CAIR4

EU AI Act Playbook

Verstehen. Vertiefen. Verwenden.

Oliver M. Merx

KI-REGULIERUNG IST EIN ERNSTES THEMA,

und dieses Playbook eine ernsthafte Publikation: Ihr Ziel ist es, das Verständnis relevanter Grundlagen der KI-Verordnung mit plakativen Bildern zu fördern. Warum Ist dies überhaupt notwendig? Reicht es nicht, wenn Juristen* die KI-Verordnung verstehen? Wenn sie das Recht der KI mittels Gesetzestext und Prüfungsschemata erlernen, vermitteln und anwenden?

Nein! KI betrifft jeden, nicht nur Juristen. Und der EU AI Act ist das zentrale Instrument, um Vertrauen der Gesellschaft in die verantwortungsvolle Nutzung von KI zu schaffen. Doch was nutzt die beste Regulierung, wenn sie nur von wenigen verstanden wird? Wenn sie für viele andere so komplex und abstrakt erscheint, dass sie eher irritiert, als Vertrauen zu fördern?

Eine knifflige Situation: Um Rechtssicherheit zu ermöglichen, muss die KI-Verordnung etablierten juristischen Regeln folgen. Sie muss dabei die hohe Dynamik der KI aufgreifen und in ebenso flexible wie dauerhaft gültige Regeln packen. Keine einfache Herausforderung.

Insofern sei an dieser Stelle betont:

- Die KI-Verordnung ist juristisch sehr gut strukturiert.
- Sie wägt fair zwischen Chancen und Risiken von KI ab.
- Sie hat das Potenzial, die EU in eine sichere KI-Zukunft zu führen.

Tatsache ist jedoch auch, dass Unternehmen, Behörden und deren Mitarbeiter verstehen müssen, was sie zu beachten haben, welche Pflichten und Rechte sie besitzen. Die Anwender wollen wiederum verstehen, weshalb sie KI innerhalb der EU vertrauen können.

Hier setzt das Playbook an: Es nutzt plakative Methoden zur Erklärung der KI-Verordnung. Sie wirken spielerisch – doch im Hinblick auf die Zielsetzung sind sie ernsthaft.

Insofern möchte dieses Playbook dazu beitragen, die KI-Verordnung nicht nur verständlicher, sondern KI insgesamt vertrauenswürdiger zu machen.

* Aus Gründen besserer Lesbarkeit wird die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

Oliver M. Merx
Rechtsassessor & Informatiker

WHO IS WHO:

Diese KI-Protagonisten und ihr Zusammenspiel werden im Playbook erläutert:

1. KI-System
2. KI-Komponenten
3. KI-Modell
4. KI-Anbieter/Betreiber
5. GPAI-System
6. GPAI-Modell
7. GPAI-Akteure
8. Verbotene KI-Praktiken
9. KI hoher Risikoklasse
10. KI mittlerer Risikoklasse
11. KI geringer Risikoklasse
12. KI-Kompetenz
13. KI-Modell-Daten
14. KI-System-Daten
15. schlechte Daten

DIE KI-VERORDNUNG SPIELERISCH EINPRÄGEN

Der EU AI Act ist das Herz des KI-Rechts. Ihn zu verstehen und souverän anzuwenden, erfordert Rechtskenntnisse als auch ein Grundverständnis von Künstlicher Intelligenz.

So ist bereits die zentrale Frage, was ein KI-System ist, nicht immer leicht zu beantworten. Ähnlich ist es bei der Unterscheidung des Quasi-Anbieters und des so genannten nachgelagerten Anbieters: Beide Rollen sind wichtig, klingen ähnlich, meinen aber etwas ganz anderes.

Doch was ist der Unterschied?

Diese und weitere Aspekte werden meist von Juristen mit trockenen rechtlichen Mitteln erklärt: Mit dem Gesetzestext, abstrakten Kriterien und Prüfungsschemata. Trotz fachlicher Richtigkeit bleiben bei diesem Ansatz allzu oft wichtige Fragen ungeklärt.

Das Playbook ergänzt den klassischen juristischen Ansatz. Unter Verwendung anerkannter Lernmethoden hilft es dabei, die abstrakten Normen des EU AI Acts zu überwinden und KI-Themen im rechtlichen Kontext plakativ einzuordnen. Und dies weitgehend ohne Verwendung von Fachbegriffen.

Erst am Ende verweist das Playbook auf Inhalte und Randnummern des dazugehörigen Skripts: **Grundwissen-KI-Recht.** Bevor man darin vertieft, welche Symbole und Begriffe mit welchen Normen des EU AI Acts zusammenspielen, kann und sollte man erst einmal nur den Text des Playbooks lesen – und sich dessen Gleichnisse einprägen.

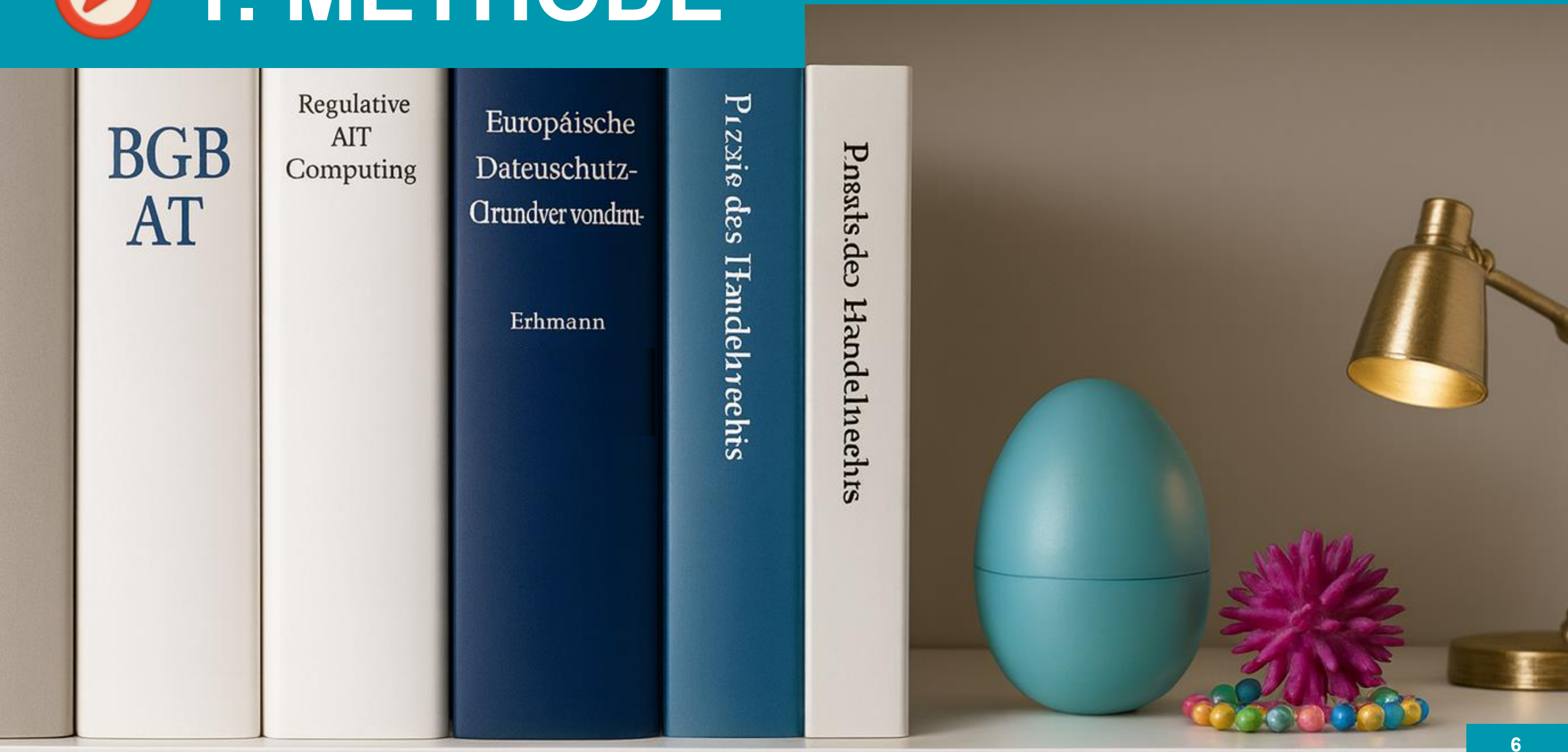
Im Zentrum des Playbooks steht nämlich eine Symbolsprache: Um Fragen von KI und des KI-Rechts zu klären, müssen Juristen, Manager, Techniker und Anwender häufig einen interdisziplinären Informationsaustausch vollziehen. Jeder nutzt dabei eine eigene Fachsprache. In internationalen Projekten kommen unterschiedliche Fremdsprachen hinzu.

Diese anspruchsvolle Kommunikation mit anschaulichen Mitteln und Methoden zu unterstützen, ist ein zentrales Anliegen des Playbooks. Insofern richtet es sich an jeden, der den EU AI Act in Grundzügen verstehen will oder operativ umsetzen muss.

Beginnen wir nun die Journey des Playbooks. Die 15 KI-Protagonisten und ihr Zusammenspiel werden in den folgenden acht Stationen erläutert:

ACHT STATIONEN

1. METHODE


BGB
AT
Regulative
AIT
Computing
Europäische
Dateuschutz-
Erhmann

LERNEN WIE GEDÄCHTNISWELTMEISTER

Die mehrfache Gedächtnisweltmeisterin Christiane Stenger verwendet ausgefeilte Mnemotechniken, um sich große Mengen abstrakter Information einzuprägen.

Ihre Methode ist einfach, aber effektiv:

- Emotionalisieren von Einzelinformationen
- Verbindung der Inhalte zu Geschichten
- Umwandeln, Abspeichern und Abrufen

Komplexe Informationen werden von ihr in fantasievolle Bilder übersetzt. Die Bilder werden in einzigartiger Weise in (lustige) Geschichten verwandelt. Mittels emotionaler Kodierung und Vernetzung lassen sich Inhalte verstehen, speichern und wieder reaktivieren.

Repetitoren nutzen seit jeher diese Technik, um abstraktes Recht anschaulich und einprägsam zu machen. So ist das „Brustgeschäft“ ein Gleichnis für das Insichgeschäft i.S.v. § 181 BGB. Oder die „Nutella-Theorie“ eine Eselsbrücke für die formelle Enteignung (Art. 14 III GG): „Nur wo Enteignung drauf steht, ist auch Enteignung drin“. Die Liste ließe sich beliebig fortsetzen.

Vor diesem Hintergrund wird das KI-System in diesem Playbook zu einem maschinellen Ei, GPAI-Modelle werden zu bunten Korallen, Daten zu Perlenketten und verbotene KI-Praktiken zu einem T-Rex.

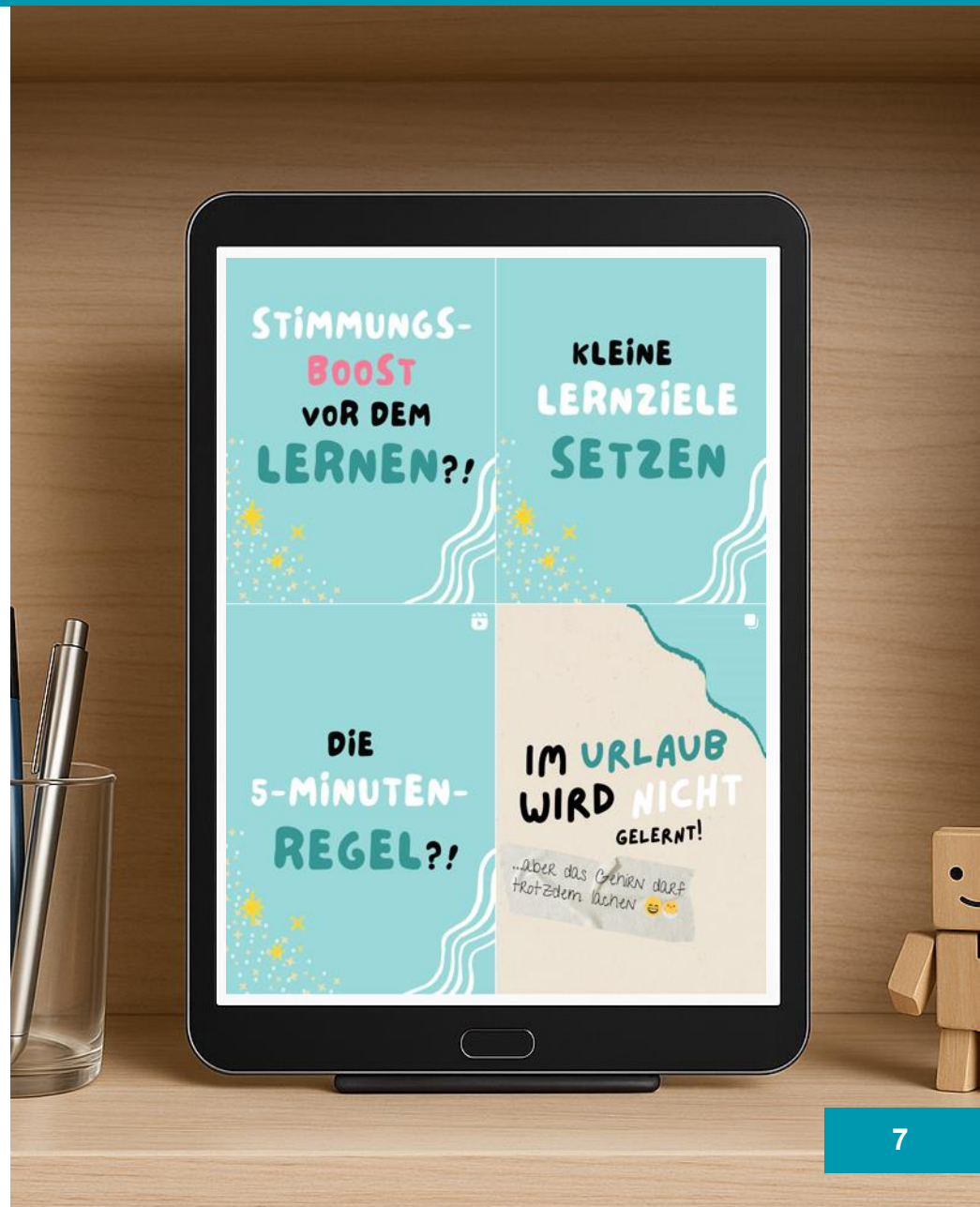
Das Playbook greift die Technik der Emotionalisierung und der spielerischen Vernetzung auf, um abstrakte Information erlebbar zu machen: Durch Symbole, Figuren und kurze, aber letztlich seriöse Geschichten.

Wer so lernt, merkt sich nicht nur Worte – viel mehr kann man komplexe Inhalte und Zusammenhänge innerlich in Sekundenschnelle abrufen, wenn sie in einer Prüfung oder in der Praxis gebraucht werden.

