüft und skaliert zu bringen.

2.2 Attribute der KI-Governance

In der grafischen Darstellung des KI-Governance-Modells wird im Zentrum der **KI-Lebenszyklus** dargestellt, der die kontinuierliche Entwicklung und Iteration von KI-Systemen symbolisiert. Um diesen Kern gruppieren sich die drei zentralen Attribute, die die internen Bedingungen in einem Unternehmen als maßgebliche Prinzipien und Treiber kennzeichnen:

- **Wirtschaftlich**: Dieses Attribut bezieht sich auf die Kosten-Nutzen-Analyse und Rentabilität eines KI-Systems. Es ist entscheidend, dass Investitionen langfristig Erträge liefern und Effizienzgewinne erzielen. Aus dem Attribut „wirtschaftlich“ lassen sich wichtige Elemente der Governance ableiten. Die wirtschaftliche Rentabilität eines KI-Systems erfordert eine sorgfältige Planung und eine nachhaltige Perspektive. Wichtig ist hier, nicht nur den direkten Nutzen (z. B. gesteigerte Effizienz) zu betrachten, sondern auch potenzielle Kosten, wie Implementierung, Wartung und mögliche Risiken, die durch rechtliche und ethische Vorgaben entstehen könnten.

- **Technisch**: Hier wird die Machbarkeit, Leistungsfähigkeit und Integration von KI-Systemen in bestehende Infrastrukturen betrachtet. Ein erfolgreiches System muss zuverlässig, skalierbar und anpassungsfähig sein.

  Technische Machbarkeit spielt eine zentrale Rolle in der Bewertung und Entwicklung eines KI-Systems und ist deshalb ein wichtiges Attribut der KI-Governance, da sie hauptsächlich den Zugang zur Governance regelt. Hier werden Themen wie bestehende Infrastruktur, Skalierbarkeit, Zuverlässigkeit und Anpassungsfähigkeit einbezogen.
- **Praktisch**: Dieses Attribut betont die Benutzerfreundlichkeit und Akzeptanz der KI-Systeme durch die Stakeholder. Ein praktisches System muss den Bedürfnissen der Nutzer entsprechen, um erfolgreich implementiert und genutzt zu werden.

  Hierzu zählt ebenso die Betrachtung der verschiedenen Stakeholder und Nutzer*innen. Technisch ausgereifte Systeme, die jedoch in ihrer Handhabung kompliziert sind, können auf Widerstand stoßen und zu geringen Nutzungsraten führen. Auch die KI-Managementsysteme, wie im AI Act gefordert, müssen sicherstellen, dass die Systeme nicht nur effizient, sondern auch leicht verständlich und anpassbar für unterschiedliche Nutzergruppen sind.

2.3 Die Kernfunktionen im Governance-Modell

Mit Hilfe von drei Governance-Kernfunktionen, wird es uns möglich entsprechend den internen Bedingungen und unter Beachtung der externen und internen Anforderungen eine nachhaltige und verantwortungsvolle KI-Implementierung zu gewährleisten:

- **Engagement**: Es ist entscheidend, eine aktive Community zu schaffen, die den Austausch von Wissen und Erfahrungen fördert. Das AI-Office spielt hier eine zentrale Rolle, indem es Initiativen koordiniert und Schulungen organisiert, um das Bewusstsein und die Akzeptanz von KI-Technologien zu stärken.

  Aktives Engagement und Wissensmanagement im Unternehmen, sind in diesem Zusammenhang besonders wichtig, da in Unternehmen häufig zentrales Wissen über die Schnittstelle zwischen Technik, Compliance, Legal und anderen berührenden Einheiten oft fehlt. Eine proaktive Community, die folgende wichtige Ableitungen übernimmt ist daher sehr wichtig: Unterstützung der KI-Entwicklung bei der Einhaltung der vielfältigen Regulatorik und deren komplexen Anforderungen, Aufbau einer Change-Strategie, Sensibilisierungsmaßnahmen und Trainingsangeboten, um der allgemeinen Belegschaft Ängste zu nehmen, die Förderung von KI-Kompetenzen voranzutreiben und die Einhaltung der regulatorischen Anforderungen bei der Nutzung der KI-Toollandschaft sicherzustellen.

- **Enablement**: Dieser Bereich fokussiert sich auf die Schaffung einer soliden Infrastruktur, die den Einsatz von KI-Systemen unterstützt. Dazu gehören technologische Ressourcen, Datenmanagement und Schulungsprogramme, die die Kompetenzen der Mitarbeiter erweitern.

  Eine solide technologische Basis gewährleistet, dass die KI-Systeme reibungslos funktionieren und skalierbar sind, während qualitativ hochwertiges Datenmanagement sicherstellt, dass KI-Anwendungen mit verlässlichen und repräsentativen Daten arbeiten. Die Schulung und Weiterbildung der Mitarbeiter befähigt diese, die Technologie nicht nur zu verstehen, sondern sie aktiv zur Wertschöpfung und Innovation zu nutzen. Für die Governance werden unter anderem Themen abgeleitet, wie flexible und anpassungsfähige Technologien zu priorisieren, da der technologische Fortschritt so schnell voranschreitet, dass es für Organisationen herausfordernd ist, immer auf dem neuesten Stand zu bleiben. Schulungsprogramme sind eine andere wichtige Ableitung, um sicherzustellen, dass Mitarbeiter*innen nicht nur theoretische Kenntnisse erlangen, sondern auch praktische Fähigkeiten, um KI-Systeme verantwortungsvoll zu entwickeln und zu nutzen.

- **Enforcement**: Hier wird sichergestellt, dass alle KI-Anwendungen ethischen Standards und gesetzlichen Vorgaben entsprechen. Die Implementierung von Kontrollmechanismen und Audits stärkt das Vertrauen der Stakeholder in KI-Technologien und fördert verantwortungsvolle Nutzung.

  Das Prinzip des Enforcement ist unverzichtbar, um sicherzustellen, dass KI-Systeme nicht nur effektiv, sondern auch revisionssicher und im Einklang mit den rechtlichen Rahmenbedingungen arbeiten. Während die Implementierung von Kontrollmechanismen und Audits eine solide Grundlage bietet, reicht dies allein nicht aus. Oft werden Audits nur periodisch durchgeführt, was bedeutet, dass zwischen den Überprüfungen Risiken übersehen werden könnten. Ableitungen werden hier hauptsächlich im Bereich der Compliance-Überprüfungen und der Stärkung der Rechenschaftspflicht und Verantwortung getroffen.

Um alles herum umschließt der äußere Kreis den **Business Value**, der den Gesamtnutzen und die strategische Bedeutung von KI für das Unternehmen verdeutlicht.

2.4 Verhinderung von Schatten KI und Anpassbarkeit der KI-Governance

Effektive Governance erfordert die klare Zuordnung von Verantwortungsdomänen, die sich nicht nur an Produkten oder Geschäftsprozessen orientieren, sondern nach spezifischen Bereichen gegliedert sind. Dieses Modell sieht die Verteilung der Governance-Domänen auf **Konformität, Sicherheit und Betrieb** vor. Für herkömmliche selbst bereitgestellte KI-Modelle liegt der Schwerpunkt auf der Einhaltung regulatorischer Vorgaben, der Sicherstellung

der Datenqualität und der Robustheit der Systeme. Auf Organisationsebene kommen hingegen zusätzliche Anforderungen hinzu, wie die Verhinderung von "Schatten-KI" und die Sicherstellung, dass die erzeugten Inhalte ethischen und rechtlichen Standards entsprechen.

"Schatten-KI" beschreibt den Einsatz von KI-Systemen, die außerhalb der offiziellen Governance-Strukturen eines Unternehmens betrieben werden, ohne angemessene Überwachung oder Einhaltung von Sicherheits- und Compliance-Vorgaben, was beispielsweise der Fall wäre, wenn eine Abteilung eine nicht genehmigte KI-Anwendung zur Automatisierung von Arbeitsprozessen einführt, ohne sie auf Datenschutz- oder Sicherheitsrisiken prüfen zu lassen. In Zeiten von low-code, no-code und API-, bzw. Browserapplikationen kann dies häufig vorkommen. Dies gilt mit verschiedenen Maßnahmen unbedingt zu vermeiden, die Konsequenzen können für ein Unternehmen gravierend sein.

Um sicherzustellen, dass im Geschäftskontext nur freigegebene und geprüfte KI-Anwendungen verwendet werden, ist ein Awareness-Programm für Mitarbeitende unerlässlich. Es muss deutlich gemacht werden, dass nur geprüfte Systeme genutzt oder eigene Anwendungen vor der Nutzung geprüft werden müssen. Gleichzeitig sollten die Prüfprozesse schlank und ressourcenschonend gestaltet werden, um eine Experimentierkultur zu fördern und das Vertrauen in die Eigenverantwortung der Mitarbeitenden zu bewahren.

Abbildung 3: Regulierung, Sicherheit, Betrieb

2.5 Arten von KI-Systemen im Fokus des KI-Governance-Modells

1. Selbst entwickelte oder angepasste externe Modelle, die in eigene Produkte und Services integriert werden.
2. Distribuierte KI-Systeme, die unverändert bleiben und dem Markt direkt zur Verfügung gestellt werden.
3. Selbst genutzte KI-Systeme oder Servicekomponenten, die ausschließlich intern verwendet werden, um spezifische betriebliche Anforderungen zu erfüllen.

Alle drei Systemtypen unterliegen denselben Governance-Mechanismen, um Sicherheit, Compliance und ethische Nutzung zu gewährleisten.

3. KI-Governance-Artefakte

Die KI-Governance Artefakte stellen zentrale Komponenten (essenzielle Dokumente, Tools und Methoden) dar, die für die Etablierung einer KI-Governance innerhalb eines Unternehmens unerlässlich sind. Diese Artefakte sind das Fundament für die Steuerung und Überwachung von KI-Lösungen. Sie zielen auf die einzigartigen Herausforderungen ab, die sich für Unternehmen durch den Einsatz von künstlicher Intelligenz ergeben.

Im Gegensatz zur traditionellen IT-Governance, erfordert die KI-Governance einen breiteren Ansatz. Sie berücksichtigt sowohl die technische Komplexität als auch die ethischen Implikationen der Nutzung von KI, die kontinuierliche Anpassungsfähigkeit der Systeme, auch nach dem Launch und die Notwendigkeit, neue Formen des Risikomanagements zu etablieren.

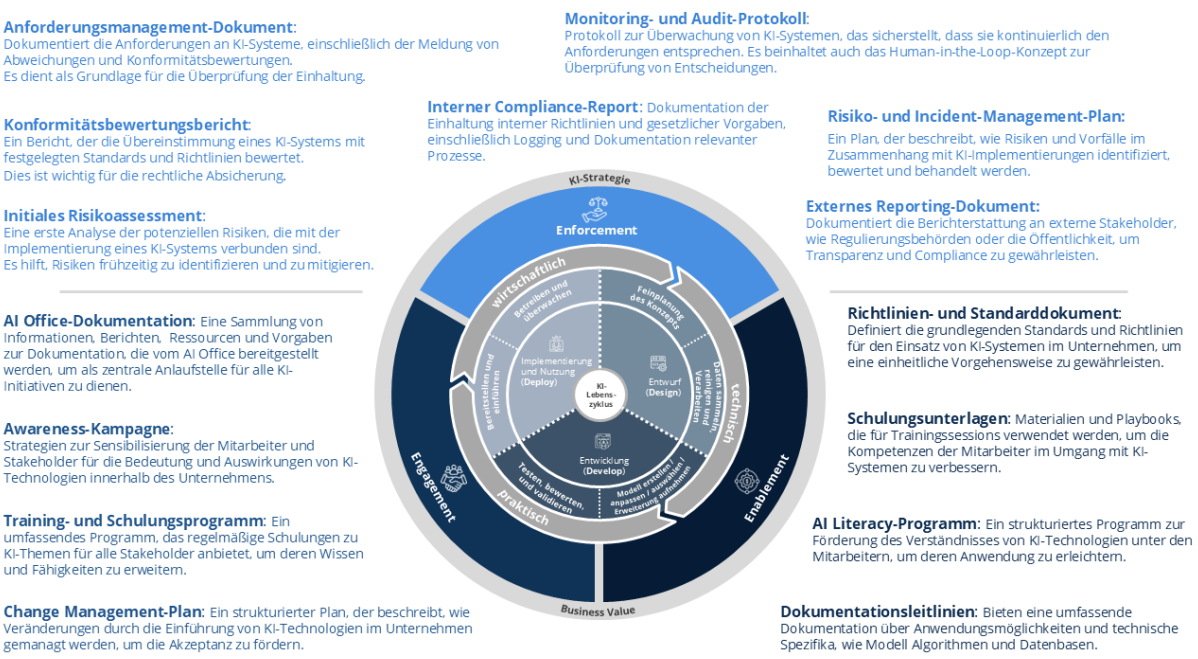

Abbildung 4: Governance Artefakte

Im Sinne des ganzheitlichen und iterativen Prozesses der KI-Governance, der eine regelmäßige Kontrolle und Aktualisierung erfordert, müssen auch diese Artefakte kontinuierlich fortgeschrieben werden.