Techniken wie die von Christiane Stenger, sind sehr wirksam. Sie werden in diesem Playbook durch eine weitere, insbesondere in der digitalen Wirtschaft weit verbreitete Methode ergänzt:

Gemeint ist das „seriöse Spielen“ mit den Produkten unserer Kindheit …

Mehr zu Christiane Stenger unter: https://www.instagram.com/christiane_stenger



SERIOUS PLAY – MEHR ALS BUNTE FIGUREN

LEGO hat es weltbekannt gemacht: Das so genannte „Serious Play“. Hochqualifizierte Experten von Konzernen, Organisationen oder Start-Ups befinden sich dabei in einem Raum. Mit bunten LEGO-Steinen oder Figuren von playmobil pro basteln sie disruptive Lösungen – und bezahlen für Workshops obendrein noch viel Geld.

Nicht ohne Grund: Hinter der spielerischen Fassade steckt ein ausgefeiltes Format zur Lösung komplexer Probleme. Insbesondere solche, die sich nicht allein mit Folien, Tabellen oder Paragraphen lösen lassen.

Speziell in der virtuellen Welt entfaltet seriöses Spielen seine große Stärke: Physische Bausteine durchbrechen die Abstraktion, und Spaß reduziert die Kontakthürden in Teams.

Die Methode ermöglicht einfache, aber anschauliche Konzepte. Aus ihnen entstehen Geschichten. Diese entwickeln sich zu Lösungen, die auf interdisziplinären Sichtweisen und Fachkenntnissen beruhen.

Nicht anders beim Recht der KI: Um regulatorische Aspekte beurteilen zu können, muss erst einmal klar sein, worum es geht: Wann ist eine Software ein KI-System oder KI-Modell? Wann ein Service ein GPAI-Modell – oder ein GPAI-System?

Erst wenn ähnlich klingende Begriffe sicher abgegrenzt werden können, kommt es im Rahmen komplexer KI-Wertschöpfungsketten zur Anwendung der passenden Normen.

Das Playbook knüpft bewusst an das seriöse Spielen an. Dabei verwendet es eine eigene Symbolwelt mit maschinellen Überraschungs-Eiern, Korallen, Perlen, Schmuckkästchen, Hütchen und sogar Kieselsteinen.

Symbole und Geschichten helfen nachgewiesener Weise, um Abstraktes greifbar zu machen. Sie eröffnen einen Raum, in dem Juristen, Techniker, Manager und Nutzer eine gemeinsame Symbolsprache nutzen können, um KI erfolgreich einzusetzen und das KI-Recht zu meistern.

Mehr zu LEGO Serious Play unter: https://de.wikipedia.org/wiki/Lego_Serious_Play
Mehr zu playmobil pro unter: https://pro.playmobil.com

SPIEL UND RECHTLICHE INHALTE VERBINDEN

Egal ob gedruckt oder digital: Sprache bleibt das Fundament juristischer Arbeit. Als Jurist muss man Gesetze, Kommentare und Rechtsprechung kennen, lesen und durcharbeiten. Nicht anders ist es beim EU AI Act.

Das Spielen ersetzt nicht das klassische juristische Handwerk! Doch KI ist abstrakt und intransparent: Selbst Experten aus IT und Technik tun sich mitunter schwer, KI eindeutig zu definieren oder ihre Wirkweise transparent zu machen. Die KI-Verordnung macht es nicht einfacher, denn sie bestimmt aus rechtlicher Sicht, was KI ist – oder nicht.

Hier setzt das Playbook an. Es ergänzt das auf dem Bild dargestellte Skript **Grundwissen KI-Recht:** Es erläutert rechtliche Aspekte im Detail. Das Playbook hilft, die juristischen Inhalte in anschauliche Bilder, Metaphern und Eselsbrücken zu übersetzen.

KI- und KI-Recht werden so „begreifbar“:

- Verstehen durch Bild & Sprache
- Behalten durch Erinnerungstechniken
- Gestalten durch Rechtstext und Playbook

Die Verbindung von Skript und Playbook ermöglicht ein agiles rechtliches Verstehen, das über bloßes Wiederholen hinausgeht: Die Inhalte bleiben juristisch präzise, werden aber erlebbar und einprägsam.

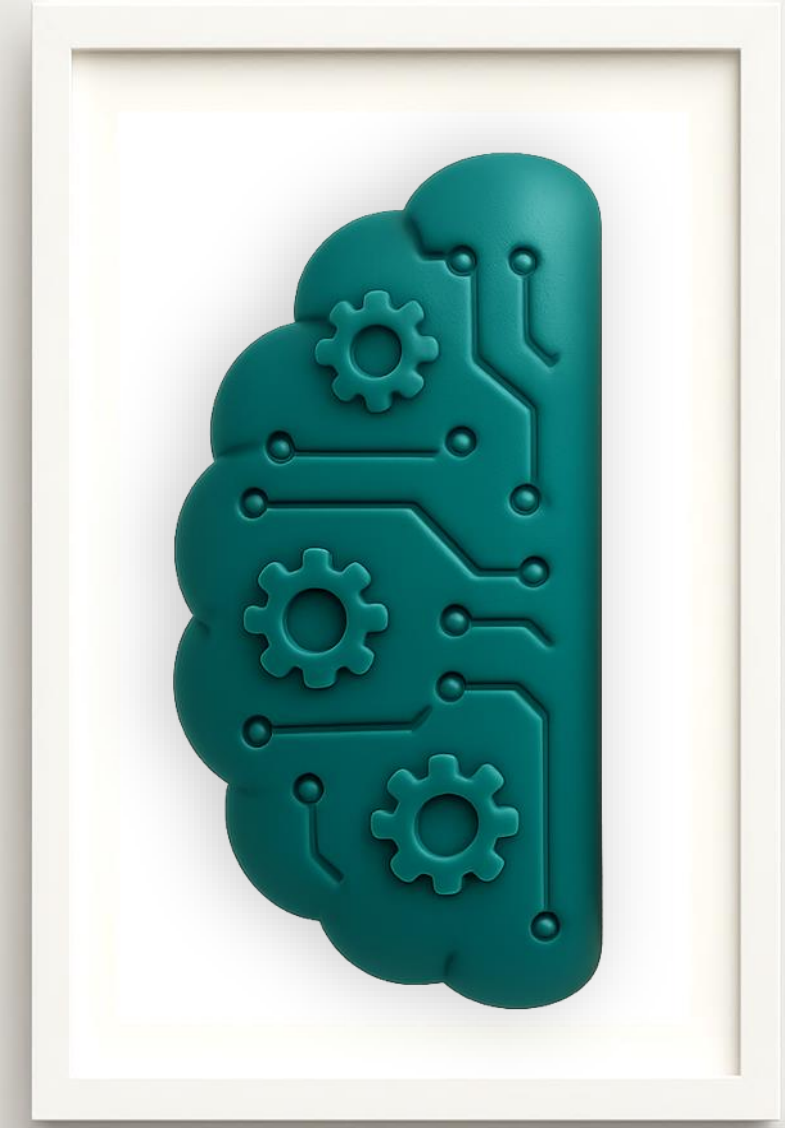
Das ist wichtig. KI-Systeme sind keine physischen Maschinen: Sie bestehen aus virtuellen Komponenten: Aus Interaktionsschnittstellen, KI-Modellen und System-Daten. Sie erhalten Inputs und generieren Outputs.

Doch wo fängt das eine an und wo hört das andere auf? Die KI-Verordnung erfordert eine genaue Differenzierung. Sie enthält über 60 Definitionen. Die Wichtigsten zu versinnbildlichen und ihr Zusammenspiel plakativ zu verdeutlichen, ist das primäre Ziel des vorliegenden EU AI Act Playbooks!

Und dann, wenn zentrale Definitionen des EU AI Acts „sitzen“, erschließt sich auch die hohe Qualität der KI-Verordnung!

Die KI-Verordnung ist gut, aber komplex. Gerade deshalb sollte man sie (zusätzlich) spielerisch erkunden und vertiefen!

Mehr zum Grundwissen-Skript unter: http://www.grundwissen-ki-recht.de



SKRIPT & PLAYBOOK

Die Methode noch einmal mit anderen Worten: Das Skript **Grundwissen KI-Recht** bildet das juristische Fundament: Es bietet exakte Definitionen, Prüfungsabläufe, Übersichten und Verweise auf Artikel des EU AI Acts sowie weiterer Gesetze.

Es liefert das rechtliche Handwerkszeug, das für die Fallprüfung in Ausbildung und erst recht in der Praxis unverzichtbar ist. Die rechtlichen Details werden dabei von der logischen linken Gehirnhälfte verarbeitet.

Das Playbook übersetzt wichtige Inhalte des EU AI Acts in prägnante Symbole, Figuren und Szenen. Es emotionalisiert und konkretisiert, wo das Skript abstrakt bleibt. Es ermöglicht den Einstieg in eine komplexe Materie und schafft Überblick. Es stimuliert auf spielerische Art die kreative rechte Gehirnhälfte.

So entsteht ein Zusammenspiel von Spiel und Logik, das ein Begreifen und Anwenden der KI-Verordnung sowie das Gestalten rechtskonformer KI vereinfacht.

Gleich geht es los!

MERKEN WIR UNS ZU STATION EINS – DER METHODE:

1. DIESES PLAYBOOK ERGÄNZT DAS SKRIPT „GRUNDWISSEN KI-RECHT“ – ES UNTERSTÜTZT PRIMÄR DESSEN VERSTÄNDNIS!
2. KLASSISCHE JURISTISCHE METHODEN SIND NACH WIE VOR UNVERZICHTBAR – SIE STOSSEN ABER BEI KI AN GRENZEN.
3. MNEMOTECHNIKEN HELFEN DABEI, ABSTRAKTE BEGRIFFE WIE „GPAI-MODELL“ ODER „QUASI-ANBIETER“ EINPRÄGSAM ZU MACHEN.
4. SERIÖSES SPIELEN HILFT, DAS KOMPLEXE ZUSAMMENSPIEL VON KI-TYPEN, RISIKEN UND AKTEUREN ZU DURCHDRINGEN.
5. DAS SKRIPT „GRUNDWISSEN KI-RECHT“ UND DAS PLAYBOOK SPRECHEN DAS GEHIRN AUF UNTERSCHIEDLICHE WEISE AN.

NUN GEHT ES WEITER MIT STATION ZWEI: DEM KI-SYSTEM

2. KI-SYSTEM

DAS KI-SYSTEM: EIN MASCHINELLES EI

Das KI-System ist der zentrale Dreh- und Angelpunkt der KI-Verordnung. Ein maschinelles Ei hilft uns dabei, die vielen Kriterien und rechtlichen Besonderheiten von KI-Systemen zu erkennen und zu bestimmen – in doppelter Hinsicht, denn in diesem und dem nachfolgenden Kapitel wird dargestellt:

- Was ein KI-System im Positiven ist.
- Und was es im Negativen nicht ist.

Das negative Ausschlussverfahren hilft oft schneller weiter als die positive Bestimmung. Gerade dann, wenn es Unklarheiten gibt.

Ein Beispiel: Stellen wir uns vor, dass der Haustürschlüssel weg ist. Beginnen wir im ersten Schritt mit der negativen Prüfung.

Überlegen wir zuerst, wo der Schlüssel mit hoher Wahrscheinlichkeit nicht verloren ging:

- Nicht in der Wohnung. Also hat man ihn woanders verloren.
- Nicht im Büro. Denn dies hat man mit dem Schlüsselbund abgeschlossen.
- Nicht im Auto. Man ist nämlich zu Fuß unterwegs gewesen … etc.

Durch negative Abgrenzung schränkt man eine Suche oder die Bestimmung von Dingen häufig rasch und effektiv ein.

Ohne die negative Abgrenzung könnte die Bestimmung von KI-Systemen langwierig und ungerichtet verlaufen. Dafür kann die Kombination von negativer Ausgrenzung und positiver Bestimmung helfen, das rechtlich Wesentliche von KI-Systemen zu erfassen.

Und um die doppelte Bestimmung im Sinne der KI-Verordnung zu ermöglichen, ist das KI-System ein maschinelles Ei.

Im Folgenden wird daher nicht nur verdeutlicht, welche positiven Merkmale das Ei hat: Es wird auch optisch klar erkennbar abgrenzt vom KI-Modell. Dessen Name klingt ähnlich, hat aber eine ganz andere Funktion und besitzt deshalb auch ein ganz anderes Symbol.

Merken wir uns: Das KI-System im Sinne der KI-Verordnung ist ein maschinelles Ei!

Kurz und knapp:

KI-System = Ei

ABGRENZUNG VON KI-SYSTEM UND PRODUKT

KI-Systeme und Produkte sind zwei verschiedene Dinge. Maschinelle Eier können in unglaublich vielen Produkten stecken: Einem Herzschrittmacher, einem Stromzähler oder einem Spielzeug. Selbst Software fällt nach der neuen Produkthaftungsrichtlinie der EU unter die Produkte. Ist das maschinelle Ei in ein Produkt integriert, spricht man von „Embedded AI“.

Oft unterliegen Produkte zusätzlichen Vorschriften: So muss Spielzeug auch ohne KI für Kinder sicher und ungefährlich sein. Daher muss der Hersteller der Puppe, die ein KI-System enthält, die Vorschriften beachten, die für Spielzeug im allgemeinen gelten. Zusätzlich muss das darin integrierte KI-System dem EU AI Act entsprechen. Dabei kommt es zur Überlagerung von Vorschriften und Zuständigkeiten. Diese werden zukünftig harmonisiert – u.a. bei kritischer Infrastruktur, Autos, medizinischen Produkten und dem erwähnten Spielzeug.

Die übergreifende Regulierung ist sinnvoll! Wichtig ist nämlich für Kinder und Eltern, dass beides sicher ist: Das Spielzeug als solches und ebenso das darin integrierte KI-System.

Ein KI-System bleibt aber ein KI-System. Egal, ob man es in ein Produkt integriert oder nicht.

Es zeichnet sich in allen Varianten durch Eigenschaften aus, die im Sinne der KI-Verordnung zu beachten sind:

- Es ist eine Maschine, die mit ihrer Umgebung interagieren kann – egal, ob diese ein Mensch, eine Puppe oder eine Software ist.
- Erhält das magische Ei eine Information als Input, leitet es den Output eigenständig aus Daten ab. Insofern ist es auch oft ein Überraschungsei.
- Niemand weiß ganz genau, welchen Output das Ei produziert. Selbst das Ei weiß es oft nicht. Das macht KI schwer berechenbar.
- Einige KI-Systeme sind lernfähig. Dann sammeln sie Daten, um bessere Ergebnisse zu ermöglichen. Aber das ist nicht zwingend.