Der Prozess hat drei Wirkungsbereiche, mit denen die KI-Governance auf das Unternehmen einwirkt. Diese sind das Enforcement, das Enablement und das Engagement (EEE). Alle Aktivitäten der KI-Governance lassen sich diesen drei Wirkungsfaktoren zu ordnen. Entweder müssen bestimmte Vorgaben gemacht und eingehalten werden (Enforcement). Entscheidungshilfen gegeben werden (Enablement) oder Entscheidungen zum Einsatz von KI-Lösungen unterstützt werden.

3.1 Artefakte zum Enforcement der KI-Governance

Anforderungsmanagement-Dokument: Dieses Dokument listet alle Anforderungen auf, die ein KI-System erfüllen muss, einschließlich der Meldepflicht bei Abweichungen und der Konformitätsbewertung. Es dient als Referenz für die Überprüfung der Einhaltung von internen und externen Vorgaben und bildet die Basis für eine strukturierte Umsetzung der Anforderungen.

Konformitätsbewertungsbericht: Dieser Bericht dokumentiert die Übereinstimmung eines KI-Systems mit den festgelegten Standards und Richtlinien. Er dient damit auch der Grundlage für die Berichte an externe Stakeholder, wie zum Beispiel Regierungsstellen.

Initiales Risikoassessment: Eine erste Analyse der potenziellen Risiken, die mit der Implementierung eines KI-Systems verbunden sind. Diese frühe Risikobewertung hilft, potenzielle Bedrohungen zu identifizieren und geeignete Maßnahmen zur Minderung dieser Risiken zu ergreifen. Dies stellt sicher, dass Entwicklungsteams sich frühzeitig mit möglichen Risiken auseinandersetzen und schon in grundsätzlichen Entscheidungen Risiken auf technischer Basis mitigieren können. Außerdem hilft es dabei, Ressourcen für Compliance und Sicherheitsüberprüfungen effektiv einzusetzen und möglicherweise von Best Practices im Unternehmen zu profitieren.

Monitoring- und Audit-Protokoll: Dieses Protokoll dokumentiert die Überwachung von KI-Systemen, um sicherzustellen, dass sie kontinuierlich, im Betrieb den festgelegten Anforderungen entsprechen. Es beinhaltet auch ein „Human-in-the-Loop“-Konzept, das die Überprüfung wichtiger Entscheidungen durch Menschen sicherstellt, welches angemessen an dem Risiko und der Sensibilität des Use Cases angepasst ist.

Interner Compliance-Report: Der Compliance-Report stellt die Einhaltung interner Richtlinien und gesetzlicher Vorgaben sicher. Er umfasst das Logging und die Dokumentation aller relevanten Prozesse und Aktivitäten und gewährleistet damit eine lückenlose Nachverfolgbarkeit der Aktivitäten und Entscheidungen. Diese müssen je nach gesetzlichen Vorgaben aufbewahrt werden.

Risiko- und Incident-Management-Plan: Dieser Plan beschreibt, wie Risiken und Vorfälle, die im Zusammenhang mit der KI-Implementierung und -Nutzung auftreten, identifiziert, bewertet und bearbeitet werden. Diese Pläne müssen je nach Sensibilität der Anwendung bewertet und angepasst werden und die Voraussetzungen für die zeitnahe Bearbeitung der Pläne geschaffen werden.

Externes Reporting-Dokument: Das externe Reporting-Dokument stellt die Berichterstattung gegenüber externen Stakeholdern, wie Regulierungsbehörden oder der Öffentlichkeit, sicher. Es dient der Transparenz und der Einhaltung von Compliance-Anforderungen.

3.2 Artefakte des Engagements der KI-Governance

AI Office-Dokumentation: Eine zentrale Sammlung von Informationen, Berichten, Ressourcen und Vorgaben, die vom AI Office bereitgestellt werden, um als zentrale Anlaufstelle für alle KI-Initiativen im Unternehmen zu dienen. Dies bündelt nicht nur die Artefakte aus dem Bereich Enforcement, sondern auch unterstützende und hilfreiche Informationen, wie Best Practices, Transparenzverpflichtungen, AGB-Module, etc.

Awareness-Kampagne: Eine Strategie zur Sensibilisierung der Mitarbeitenden und Stakeholder über die Bedeutung und Auswirkungen von KI-Technologien im Unternehmen. Die Awareness-Kampagne sorgt für ein besseres Verständnis und Akzeptanz von KI-Systemen im Unternehmen, strebt an, Angst zu nehmen und unternehmensweite Rechtssicherheit zu schaffen, um Entwicklungsteams in ihren Aufgaben zu entlasten.

Training- und Schulungsprogramm: Ein umfassendes Schulungsprogramm, das regelmäßige Trainings zu verschiedenen KI-Themen für alle Stakeholder anbietet. Das Wissen und die Fähigkeiten der Mitarbeitenden sollen kontinuierlich erweitert und sichergestellt werden, dass alle mit den neuesten Entwicklungen, zu nutzenden Anwendungen und Best Practices vertraut sind. Es baut Berührungsängste im Unternehmen ab und sorgt dafür, dass auch horizontal alle Mitarbeitenden lernen (Teil-) Aspekte ihrer Arbeit sinnvoll zu automatisieren.

Change Management-Plan: Ein strukturierter Plan, der beschreibt, wie Veränderungen, die durch die Einführung von KI-Technologien im Unternehmen entstehen, gemanagt werden. Ziel ist es, die Akzeptanz und erfolgreiche Implementierung von KI-Systemen zu fördern und zu skalieren.

3.3 Artefakte zum Enablement der KI-Governance

Richtlinien- und Standarddokument: Definiert die grundlegenden Standards und Richtlinien für den Einsatz von KI-Systemen im Unternehmen, um eine einheitliche Vorgehensweise auf Unternehmensebene oder für definierte Sektoren und Anwendungsgebiete sicherzustellen.

Schulungsunterlagen: Materialien und Playbooks, die für Trainingseinheiten verwendet werden, um die Kompetenzen der Mitarbeitenden im Umgang mit KI-Systemen zu verbessern.

AI Literacy-Programm: Ein strukturiertes Programm zur Förderung des Verständnisses von KI-Technologien unter den Mitarbeitenden, um deren Anwendung zu erleichtern. Je nach Anwendung kann es vorkommen, dass ein dezidiertes AI-Literacy Programm für einen besonders sensiblen Anwendungsfall erstellt werden muss, um die Nutzenden zu schulen.

Dokumentationsleitlinien: Bieten eine umfassende Dokumentation über Anwendungsmöglichkeiten und technische Spezifika, wie Modelle, Algorithmen und Datenbasen in KI-Projekten genutzt werden sollten.

4. KI-Governance und bestehende Unternehmensprozesse

Im Unternehmen existieren bereits zahlreiche etablierte Prozesse, die sich über Jahre hinweg bewährt haben und eine solide Grundlage bieten. Angesichts der Einführung von KI-Technologien ist es jedoch wichtig, diese Prozesse sorgfältig zu überprüfen und teilweise neu zu gestalten. Es gilt, Doppelarbeit und unnötige bürokratische Hürden zu vermeiden, die durch unkoordinierte Parallelstrukturen und Workarounds entstehen könnten. Da KI-Innovationen als horizontale Themen alle Abteilungen und Geschäftsbereiche betreffen, müssen bestehende, effiziente Prozesse an die neuen Anforderungen der KI-Entwicklung und -Implementierung angepasst werden.

Wichtig ist dabei, KI nicht isoliert zu betrachten. Stattdessen sollten die Schnittstellen zwischen den verschiedenen Unternehmensbereichen neu definiert und enger miteinander verzahnt werden. Die bestehenden Strukturen bieten eine wertvolle Basis, auf der die neuen Anforderungen aufbauen können. Die Optimierung dieser Prozesse ist entscheidend, um den gesamten Wert der KI-Innovation im Unternehmen zu realisieren und sicherzustellen, dass alle Einheiten reibungslos und effizient zusammenarbeiten.

Folgende zentrale Prozesse müssen im Unternehmen optimiert und an die neuen Herausforderungen angepasst werden:

4.1 Strategie und Planung

Die Strategie und die damit verbundenen Prinzipien legen den Rahmen fest, in dem KI-Systeme im Unternehmen entwickelt und eingesetzt werden. Sie bestimmen die langfristige Ausrichtung und Priorisierung von KI-Initiativen und sorgen dafür, dass diese im Einklang mit den übergeordneten Zielen des Unternehmens stehen. Die Prinzipien dienen als Richtlinien, an denen sich alle operativen Entscheidungen rund um KI orientieren.

Warum ist eine Änderung in der Strategie und den Prinzipien notwendig?

Mit der Einführung von KI-Technologien verändern sich die Anforderungen an die strategische Planung grundlegend. KI-Initiativen sind oft komplex, interdisziplinär und betreffen verschiedene Geschäftsbereiche – oft auch Geschäftsbereiche, die bisher nur wenig Digitalisierung erfuhren. Eine klare KI-Strategie ist wichtig, um Use Cases gezielt auszuwählen, zu priorisieren und deren Nutzen für das gesamte Unternehmen zu maximieren. Ohne eine solche strategische Ausrichtung besteht die Gefahr, dass KI-Projekte isoliert oder ohne klares Ziel verfolgt werden, was zu ineffizienten Ressourceneinsätzen und verpassten Chancen führen kann.

Zusätzlich erfordert die Einführung von KI-Systemen neue Entscheidungsprinzipien, die spezifische Herausforderungen wie die Auswahl der technischen Infrastruktur ("Cloud first" vs. „Build before buy“) und die Definition von Architekturprinzipien berücksichtigen. Diese Prinzipien müssen flexibel und anpassbar sein.

- **Alignment der KI-Strategie mit der Unternehmensstrategie:** Die Auswahl und Priorisierung der Use Cases muss im Einklang mit der übergeordneten KI-Strategie und der Strategie des Unternehmens stehen.
- **Bestehende Prinzipien wiederverwenden und/oder anpassen:** Die bereits etablierten strategischen Prinzipien sollten überprüft und, wenn möglich, weiter genutzt werden. Es gilt sicherzustellen, dass die Grundsätze des Unternehmens – wie z.B. Agilität oder Nachhaltigkeit – auch bei der Einführung von KI eingehalten werden.
- **Neue Entscheidungsprinzipien entwickeln:** Der Bedarf an klaren Architekturprinzipien ist im KI-Kontext besonders hoch, da die meist vielen kleinen Initiativen im Unternehmen von einheitlichen Best Practices und Prinzipien profitieren können. Entscheidungen wie „Cloud first“ oder „Build before buy“ müssen frühzeitig festgelegt werden, um eine klare strategische Richtung vorzugeben und technische Implementierungen zu vereinfachen.

4.2 Demand-Prozess

Der Demand-Prozess beschreibt den strukturierten Weg, auf dem neue Ideen oder Innovationsprojekte im Unternehmen identifiziert, bewertet und in die Umsetzungsphase überführt werden.

Warum ist die Änderung im Demand-Prozess notwendig?

Mit der Einführung von KI-Technologien müssen zusätzliche Faktoren berücksichtigt werden, die bisher in klassischen Innovationsprozessen keine zentrale Rolle gespielt haben.

Vor allem das Risiko muss bereits in einer frühen Phase des Prozesses erkannt und gründlich abgeschätzt werden. KI-Projekte bringen potenziell höhere Risiken mit sich, sei es im Hinblick auf ethische Fragen, Datensicherheit oder

potenzielle Haftungsrisiken. Diese Risiken sollten nicht erst in späteren Projektphasen, sondern von Anfang an identifiziert und analysiert werden, um fundierte Entscheidungen zu treffen.

Darüber hinaus ist es entscheidend, die Compliance-Kosten frühzeitig in den Prozess zu integrieren. Der Demand-Prozess muss sicherstellen, dass alle mit der KI verbundenen regulatorischen Anforderungen klar definiert und deren Einhaltung als Teil der Projektkosten berücksichtigt wird. Diese Compliance-Kosten fließen direkt in die Berechnung des Returns on Investment (ROI) ein und sind ein Schlüsselfaktor bei der Bewertung der wirtschaftlichen Machbarkeit eines KI-Projekts. Ohne diese frühzeitige Berücksichtigung besteht die Gefahr, dass Projekte finanziell unterschätzt und die ROI-Berechnungen unrealistisch optimistisch ausfallen.

Anpassungen des Demand-Prozesses:

- **Frühe Transparenz über Compliance-Kosten:** Um fundierte Entscheidungen treffen zu können, müssen die Compliance-Kosten schon in der Konzeptphase detailliert erfasst und bewertet werden.
- **Implementierung nach Wert und Ressourcen:** Der Demand-Prozess priorisiert Projekte nach ihrem erwarteten Wertbeitrag und den verfügbaren Ressourcen.
- **Risiko- und Rollenklassifizierung:** Durch eine strukturierte Risikoanalyse, insbesondere bei Hochrisiko-Modellen, wird ein 4-Augen-Prinzip eingeführt. Dies hilft, Verantwortlichkeiten klar zu definieren und Risiken zu minimieren.
- **Iterative Überprüfung:** Projekte und ihre Risiken sowie Kosten müssen regelmäßig überprüft und neu bewertet werden, um flexibel auf Veränderungen reagieren zu können.