Merken wir uns: Das Ei im Sinne der KI-Verordnung ist eine Maschine, die mit der Umwelt interagiert! Kann sie nicht interagieren oder agiert sie nicht maschinell, dann ist es auch kein KI-System im rechtlichen Sinne.

VERTRAUEN IN KI: DAS WICHTIGSTE ZIEL

Die vorherigen Beispiele haben verdeutlicht, wie unterschiedlich KI-Systeme eingesetzt werden können. Je nach Einsatzgebiet sind damit auch Chancen und Risiken unterschiedlich zu bewerten.

KI-Nutzer und die von der KI-Nutzung Betroffenen sollen sich stets darauf verlassen können, dass KI-Systeme vertrauenswürdig sind und verantwortungsvoll verwendet werden. Daher enthält die KI-Verordnung verschiedene Risiko-Klassen.

Das bedeutet u.a., dass KI-Systeme, die unzumutbar gefährlich sind, gar nicht erst auf dem Markt angeboten und genutzt werden dürfen. Daher sind z.B. Spielzeuge verboten, die Kinder mittels KI manipulieren könnten.

Man muss jedoch ganz genau hinschauen:

- Manche KI-Systeme wirken auf den ersten Blick harmlos. So sind die kleinen Vögel besonders niedlich, aber gerade sie könnten kleine Kinder manipulieren.
- Anders hingegen die Schlange. Sie löst wie von selbst bei vielen Menschen Unbehagen aus. Dabei ist sie oft ganz harmlos und sogar das Symbol der Medizin!

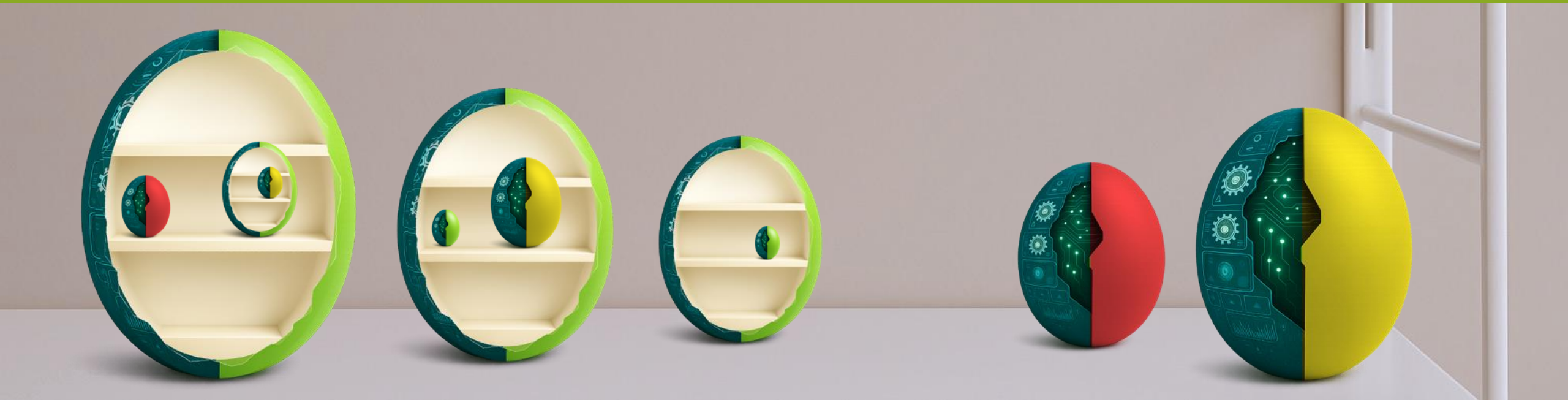
Der erste Anschein kann trügen. Doch damit nicht genug: Risiken entstehen nämlich nicht nur durch „böse“ KI, sondern häufig durch komplexe, intransparente oder falsch eingesetzte KI.

Gerade in der Bedienung liegt oft das größte Problem: Wer will es einer nützlichen Biene verübeln, dass sie zusticht, wenn man sie ärgert. Daher ist die Schulung von Menschen, die mit KI arbeiten, eine der ganz wichtigen Aspekte der KI-Verordnung: KI will und muss kompetent bedient werden!

Durch die Vermittlung von KI-Kompetenz sind Anwender in der Lage, KI richtig einzusetzen und auch ihre Risiken besser abzuschätzen.

Das gilt aber nicht unbegrenzt, denn wie sich ein KI-System unter welchen Umständen verhält, und was sich in einem KI-System befindet, ist „von außen“ kaum zu beurteilen. Das liegt u.a. daran, dass KI-Systeme viele Komponenten enthalten, die interagieren – darunter auch weitere KI-Systeme.

Um das Zusammenspiel zu verdeutlichen, werfen wir nun einen Blick auf das Matrjoschka-Prinzip von KI-Systemen.



DAS MATRJOSCHKA-PRINZIP: EI IN EI IN EI …

Um verschachtelte Architekturen von KI-Systemen erahnen zu können, hilft der Blick ins Innere eines KI-Systems weiter.

Dabei stoßen wir auf ein interessantes Phänomen: KI-Systeme können andere KI-Systeme in sich integrieren. Ein maschinelles Ei kann also seinerseits viele weitere Eier enthalten, die ihrerseits KI-Systeme enthalten: So ähnlich wie Matrjoschka-Puppen sind die KI-Eier dann ineinander verschachtelt.

Bildlich gesprochen: Ein Ei im Ei im Ei.

Dann wird es anspruchsvoll, denn jedes KI-System ist im Rahmen komplexer KI-Wertschöpfungsketten normalerweise separat zu bewerten. Zusammen ergeben sie jedoch ein neues Ganzes, das als Gesamtheit mit allen integrierten Komponenten den Anforderungen des EU AI Acts gerecht werden muss. Das ist komplex – aber Realität und wichtig!

So kann z.B. ein medizinisches Ei aus einem Sprachmodell mit speziellem Wörterbuch, einer Bild-KI, einer Diagnose-KI und weiteren Komponenten bestehen. Und jede dieser Komponenten kann seinerseits weitere KI-Systeme enthalten. Das ist von Vorteil, denn so können auf modulare Art besonders leistungsfähige KI-Systeme entstehen.

Wichtig ist deshalb, dass man im Rahmen einer KI-Wertschöpfungskette mit vielen Komponenten den Überblick behält ...

Schauen wir uns deshalb das Ei noch etwas genauer an. Es hat nämlich drei Fächer, die den Überblick der Komponenten vereinfachen.

DREI FÄCHER FÜR KOMPONENTEN

Viele KI-Systeme sind arbeitsteilig organisiert. Dafür besitzen sie drei Fächer:

- Das oberste dient der Interaktion mit der Umwelt: Das Ei muss Information als Input erhalten können und als Output wieder ausgeben können, um die Umwelt zu gestalten. Beispiele wären eine Tastatur, ein Mikrophon, ein Joystick oder ein Sensor.
- Das mittlere Fach enthält die autonome Intelligenz. Sie steckt im KI-Modell: Einer Art Gehirn. Es enthält eine große Menge trainierter Daten, die tief im Inneren des Modells gespeichert sind. Mit dem Modellwissen kann ein generatives KI-System wie ein Chatbot bereits viele Fragen selbständig beantworten – ohne weitere Daten.
- Aber: Nach dem Ende des Trainierens ist das KI-Modell nicht immer auf dem neuesten Stand. Daher könnte es glauben, dass Angela Merkel nach wie vor Kanzler ist. Um aktuell zu sein und zu bleiben, kann das untere Fach z.B. Echtzeit-Suchen durchführen oder Fachdaten enthalten und speichern. Darunter auch Nutzerdaten oder einen Sessionspeicher.

Die Differenzierung der drei Fächer ist u.a. aus Datenschutzgründen von Bedeutung: Es macht einen großen Unterschied, ob Nutzerdaten im zweiten oder dritten Fach landen. Werden sie im KI-Modell gespeichert, sind sie oft nur unter großen Aufwänden wieder entfernbar. Werden sie in einer Datenbank gespeichert, reicht in vielen Fällen ein einfacher Klick, um sie zu löschen.

Auf das unterste Fach kommen wir später noch genauer zu sprechen. Schauen wir uns daher erst einmal das mittlere Fach genauer an: Dort entdecken wir gleich zwei unterschiedliche Formen integrierter Intelligenz:

- Ganz links: Die Intelligenz kann aus einem integrierten KI-System kommen (Ei in Ei).
- Sie kann aber auch direkt aus einem KI-Modell kommen (rechte Seite). Die KI-Verordnung differenziert mehrere Modell-Varianten, die man unterscheiden muss.

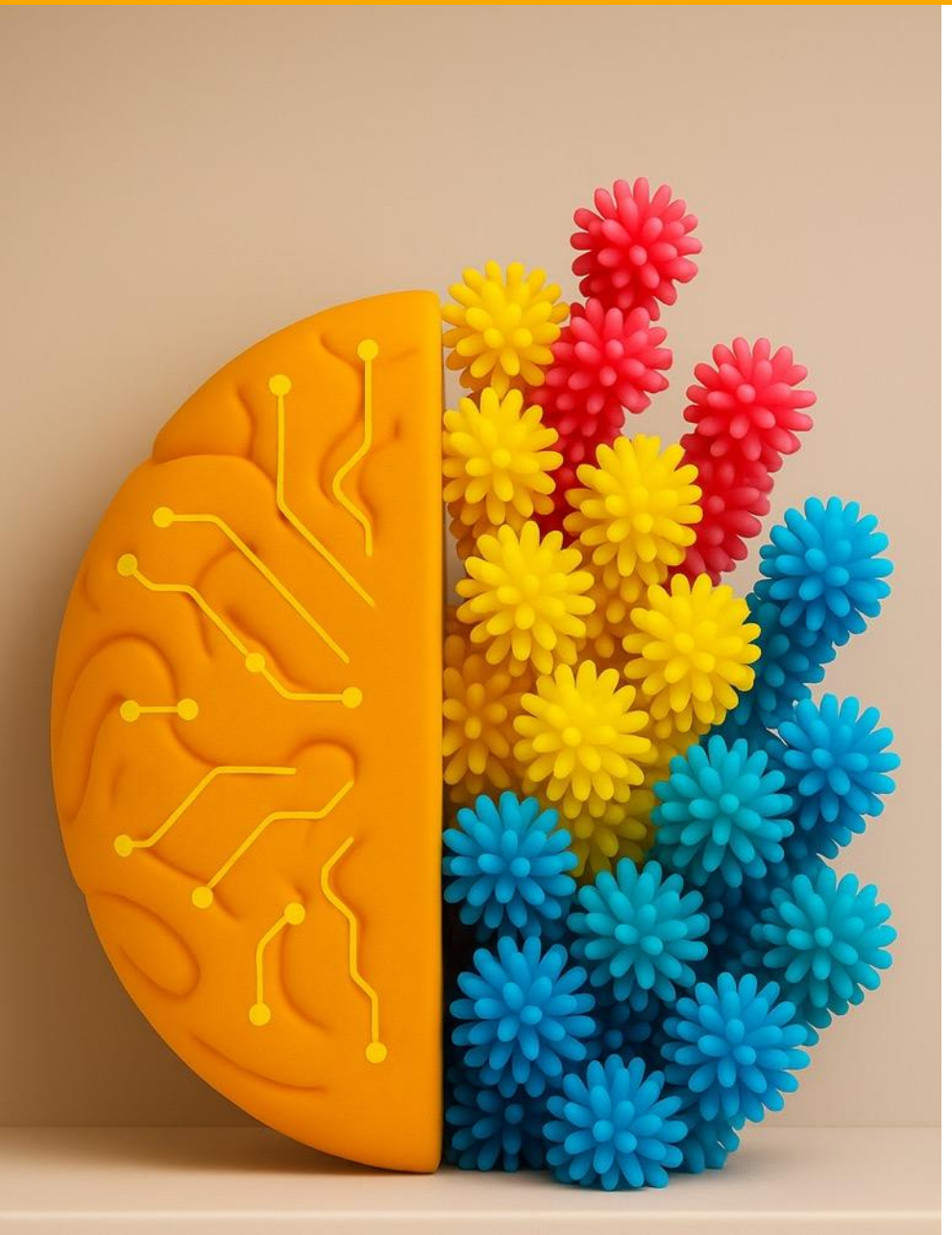
Das so genannte „GPAI-Modell“ (die bunte Koralle mitte/ rechts) ist besonders wichtig. Es wurde im EU AI Act genauer geregelt! Dazu nun mehr in Station drei.

MERKEN WIR UNS ZU STATION ZWEI – DEN KI-SYSTEMEN:

1. ZENTRALES ZIEL DER KI-VERORDNUNG IST DIE SCHAFFUNG VON VERTRAUEN IN KI-SYSTEME – EGAL WELCHER ART.
2. EIN KI-SYSTEM KANN IN EINEM PRODUKT STECKEN ODER SELBST EIN PRODUKT SEIN. SO ODER SO: ES UNTERLIEGT DEM EU AI ACT!
3. KI-SYSTEME KÖNNEN KI-SYSTEME ENTHALTEN – WIE BEI MATRJOSCHKA-PUPPEN. DAS MACHT DIE BEWERTUNG ANSPRUCHSVOLL.
4. EIN KI-SYSTEM IST EINE MASCHINE. SIE BRAUCHT INPUT, VERARBEITET IHN SELBSTSTÄNDIG UND ERZEUGT EINEN OUTPUT.
5. DAS MASCHINELLE EI HAT DREI FÄCHER: FÜR DIE INTERAKTION MIT DER UMWELT. FÜR DIE INTELLIGENZ. UND FÜR WEITERE DATEN.

NUN GEHT ES WEITER MIT STATION DREI: DEM GPAI-MODELL

3. GPAI-MODELL



DAS GPAI-MODELL: MAL KORALLE, MAL RIFF

Wenn das KI-System ein maschinelles Ei ist, dann ist das GPAI-Modell eine bunte lebendige Koralle: Ein kleines Ökosystem.

Die Koralle ist das vielseitige intelligente Gehirn (generativer) KI-Systeme: Sie ist das, was denkt und Inhalte erzeugt: Texte, Bilder, Audio-Files oder täuschend echte Videos.

„GPAI“ steht für „General Purpose AI“: Das ist die Bezeichnung für ein „KI-Modell mit allgemeinem Verwendungszweck“. Diese besonders leistungsfähige Variante eines KI-Modells wird in der KI-Verordnung als einzige genauer definiert und geregelt.

Nicht definiert ist dafür das deutlich kleinere und spezialisiertere KI-Modell. Es ist im Vergleich zur Koralle ein Polyp: Das einzelne, winzige Tierchen, aus dem die Koralle und letztlich sogar ein großes Korallenriff besteht.

Und so wird auch klar, wie Polyp und Koralle zusammenspielen: Ein Polyp kann mit der Zeit immer größer, verzweigter, eigenständiger, vielseitiger werden. Dann wird ein Polyp zur Koralle. Und auch die Koralle kann weiter wachsen: Zu einem Korallenriff!

Ein Korallenriff ist schön, aber nicht ungefährlich. Deshalb widmet ihm der EU AI Act eigene Regeln: Es sind Auflagen für „GPAI-Modelle mit systemischen Risiken“.

Fassen wir kurz zusammen:

1. Einfaches KI-Modell = Polyp
2. Vielseitiges GPAI-Modell = Koralle
3. GPAI-Modell mit systemischen Risiken = Korallenriff

Alle drei sind keine KI-Systeme: Sie sind wie ein Gehirn ohne Körper und eigene Sinne. Ihnen fehlt das oberste Fach des machinellen Ei‘s. Ihr Platz ist dessen mittleres Fach. Und von dort aus machen sie das Ei intelligent.

Nun noch einmal: Polypen werden von der KI-Verordnung nicht definiert und kaum geregelt. Anders bei Korallen und Korallenriffen. Für sie gibt es besondere Vorschriften. Dazu gleich mehr.

Merken wir uns erst einmal das Bild, das die generative Intelligenz symbolisiert:

GPAI-MODELL = KORALLE

KORALLE IN BUNTEM EI

Die Koralle ist erst spät im EU AI Act aufgenommen worden. Nach dem Aha-Effekt – als ChatGPT veröffentlicht wurde: Viele Vorschriften der KI-Verordnung sind überwiegend oder ausschließlich mit dem GPAI-Modell verbunden. Nicht ohne Grund!

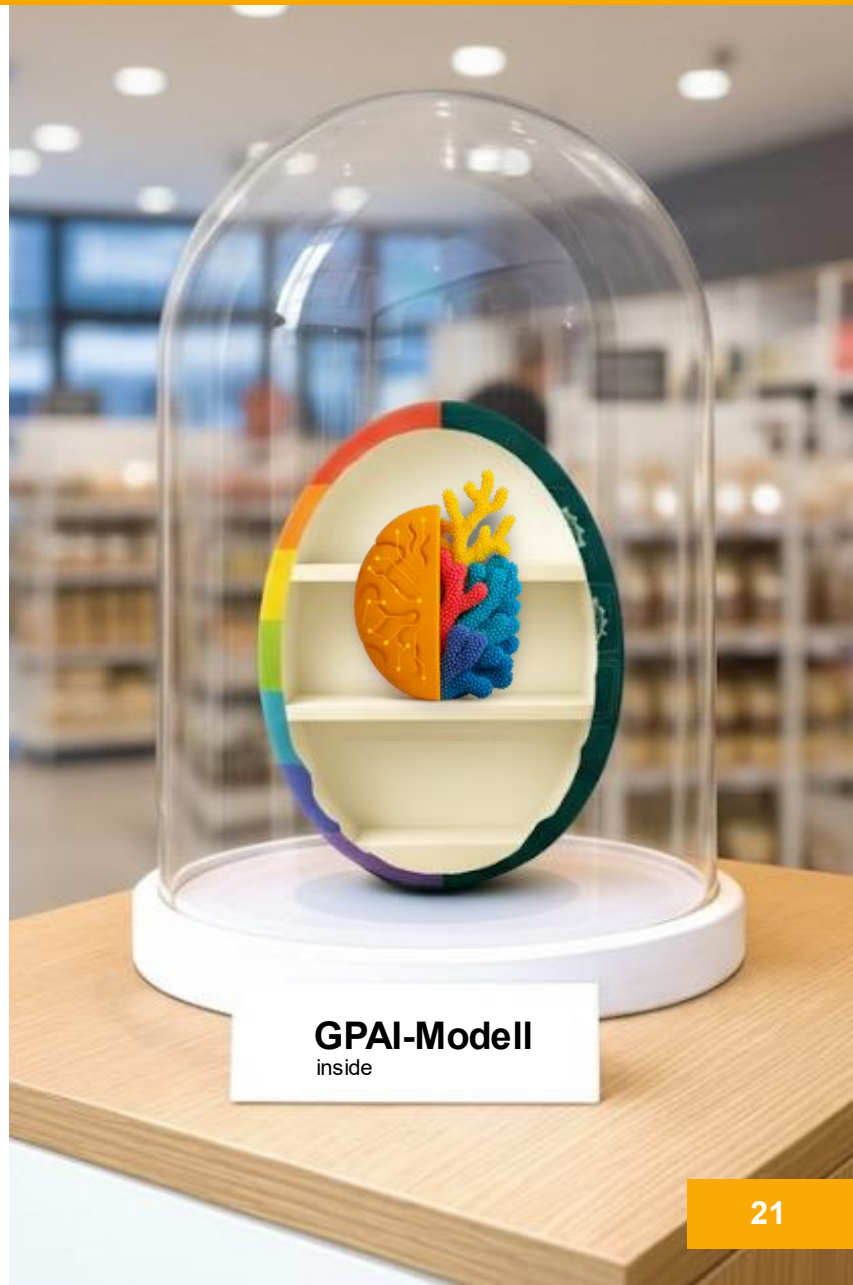
Es ist der Motor des GPAI-Systems. Das ist ein ganz besonderes leistungsfähiges KI-System:

- Sein Gehirn ist kein kleiner spezialisierter Polyp, sondern die große vielseitige Koralle.
- Das Ei des GPAI-Systems ist daher ebenso bunt wie die Koralle. Wie ein Regenbogen.
- Die vielen Farben repräsentieren die Vielseitigkeit des GPAI-Systems: Es kann viele Aufgaben mit hoher Kompetenz erledigen.

Wir werden noch sehen, wie sinnvoll es ist, die verschiedenen Eier-Typen sowie die darin befindlichen Polypen, Korallen oder Korallenriffe zu unterscheiden.

Wichtig ist, dass wir nun wissen, dass es verschiedene KI-Systeme (normales KI-System und GPAI-System) und dass es mehrere Modelle gibt (spezifisches KI-Modell, GPAI-Modell sowie GPAI-Modell mit systemischen Risiken).

Toll, wie schnell du lernst!



DIE KI-MODELL-FAMILIE

Der EU AI Act kennt also mehrere KI-Modelle, und er definiert auch verschiedene KI-Systeme. Ein Spielzeug nutzt meist ein einfaches KI-System. Es wird mit Batterien betrieben und kann wenige, aber spezielle Funktionen ausüben. Es lässt eine Spielzeug-Puppe sprechen oder die Augenfarbe ändern. Im magischen Ei arbeitet dann ein Mini-KI-Modell.

Ähnlich und doch anders ist es bei einem Fertigungsroboter. Er kann mit einem spezialisierten KI-System, das ein selbstlernendes KI-Modell enthält, erstaunliche Dinge vollbringen. Der EU AI Act reguliert nicht die Polypen, also die spezialisierten KI-Modelle. Es gibt einfach zu viele mögliche KI-Techniken auf Ebene der KI-Modelle. Der EU AI Act will technisch neutral bleiben, denn die Innovation von KI-Modellen schreitet rasant voran. Reguliert ist daher nur das KI-System, also das maschinelle Ei, in das ein Polyp integriert wurde. Das reicht aus.

Integriert man nun ein GPAI-Modell (also eine Koralle) in ein KI-System, dann entsteht wie von selbst ein GPAI-System. Häufgster Fall ist – wie auf dem rechten Bild – ein KI-Chatbot: Er kann unglaublich vielseitig sein: Texte erstellen und Musik produzieren und mit Menschen interagieren. Die Koralle allein kann das nicht, denn ihr fehlt das oberste Fach zur Interaktion. Gleichwohl ist die Koralle reguliert. Wer sie anbietet, besitzt Transparenzpflichten. Dazu gleich mehr.

Nun erfahren wir, wie die Koralle das GPAI-System zu einem Multitalent macht!

VIELSEITIG UND KOMPETENT

Erst die Koralle macht das sie umgebende GPAI-System zum echten Alleskönner:

- Es kann mit seinem Weltwissen Fragen aller Art beantworten.
- Es kann Kochrezepte empfehlen und individuelle Schönheitstipps geben.
- Es kann fremde Länder beschreiben oder Urlaubstrips empfehlen.
- Häufig kann es auch Bilder und z.T. sogar Sounds und Videos perfekt erstellen.

All das auf Basis der vielen Fähigkeiten einer bunten Koralle! Ihre Trainingsdaten erlauben auch die Vernetzung von Information z.B. eine Bildbeschreibung nach einem Image-Upload, oder dessen Veränderung auf Basis textlicher Vorgaben.

Diese multimodalen GPAI-Modelle, die Bild, Sprache und vieles mehr beherrschen, ermöglichen enorme Chancen:

- Für Privatpersonen
- Für Unternehmen
- Für Organisationen

Der wahre Alleskönner ist also das GPAI-Modell. Doch ohne das umgebende GPAI-System bleibt die Koralle arbeitslos: Sie erhält weder Inputs, noch kann sie Outputs generieren. Sie ist wie ein Motor ohne Karosserie. Und umgekehrt genauso: Ohne das GPAI-Modell ist das umgebende GPAI-System einfach nur normale Software.

Eine, die nicht dem EU AI Act unterliegt, weil ein magisches Ei ohne eine Koralle, einen Polypen oder einem riesigen Korallenriff im mittleren Fach nicht wirklich intelligent ist.

Apropos Korallenriff: Schauen wir uns doch dieses GPAI-Modell noch etwas näher an. Es ist ein besonders großes KI-Modell mit allgemeinem Verwendungszweck. Es hat aber zusätzlich systemische Risiken. Diese Risiken entstehen u.a. durch sehr große Leistung oder eine besonders hohe Verbreitung.

Korallenriffe sind maximal vielseitig. Deshalb sind sie oft sehr begehrt. Doch genau das führt bei einem Korallenriff zu einzigartigen Risiken. Welche das sind, erfahren wir durch einen Blick in das Ökosystem des Korallenriffs.

Eine faszinierende Welt!

SCHÖN UND DOCH RISKANT

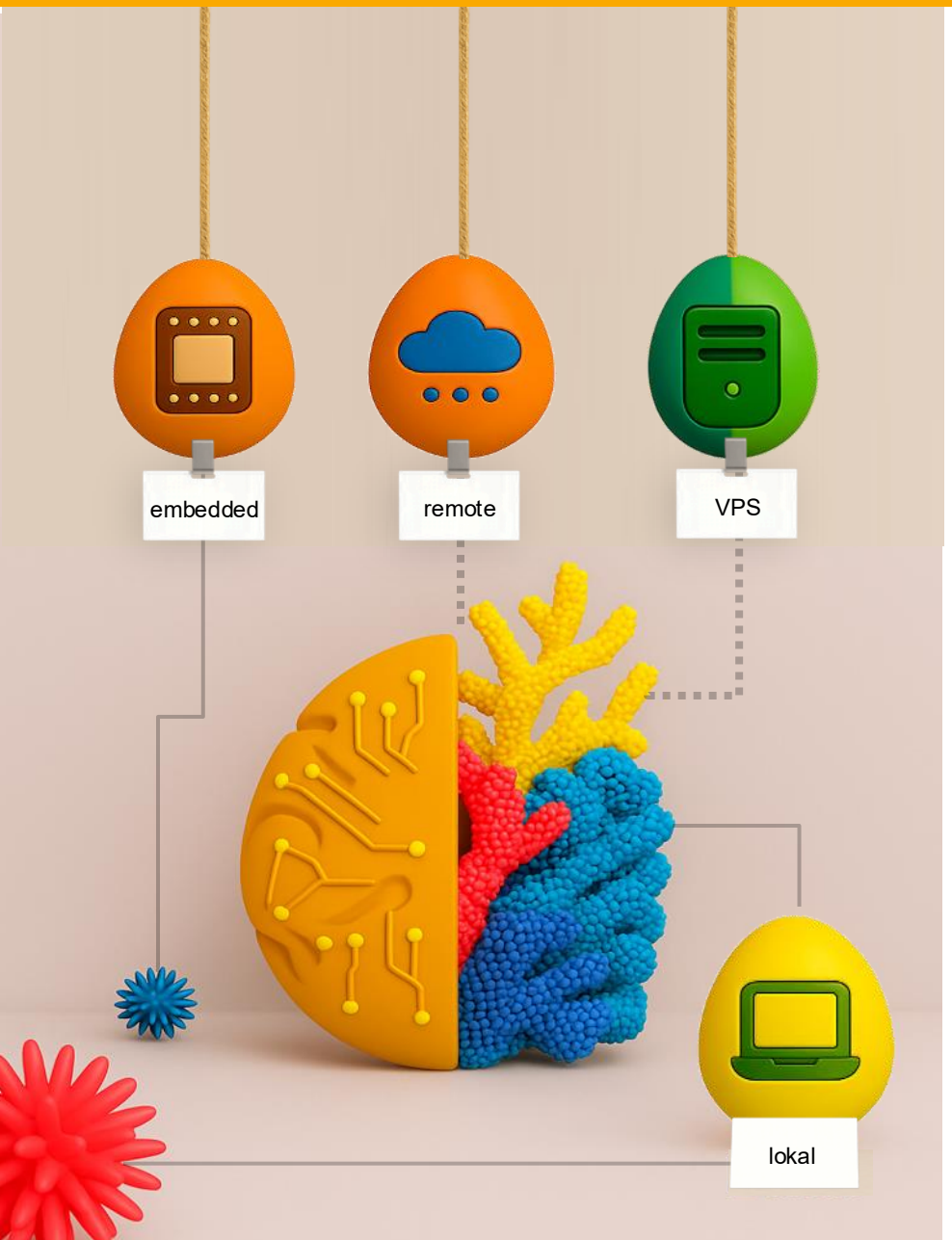
Es scheint offenkundig: Je größer und vielfältiger die Korallen werden, je mehr sie sich zu einem riesigen, wunderschönen Korallenriff entwickeln, desto stärker wird ihre Anziehungskraft. Immer mehr Fische strömen herbei.

Doch genau darin liegt auch eine Gefahr:

- Was anfangs ein farbenfroher Lebensraum war, wird durch seine Reichweite und Vernetzung zu einem hoch vernetzten Gesamtsystem, in dem ein einziger Fehler weitreichende Folgen haben kann.
- Ein riesiges Riff bringt nicht nur Vielfalt, sondern auch Verwundbarkeit: U.a. die Gefahr einer Korallenbleiche.

Wenn etwas kippt, dann betrifft es plötzlich alle – das ganze Ökosystem: Aufgrund systemischer Risiken! Sie sind unsichtbar, komplex und über die gesamte Wertschöpfungskette vorhanden. Deshalb unterliegen die besonders großen und weltweit verbreiteten GPAI-Modelle in der EU besonderen Sicherheitsauflagen. Das macht es für ihre Anbieter anspruchsvoller, aber für die Gesellschaft insgesamt sicherer. Das ist gut so!