4.3 Compliance-Prozess

Der Compliance-Prozess umfasst alle Schritte, die sicherstellen, dass ein Unternehmen gesetzliche Vorgaben, regulatorische Anforderungen und interne Richtlinien einhält.

Warum ist eine Änderung im Compliance-Prozess notwendig?

Mit der Einführung von KI-Technologien entstehen neue, komplexe regulatorische Anforderungen, die sich je nach Risikoklasse des KI-Systems stark unterscheiden können. Besonders KI-Systeme mit hohem Risiko unterliegen strikten Vorgaben, die überwacht und regelmäßig überprüft werden müssen. Ein nicht konformes KI-System kann zu erheblichen rechtlichen und finanziellen Konsequenzen führen. Die frühzeitige Einbindung der Compliance Anforderungen kann Entwicklungsteams außerdem dabei unterstützen, die Risiko-Höhe des KI-Modells zumindest teilweise zu minimieren. Zum Beispiel kann ein Zerlegen einer Aufgabe in Teilschritte durch voneinander abgetrennte Modelle dazu führen, dass nur Modelle, die signifikante Entscheidungen treffen, als Hoch-Risiko System gelten, was die Compliance Kosten für die gesamte Anwendung massiv begrenzen kann.

Anpassungen des Compliance-Prozesses:

- **Frühe Kommunikation von Anforderungen:** Es ist notwendig, dass alle Compliance-Anforderungen klar an die relevanten Abteilungen kommuniziert werden, um eine konsistente Umsetzung sicherzustellen oder Minimierungsstrategien zu entwickeln.
- **Transparenz über Compliance-Anforderungen:** Bereits zu Beginn des KI-Lebenszyklus müssen alle relevanten Compliance-Auflagen klar definiert und in den Prozess integriert werden. Dies ermöglicht eine frühzeitige Risikobewertung und reduziert spätere Verzögerungen.
- **Verpflichtendes Konformitätsassessment und Auditprozesse:** Der Compliance-Prozess erfordert ein kontinuierliches Monitoring der Systeme, unterstützt durch Audits und regelmäßige Konformitätsprüfungen, um die Einhaltung der Vorschriften auch nach der Einführung sicherzustellen.

4.4 Solution Design

Das Solution Design bezieht sich auf den Prozess, in dem eine technische Lösung – in diesem Fall ein KI-System – entworfen, bewertet und für die Implementierung vorbereitet wird.

Warum ist eine Änderung im Solution Design notwendig?

KI-Systeme bringen einzigartige Herausforderungen mit sich, die weit über klassische Softwareentwicklungsprozesse hinausgehen (Bsp.: Bias, Fairness, Transparenz, ...). Ein unzureichendes Design kann zu unvorhergesehenen Risiken wie Verzerrungen in den Ergebnissen oder schwerwiegenden Sicherheitsproblemen führen.

Darüber hinaus muss das Solution Design sicherstellen, dass die Cybersecurity und die Skalierbarkeit des KI-Systems angemessen berücksichtigt werden. Zudem muss das Design so gestaltet werden, dass es auch in verschiedenen Umgebungen und unter variablen Bedingungen zuverlässig funktioniert.

Das System muss daher durchgehend überwacht werden und es muss sichergestellt werden, dass die festgelegten Kriterien für Performance, Sicherheit und Transparenz eingehalten werden. Zudem sind klare Verantwortlichkeiten und ein funktionierendes Incident Management notwendig, um im Falle von Problemen oder Sicherheitsvorfällen schnell und effizient reagieren zu können.

- **Governance Tools:** Tools wie Collibra oder LeanIX sollten genutzt werden, um kontinuierlich die Model Health, Service Health und die Sicherheit des KI-Systems zu überwachen.
- **Risiken frühzeitig betrachten:** Frühzeitige Berücksichtigung von Fairness und Bias
- **Performance Bewertung und Skalierbarkeit:** Klare Metriken für die Performance-Bewertung festlegen, die an den spezifischen Use Case angepasst sind. Dies beinhaltet auch die Bewertung der Skalierbarkeit und die Berücksichtigung von Umgebungsbeschränkungen.
- **Cybersecurity:** Abhängig von den spezifischen Angriffsvektoren des Systems müssen geeignete Sicherheitsmechanismen eingebaut werden, um potenzielle Bedrohungen zu minimieren. Sicherheitsmaßnahmen müssen Teil des Grunddesigns sein, nicht eine nachträgliche Ergänzung.
- **Rollen, Verantwortlichkeiten und Incident Management:** Es müssen klare Verantwortlichkeiten festgelegt werden, um die Umsetzung der Sicherheits- und Performanceanforderungen sicherzustellen und ein strukturiertes und effektives Incident Management sicherzustellen.

4.5 Monitoring / Operation Management

Monitoring und Operationsmanagement bezieht sich auf die kontinuierliche Überwachung und Wartung von KI-Systemen im laufenden Betrieb.

Warum ist eine Änderung im Monitoring / Operation Management notwendig?

KI-Modelle nach unserer Definition entwickeln sich nach ihrer Implementierung ständig weiter. Ohne ein effektives Monitoring kann die Robustheit oder Qualität der Ergebnisse nachlassen, und es besteht das Risiko, dass die Modelle unvorhersehbare oder unerwünschte Verhaltensweisen zeigen. Dies ist vor allem schwer zu erkennen, wenn sich diese Verzerrung nur langsam einschleicht. Darüber hinaus ist ein Monitoring Konzept für Hoch-Risiko Modelle auf Basis des AI Acts verpflichtend.

Alle wichtigen Stakeholder – zum Beispiel des Operations-Teams, der Compliance-Abteilung und des Managements – müssen stets Zugriff auf aktuelle Informationen über den Zustand und die Performance der KI-Systeme haben. Dies erfordert Custom Metrics, die auf die spezifischen Anforderungen des Unternehmens und des Anwendungsfalls zugeschnitten sind.

- **Kontinuierliche Überwachung:** Die Ergebnisse von KI-Modellen müssen kontinuierlich auf Qualität und Verhalten überprüft werden. Dies umfasst die Gewährleistung der Robustheit und Richtigkeit der Modelle sowie das Einhalten von Performance-Metriken.
- **Custom Metrics und Audit:** Es sollten maßgeschneiderte Metriken entwickelt werden, die die Performance, Sicherheit und Konformität der Modelle überwachen. Zudem müssen Audit Trails eingerichtet werden, um alle wesentlichen Entscheidungen und Modelländerungen nachvollziehbar zu dokumentieren. Diese Metriken, die Extensität und Intensität der Überwachung und Audits sollte immer angemessen am Anwendungsfall konzipiert und durchgeführt werden.
- **Einbindung in die bestehende Unternehmensinfrastruktur:** Zum Beispiel in die Unternehmensprozesse wie Ticketing-Systeme, Health Scores und Reporting – Dashboards
- **Notausschalter / Death Switch:** Ein Death Switch sollte eingerichtet werden, um im Falle eines schwerwiegenden Fehlers das betroffene Modell automatisch zu deaktivieren. Der Prozess, um diesen zu aktivieren, sollte allen Stakeholdern transparent und zugänglich vorliegen.
- **Reporting an das AI Office:** Dies stellt sicher, dass alle relevanten Daten und Vorfälle dokumentiert werden. Dadurch können Entscheidungen auf Grundlage verlässlicher Daten getroffen und notwendige Anpassungen zeitnah und strategisch umgesetzt werden.

5. Neue Anforderungen und Capabilities, die für die erfolgreiche KI-Einführung notwendig sind

Mit der Einführung von KI-Technologien im Unternehmen entstehen neue Anforderungen und Fähigkeiten, die bisher in traditionellen Prozessen nicht vorhanden waren oder in dieser Form nicht erforderlich waren.

Auf übergeordneter Ebene müssen folgende Fähigkeiten in Unternehmen entwickelt werden, um den effektiven Umgang mit KI-Anwendungen und Regulatorik sicherzustellen:

- Kompetenz im Umgang mit regulatorischen Anforderungen (AI Act)
- KI spezifische Risikobewertungskompetenz
- Fähigkeit zur interdisziplinären Zusammenarbeit, im speziellen in der effektiven gemeinschaftlichen Zusammenarbeit zwischen Compliance / Legal und den Entwicklungsteams. Hier ist es entscheidend, wie die Prozesse und Tools zur Compliance Überwachung gestaltet werden, denn bürokratische Hürden, komplizierte Prozesse und unverständliche, bzw. schwer zugängliche Tools können den Innovationsprozess ausbremsen.

Eine detaillierte Beschreibung dieser Anforderungen und der bereitzustellenden Capabilities wurde im Kontext der EU AI Act Analyse zusammengetragen und ist im Deep Dive zum AI Act nachzulesen.

6. Ethik

Ethisches Handeln wird von Unternehmen erwartet, weil es das Vertrauen der Öffentlichkeit stärkt und langfristige Kundenloyalität fördert[4]. Gesellschaftliche Erwartungen und regulatorische Anforderungen, wie der europäische AI Act, setzen ethische Standards durch. Unternehmen, die ethisch agieren, sind weniger anfällig für rechtliche und finanzielle Risiken und profitieren langfristig wirtschaftlich[5]. Zudem achten Verbraucher und Talente verstärkt auf das Verhalten von Unternehmen und bevorzugen jene, die verantwortungsvoll handeln[6]. Ethisches Verhalten trägt nicht nur entscheidend zur Reputation und Stabilität eines Unternehmens bei, sondern ist auch ein Schlüsselfaktor für das Gewinnen und Halten von hochqualifizierten Fachkräften, die zunehmend Wert auf ethische Arbeitsumfelder legen[7].

Angesichts dieser zunehmenden Erwartung an ethisches Handeln, das nicht nur von der Öffentlichkeit, sondern auch von regulatorischen Rahmenbedingungen wie dem AI Act vorgegeben wird, benötigen Unternehmen klare ethische Leitlinien und Frameworks, um Vertrauen und Stabilität zu sichern und somit Haftung und Reputationsverlust zu vermeiden. In diesem Kontext spielen ethische Leitlinien eine zentrale Rolle, da sie den Umgang mit Künstlicher Intelligenz in einer Weise regeln, die gesellschaftliche und regulatorische Erwartungen erfüllt.

[4] Bhattacharya, C. B., & Sen, S. (2020). Sustainability: How stakeholder engagement leads to competitive advantage. *Journal of Business Ethics*, 161(2), 317-329.
[5] Eccles, R. G., Ioannou, I., & Serafeim, G. (2019). Corporate sustainability: A strategy? *Management Science*, 65(12), 5661-5680.
[6] Jones, D. A., Willness, C. R., & Heller, K. W. (2019). Corporate social responsibility attributions and employee engagement: The role of perceived external prestige and internal respect. *Journal of Business and Psychology*, 34(2), 239-252.

[7] Gond, J. P., El Akremi, A., Swaen, V., & Babu, N. (2017). The psychological microfoundations of corporate social responsibility: A person-centric systematic review. *Journal of Organizational Behavior*, 38(2), 225-246.

Ethische Grundsätze im Umgang mit Künstlicher Intelligenz können je nach Region und kulturellem Kontext stark variieren. Während in Europa der Schwerpunkt auf dem Schutz der individuellen Rechte, wie Privatsphäre und Datenhoheit, liegt, verfolgt China einen Ansatz, der zum Beispiel die gesellschaftliche Stabilität und die Kontrolle über technologische Entwicklungen betont. Diese Unterschiede spiegeln sich in den jeweiligen ethischen Rahmenwerken wider, die festlegen, wie KI eingesetzt werden sollte.

Die Europäische Union hat spezifische ethische Leitlinien für vertrauenswürdige KI formuliert, die als Grundlage für den verantwortungsvollen Einsatz dieser Technologien dienen. Diese Leitlinien adressieren wesentliche Aspekte wie den Vorrang menschlicher Aufsicht, die technische Sicherheit, den Schutz der Privatsphäre und die Gewährleistung von Transparenz. Darüber hinaus betonen sie die Notwendigkeit von Vielfalt, Fairness und gesellschaftlicher Verantwortung.

Diese Rahmenwerke bieten eine solide Grundlage für Unternehmen, um sicherzustellen, dass ihre KI-Systeme nicht nur funktional, sondern auch ethisch vertretbar sind. Zusätzlich zu den europäischen Richtlinien existieren weitere nationale und globale Ethik-Frameworks, die Unternehmen als Orientierung dienen können.

Ethische Grundsätze in eine Governance implementieren

Es ist eine besondere Herausforderung ethische Grundsätze in konkrete KI-Anwendungen zu überführen. Es reicht nicht aus, ethische Prinzipien auf einer allgemeinen Ebene zu definieren; sie müssen vielmehr in spezifische Anwendungsfälle übersetzt werden.