Beachten wir also: GPAI-Modelle mit systemischen Risiken unterliegen zusätzlichen Auflagen. Sie sorgen dafür, dass eine Korallenbleiche nicht zur Zerstörung ganzer Ökosysteme führt. Aber wie passt ein riesiges Korallenriff eigentlich in ein maschinelles Ei?



INTEGRATION DER KI-MODELLE IM KI-SYSTEM

KI-Modelle können auf unterschiedliche Art und Weise mit KI-Systemen verbunden sein. Die Verbindungsart entscheidet u.a. darüber, wie flexibel, leistungsfähig oder kontrollierbar das Gesamtsystem ist.

Von den folgenden vier Varianten sollte man zumidest schon mal gehört haben:

a) Remote (über eine öffentliche Cloud)

- Das Modell läuft auf einem entfernten Server (z. B. OpenAI, google, AWS, Azure).
- Das System sendet Anfragen über eine Schnittstelle (API mit API-Key).
- Der Vorteil: Hohe Rechenleistung, aktuelle Modelle und super Infrastruktur.
- Der Nachteil: Abhängigkeit u. Datenschutz.

b) VPS (Virtual Private Server)

- Das Modell läuft auf einem eigenen privaten, aber entfernten Server.
- Der Zugriff erfolgt kontrollierter als bei öffentlichen Cloud-Diensten.
- Der Vorteil: Gute Kontrolle u. Skalierbarkeit.
- Der Nachteil: Wartungsaufwand und das Erfordernis versierter KI-Expertise.

c) Lokal (auf lokalen Computer o. Server)

- Das Modell wird auf dem Gerät oder Netzwerk des KI-Systems betrieben.
- Es ist keine Internetverbindung nötig.
- Der Vorteil: Guter Datenschutz, geringe externen Abhängigkeiten.
- Der Nachteil: Eingeschränkte Rechenleistung, aufwändige Updates.

d) Embedded (in Gerät o. Chip integriert)

- Das Modell ist fest im KI-System eingebettet, z. B. in einem Roboter oder IoT-Gerät.
- Der Vorteil: Realtime-Fähigkeit, extrem niedrige Reaktionszeit, Energieeffizienz.
- Der Nachteil: Geringe Flexibilität, häufig keine Updates möglich o. aufwändig.

Obwohl die Integration nicht direkt vom EU AI Act reguliert wird, kann die Art der Anbindung u.a. darüber entscheiden, wer Anbieter ist oder nicht**.** Dazu mehr in Station acht.

Also: KI-Modelle können auf verschiedene Weise in ein KI- oder GPAI-System integriert werden!

Unabhängig davon nun ein paar Worte zu typischen Tücken – speziell von Korallen.

ES GIBT AUCH TÜCKEN VON KORALLEN

Nun zu einem besonders wichtigen Hinweis: Die Koralle hat viel mit dem menschlichen Gehirn gemeinsam: Da sind zunächst die Windungen die sich ähneln. Die Koralle kann zudem wie ein echtes Gehirn

1. logisch denken und
2. kreativ gestalten.

Bildlich gesprochen besitzen Korallen zwei Gehirnhälften. Diese können sich einerseits ergänzen, aber auch miteinander in Konflikt geraten. Dann entstehen überraschende Outputs und Antworten – sie werden „Halluzinationen“ genannt.

Das GPAI-Modell erfindet dann Dinge, die objektiv nicht stimmen, aber plausibel klingen. So kann es ein historisches Geschehen in allen Details beschreiben, nennt aber ein falsches Datum.

Und wenn die Koralle trotz aller Hinweise hartnäckig bei ihrer Behauptung bleibt und mit abenteuerlichen Argumenten begründet, weshalb sie recht hat, dann kommt es zum „Münchhausen-Effekt“: Das Modell beginnt, fortgesetzt zu „flunkern“.

Dies ist wichtig, denn wer eine Koralle in sein KI-System integriert und am Markt anbietet, trägt auch die Verantwortung, wenn die Koralle Fehler macht. Diese werden dem maschinellen Ei zugerechnet. Gleiches gilt für Verletzungen von Urheberrechten: Das GPAI-Modell kann selbst keine Werke ausliefern. Ihm fehlt das erste Fach mit den Interaktionsinstrumenten.

Deshalb und aus vielen anderen Gründen ist derjenige, der eine Koralle in sein KI-System integriert und es dadurch zum GPAI-System macht, auf wichtige Informationen angewiesen, z.B.:

- Wie wurde die Koralle trainiert?
- Mit welchen Daten und Methoden?
- Mit welchen Fähigkeiten (Bild/Text)?

Um diese Information zu gewährleisten, regelt der EU AI Act Rechte und Pflichten, die an bestimmte Akteure gebunden sind.

Schauen wir uns vor diesem Hintergrund zuerst die Akteure und danach die Risikoklassen und der sich aus der KI-Verordnung ergebenden Pflichten an!

MERKEN WIR UNS ZU STATION DREI – DEN GPAI-MODELLEN:

1. DAS GEHIRN EINES KI-SYSTEMS IST DAS KI-MODELL. DER EU AI ACT TRENNT DREI TYPEN: POLYPEN, KORALLEN UND KORALLENRIFFE.
2. KLEINE SPEZIFISCHE KI-MODELLE SIND POLYPEN. GROSSE VIELSEITIGE GPAI-MODELLE SIND BUNTE KORALLEN ODER KORALLENRIFFE.
3. DAS KORALLENRIFF BESITZT SYSTEMISCHE RISIKEN: ES MUSS DAHER BESONDERS GUT VOR DER KORALLENBLEICHE GESICHERT SEIN.
4. KI-MODELLE KÖNNEN AUF VERSCHIEDENE ART IN KI-SYSTEME INTEGRIERT WERDEN: U.A. REMOTE, VPS, LOKAL ODER EMBEDDED.
5. KORALLEN KÖNNEN HALLUZINIEREN UND FEHLER BEGEHEN. DAHER MUSS TRANSPARENT SEIN, WIE SIE FUNKTIONIEREN.

NUN GEHT ES WEITER MIT STATION VIER: DEN AKTEUREN

4. AKTEURE

AKTEURE: MULTIPLE HÜTCHENSPIELER

Nun zu den beiden wichtigsten Akteuren im Sinne der KI-Verordnung: Dem Anbieter und dem Betreiber.

Der EU AI Act nennt noch viele weitere Akteure z.B. den Produkthersteller, Einführer und Händler oder den Bevollmächtigten. Sie sind aber seltener oder zudem spezifischer.

Es ist auch so anspruchsvoll genug! Denn die Rollen im Sinne der KI-Verordnung sind nicht statisch. Sie können wechseln: So kann ein Akteur den Anbieter- als auch den Betreiber-Hut für ein KI-System und zusätzlich noch einen Hut als nachgelagerter Anbieter für ein GPAI-Modell tragen.

Was würde sich daher mehr anbieten als die Kopfbedeckung, um die wichtigsten Akteure zu unterscheiden?

Wir werden sehen, dass die Hüte ein ebenso nützliches wie unterhaltsames Element zur Unterscheidung von Akteuren sein können. In diesem Sinne sind alle in der KI-Verordnung definierten Akteure im positiven Sinne Hütchenspieler. Wer Hüte trägt, besitzt nicht nur Verantwortung, sondern z.T. auch Rechte.

Bevor wir das Farbenspiel beginnen können, müssen wir erst einmal seine Regeln lernen. Und das bedeutet: Wir müssen nicht nur die Rollen kennen, sondern auch ihren Bezug zu KI-Eiern, KI-Korallen und Korallenriffen.

So gibt es den Begriff „Anbieter“ im Sinne der KI-Verordnung in gleich vier Varianten:

- Als Anbieter eines KI-/GPAI-*Systems*.
- Als Quasi- bzw. Zweitanbieter eines KI- oder GPAI-*Systems*.
- Als Anbieter eines GPAI-*Modells*.
- Als nachgelagerter Anbieter eines GPAI- oder sonstigen KI-*Modells*.

Puh. Das macht die Kommunikation wirklich kompliziert! Man darf also nicht einfach nur „Anbieter“ sagen. Man muss auch ergänzen, wovon jemand Anbieter ist. Und: Zu welchem Zeitpunkt dies der Fall war oder ist.

Und die Hütchen helfen uns dabei, hier Übersicht und Ordnung hineinzubringen.

Halten wir fest: Akteure im Sinne des EU AI Acts tragen farbige Hütchen!

Akteur = Hütchenspieler

Beispiel: OpenAI

EIN AKTEUR MIT DREIFACHER KI-TIARA

Wir wissen nun, dass Akteure im Sinne der KI-Verordnung kleine Hütchen tragen. Und wir wissen, dass wir mehrere Rollen unterscheiden müssen.

Aus diesem Grund ist es auch möglich, dass ein Akteur gleich mehrere Hütchen trägt. So ist das linke Bild ein KI-Unternehmen wie google, OpenAI, mistral, deepseek oder Antrophic:

Diese Akteure bieten beides an:

- GPAI-*Systeme* als auch
- verschiedene GPAI-*Modelle*

Die GPAI-Systeme sind die Chatbots, die Namen wie gemini, ChatGPT oder Claude tragen. Wir erkennen sie als buntes Ei auf der rechten Seite des Bildes.

Und die GPAI-Modelle? Sie heißen z.B. bei OpenAI gpt-5, gpt-4o, gpt-4-mini usw. Die Figur hält sie als Koralle auf der linken Seite in ihrer Hand.

Damit zur dreifachen Tiara:

- Das gelbe Hütchen ist Symbol für die Rolle als Anbieter eines GPAI-Modells.
- Das orange Hütchen für die Rolle als Anbieter eines GPAI-Systems.
- Und das rote Hütchen signalisiert die zusätzliche Rolle als Betreiber des GPAI-Systems.

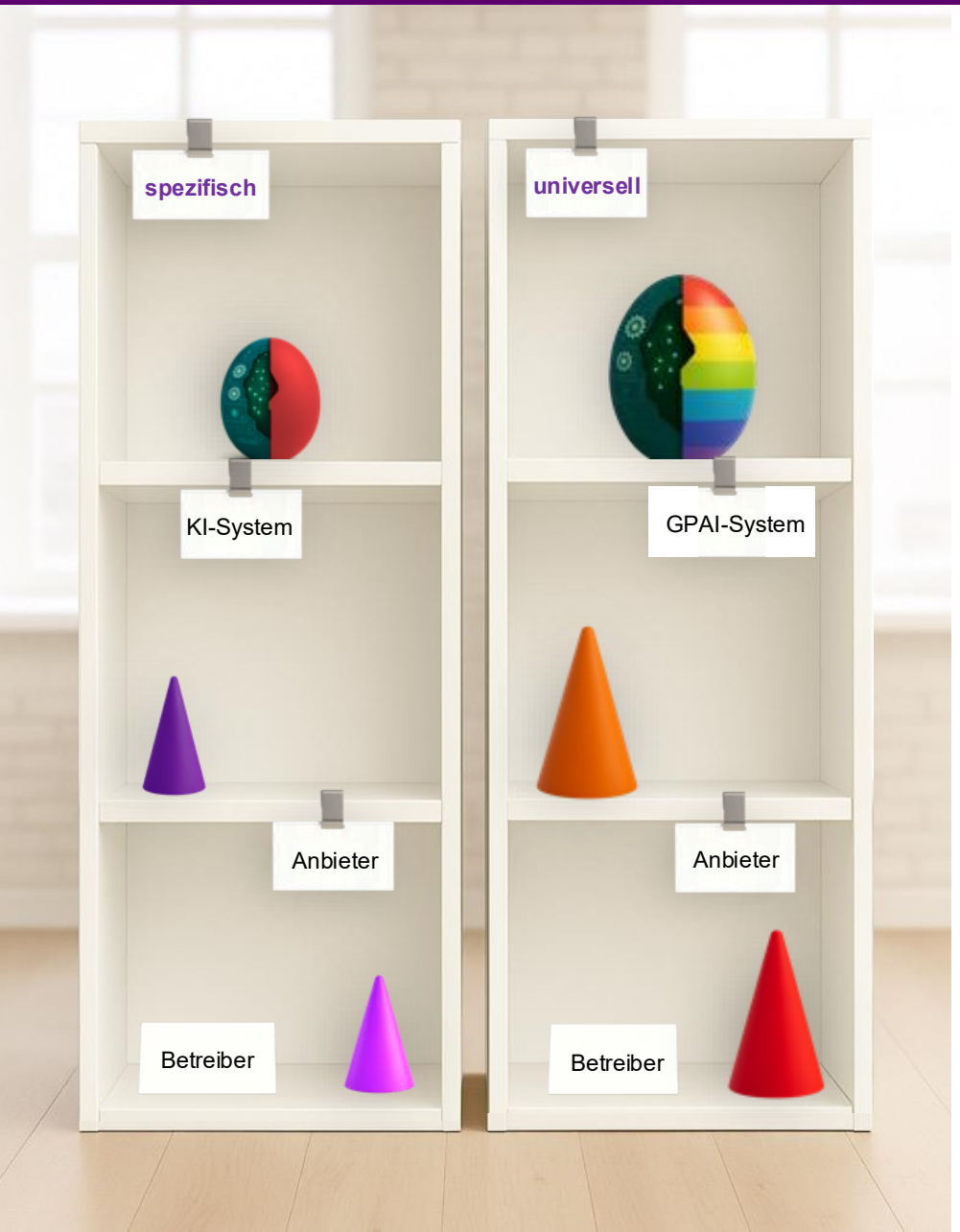
Streng genommen müssten Unternehmen wie OpenAI nicht nur ein gelbes Hütchen tragen, sondern für jedes einzelne GPAI-Modell, also jede Koralle bzw. Korallenriff eines. Dies ist wichtig, da jede Koralle andere Fähigkeiten hat.

Wir müssen hier erst einmal wissen, dass jeder Akteur entweder eine einzelne Rolle besitzen kann – dann nur ein Hütchen, z.B. ein pinkes oder rotes Hütchen als Betreiber.

Ein Akteur kann aber auch viele Hütchen tragen – wie hier als Anbieter eines GPAI-Modells (gelb) und GPAI-Systems (orange) sowie als Betreiber des GPAI-Systems (rot).

Auf den nächsten beiden Seiten erfahren wir, welche Hütchen es gibt und wofür ihre Farbe steht.

Prinzip klar? Dann weiter!



BETREIBER GIBT ES NUR BEI SYSTEMEN

Beginnen wir mit den Akteuren für die beiden System-Typen:

- Links das normale“, oft spezialisierte KI-*System* – symbolisiert durch ein einfarbiges, etwas kleineres Ei (links).
- Das vielseitige und daher bunte (und hier rechts etwas größer dargestellte) Ei als Symbol für GPAI-*Systeme*.

Für beide Varianten gibt es sowohl die Rolle des Anbieters als auch die Rolle des Betreibers. Das ist eine wichtige Aussage, denn wir lernen auf der nächsten Seite, dass es auch noch für GPAI-*Modelle* Anbieter gibt.

Betreiber gibt es dafür ausnahmslos nur für KI- und GPAI-*Systeme* – nicht für Modelle!

Nun zu den Hüten für Anbieter und Betreiber: Wir finden sie im mittleren und unteren Fach. Der Anbieter eines einfachen KI-Systems hat ein lila Hütchen und der Betreiber ein Hütchen in pink. Beide sind etwas kleiner als die entsprechenden Hütchen bei GPAI-Systemen. Sie sind ja spezialisiert.

Bei Korallen ist die Farbe für Anbieter orange und für Betreiber rot. So wissen wir: Wer ein rotes Hütchen trägt, ist Betreiber eines GPAI-Modells, und wer ein lila Hütchen trägt, ist Anbieter eines spezialisierten KI-Systems.

Wer den EU AI Act schon kennt, könnte fragen, warum beide KI-System-Typen andere Farben für die Rolle von Anbieter und Betreiber haben. Die KI-Verordnung sieht dies eigentlich nicht vor. Aber: Es gibt bestimmte Pflichten, die fast ausschließlich die Anbieter und Betreiber von GPAI-Systemen betreffen – und kaum die von einfachen KI-Systemen. Deshalb werden die Farben bewusst unterschieden.

Nun noch einmal zur Klarstellung:

- Trägt eine Figur ein oranges und ein rotes Hütchen, dann ist es ein Anbieter und Betreiber eines GPAI-Systems.
- Damit hat dieser Akteur auch doppelte Pflichten: Als Anbieter und Betreiber. Dazu später mehr in Station sechs.

Blicken wir jetzt auf die Modell-Typen – für die gibt es zwei weitere farbige Hütchen: Gelb und blau!

(NACHGELAGERTE) KORALLEN-ANBIETER

Die KI-Verordnung bestimmt, dass es bei KI-*Modellen* nur Anbieter von Korallen oder Korallenriffen gibt. Für kleine spezialisierte Polypen sieht die KI-Verordnung hingegen keine Anbieterrolle vor.

Deshalb fehlt das Hütchen auf der linken Seite unter dem Polypen: Eigentlich gibt es dieses Hütchen gar nicht. Aber eben nur eigentlich … Es ist ein wenig kompliziert, denn das fehlende Hütchen bedeutet am Ende nur, dass der Anbieter eines KI-*Systems* kein fremdes KI-*Modell* verwendet.

Daher kann es trotzdem einen nachgelagerten Anbieter des KI-Modells geben: Dann nämlich, wenn bei einem einfachen KI-System ein KI-Modell (also ein Polyp) verwendet wird, den jemand anders hergestellt hat. In diesem Fall wird der Anbieter dieses KI-Modells zum „nachgelagerten“ Anbieter des Polypen, der im KI-System verwendet wird.

Ganz ähnlich bei GPAI-*Modellen*: Nehmen wir ein Unternehmen, das seinen eigenen Chatbot nutzt und dafür ein GPAI-Modell von gemini, OpenAI oder Mistral verwendet:

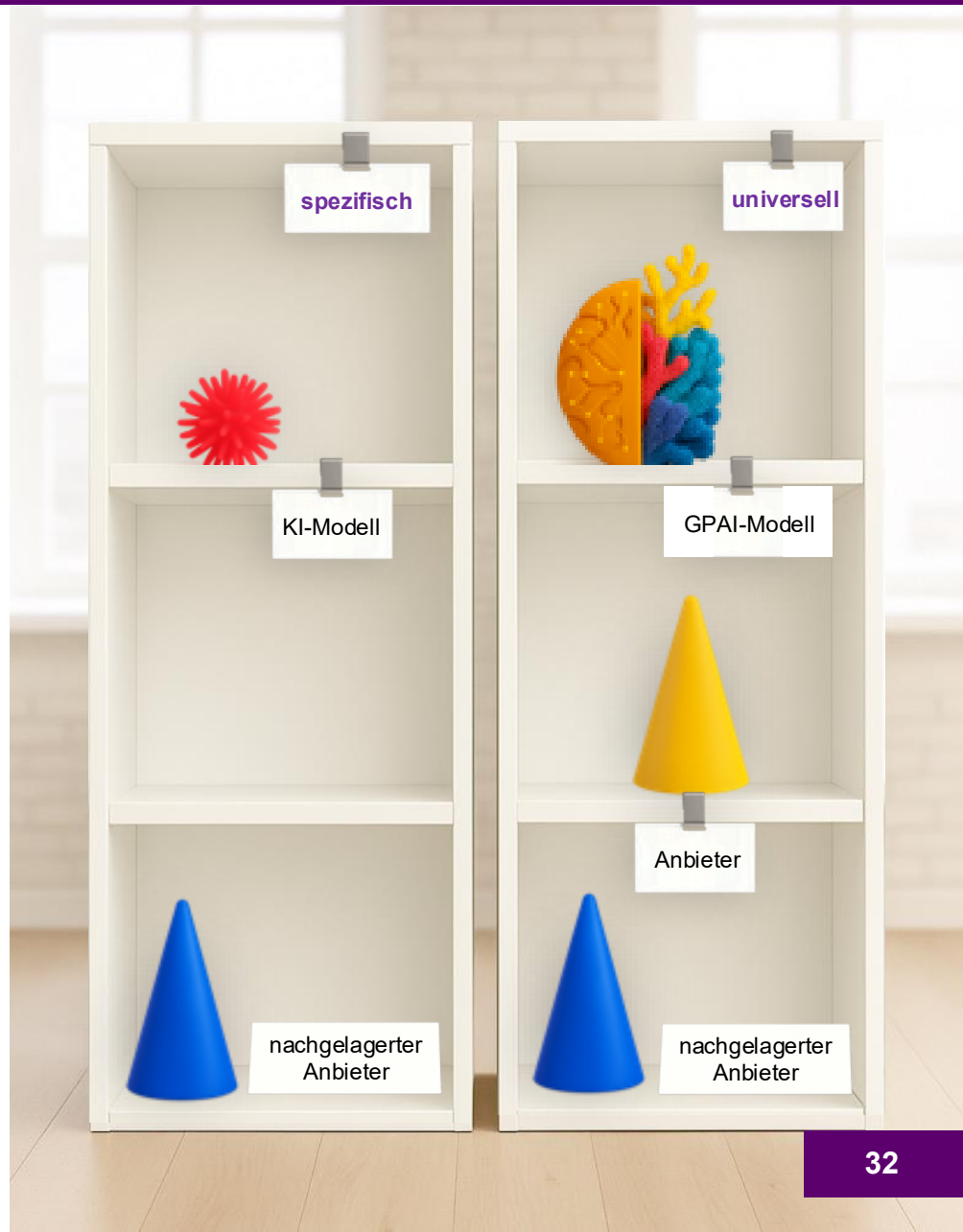
- Dann sind OpenAI, Google & Mistral die Anbieter des GPAI-Modells. Dann tragen sie ein gelbes Hütchen.
- Das Unternehmen, das diese Modelle verwendet, ist dann nachgelagerter Anbieter des GPAI-Modells und trägt ein blaues Hütchen.

Das ist wichtig, denn so hat der nachgelagerte Anbieter von GPAI-Modellen einen Anspruch auf vielerlei Informationen über das GPAI-Modell: Wie wurde es trainiert? Mit welchen Daten etc.?

Blaues Hütchen bedeutet somit, dass ich als Anbieter eines KI- oder GPAI-Systems kein eigenes, sondern ein fremdes KI-Modell benutze.

Integriert man ein GPAI-Modell, hat man Ansprüche gegen dessen Anbieter, der bei GPAI-Modellen ein gelbes Hütchen trägt.

Um diese und die Seite davor noch einmal im Zusammenhang darzustellen, werfen wir nun einen Blick auf eine KI-Wertschöpfungskette. Dann wird das Ganze noch klarer.



DIE GPAI-HÜTCHENKETTE – VOM ANBIETER DES MODELLS BIS ZUM NUTZER

Figur Nr. 1 ist Anbieter eines GPAI-Modells, also z.B. google, OpenAI oder Mistral. Daher das gelbe Hütchen für die Koralle. Figur Nr. 2 ist Anbieter des bunten GPAI-Ei‘s und nachgelagerter Anbieter der GPAI-Koralle.

Daher besitzt diese Figur zwei Hütchen (blau & orange). Figur 3 ist Betreiber des GPAI-Systems. Sie trägt deshalb ein rotes Hütchen. Die vielen Nutzer des Systems tragen (zunächst) keine Hütchen. Sie haben nämlich keine rechtlich definierte Rolle.

Die verschiednen Farben der Hütchen helfen nicht nur, die Rollen der verschiedenen Akteure zu erkennen. Sie verdeutlichen auch das Inverkehrbringen und die Inbetriebnahme. Weshalb? Das erfahren wir auf der nächsten Seite.

INVERKEHRBRINGEN, INBETRIEBNAHME UND VERANTWORTLICHE VERWENDUNG

Bleiben wir daher noch einen Moment bei dem vorherigen Bild. Ein Inverkehrbringen kann bereits vorliegen, wenn ein Anbieter einer Koralle oder eines GPAI-Systems oder sonstigen KI-Systems dieses an den Vertrieb zum Verkauf übergibt. Und eine Inbetriebnahme kann schon dann vorliegen, wenn ein KI- oder GPAI-System im Intranet intern genutzt wird. Mit Inverkehrbringung werden Akteure zu Anbietern und mit der eigenverantwortlichen Nutzung werden Akteure (zusätzlich) zu Betreibern.

Die vielen Farben der Hütchen helfen aber nicht nur, die Rollen der verschiedenen Akteure zu erkennen. Sie verdeutlichen auch die Verbreitung der verschiedenen Rollen im Weltatlas der KI-Akteure. Den lernen wir jetzt kennen.

DER WELTATLAS DER KI-AKTEURE

Die KI-Verordnung gilt nur in der EU. Sie betrifft die Akteure, die KI-Technologie in der EU anbieten oder betreiben. Es gibt aber auch Akteure von außerhalb der EU, die KI-Systeme erstellen und in der EU in Verkehr bringen oder in Betrieb nehmen.

Die Weltkarte der KI-Akteure verdeutlicht insofern mehreres gleichzeitig:

- Unternehmen von außerhalb der EU müssen die Regeln und Sicherheitsstandards genauso wie europäische Unternehmen einhalten, ...
- … wenn sie KI- auf den europäischen Markt bringen oder deren Ergebnisse dort genutzt werden.

Und damit zu einer wichtigen Botschaft des Akteur-Weltatlas: Er zeigt, dass aus der EU vor allem Anbieter und Betreiber von spezialisierten KI-Systemen kommen. Solche, die keine GPAI-KI sind.

Die großen Anbieter für GPAI-Modelle sowie Anbieter und Betreiber von weltweit genutzten GPAI-Systemen kommen nämlich fast alle aus den USA und China.

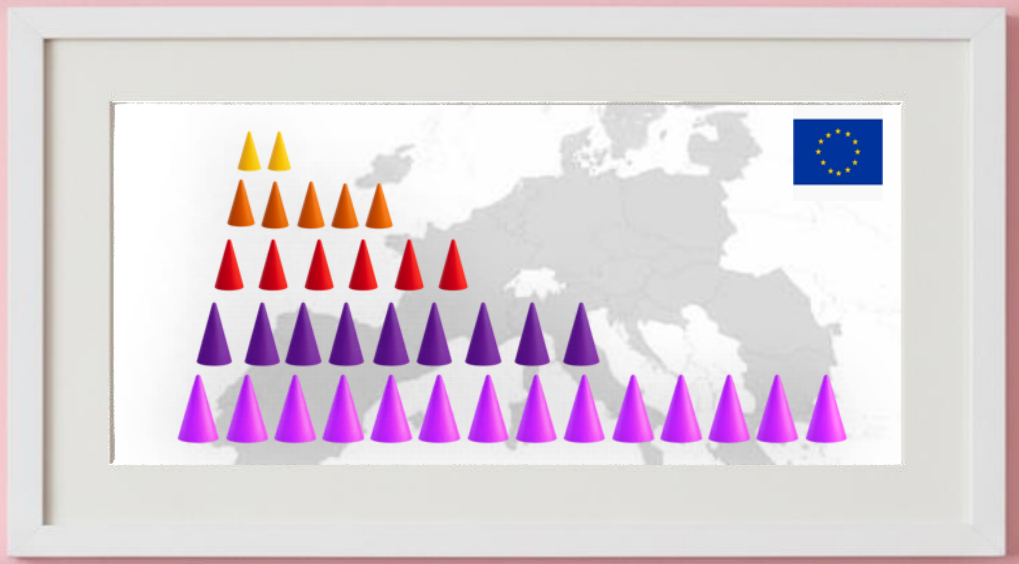
Insofern gibt es in der EU kaum Anbieter mit gelben Hütchen. Dafür ganz viele Betreiber mit pinken Hütchen: In nahezu allen Branchen findet man sie: Die Betreiber von spezifischen KI-Systemen. Hinzu kommen die vielen Anbieter für spezifische KI-Systeme aus der EU (lila).

Orange und rote Hütchen sind auch verbreitet – weil viele Unternehmen und Behörden ihre eigenen Chatbots entwickeln lassen und selbst anbieten bzw. betreiben.

Aber: Die meisten Nutzer verwenden nach wie vor die GPAI-Modelle und -Systeme aus den USA und China. Und genau deshalb unterliegen ihre weit verbreiteten Services besonderen Kriterien: Sie sind aufgrund ihrer Verbreitung Korallenriffe und bergen das Risiko der Korallenbleiche! Dem gilt es in der EU vorzubeugen.

So, am Ende dieser Station wird es noch einmal richtig spannend: Wenn die Akteure die Hütchen wechseln oder sie neue Hüte dazubekommen.

Jetzt ein Hütchen-Trick



DIE NACHTRÄGLICHE ANBIETERSCHAFT

Schauen wir uns den Akteur auf der linken Seite erst einmal etwas genauer an:

- Er trägt unten ein pinkes Hütchen. Er ist also primär Betreiber eines spezifischen KI-Systems. Eines grünen Ei‘s.
- Darüber trägt die Figur aber auch ein lila-Hütchen. Sie ist also darüber hinaus zusätzlich Anbieter des KI-Systems.

Hmmm. Aber irgendwas stimmt hier nicht, denn Normalerweise ist die Reihenfolge andersrum:

- Zuerst unten das lila Hütchen des Anbieters …
- … dann erst das Betreiber-Hütchen …

Bevor ein KI-System in Betrieb genommen werden kann, muss es aber doch zuerst in Verkehr gebracht worden sein oder?!