Um ethische Risiken in der Unternehmens-Governance effektiv zu managen, sollte ein spezifischer Sonderprozess eingeführt werden, der sich auf KI-Anwendungen konzentriert, die ein hohes Potenzial für Reputationsrisiken aufweisen. Dieser Sonderprozess würde sicherstellen, dass besonders sensible Projekte einer intensiveren Prüfung unterzogen werden, um potenzielle Probleme frühzeitig zu identifizieren und zu adressieren.

Für besonders sensible KI-Projekte, die potenziell hohe ethische Risiken bergen, kann ein spezieller Governance-Sonderprozess etabliert werden. Dieser beginnt mit einem **Check** in der Planungsphase, bei dem mittels Risikoabschätzung oder gezielten Fragestellungen ethisch kritische Projekte identifiziert werden. Anschließend folgt ein **Ethik-Assessment**, bei dem ein spezialisiertes Ethik-Team oder Board eine detaillierte Analyse durchführt, um die ethischen Implikationen des Projekts zu bewerten. Die **Ergebnisse** dieses Assessments werden schließlich dokumentiert und in Form von Empfehlungen oder verbindlichen Vorgaben in die Projektplanung integriert. Dieser Prozess stellt sicher, dass ethische Überlegungen systematisch berücksichtigt und Risiken frühzeitig adressiert werden.

Wichtige Frameworks zur Identifizierung und Bewertung von Risiken Künstlicher Intelligenz

- **ISO/IEC JTC 1/SC 42:** Internationale Standards zur Implementierung von KI-Systemen mit Fokus auf Ethik und Fairness.
- **AI RMF (AI Risk Management Framework):** Von NIST entwickelt, bietet Richtlinien zu Sicherheit, Fairness und Transparenz.
- **AI Ethics Guidelines der EU:** Fokus auf Transparenz, Verantwortlichkeit und Datenschutz.
- **ASAM:** Bewertet Risiken algorithmischer Systeme und deren gesellschaftliche Auswirkungen.

- **AI Incident Database (AIID):** Dient der Erfassung von Fehlfunktionen und Risiken von KI-Systemen.
- **FAT/ML (Fairness, Accountability, and Transparency in Machine Learning):** Tools zur Sicherstellung von Fairness und Transparenz.
- **IEEE Ethically Aligned Design:** Entwickelt ethische Prinzipien für KI-Entwicklung und Implementierung.

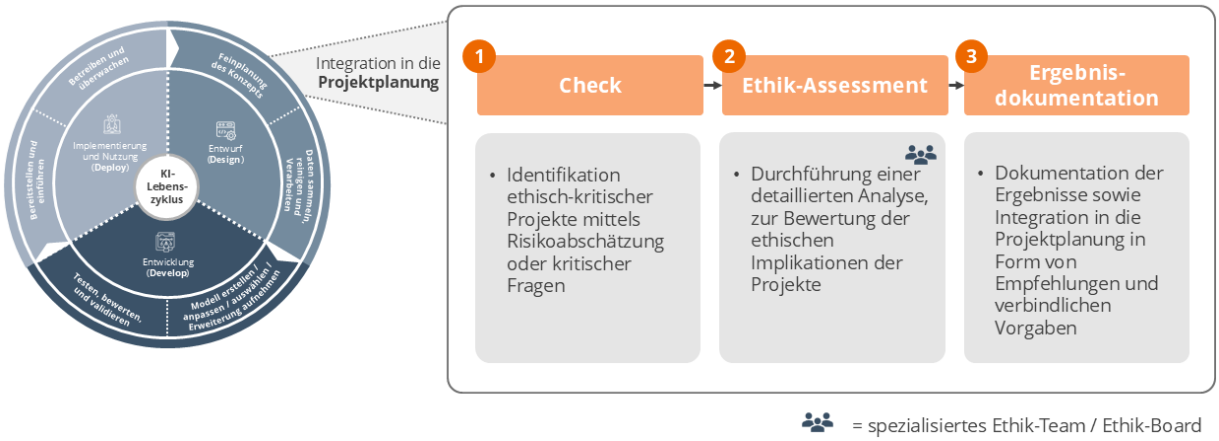

Abbildung 5: Governance Sonderprozess

7. Regulatorische Betrachtungen – Deep Dive EU AI Act

Eine effektive KI-Governance muss auf relevanten Regulierungen aufbauen, die den Einsatz von KI-Systemen beeinflussen. Im weiteren Verlauf werden wir den AI Act näher beleuchten, doch dieser ist nur eine von vielen Regulierungen, die für KI-Systeme von Bedeutung sind. Neben Datenschutz und Datensicherheit müssen auch sektor- oder lokalrelevante Vorgaben berücksichtigt werden, die je nach individuellem Anwendungsfall variieren können.

Die nachfolgenden Betrachtungen beziehen sich auf das *Gesetz über künstliche Intelligenz, in seiner Amtsblattfassung vom 13. Juni 2024*[8] und seinen Aktualisierungen bis zum 01. August 2024.

7.1 Der EU AI Act

Der AI Act ist seit dem 1. August 2024 in Kraft und markiert den ersten umfassenden Rechtsrahmen für Künstliche Intelligenz in der Europäischen Union. Ziel des Gesetzes ist es, den sicheren, transparenten und ethisch verantwortungsvollen Einsatz von KI-Systemen sicherzustellen. Für Unternehmen, die KI-Systeme auf dem Europäischen Markt entwickeln, deployen oder nutzen, bedeutet dies, dass sie ihre KI-Anwendungen an strengen Vorschriften ausrichten müssen, insbesondere wenn diese als risikoreich eingestuft werden.

Die Umsetzung des AI Acts erfolgt schrittweise: Ab Februar 2025 gilt ein Verbot für KI-Systeme, die als unannehmbares Risiko gelten. Ab August 2025 treten die Regeln für allgemeine Modelle („General Purpose AI Systems“) in Kraft, begleitet von der Ernennung der zuständigen Behörden. Bis Februar 2026 wird die Kommission Überwachungspläne für Hochrisiko-KI-Systeme vorlegen, und ab August 2026 gelten zusätzliche Verpflichtungen für

[8] EU AI Act: https://artificialintelligenceact.eu/de/

solche Systeme in sensiblen Bereichen. Diese gestaffelte Einführung des AI Acts bietet Unternehmen Zeit zur Anpassung, erfordert jedoch eine frühzeitige Integration der Regulierungen in die Unternehmensstrategie. Für international tätige Firmen ist es essenziell, den AI Act in Verbindung mit weiteren lokalen und sektoralen Vorschriften zu betrachten, um umfassend compliant zu bleiben.

Aus dem AI Act ergeben sich zahlreiche verpflichtende Prozesse, Tools sowie spezifische Rollen und Verantwortlichkeiten, die in das Governance-Framework eines Unternehmens integriert werden müssen.

Folgende Aspekte müssen für jede KI-Anwendung im Unternehmen bestimmt werden:

- Alle KI-Systeme, die unter die Definition von KI gemäß dem AI Act fallen, müssen sorgfältig auf mehrere Schlüsselfaktoren überprüft werden. Zunächst ist zu klären, ob das System tatsächlich unter die Definition von KI im Sinne des AI Acts fällt. Anschließend muss der territoriale Anwendungsbereich geprüft werden, da der AI Act sowohl für Anbieter gilt, die KI-Systeme innerhalb der Union bereitstellen oder in Betrieb nehmen, als auch für solche, die ihren Sitz in einem Drittland haben, sofern das durch das KI-System erzeugte Ergebnis in der Union verwendet wird. Es ist ebenfalls entscheidend zu bestimmen, welche Rolle das Unternehmen im Zusammenhang mit dem KI-System einnimmt, sei es als Anbieter, Entwickler oder Nutzer. Darüber hinaus muss untersucht werden, ob das System ein General-Purpose AI (GPAI) Modell enthält. Schließlich ist die Risikoeinstufung der Anwendung zu analysieren.
- Neben dem AI Act können lokale und sektorale Regularien massiv die Entwicklung von KI-Modellen beeinflussen und müssen sorgfältig überprüft werden. Hierzu gehören unter anderem die Datenschutzgrundverordnung, die Maschinenrichtlinie, die Produkthaftungsrichtlinie und die Richtlinie für allgemeine Produktsicherheit. Je nach Sektor können noch relevante industrie-spezifische Richtlinien und Umweltauflagen geltend werden.

7.2 Rolle eines Unternehmens im Sinne des EU AI Acts

Im Allgemeinen existieren derzeit drei verschiedene Arten von KI-Modellen in Unternehmen, die jeweils unterschiedliche Governance-Anforderungen nach dem AI Act haben. Diese drei Arten können nach der jeweiligen Verantwortung in der Lieferkette abgeleitet werden. Die Verantwortung eines Unternehmens variiert je nach Rolle (AI Act), die es im Umgang mit dem jeweiligen Modell übernimmt. Diese Rollen bestimmen den Zugang zur Governance, insbesondere in Bezug auf die Registrierung und Risikokategorisierung der KI-Systeme.

1. **Provider**: Das Unternehmen entwickelt ein KI-Modell selbst oder nimmt eine signifikante Änderung an einem bestehenden Modell vor (z.B. durch Finetuning) oder vertreibt es unter eigenem Namen oder Marke.

   Der AI Act definiert einen Provider als jede Person, die ein KI-System entwickelt oder entwickeln lässt und es mit dem Ziel bereitstellt, es auf den Markt zu bringen oder in Betrieb zu nehmen. In dieser Rolle trägt das Unternehmen die volle Verantwortung für die Einhaltung aller regulatorischen Vorgaben und die Konformität des Systems.

2. **Distributor**: Wenn das Unternehmen ein KI-Modell ohne signifikante Änderungen weiterverkauft oder hostet, wird es zum Distributor.

   Laut AI Act stellt ein Distributor ein KI-System zur Verfügung, ohne dass dabei wesentliche Änderungen vorgenommen werden. Diese Rolle umfasst vor allem die Sicherstellung der Compliance, aber weniger technische Verantwortung als beim Provider.

3. **Deployer**: Nutzt ein Unternehmen ein KI-Modell im geschäftlichen Kontext, beispielsweise zur Automatisierung von Prozessen oder für die Kundeninteraktion, wird es zum Deployer.

   Der AI Act definiert einen Deployer als jede Person, die ein KI-System verwendet, insbesondere im Rahmen einer kommerziellen Tätigkeit. Diese Rolle verlangt, dass das Unternehmen die Nutzung des Systems überwacht und sicherstellt, dass es den vorgesehenen Zwecken entsprechend und sicher betrieben wird. Die Herausforderung für Unternehmen besteht darin, dass vorhandene Systeme und Tools, die in den Arbeitsprozessen verwendet werden, wie zum Beispiel ein Online-Kollaborationstool in ihren Dienst ein KI-System integriert. Häufig wird nicht der Einkauf, sondern der Endnutzende darüber informiert. Da Unternehmen ein Risiko-Assessment für alle KI-Anwendungen durchführen müssen, in deren Wertschöpfungskette sie sich befinden, müssen Prozesse zum Risiko-Assessment aller KI-Systeme entwickelt werden und ausreichend Awareness bei allen Mitarbeitenden geschaffen werden, diese Prozesse zu bedienen. (Siehe auch „Neue Anforderungen und Capabilities, die für die erfolgreiche KI-Einführung notwendig sind“)

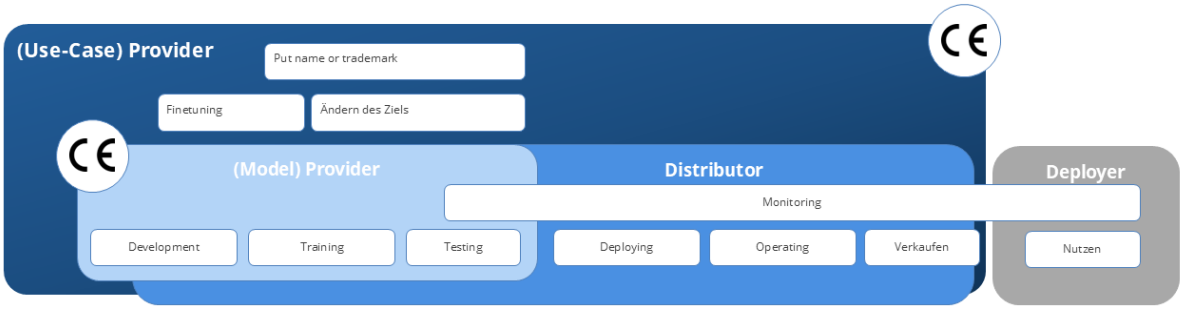

Abbildung 6: Rollen

Alle Szenarien erfordern einen klaren Zugang zur Governance, der die Registrierung und Risikokategorisierung nach dem AI Act einschließt, sowie die Dokumentation der Compliance-Maßnahmen.