Richtig. Der Regelfall ist: Anbieter-Hütchen zuerst, dann Betreiberhütchen. Gleiches gilt bei GPAI-Systemen (orange & rot).

Der lila Hut des Anbieters wurde hier nachträglich aufgesetzt. Zu einem Zeitpunkt, an dem die Figur bereits Betreiber gewesen ist.

Wie ist das möglich? Ganz einfach!: Es handelt sich hier um einen so genannten Quasi- oder Zweitanbieter. Beleg dafür sind der Schraubenzieher und das gleiche Logo auf Figur und Ei.

- Der Schraubenzieher zeigt, dass der Betreiber am Ei herumgeschraubt hat. Damit wurde es wesentlich verändert.
- Das Logo macht zudem deutlich, dass der Betreiber nach außen den Eindruck erweckt, selbst Anbieter zu sein. Zum Beispiel, indem das System unter einer eigenen URL mit eigenem Namen im Internet oder Intranet betrieben wird.

Beides führt zur Quasi-Anbieterschaft:

- Die wesentliche Veränderung eines KI-Systems und
- die Verwendung mit eigenem Namen oder mit eigenen Marken.

Besonders wichtig ist dies bei den Fällen von Hoch-Risiko-KI. Diese werden wir jetzt in Station fünf kennenlernen:

Den Risikoklassen

MERKEN WIR UNS ZU STATION VIER – DEN AKTEUREN:

1. DIE AKTEURE DER KI-VERORDNUNG HABEN ROLLEN. JEDE ROLLE HAT EIN HÜTCHEN MIT EINER EIGENEN FARBE.
2. EIN AKTEUR KANN MEHRERE HÜTCHEN TRAGEN: Z.B. ALS ANBIETER (LILA) UND BETREIBER (PINK) EINES SPEZIFISCHEN KI-SYSTEMS.
3. DIE HÜTCHEN VERDEUTLICHEN VERSCHIEDENE ROLLEN IN DER KI-WERTSCHÖPFUNGSKETTE – VOM ANBIETER BIS ZUM NUTZER.
4. IN DER EU SIND DIE GELBEN HÜTCHEN FÜR ANBIETER VON GPAI-MODELLEN SELTEN. HÄUFIG SIND DAFÜR DIE VON BETREIBERN (PINK).
5. QUASI-ANBIETER SIND BETREIBER, DIE NACHTRÄGLICH ZU ANBIETERN WERDEN KÖNNEN UND DAHER ZWEI HÜTCHEN TRAGEN.

NUN GEHT ES WEITER MIT STATION FÜNF: DEN RISIKO-KLASSEN

5. RISIKO-KLASSEN

DIE RISIKO-KLASSEN: TIERISCH ERNST!

KI ermöglicht unglaubliche Chancen. Aber: Sie birgt auch Risiken. Ein Gesetz wie die KI-Verordnung hat vor allem das Ziel, die Risiken von KI zu erkennen und zu entschärfen.

So weit so gut – aber was haben die Papageien und das grüne Etwas auf dem rechten Bild mit den Risiken von KI zu tun? Und was ist mit dem Vögelchen, der Schildkröte und dem T-Rex auf der Seite zuvor? Was ist ihr Bezug zu den beiden Eiern im Nest?

Ganz einfach: Sie symbolisieren unterschiedliche Risiken bei der Verwendung von maschinellen Eiern. Es geht um deren Output.

Und die gezeigten Tiere können alle als Output aus einem Ei herausschlüpfen, z.B.:

- Ein Vogel (und damit auch ein Papagei),
- eine Schildkröte,
- eine Schlange,
- oder ein Krokodil,

Und auch ein Dinosaurier ist potenzieller Output. Ein T-Rex: Der Urahn des Huhns – dem heutzutage vielleicht nächsten Verwandten des Urzeit-Giganten.

Der T-Rex gilt als eines der gefährlichsten Landlebewesen aller Zeiten. Er ist ausgestorben. Genau deshalb symbolisiert er jene Risiken, die unter allen Umständen verboten sein müssen – und somit quasi aussterben.

Schon wird klar: Aus Eiern können sehr unterschiedliche Outputs kommen, harmlose und richtig gefährliche. Manche davon sind so gefährlich, dass man sie verbieten muss.

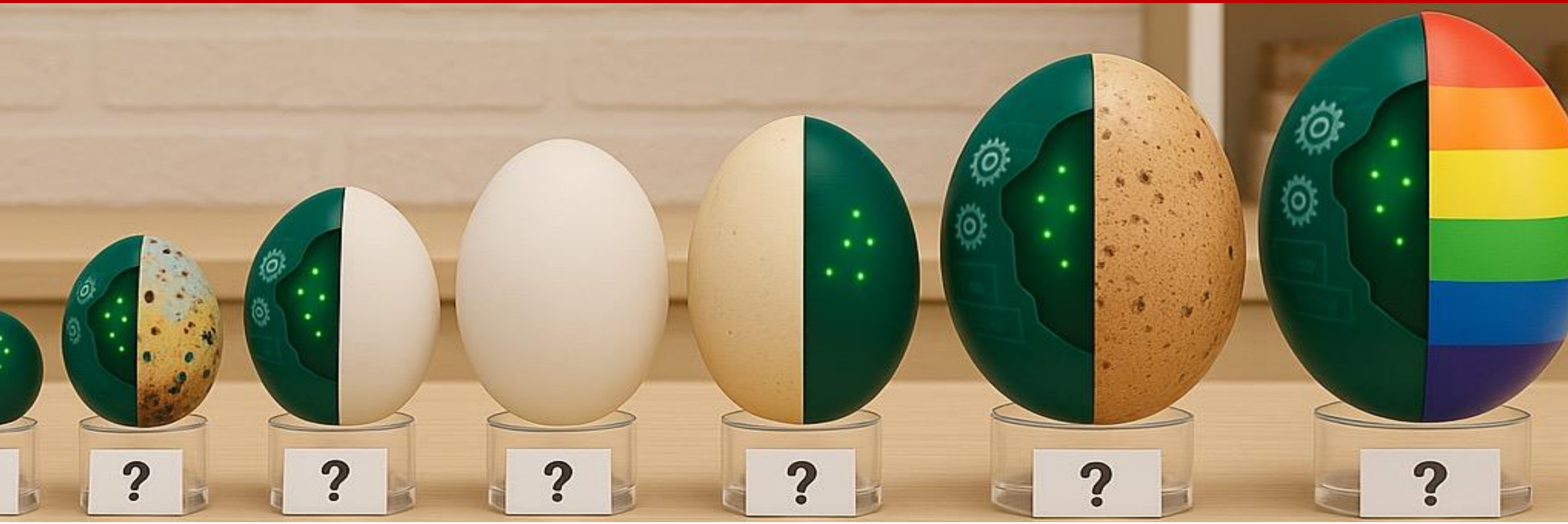
Damit schließt sich ein Kreis:

- Es gibt verbotene KI-Praktiken.
- Dann gibt es noch Risikoklassen für Hochrisiko-KI sowie für mittel und kaum riskante KI-Anwendungen.
- Die Risiko-Klassen des EU AI Acts beziehen sich auf KI-Systeme, also das maschinelle Ei – nicht auf die Modelle darin!

Und all die Tiere, die zuvor aufgezählt wurden, schlüpfen aus Eiern: Sie stehen für deren unterschiedliche Risiken.

Merken wir uns:

Risiko-Klasse = Tier aus Ei

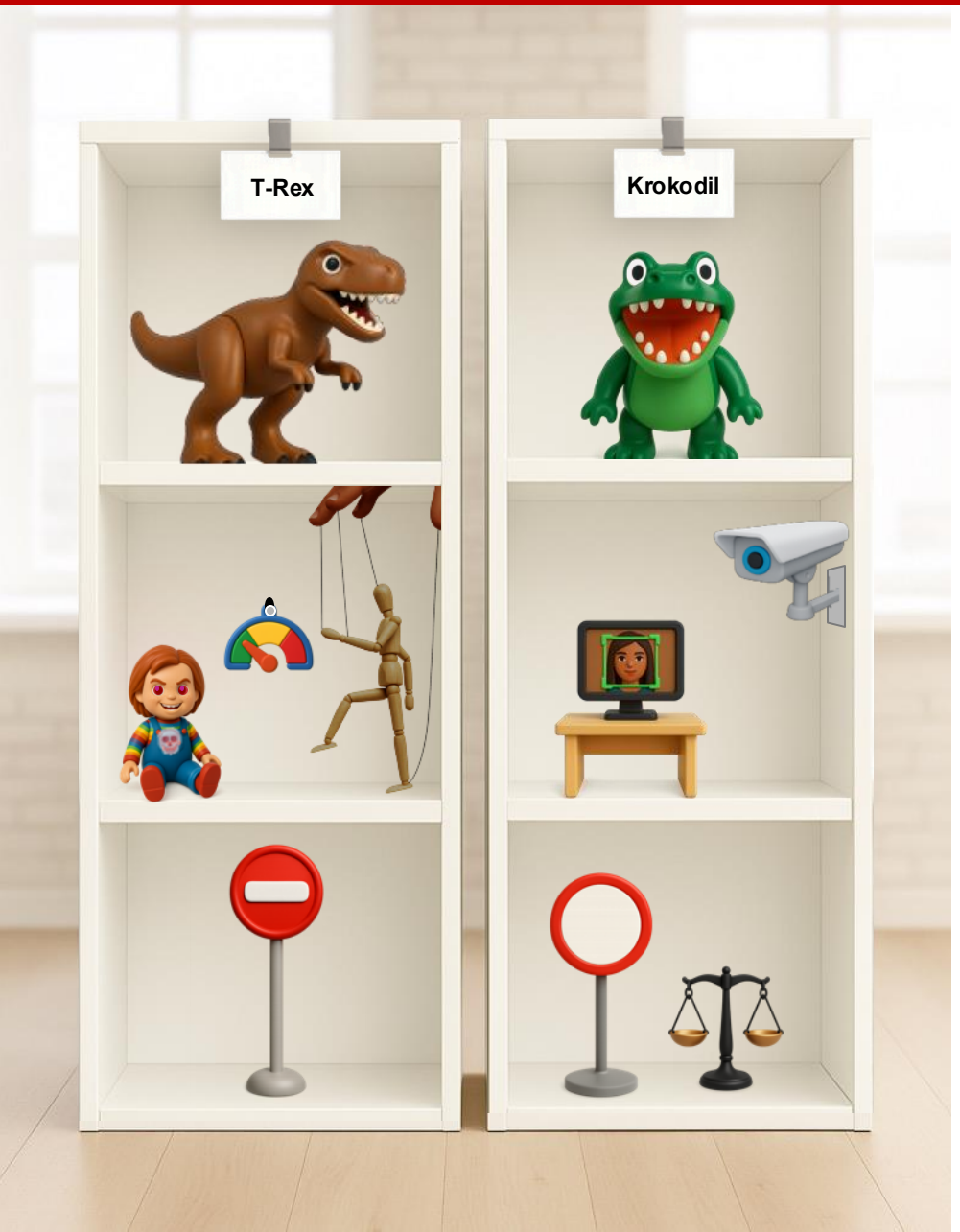


WELCHES EI IST HARMLOS? WELCHES IST RISKANT?

KI-Systeme sind in vieler Hinsicht Überraschungseier: Wir wissen nie ganz genau, was aus ihnen herausschlüpft. Von außen ist es kaum erkennbar. Wie wollen wir dann vertrauen? Woher wissen wir, welches Ei welche Risiken birgt?

Die KI-Verordnung enthält daher eine Art Güteklassen-System für KI-Eier. Darunter die Klasse der verbotenen KI-Praktiken und drei weitere Risiko-Klassen. Und das Gute: Den allermeisten KI-Eiern dürfen wir vertrauen! Sie sind Güteklasse 1 und damit voll vertrauenswürdig. Das gilt übrigens für alle Güteklassen. Vorausgesetzt, dass deren Vorgaben korrekt umgesetzt werden.

Natürlich mit Ausnahme der verbotenen KI-Praktiken. Die schauen wir uns jetzt näher an.



VERBOTENE KI-PRAKTIKEN: T-REX VS. KROKODIL

Es gibt zwei Arten verbotener KI-Praktiken im Sinne der KI-Verordnung:

- Solche, die ausnahmslos verboten sind („T-Rex“-Praktiken) und
- solche, die grundsätzlich verboten, aber unter Auflagen im Einzelfall erlaubt sind bzw. Ausnahmen besitzen („Krokodile“).

Wichtig ist dabei das Wort „Praktiken“: Es geht also um die Art, wie KI-Systeme verwendet werden: Sie führt zum Verbot der KI, die hinter einer Praktik steht.

Zunächst zu den verbotenen „T-Rex-Praktiken“. Ihr Verbot dient dem Schutz von besonders wichtigen Werten. So dürfen schutzbedürftige Menschen und Kinder nicht durch KI manipuliert werden. Auch Social Scoring ist absolut verboten. Es gibt noch weitere Verbote dieser Art.

Bei T-Rex-Verboten darf ein KI-System gar nicht erst in Verkehr gebracht werden. Ein Risiko darf sich also gar nicht erst realisieren – es geht um bestmögliche Prävention.

T-Rex-Verbote gelten für alle Verwender, egal ob staatlich oder wirtschaftlicher Art.

Damit zu den Krokodilen. Die sind – anders als der T-Rex – noch nicht ausgestorben. Aber trotzdem keine Schmusetiere.

Bei ihnen besteht ein grundsätzliches Verbot, aber eines mit Auflagen oder Ausnahmen:

- So ist z.B. die Emotionserkennung am Arbeitsplatz verboten. Aber: Es gibt u.a. die Ausnahme medizinischer Zwecke.
- Bestimmte Formen biometrischer Fernidentifikation sind ebenfalls verboten, aber unter strengen Auflagen erlaubt.

Einige Krokodil-Verbote betreffen allein den Staat: Er soll riskante KI nur unter bestimmten Voraussetzungen nutzen dürfen.

Insgesamt können wir froh sein, dass der EU AI Act weder T-Rex noch Krokodile frei herumlaufen lässt. Dies hilft, das Grundvertrauen in die KI-Nutzung zu erhöhen.

Um noch mehr Vertrauen zu bewirken, hat die KI-Verordnung auch noch solche Use Cases reguliert, von denen typischerweise hohe Risiken ausgehen. Die werden auf der nächsten Seite vorgestellt.

HOCH-RISIKO-KI IST OFT SPEZIFISCH

Bei den Hochrisiko-Use-Cases müssen wir zunächst betonen: Sie sind durchweg erlaubt. Viele Hochrisiko-KI-Anwendungen sind zudem sehr nützlich:

- Zum Beispiel medizinische KI
- oder KI für die Energieversorgung
- sowie intelligente Notrufbewertungen.