Der AI Act unterscheidet zwischen KI-Modellen und KI-Systemen, wobei beide Konzepte unterschiedliche Anforderungen an die Governance stellen. Ein KI-Modell umfasst die Algorithmen und Techniken, die für bestimmte Aufgaben entwickelt werden, wird jedoch in der Regel nicht direkt an Endnutzer bereitgestellt. Stattdessen wird es in ein KI-System integriert, das zusätzliche Komponenten wie Benutzeroberflächen und technische Infrastruktur enthält, um das Modell für den praktischen Einsatz nutzbar zu machen.

Ein Beispiel für diese Unterscheidung sind Systeme wie ChatGPT oder Microsoft Copilot, die auf dem GPT-4-Modell von OpenAI basieren. Während das GPT-4-Modell die eigentliche Rechenarbeit erledigt, stellen KI-Systeme wie ChatGPT die Verbindung zu den Endnutzern her, indem sie eine benutzerfreundliche Schnittstelle anbieten.

Um sowohl KI-Modelle als auch KI-Systeme effektiv zu regulieren, müssen Governance-Systeme flexibel gestaltet sein. Diese Systeme müssen in der Lage sein, die Kontrolle über die Entwicklung und Nutzung von KI-Modellen sicherzustellen, insbesondere in Umgebungen, in denen sowohl zugekaufte als auch selbst entwickelte Modelle eingesetzt werden.

7.3 Die Ermittlung der Anforderungen auf Basis des AI Acts

Was wird reguliert:

Laut AI Act ist KI ein "System, das auf maschinellem Lernen oder anderen Techniken basiert und darauf ausgelegt ist, mit unterschiedlichem Grad an Autonomie Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern würden". Systeme, die unter diese Definition fallen sind daher regulierungsbedürftig.

Welche verschiedenen KI-Systeme werden reguliert?

Neben der oben genannten Definition von KI wird zusätzlich noch GPAI definiert:

GPAI-Modelle (General Purpose AI-Modelle) werden definiert als KI-Modelle, die:

- Mit einer großen Menge an Daten unter Verwendung von selbstüberwachendem Lernen im großen Maßstab trainiert wurden.
- Eine erhebliche Allgemeinheit aufweisen, d.h. sie können kompetent eine Vielzahl unterschiedlicher Aufgaben ausführen.
- In eine Vielzahl von nachgelagerten Systemen oder Anwendungen integriert werden können.

Zeitplan der Umsetzungsanforderungen:

Die Umsetzung des AI Act erfolgt in verschiedenen Phasen, um Unternehmen ausreichend Zeit zur Anpassung zu geben:

- **August 2024:** Der AI Act tritt offiziell in Kraft.
- **Februar 2025:** Verbot von KI-Anwendungen, die in die Kategorie "unannehmbares Risiko" fallen. Für Unternehmen bedeutet das die Auflage, eine Inventur aller KI-Systeme durchzuführen, um KI-Systeme vom Markt zu nehmen, welche unter die verbotenen Praktiken fallen könnten.
- **Mai 2025:** Fertigstellung von Verhaltenskodizes für allgemeine KI.
- **August 2025:** Anwendung der Regeln für allgemeine KI und Ernennung der zuständigen Behörden. Für Unternehmen bedeutet dies, dass sichergestellt werden muss, dass GPAI-Modelle ein CE-Zeichen besitzen und für die entsprechende Anwendung verwendet werden können.
- **Februar 2026:** Vorlage der Spezifikation der Richtlinien zur praktischen Umsetzung des AI Acts inklusive von Überwachungsplänen für Hochrisiko-KI-Systeme.
- **August 2026:** Anwendung der Verpflichtungen für Hochrisiko-KI-Systeme in spezifischen Bereichen. Für Unternehmen bedeutet dies, dass eine vollständige, nach EU-Standards ausgerichtete KI-Governance im Unternehmen implementiert sein muss.
- **August 2027:** Hochrisiko-KI-Systeme, die in sicherheitskritischen Bereichen eingesetzt werden, müssen zusätzliche Sicherheitskomponenten implementieren. Für unternehmen bedeutet dies eine Erweiterung ihrer KI-Governance
- **Ende 2030:** Verpflichtungen für den großflächigen Einsatz bestimmter KI-Systeme in IT-Infrastrukturen.

Wie wird reguliert:

Zunächst muss geklärt werden, ob die KI im **territorialen Scope** des AI Acts liegt:

Bereitstellung und Inverkehrbringen in der EU:

- Der AI Act gilt für KI-Systeme, die auf dem europäischen Markt angeboten oder in Betrieb genommen werden, unabhängig davon, wo sie entwickelt wurden.

Nutzung und Auswirkungen innerhalb der EU:

- KI-Systeme, die außerhalb der EU entwickelt oder bereitgestellt werden, unterliegen ebenfalls dem AI Act, wenn die Ergebnisse dieser Systeme in der EU genutzt werden oder wenn das System auf Personen oder Unternehmen in der EU einen Einfluss hat.

Als nächstes gilt, zu analysieren, ob das KI-System zu den **verbotenen Praktiken** (Artikel 5) gehört, oder es sich um eine Ausnahme handelt.

Im Weiteren müssen drei Aspekte analysiert werden:

1. ob das System auf Basis eines oder mehreren GPAI-Modellen entwickelt wurde (Artikel 3 (63)).
2. In welcher Rolle sich das Unternehmen befindet (Artikel 3 (3/4)).
3. Welche Risiko-Klassifizierung der Anwendung zuzuordnen ist (Artikel 6, Annex I & II, Artikel 50).

Aus dieser Analyse können dann die Anforderungen an den speziellen Use Case abgeleitet werden.

7.4 Resultierende Anforderungen der regulatorischen Umsetzung für Unternehmen

Folgende Fähigkeiten müssen in Unternehmen entwickelt werden, um den effektiven Umgang mit KI-Anwendungen und Regulatorik sicherzustellen:

Definition der (regulatorischen) Anforderungen

Die Risikoklassifizierung eines KI-Systems bestimmt den Umfang der Compliance-Maßnahmen:

- Durch den Einsatz von KI-Systemen und die damit verbundenen regulatorischen Anforderungen, wie dem AI Act, wird es notwendig, bereits zu Beginn des KI-Lebenszyklus Klarheit über die Einhaltung von Compliance-Vorgaben zu schaffen, damit Aufwände und Ressourcen schon zu Beginn abgeschätzt werden können, oder durch verschiedene (technische / architektonische) Entscheidungen das Risiko minimiert werden kann.
- Falls ein externes KI-Modell eingesetzt wird, muss darüber hinaus sichergestellt werden, dass dieses Modell den festgelegten Compliance-Anforderungen entspricht. Die Lizenzbedingungen und zukünftig die CE-

Kennung des Modells müssen gründlich geprüft werden, um sicherzustellen, dass das System für den vorgesehenen Einsatz legal und regelkonform ist.

Anforderungen und Fähigkeiten:

- Standardisierung der Risikobewertung: Zunächst muss eine Möglichkeit geschaffen werden, die Risiko-Höhe standardisiert einzuordnen und zu dokumentieren.
- Überprüfung und Validierung externer KI-Modelle: Dazu gehört das Verständnis der Lizenzbedingungen und der rechtlichen Rahmenbedingungen, sowie, die CE-Kennzeichnung zu bewerten und sicherzustellen, dass das Modell die gesetzlichen Vorschriften und Compliance-Anforderungen erfüllt.
- Teams müssen in der Lage sein, technische und rechtliche Anforderungen zu analysieren und zu kombinieren, bzw. strategische Pläne und Entscheidungen über die Minimierung von Risiken zu entwickeln und in die Projektplanung einzubeziehen. Auf Basis dessen muss eine möglichst realistische Ressourcenabschätzung generiert werden.

Eigenentwicklung vs. Fremdservice von General Purpose AI Modellen

Basieren Use Cases auf einem GPAI-Modell, kommen für solche Modelle zusätzlich zu den Risikoklassen-Anforderungen und den Rollendefinitionen noch spezifischen Modellanforderungen hinzu. Diese müssen künftig entweder vom Unternehmen selbst eingehalten oder über den externen Modellprovider durch Lizenzprüfungen abgeklärt werden. Dies ist besonders wichtig, da Provider für bestimmte Use Cases oder Risikoklassen ihre Modelle zukünftig ausschließen können, wenn sie die Anforderungen nicht erfüllen.

Unternehmen müssen sicherstellen, dass alle Lizenzanforderungen für KI-Modelle, die von externen Anbietern bezogen werden, gründlich geprüft werden. Die eingesetzten Modelle müssen daraufhin geprüft werden, ob sie für den vorgesehenen Use Case und die jeweilige Risikoklasse geeignet sind. Dies erfordert eine detaillierte Evaluierung sowohl der technischen Spezifikationen als auch der rechtlichen Anforderungen an das Modell.

Anforderungen und Fähigkeiten:

- Wenn Unternehmen auf Eigenentwicklung setzen, müssen sie die Fähigkeit, Prozesse und Tools entwickeln, ihre Modelle so zu gestalten, dass sie den regulatorischen und technischen Anforderungen gerecht werden.
- Unternehmen, die auf Fremdservice setzen, müssen die Fähigkeit entwickeln, Partnerschaften mit Modellanbietern zu pflegen, bzw. die Prozesse hierfür zu entwickeln. Dies umfasst, Lizenzüberprüfungen, Vertragsverhandlungen, die Klärung, ob das Modell langfristig den Anforderungen des Unternehmens gerecht werden kann und ggf. regelmäßige Audits.

Mandatierung

Mandatierung bezieht sich auf die offizielle Ermächtigung und Verpflichtung, bzw. Erlaubnis des Unternehmens oder bestimmter Akteure, die KI- Anwendung zu entwickeln.

KI-Initiativen sind komplex, interdisziplinär und mit potenziellen Risiken verbunden – wie Datenschutzverletzungen, algorithmische Verzerrungen oder Sicherheitsprobleme. Des Weiteren ist die Berechnung des ROI einer KI-Anwendung kompliziert. Die Mandatierung schafft eine zentrale Instanz oder einen zentralen Prozess, der Entwicklungsteams dazu berechtigt eine Anwendung zu entwickeln, Entscheidungen darüber zu treffen, überblickt,

ob die Risiken für das Unternehmen ausreichend gemanagt oder mitigiert werden können und sicherzustellen, dass KI-Systeme den festgelegten Anforderungen gerecht werden.

Risikobewertung und ROI-Analyse: Für die Mandatierung muss die Integration der Risiko- und Rollenbewertung in die strategische Planung und die Finanzanalyse sichergestellt werden. Dies bedeutet, dass das Risiko-Assessment gemeinsam mit dem erwarteten Return on Investment (ROI) analysiert und als Grundlage für Mandatierungsentscheidungen verwendet wird. Denn KI-Systeme werden gemäß dem AI Act in Risikoklassen eingeteilt. Eine höhere Risikoklassifizierung bedeutet höhere Compliance- Anforderungen. Bei der Mandatierung wird die Risikohöhe und die zu erwarteten Kosten hierzu, und eine präzise Rollendefinition für die daraus resultierenden Verantwortlichkeiten vorgelegt.

Anforderungen und Fähigkeiten:

- Es muss eine standardisierte Berechnung des ROI erstellt werden, die es ermöglicht, dass die finanzielle Bewertung eines KI-Projekts in Verbindung mit der Risikoeinschätzung betrachtet wird.
- Es muss eine zentrale Instanz oder ein Prozess eingerichtet werden, das berechtigt ist und berechtigt, KI-Projekte zu genehmigen oder abzulehnen. Diese Instanz trägt die Verantwortung dafür, zu entscheiden, ob ein KI-System entwickelt und eingesetzt wird. Sie stellt sicher, dass alle Compliance-Anforderungen, strategischen Ziele und Risikobewertungen umfassend berücksichtigt werden und dass die Investition für das Unternehmen tragfähig ist.
- Für jede Mandatierung müssen präzise Verantwortlichkeiten und Rollen definiert werden. Dies bedeutet, dass die Personen, die für die Risikobewertung, die Compliance-Überwachung und die Entwicklung eines KI-Systems verantwortlich sind, festgelegt werden. So wird sichergestellt, dass klare Zuständigkeiten bestehen und die Verantwortung für den gesamten Prozess übernommen wird.

Konformitäts-Assessment

Durch den AI Act und andere regulatorische Vorschriften werden die meisten KI-Systeme zukünftig spezifischen Auflagen unterliegen, abhängig von ihrer Risikoklassifizierung. Nur für Systeme mit minimalem Risiko ist ein White Listing vorgesehen, während für alle anderen Systeme umfassendere Compliance-Prüfungen und -Prozesse erforderlich sind. Diese Anforderungen müssen künftig vor dem Launch überprüft werden, hierzu werden interne Prozesse notwendig, auch externe Auditierungen können notwendig werden.

Anforderungen und Fähigkeiten:

- Unternehmen müssen für alle Risikoklassen passende Prozesse zur Einhaltung von Compliance-Vorgaben entwickeln.
- Für KI-Systeme, die als hohes Risiko eingestuft werden, schreibt der AI Act vor, dass diese einer externen Prüfung durch eine benannte Stelle (Notified Body) unterzogen werden müssen, um sicherzustellen, dass sie den regulatorischen Anforderungen entsprechen.
- Unternehmen müssen nicht nur vor dem Launch eines KI-Systems, sondern auch kontinuierlich während des gesamten Lebenszyklus sicherstellen, dass die Compliance-Vorgaben eingehalten werden. Dies erfordert eine fortlaufende Überwachung und gegebenenfalls erneute Konformitätsbewertungen, insbesondere bei signifikanten Änderungen des Systems.

- Die Auflagen zur Erstellung und Verwaltung technischer Dokumentationen müssen erfüllt sein und revisionssicher eingehalten werden.
- Die Fähigkeiten und Prozesse zur Kooperation mit einem externen Notified Bodies, die für die Zertifizierung von Hochrisiko-KI-Systemen zuständig sind. Diese Zusammenarbeit umfasst die Bereitstellung aller notwendigen Unterlagen und die Durchführung von Audits in Zusammenarbeit mit den externen Prüfern.
- Die Fähigkeit zur Identifikation von signifikanten Änderungen an KI-Systemen und rechtzeitig eine erneute Konformitätsbewertung anzustoßen, wenn diese Änderungen die regulatorischen Anforderungen beeinflussen könnten.

Überwachung, Überprüfung und Monitoring

Da viele KI-Modelle, insbesondere solche mit hohem Risiko (z.B. GPAI-Modelle mit systemischem Risiko), strikten Auflagen unterliegen, müssen diese fortlaufend auf ihre Konformität überprüft werden. Einmalige Prüfungen vor dem Einsatz reichen oft nicht aus, da KI-Systeme dynamisch sind und durch neue Daten oder Änderungen im Umfeld kontinuierlich neu bewertet werden müssen. Unternehmen müssen daher zentrale Einheiten schaffen, die das Risiko, die Compliance und mögliche Incidents überwachen, aber auch für die interne Bewertung ist das Monitoring wichtig. Die Meldepflicht an die EU bei Zwischenfällen erfordert darüber hinaus ein schnelles und strukturiertes Incident-Management.

Anforderungen und Fähigkeiten:

- Unternehmen sollten eine zentrale Einheit oder Prozesse einrichten, die das Risiko und die Compliance-Aktivitäten aller KI-Systeme überwacht. Diese Risiken sollten proaktiv überwacht werden, um potenzielle Probleme frühzeitig zu identifizieren. Dies erfordert spezialisierte Tools zur Risikoüberwachung, die kontinuierlich alle relevanten KPIs und Compliance-Anforderungen überwachen.
- Unternehmen müssen ein strukturiertes Incident-Management-System implementieren, das es ermöglicht, Vorfälle, die im Zusammenhang mit KI-Systemen auftreten, sofort zu erkennen, zu dokumentieren und an die zuständigen Behörden der EU zu melden.

Training, Awareness und Wissen

Mit dem zunehmenden Einsatz von KI-Systemen in Unternehmen müssen sowohl Endnutzer als auch Mitarbeitende laut AI Act über ausreichende AI Literacy verfügen, um den richtigen Umgang mit diesen Technologien zu gewährleisten. Zusätzlich tragen ein fundiertes Schulungsangebot und kontinuierlicher Wissenstransfer entscheidend zur Förderung von KI im Unternehmen im Sinne eines erfolgreichen Change-Managements bei.

Wenn Mitarbeitende und Führungskräfte umfassend geschult sind und die Vorteile, Risiken und Einsatzmöglichkeiten von KI-Technologien verstehen, wird nicht nur die Akzeptanz der neuen Systeme gesteigert, sondern auch das Vertrauen in deren Nutzung gefördert. Dies hilft, Widerstände gegen den Wandel zu minimieren, da Unsicherheiten abgebaut und konkrete Anwendungsbeispiele aufgezeigt werden können. Ein hohes Wissensniveau und praxisorientierte Schulungsangebote sorgen dafür, dass die Einführung von KI nicht als Belastung, sondern als Chance zur Optimierung wahrgenommen wird.

Anforderungen und Fähigkeiten:

- Entwicklung von praxisorientierten Schulungen, die auf die jeweiligen Aufgaben und Verantwortlichkeiten der Mitarbeitenden abgestimmt sind.
- Mitarbeitende und Endnutzende, die in direkten Kontakt mit KI-Systemen kommen, müssen über deren Funktionen und Einschränkungen informiert werden. Hierzu müssen Mechanismen und Prozesse entwickelt werden, um offen und transparent über den Einsatz von KI-Technologien zu kommunizieren. Dies erfordert die Fähigkeit, technische Informationen so aufzubereiten, dass sie für Nicht-Experten verständlich sind und die richtigen Erwartungen gesetzt werden.

8. Der KI-Lebenszyklus und die Governance

Der Lebenszyklus einer KI-Lösung umfasst alle Phasen, die eine KI-Anwendung von der Konzeptplanung bis zur Bereitstellung und dem laufenden Betrieb durchläuft. Der Prozess ist kontinuierlich und iterativ, was bedeutet, dass eine KI-Lösung regelmäßig überwacht und verbessert wird, um den sich eventuell wandelnden Anforderungen und Daten gerecht zu werden.

Übersicht

Der Entwurf einer KI-Lösung stellt die konzeptionelle Grundlage dar. In dieser Phase wird die KI-Lösung entsprechend des Anforderungsprofils geplant und spezifiziert. Dies umfasst die genaue Feinplanung des Konzepts sowie die Zusammenstellung der für die Anwendung erforderlichen Daten. Diese Daten werden ggf. durch eine notwendige Reinigung und Verarbeitung vorbereitet, um eine optimale Grundlage für die Entwicklung zu schaffen.

In weiterem werden die einzelnen Phasen systematisiert beschrieben:

- **Fokus** beschreibt die Besonderheit an dieser Phase im Lebenszyklus, und worauf ein besonderes Augenmerk gelegt werden sollte.
- **Interne und externe Anforderungen** beschreiben KI-spezifischen Anforderungen im Sinne der Ergänzung zu generellen Anforderungen an IT-Systeme, Produkte und Services.
- **Betroffene Prozesse** beschreiben, welche Prozessen im Unternehmen durch die Einführung einer KI-Lösung beeinflusst werden.
- **Artefakte** beziehen sich auf die hier im Whitepaper erfolgte Zusammenstellung an Tools, Methoden, Dokumenten und Werkzeugen. Sie müssen neu, als Teil der zu etablierenden KI Governance (speziell für KI-Anwendungen) entwickelt werden und haben unternehmensspezifischen Charakter.

8.1 Holistische Bewertung und Einordnung des Business Demands

Die präzise und systematische Demand-Analyse ist eine der entscheidenden Grundlagen für den erfolgreichen Einsatz und die Steuerung von KI im Unternehmenskontext. Sie ermöglicht es die Notwendigkeit und Machbarkeit von KI-Einsätzen präzise zu bewerten und strategische Fehlinvestitionen zu vermeiden. Durch eine fundierte Analyse werden sowohl technische als auch organisatorische Risiken frühzeitig erkannt, was die erfolgreiche

Integration von KI-Lösungen in bestehende Geschäftsprozesse sicherstellt und langfristig Wettbewerbsvorteile schafft. Außerdem soll hier sichergestellt werden, dass ein Problem oder einen Bedarf (Need) erkannt wird und dann realistisch zu bewerten, ob der Einsatz von KI überhaupt sinnvoll ist. Diese frühzeitige Prüfung stellt sicher, dass nur dann KI implementiert wird, wenn es klare Vorteile und Mehrwerte für das Unternehmen gibt. Zudem hilft die Demand-Analyse, alle relevanten Dimensionen – wie Kosten, technische Anforderungen, organisatorische Auswirkungen und ethische Überlegungen – realistisch zu berechnen.

8.2 Das Demand Management

Unternehmen haben es derzeit schwer den Wert einer KI zu messen. Dies liegt vor allem an folgenden Punkten:

- Der Einfluss einer KI ist kaum abzugrenzen und zu isolieren, zum Beispiel kann schwer erkannt werden, ob der Umsatzanstieg durch eine verbessere Nutzungserfahrung oder den Einsatz von KI kommt[9]. Viele Vorteile wie Kundenzufriedenheit, Risikomanagement oder Markentreue sind schwer monetär messbar, tragen aber zu langfristigem Wachstum bei[10],[11]. Auf der anderen Seite kann ein unsachgemäßer Einsatz von KI genau diese Bereiche schädigen, der tatsächliche Einfluss ist hier aber oft erst nach Monaten oder Jahren messbar.
- Die Implementierung von KI erfordert oft umfangreiche Investitionen in Dateninfrastruktur, Fachkräfte und Werkzeuge, was die Berechnung der Kosten erschwert. Dazu kommen hohe Wartungs- und Weiterentwicklungskosten, die den ROI weiter verzögern können.[12]
- Auch der Aufbau von KI-Governance, Cybersecurity, ein geeignetes Datenmanagement kann zunächst hohe Kosten erfordern.
- Eine besondere Herausforderung besteht auch darin, dass eine nicht ausreichende Betrachtung der Risiken und Kosten, die durch die verschiedenen Implikationen einer Anwendung aufkommen, der ROI nachträglich stark abweicht. Dies betrifft vor allem die Compliance Kosten. Fällt eine Anwendung in den Hoch-Risiko Bereich ist mit hohen Compliance Kosten zu rechnen. Eine frühe Transparenz – schon im Demand-Prozess ist kritisch, um die Anwendung entweder in ihrem Aufbau anders zu planen oder die Kosten in den ROI möglichst realistisch einzubinden.

Auf Basis dieser Erkenntnis entstand ein Framework, nach welchem sich der ROI einer Anwendung analysieren lässt:

Business Case

Im ersten Schritt wird im Rahmen des Business Case geprüft, ob KI eingesetzt werden soll und ob ein Produkt oder Prozess durch KI angereichert wird. Es wird untersucht, welchen Mehrwert die KI-Lösung für das Unternehmen generiert und wie sie in den übergeordneten Geschäftsprozess eingebettet werden kann. Ein wichtiger Aspekt ist hierbei die Frage, ob sich der Einsatz von KI lohnt und ob durch den Einsatz von KI der Return on Investment (ROI) maximiert werden kann.

Zentrale Fragen:

- Welche spezifischen Probleme oder Herausforderungen soll die KI-Lösung lösen?
- Welche quantifizierbaren Vorteile bietet der Einsatz von KI gegenüber bestehenden Lösungen?

[9] PwC. Defining and Measuring Return on Investment for AI. LINK
[10] AiExponent. AI Return on Investment: How to Measure the Business Value of AI. LINK
[11] Slalom. ROI in AI: Measure Value to Deliver Value. LINK
[12] Wallaroo.AI. Why 90% of AI Projects Fail to Hit ROI Targets (And What to Do About It). LINK

- Wie wird der Erfolg der KI-Lösung im Kontext des Business Case gemessen?

Compliance

Ein wesentlicher Bestandteil des Anforderungsprofils ist die Compliance. Hier wird geprüft, welche regulatorischen Vorgaben (territorial oder sektoral) bei der Entwicklung und Implementierung der KI-Lösung zu beachten sind. Es geht darum, sicherzustellen, dass die Lösung alle relevanten Gesetze und Regelungen einhält. Außerdem sollten hier Haftungsrisiken betrachtet werden, die bei einem Ausfall oder Fehlverhalten eingegangen werden.

Bevor KI-Lösungen eingesetzt werden, die Arbeitnehmer direkt betreffen, muss der Betriebsrat als Vertreter der Mitarbeiterinteressen einbezogen werden. Dies ist erforderlich, um sicherzustellen, dass die Lösung in Übereinstimmung mit den Arbeitsgesetzen und den Rechten der Arbeitnehmer implementiert wird. Die frühzeitige Beteiligung des Betriebsrats fördert nicht nur das Vertrauen der Belegschaft, was in Zeiten des Fachkräftemangels wichtig ist für den Talenterhalt, sondern stellt auch sicher, dass die KI-Anwendung keine negativen Auswirkungen auf die Arbeitsbedingungen hat.

Die rechtlichen Anforderungen, die eine KI-Lösung erfüllen muss, hängen stark von den jeweiligen Geschäftsfeldern, Standorten und den gewählten Bereitstellungsoptionen ab. Unterschiedliche territoriale und sektorspezifische Vorschriften erfordern eine genaue Analyse, um sicherzustellen, dass die KI-Lösung rechtskonform implementiert wird. Dies sollte dringend vor der Entwicklung der Anwendung berücksichtigt werden, um zum Teil hohe Haftungszahlungen zu vermeiden.

Wie zuvor und im Kapitel AI Act beschrieben, sollte im Demand-Prozess die Risikoklassifizierung auf Basis des AI Acts durchgeführt werden. Diese bestimmt die Anforderungen an die Anwendung.

Zentrale Fragen:

- Welche spezifischen Vorschriften und Gesetze müssen für die Implementierung der KI-Lösung eingehalten werden (z.B. DSGVO, AI Act)?
- Sind internationale Regularien relevant, falls die Lösung global eingesetzt wird?
- Welche kontinuierlichen Kosten müssen für die Anwendung für die Compliance mit einberechnet werden?

Qualitätsmanagement

Das Qualitätsmanagement stellt sicher, dass die KI-Lösung den Business-Anforderungen entspricht und die erwartete Qualität über den gesamten Lebenszyklus hinweg gewährleistet ist. Datenqualität und Vorhersagequalität sind dabei zentrale Faktoren. Eine hohe Datenqualität bildet die Grundlage für präzise und verlässliche Ergebnisse der KI-Modelle. Um konsistente Qualitätsstandards zu sichern, ist eine umfassende Normierung erforderlich, die eine einheitliche Bewertung und Überwachung der Lösung über verschiedene Systeme und Prozesse hinweg ermöglicht:

In einigen Branchen existieren bereits spezifische Normierungsanforderungen, die auf KI-Systeme angewendet werden können. Für Unternehmen ist es wichtig, diese Anforderungen frühzeitig zu integrieren, da dies nicht nur Vertrauen in die Technologie schafft, bzw. bei Partnern vorausgesetzt wird, sondern auch die Skalierbarkeit und Anpassungsfähigkeit der Lösung verbessert.

Ein weiterer Schwerpunkt des Qualitätsmanagements ist die Implementierung von Test-, Trainings- und Betriebsverfahren, um sicherzustellen, dass die KI-Lösung auch im laufenden Betrieb stabil und verlässlich bleibt. Regelmäßige Tests und Schulungen minimieren das Risiko von Bias oder dem Abdriften von Modellen. Automatisierte Systeme zur Überwachung der Datenqualität helfen, korrekte und konsistente Vorhersagen zu gewährleisten.

Für Unternehmen, die KI-Lösungen in sensiblen Bereichen einsetzen, ist es besonders wichtig, dass durch das Qualitätsmanagement potenzielles Fehlverhalten oder Reputationsschäden vermieden werden. Dies erhöht nicht nur die Effizienz, sondern schützt auch vor rechtlichen und ethischen Risiken.

Zentrale Fragen:

- Können wir für die spezifische Anwendung Konsistenz und Zuverlässigkeit der Datenqualität gewährleisten? Sind die Daten vollständig und korrekt?
- Wie oft und durch welche Prozesse wird die Leistung der KI-Lösung überprüft und validiert? Sind diese Prozesse bereits etabliert?
- Welche Qualitätsstandards werden für die Implementierung der KI-Lösung festgelegt (z.B. ISO-Normen, interne Richtlinien)?

Business-Anforderungen

Die Business-Anforderungen beschreiben, welchen Mehrwert die KI-Lösung für das Unternehmen oder das Produkt liefert. Hier wird bewertet, welche Kompetenzen im Unternehmen vorhanden sind oder entwickelt werden müssen, um die KI-Lösung effektiv umsetzen zu können. Darüber hinaus müssen die Risiken bewertet werden, die mit der Einführung der KI-Anwendung einhergehen, insbesondere im Hinblick auf potenzielle betriebliche Herausforderungen. Dies sollte immer im Zusammenhang mit dem Compliance-Risiko betrachtet werden.

Der Wert einer KI-Lösung wird anhand ihres Beitrags zum Unternehmensergebnis bemessen. Dies bedeutet, dass die Lösung einen klaren, messbaren Mehrwert liefern muss, der in Einklang mit der übergeordneten Unternehmensstrategie und dem bestehenden Produktportfolio steht.

Neben den Vorteilen müssen auch potenzielle Risiken berücksichtigt werden, die mit der Einführung einer KI-Lösung einhergehen. Diese Risiken umfassen betriebswirtschaftliche, technische, regulatorische und ethische Aspekte. Diese sollten sich aus den anderen Dimensionen ergeben und abgeleitet werden. In dieser Dimension werden sie dann monetär berechnet.

Zentrale Fragen:

- Welche operativen Veränderungen sind notwendig, um die KI-Lösung effizient im Unternehmen zu nutzen?
- Ist zur Erfüllung der Business Anforderungen notwendig, den Geschäftsprozess oder das Produkt durch KI anzureichern?
- Wie beeinflusst die Einführung der KI-Lösung die bestehenden Geschäftsprozesse oder Strukturen? Wie „bereit“ ist das Unternehmen für die Einführung?

Lösungsanforderungen

Die Lösungsanforderungen beschäftigen sich mit der Frage, wie die technische Lösung so gestaltet werden kann, dass sie optimal auf die bestehenden Anforderungen abgestimmt ist.

Bei der Einführung von KI-Lösungen muss eine Abwägung zwischen dem Potenzial der Technologie und den möglichen Risiken erfolgen. KI-Lösungen können in verschiedenen Formen im Unternehmen integriert werden. Sie finden sich in Produkten, spezifischen Features oder als SaaS-Lösungen (Software-as-a-Service). Ein weiterer zentraler Entscheidungspunkt ist die Frage, ob eine KI-Lösung gekauft, eine bestehende Lösung erweitert oder eine neue Lösung eigenentwickelt werden soll. Diese Entscheidung hängt von den Ressourcen, der zeitlichen Dringlichkeit und den langfristigen Zielen des Unternehmens ab. Die erfolgreiche Einführung und der Betrieb einer KI-Lösung erfordern spezifische Kompetenzen im Unternehmen. Diese umfassen sowohl die technischen Fähigkeiten zur Implementierung der Lösung als auch das Wissen, wie die notwendige Infrastruktur bereitgestellt und gewartet wird. Unternehmen müssen sicherstellen, dass das interne Know-how vorhanden oder entwickelt wird.

Zentrale Fragen:

- Welche Form der KI-Lösung (Produkt, Feature oder SaaS) passt am besten zur aktuellen Geschäftsstrategie des Unternehmens und zum Anwendungsfall?
- Welche Ressourcen (Mitarbeiter, Budget, Zeit) sind erforderlich, um die KI-Lösung zu implementieren und zu betreiben?
- Soll die KI-Lösung gekauft, eine bestehende Lösung erweitert oder eine komplett neue Lösung eigenentwickelt werden, um das aktuelle Problem zu lösen?
- Wie skalierbar ist die Lösung?

Bereitstellungsoptionen

Aus der Analyse und Betrachtung der Business Demands und den Anforderungen des Business Case lassen sich die passenden Bereitstellungsoptionen für die KI-Lösung ableiten.

Die Bereitstellungsoption einer KI-Lösung richtet sich nach ihrem Anwendungszweck. Handelt es sich um eine Lösung, die beispielsweise Vorhersagen treffen soll (wie Wartungsintervalle für Maschinen), oder um eine Lösung, die Artefakte wie Bilder oder Texte generiert (etwa Untertitel für Videos)? Ein weiterer wichtiger Faktor bei der Wahl der Bereitstellungsoption ist die Abwägung von Kosten und Nutzen. Die Langfristigkeit einer KI-Lösung wird ebenfalls durch die Bereitstellungsoption beeinflusst. Die Entwicklung eigener generativer Modelle ist eine langfristige Entscheidung, die mit erheblichen Investitionen in die Weiterentwicklung und Nutzung verbunden ist. Hier muss abgewogen werden, ob die Flexibilität und Kontrolle durch Eigenentwicklung bevorzugt wird oder eine schnell verfügbare Standardlösung gewählt wird, die weniger Anpassung erfordert.

Zentrale Fragen:

- Welche Modelle sind für die Bereitstellung der KI-Anwendung am besten geeignet? Ab August 2025: Ist das Modell per CE-Zeichen in der EU zugelassen und für die spezifische Anwendung zu verwenden?
- Wie flexibel ist die Lösung im Hinblick auf zukünftige Anpassungen oder Erweiterungen? Wie flexibel sind unsere Prozesse bei der Anpassung und Erweiterung der Modelle?
- Welche langfristigen Wartungs- und Supportanforderungen entstehen bei der gewählten Bereitstellungsoption?

8.3 Die Entwurfsphase

In der Phase des Entwurfs werden generative oder vorausschauende KI-Lösungen für Produkte oder Geschäftsprozesse in Zusammenarbeit mit den Fachbereichen konzeptionell erarbeitet. Dieser Prozess bildet das Fundament für den erfolgreichen Einsatz von KI in Unternehmen und konzentriert sich darauf, die Machbarkeit und den Mehrwert der Lösung zu bewerten.

Fokus

Im Fokus dieser Phase steht die Chancen- und Risikoanalyse für den Einsatz von KI-Lösungen im spezifischen Business Case. Es wird untersucht, ob eine KI-Lösung technisch realisierbar und wirtschaftlich sinnvoll ist. Aspekte wie Machbarkeit, Wirtschaftlichkeit und die Effektivität der Lösung werden im Detail geprüft. Dabei ist zu beachten, dass nicht jede Anforderung eine KI-Lösung erfordert. Das Ergebnis des Entwurfsprozesses muss daher nicht immer in einer Implementierung münden – in manchen Fällen kann es sinnvoller sein, auf KI zu verzichten. Dies gilt vor allem für Anwendungen in hoch regulierten Bereichen, oder, wenn die Datenlage unsicher oder unzureichend ist.

Ziel des Entwurfsprozesses ist oft die Erstellung eines High-Level Solution Designs, das als Basis für die weiteren Schritte dient.

Interne und externe Anforderungen

In dieser Phase ist es essenziell, die technischen und wirtschaftlichen Voraussetzungen für eine KI-Lösung realistisch zu bewerten. Gegen den weit verbreiteten KI-Hype muss eine nüchterne Analyse der Chancen und Risiken erfolgen. Neben der technischen Machbarkeit müssen auch die Kosten-Nutzen-Aspekte berücksichtigt werden. Eine gründliche Risikobewertung stellt sicher, dass potenzielle Probleme frühzeitig identifiziert und gemanagt werden können. Darüber hinaus sind auch die rechtlichen und betrieblichen Rahmenbedingungen und Kostenfaktoren zu berücksichtigen, um sicherzustellen, dass die Lösung nicht nur intern sinnvoll ist, sondern auch externen Anforderungen gerecht wird.

Betroffene Prozesse

- Demand-Prozess
- Security-Prozess
- Software-Development-Lifecycle-Prozess
- Enterprise Architecture Management
- Solution Scouting

Artefakte

- Initiales Risiko-Assessment

- Richtlinien- und Standarddokument
- Change-Management-Plan
- High-Level Solution Design

8.4 Die Entwicklungsphase

In der Entwicklungsphase wird die KI-Lösung detailliert ausgearbeitet und unter Berücksichtigung aller rechtlichen, ethischen und wirtschaftlichen Anforderungen erprobt. Dieser Schritt im Lebenszyklus einer KI-Lösung stellt sicher, dass die Lösung den geschäftlichen Anforderungen entspricht und sich als tragfähig für den realen Einsatz erweist.

Fokus

In dieser Phase geht es darum herauszufinden, ob die KI-Lösung, die im Business Case definierten Anforderungen erfüllen kann. Bei der Entwicklung stehen verschiedene Aspekte im Vordergrund, darunter die Time-to-Market, der Time-to-Value und die Performance der Lösung. Dabei muss auch berücksichtigt werden, wie gut die Lösung Anomalien und Abweichungen erkennt und ob sie skalierbar sowie erklärbar (explainability) ist. Sollte es notwendig sein, können hier Anpassungen am Solution Design vorgenommen werden, um die gewünschte Performance zu erzielen.

Die Lösung wird umfangreich getestet, um sicherzustellen, dass sie den definierten Kriterien entspricht. Ein besonderes Augenmerk liegt dabei auf der Erfüllung spezifischer Dokumentationsvorgaben, um sicherzustellen, dass alle regulatorischen und technischen Anforderungen transparent nachvollzogen werden können.

Interne und externe Anforderungen

- **Dokumentation:** Alle Prozesse und technischen Schritte müssen sauber dokumentiert werden, um Transparenz zu gewährleisten. Vor allem Hoch-Risiko Anwendungen haben laut AI Act strenge Dokumentationsvorschriften mit einer Aufbewahrungszeit von 10 Jahren (Artikel 18).
- **Business Case:** Die Lösungen müssen sich an den definierten Anforderungen des zuvor definierten Business Cases orientieren und dessen Ziele erfüllen.
- **Leit- und Richtlinien:** Die Lösungen sollen entsprechend den vorgegebenen internen und externen Richtlinien implementiert werden, um rechtliche und ethische Standards einzuhalten. Die besondere Herausforderung liegt hier, Richtlinien in praxisnahe Handlungsanforderungen zu übersetzen.

Betroffene Prozesse

Die betroffenen Prozesse werden hier exemplarisch aufgelistet und nach gängigen Bezeichnungen benannt, wie sie in vielen Unternehmen üblich sind. Für die individuelle Umsetzung müssen die Prozesse in die jeweilige übergeordnete Gesamtstrategie des Unternehmens angepasst werden.

- ML-Ops-Prozess
- Dev-Ops-Prozess
- Testing-Prozess

- Security-Prozess
- Information-Security-Prozess

Laut Artikel 15 des AI Acts müssen Hochrisiko-KI-Systeme in einer Weise entwickelt werden, dass sie ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreichen. Diese Systeme müssen über ihre gesamte Lebensdauer hinweg konsistent funktionieren. Hierbei sind technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit zu gewährleisten.

Hier ist zu beachten, dass für den gesamten Lebenszyklus der GDPR, bzw. die DSGVO zu berücksichtigen ist.

Artefakte

- Interner-Compliance-Report
- Externer-Reporting-Dokument
- Lösungsdokumentation
- Change-Management-Dokument
- Dokumentationsleitlinie
- Konformitätsbewertungsbericht

Hoch-Risiko Systeme müssen ein dezidiertes Konformitäts-Assessment durchlaufen, bevor sie auf den Markt gebracht werden können (Artikel 43)

8.5 Implementierung und Nutzung

Fokus

Der Schwerpunkt dieser Phase liegt auf der Einführung der KI-Lösung in den Markt oder das Unternehmen. Dieser Prozess wird durch Dokumentation und Schulungen begleitet, um sicherzustellen, dass alle Beteiligten wissen, wie die Lösung eingesetzt und überwacht werden kann. Häufig begegnen die Nutzer dieser neuen Technologie mit Vorbehalten, insbesondere bei semi-autonomen oder vollautonomen Systemen, die Entscheidungen autonom treffen oder Aufgaben ohne menschliches Eingreifen ausführen können. Deshalb ist es wichtig, dass die Funktionsweise und die Grenzen der KI-Lösung genau definiert und erklärt werden. Auch die technische Weiterentwicklung der Lösung ist essenziell, um sicherzustellen, dass sie stets den aktuellen technologischen Standards entspricht.

Interne und externe Anforderungen

- **Dokumentation der Lösung:** Es muss sichergestellt werden, dass die Lösungen so dokumentiert sind, dass sie betrieben, gewartet und bei Bedarf weiterentwickelt werden können, aber auch, dass sie intern

modular für andere Anwendungsfälle verwendet werden können. An Hoch-Risiko Systeme gelten für die Dokumentation hohe und standardisierte Anforderungen.

- **Zugänglichkeit und Verständlichkeit:** Die Dokumentation muss für alle beteiligten Akteure zugänglich und verständlich sein, insbesondere für jene, die keine tiefergehenden technischen Kenntnisse besitzen. Aus der Dokumentation wird abgeleitet, welche Stakeholder die Anwendung zukünftig verwenden und wie diese über die Anwendung aufzuklären sind. Im Sinne der Transparenzverpflichtung (Artikel 50) muss sichergestellt werden, dass die betroffenen Personen informiert sind, wenn sie mit einem KI-System interagieren.
- **Monitoring:** Die Überwachung der KI-Lösung muss den gesetzlichen Anforderungen entsprechen und sicherstellen, dass mögliche Risiken frühzeitig erkannt und gemanagt werden können. Laut Artikel 72, gelten für Hoch-Risiko Systeme folgende Anforderungen: Die Erstellung eines strategischen Überwachung-Plans, das Einrichten eines Überwachungssystems, die aktive und systematische Datenerhebung, wie das System agiert.

Betroffene Prozesse

- Informations-Sicherheits-Management
- Knowledge-Management-Prozesse
- Security Incident und IT Service Continuity Management (ITSCM)
- Enterprise Architecture Management

Incident Management: Festlegung von Prozessen für den Umgang mit Störungen und Fehlern während des Betriebs der KI-Lösung. Auch hier gelten für Hoch-Risiko Systeme gesetzliche Anforderungen nach Artikel 73.

Risikomanagement: Überwachung potenzieller Risiken im Zusammenhang mit der Einführung und Nutzung der KI-Lösung. Besondere Betrachtung findet hier der Übertrag in den Unternehmens-Risikomanagement Prozess. Da das Risiko von Haftung für KI-Anwendungen bei Übertritt der beiden wichtigsten Regularien AI Act, bzw. GDPR bei 7%, bzw. 4% des weltweiten Umsatzes liegt, sind Risiken von KI-Anwendungen unbedingt auf Unternehmensebene zu betrachten.

Anhang

A. Methode, Ablauf und Ergebnis

Der Workstream "KI-Governance" des CBA Lab wurde ins Leben gerufen, um ein umfassendes KI-Governance-Modell zu entwickeln, das Unternehmen dabei unterstützt, die Risiken der KI-Nutzung zu minimieren und gleichzeitig das volle Potenzial der Technologie auszuschöpfen. Dabei sollten technische, ethische, regulatorische, wirtschaftliche und organisatorische Aspekte des gesamten KI-Lebenszyklus abgedeckt werden.

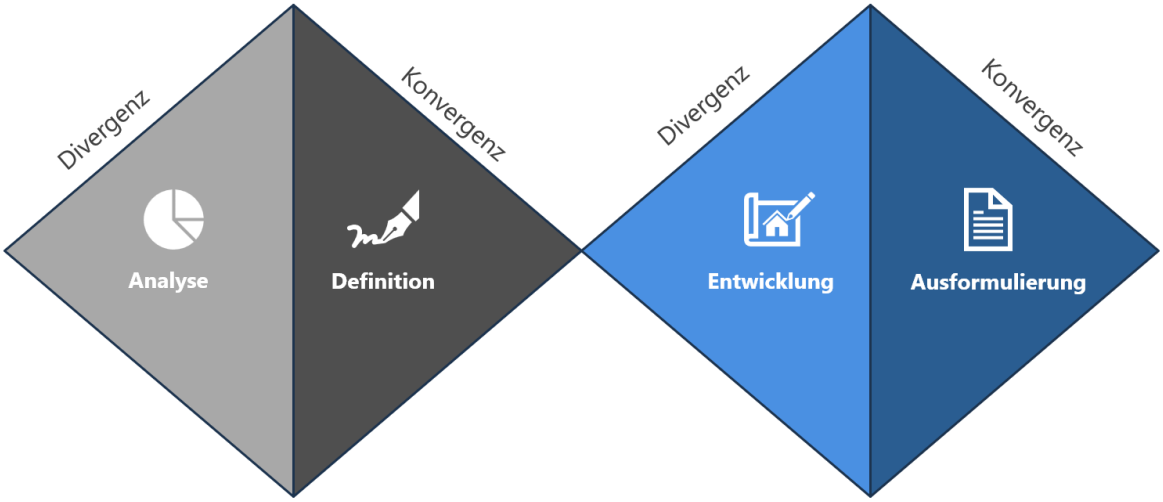

Abbildung 7: Design Thinking - Double Diamond

Der Entwicklungsprozess orientierte sich am Double-Diamond-Prozess aus der Design Thinking Methode, der in vier Phasen unterteilt ist: Analyse, Definition, Entwicklung und Ausformulierung.

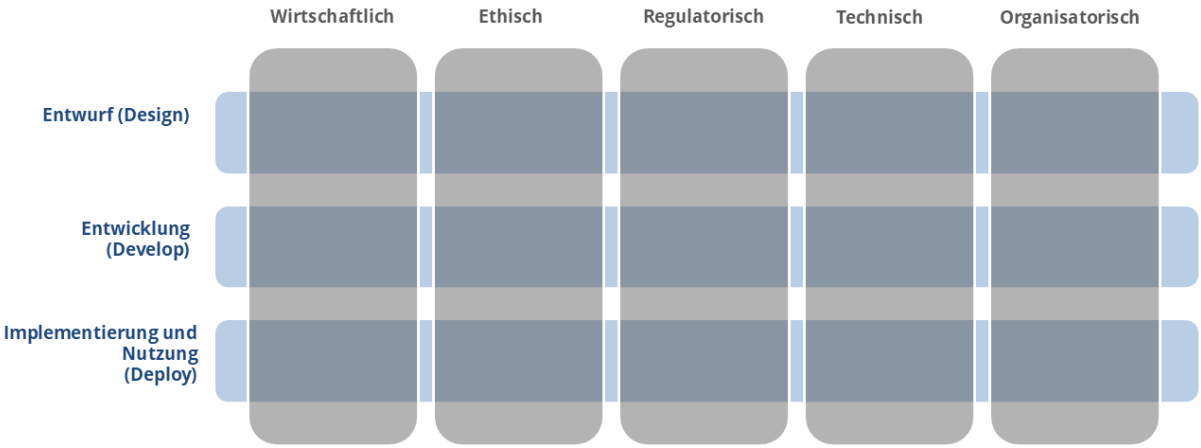

Abbildung 8: Matrix-Teams

In der Analysephase wurde der aktuelle Fortschritt in der Thematik der Unternehmen analysiert, Problemfelder und Anforderungen identifiziert sowie die Teilnehmenden in horizontale und vertikale Teams unterteilt. Die horizontalen Teams arbeiteten an den verschiedenen Phasen des KI-Lebenszyklus (Konzeption, Entwicklung, Implementierung und Nutzung), während die vertikalen Teams nach den fünf Dimensionen wirtschaftlich, ethisch, regulatorisch, technisch und organisatorisch (WERTO) organisiert waren. Die horizontalen Teams arbeiteten funktionsübergreifend, um Silo-Denken zu vermeiden, während die vertikalen Teams den Wissensaustausch innerhalb ihrer Fachgebiete förderten.

Die Definitionsphase diente dazu, wichtige Themen und Problemfelder zu priorisieren und Themen-Ownern zuzuweisen, die für deren kontinuierliche Berücksichtigung verantwortlich waren. In der Entwicklungsphase erarbeiteten die Teams ein prozessorientiertes KI-Governance-Modell, das die identifizierten Herausforderungen und Anforderungen abdeckte. Abschließend wurden in der Ausformulierungsphase die Ergebnisse zusammengeführt, visualisiert und in ein Whitepaper integriert.

Der Workstream bestand aus neun Workshop-Einheiten, beginnend mit einem dreistündigen Kickoff-Meeting, gefolgt von acht wöchentlichen zweistündigen Check-Ins. Das Kickoff-Meeting beinhaltete Vorträge, Statusberichte der Unternehmen und ein Brainstorming, das zur Themenkonsolidierung und Bildung der horizontalen und vertikalen Teams führte. In den wöchentlichen Check-Ins wurde der Fortschritt besprochen, Definitionen geklärt und Modellvorschläge präsentiert.

Das Ergebnis des Workstreams ist das Whitepaper, in dem ein umfassendes und praxisnahes KI-Governance-Modell ausgearbeitet wurde. Die Inhalte des Whitepapers umfassten die Ergebnisse aller Teams und wurden im Laufe des Prozesses mehrfach iteriert und herausgefordert. Das Modell bietet Unternehmen einen umfassenden Ansatz zur Umsetzung von KI-Governance, der die wirtschaftlichen, ethischen, regulatorischen, technischen und organisatorischen Aspekte entlang des gesamten KI-Lebenszyklus berücksichtigt.

B. Glossar

AI-Office
Ein AI Office in einem Unternehmen ist eine spezialisierte Einheit, die sich der Verwaltung, Steuerung und Förderung des Einsatzes von Künstlicher Intelligenz (KI) widmet. Es koordiniert Initiativen zur Implementierung von KI-Systemen, stellt sicher, dass die notwendigen Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter stattfinden, und unterstützt dabei, KI-Technologien sicher und effektiv zu integrieren. Das AI Office dient auch als zentrale Anlaufstelle für den Wissensaustausch und die Erarbeitung von Best Practices. Es fördert den sicheren und ethischen Einsatz von KI, um sowohl die Akzeptanz als auch das Verständnis für KI-Systeme im gesamten Unternehmen zu stärken. Je nach Organisationsgröße kann es sich hierbei um verschiedene Konzepte des AI Offices handeln, von einer oder mehreren Teilzeitpositionen mit Community-Charakter bis hin zu einem Competenz-Center.

AI-Literacy
(übersetzt aus dem Englischen) "AI-Kompetenz (AI Literacy) bedeutet Fähigkeiten, Wissen und Verständnis, die es Anbietern, Anwendern und betroffenen Personen ermöglichen, im Rahmen dieser Verordnung fundierte Entscheidungen über den Einsatz von KI-Systemen zu treffen. Zudem soll die AI-Kompetenz das Bewusstsein für die Chancen und Risiken von KI und die möglichen Schäden, die sie verursachen kann, fördern“.

C. Abbildungsverzeichnis

Impressum

Herausgeber
Cross-Business-Architecture Lab e. V.
Hinter Hoben 149
53129 Bonn
Telefon: +49 228 55 51 131
E-Mail: info@cba-lab.de
www.cba-lab.de
https://twitter.com/cba_lab
https://de.linkedin.com/company/cba-lab

Vertretungsberechtigte Vorstände
Joachim Schmider, 1. Vors.
Dr. Arun Anandasivam
Prof. Dr. Johannes Helbig
Dr. Karsten Schweichhart (V. i. S. d. P.)