Hochrisiko-KI ist also nicht unbedingt „böse“. Es geht vielmehr in vielen Fällen darum, sicherzustellen, dass die Funktionen alle korrekt funktionieren und keine Fehler auftreten, welche die Gesundheit oder andere wichtige Güter wie die demokratische Grundordnung schädigen könnten.

Werfen wir nun zuerst einen Blick auf das linke Regal. Dort sehen wir das Symbol der Schlange. Es ist eine besonders positive Art: Eine Äskulapnatter. Sie ist seit der Antike das Symbol der Heilkunde, der Gesundheit und des ärztlichen Standes.

Darunter, im mittleren Fach, sehen wir die Symbole für weitere typische Hochrisiko-Use-Cases: Finance, Kritische Infrastrukturen oder Luftfahrt.

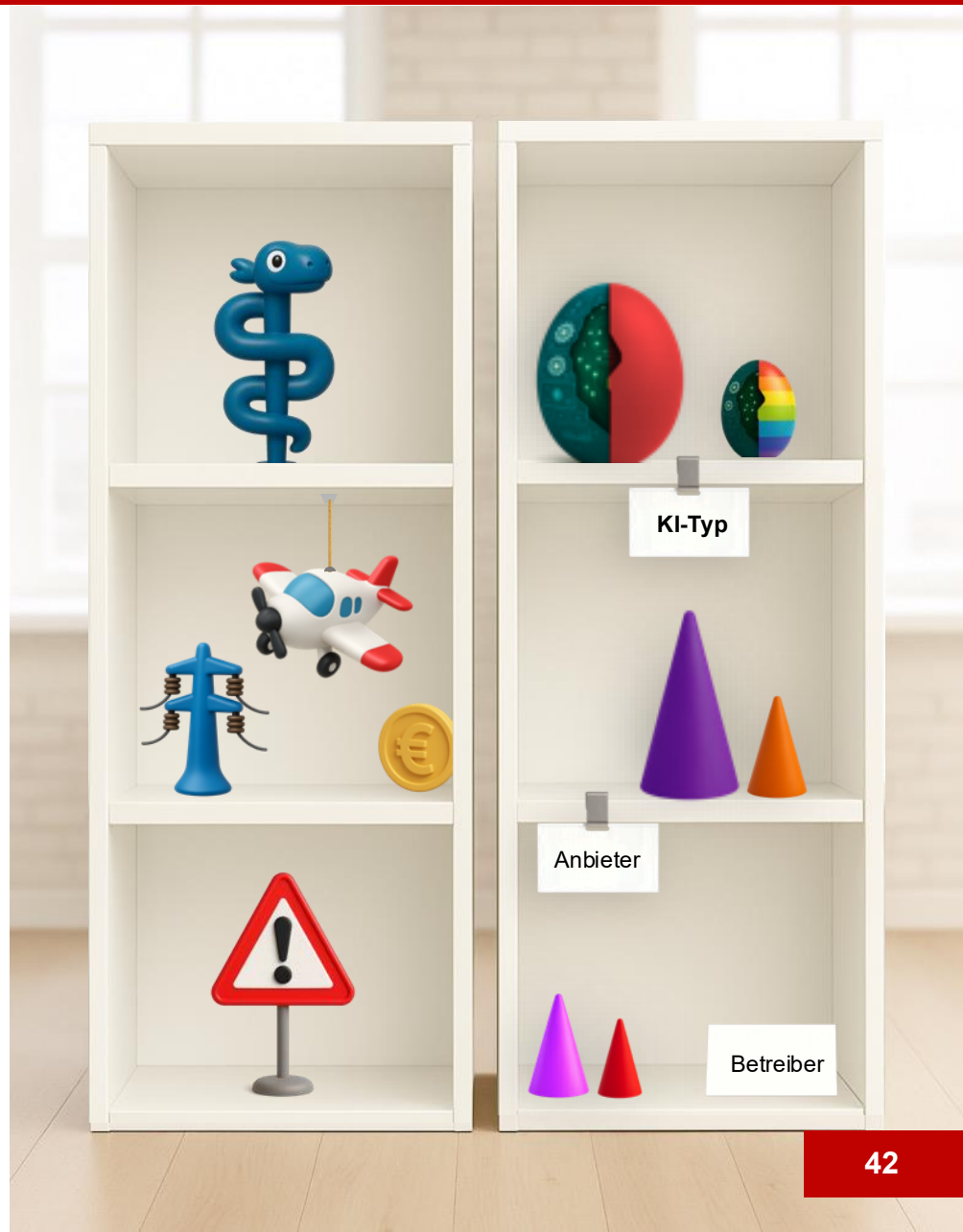
Natürlich gibt es noch viele weitere Fälle: Gerade am Arbeitsplatz muss beim Einsatz von KI ganz viel beachtet werden, u.a. um Diskriminierung vorzubeugen.

Schauen wir jetzt zur rechten Seite des Regals. Dort wird deutlich, welche Bedeutung die Hütchen im Risiko-Kontext haben.

Hochrisiko-KI steht oft mit spezifischen KI-Systemen im Zusammenhang (rotes Ei). Seltener ist die Kombi von GPAI-System (buntes Ei) und Hochrisiko-KI, z.B. bei Medizinischen Ratgebern oder HR-Prozessen.

Die besonderen Pflichten, die für Anbieter und Betreiber von Hochrisiko-KI bestehen, werden im rechten Regal unterschiedlich betont: Daher ist das rote Ei größer und auch die Hütchen für dessen Anbieter und Betreiber sind größer als beim bunten Ei und den dazugehörigen Hütchen – einfach deshalb, weil diese Kombi hier eher selten ist.

Das gleiche Prinzip gilt bei mittleren Risiken genau umgekehrt: Hier ist – wie wir gleich sehen werden – das bunte Ei viel häufiger anzutreffen.



MITTLERE RISIKEN: MEIST EIN FALL VON GPAI

Wie wir zuvor gelernt haben, können bestimmte KI-System-Typen besonders häufig bei einer der drei erlaubten Risiko-Klassen auftauchen.

Auf die mittlere Risikoklasse übertragen bedeutet dies: Hier sind besonders häufig GPAI-Systeme, also bunte Eier anzutreffen.

Das ist auch ganz einfach zu erklären: Um Deepfakes herzustellen, oder Fake News zu verbreiten oder Chatbots zu ermöglichen, die von Menschen kaum zu unterscheiden sind, benötigt man unglaublich große Datenmengen. Und die findet man vor allem in solchen KI-Systemen, die eine bunte Koralle oder sogar ein ganzes Korallenriff integriert haben.

Und das sind: GPAI-Systeme!

Deshalb macht es auch so viel Sinn, die Anbieter und Betreiber von GPAI-Systemen mit eigenen Hütchenfarben zu kennzeichnen. Bunte Eier unterliegen nämlich besonders häufig Transparenzpflichten!

Sie müssen kenntlich machen, wann man es mit einer KI und wann mit einem Menschen zu tun hat, falls man z.B. einen Beratungsservice benutzt. Oft sind die Stimmen eines Menschen oder einer KI kaum mehr zu unterscheiden. Genau das kann irritieren.

Da auch Papageien wie Menschen reden können, liegt es nahe, diesen bunten Vogel als Symbol dieser Risiko-Klasse zu verwenden: Er paßt auch farblich gut zum bunten Ei – oder?

Die positive Nachricht für alle, die ein spezifisches KI-System, also ein einfarbiges Ei mit einem Polypen darin anbieten oder betreiben: Bei ihnen spielen die Transparenz-Pflichten der mittleren Risikoklasse nur selten eine Rolle. Auszuschließen ist es jedoch nicht.

Und so haben wir hier nicht nur etwas über Risiken erfahren, sondern auch über ihre unterschiedliche Relevanz für Anbieter und Betreiber von bunten oder einfarbigen Eiern.

Kommen wir damit zu der letzten Gruppe der vier Risiko-Klassen: Den geringen Risiken.

SCHILDKRÖTEN: MIT ABSTAND AM HÄUFIGSTEN

Nun zur besten Nachricht: Die allermeisten KI-Use-Cases sind solche der geringen Risiko-Klasse. Das heißt, dass wir ihnen als Verbraucher und Anwender vertrauen dürfen – auch ohne große Vorgaben für deren Anbieter und Betreiber.

Das ist u.a. deshalb wichtig, weil die KI-Use-Cases dieser Risiko-Klasse nicht nur häufig, sondern auch besonders vielseitig sind: Man kann die vielen möglichen Varianten gar nicht aufzählen, die vorstellbar sind, z.B.:

- Intelligente Spamfilter,
- Übersetzungsprogramme oder
- selbstlernende Industrie-Roboter,
- clevere Zahnbürsten,
- KI in Home-Entertainment
- und, und, und …

Aus diesem Grund hat das linke Regal in der Mitte ganz viele farbige Bauklötzchen - als Symbol für die Vielfältigkeit dieser Risikoklasse. Für diese KI-Use-Cases heißt es: Freie Fahrt voraus!

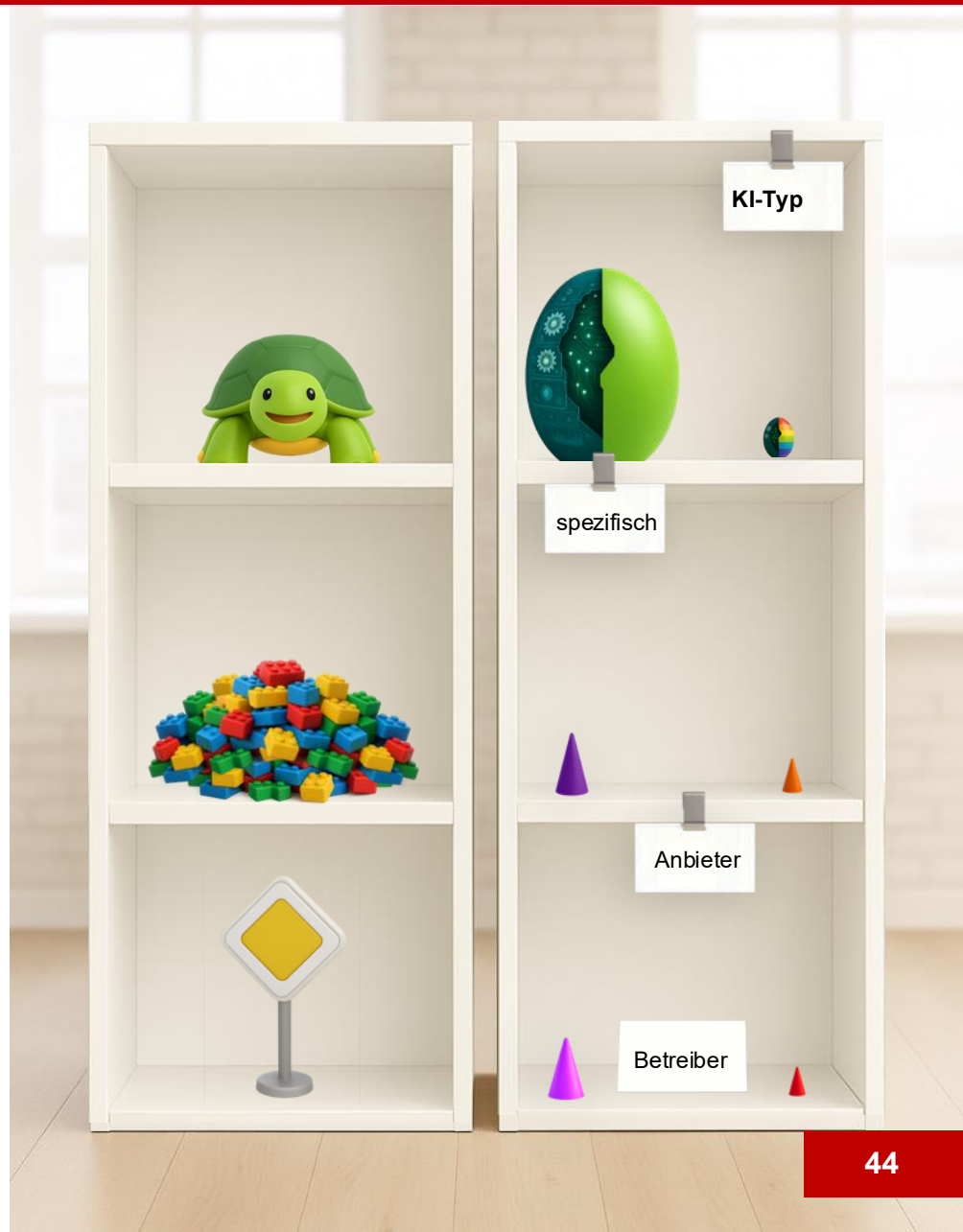
Das spiegelt sich auch auf dem rechten Regal wider. Dort sehen wir ein besonders großes grünes Ei. Spezialisierte KI-Systeme sind nämlich in dieser Gruppe überproportional häufig. Und das liegt daran, dass GPAI-Systeme, also die bunten Eier, hier besonders selten sind:

- Sie unterliegen meist der mittleren Risiko-Klasse, die zuvor dargestellt wurde.
- Sie haben daher Transparenzpflichten zu beachten, also können sie hier nur dann auftauchen, wenn sie für ganz einfache und spezielle Aufgaben eingesetzt werden. Das ist tatsächlich selten!
- Und dann besteht auch keine Verwechslungsgefahr mehr mit einem Papagei.

Die nächste gute Nachricht: Anbieter und Betreiber haben in dieser Risikogruppe auch kaum Pflichten zu erfüllen – bis auf eine. Denn sie müssen, ebenso wie alle Akteure der anderen Risiko-Gruppen, in ausreichendem Umfang KI-Kompetenz vermitteln.

Zu diesen und weiteren Aufgaben gibt es mehr Infos in der nächsten Station, denn T-Rex, Schlange, Papagei, Schildkröte …

… habe ich verstanden!



MERKEN WIR UNS ZU STATION FÜNF – DEN RISIKO-KLASSEN:

1. ES GIBT VIER RISIKO-KLASSEN: VERBOTENE KI-PRAKTIKEN UND USE-CASES MIT HOHEM, MITTLEREN UND GERINGEN RISIKEN.
2. VERBOTE SIND SEHR SELTEN. EINIGE GELTEN IMMER (T-REX). ANDERE BESITZEN AUSNAHMEN ODER AUFLAGEN (KROKODILE).
3. USE CASES DER HOHEN RISIKO-KLASSE SIND OFT SEHR NÜTZLICH (ÄSKULAP). GENAU DESHALB MÜSSEN SIE SICHER FUNKTIONIEREN.
4. MITTLERE RISIKEN BERUHEN MEIST AUF GPAI. EINE KI KANN WIE EIN PAPAGEI IMITIEREN. ES MUSS KLAR SEIN, WANN DIES DER FALL IST.
5. DIE GERINGEN RISIKEN SIND VIELFÄLTIG UND BESONDERS HÄUFIG: MERKEN WIR UNS DAZU DIE FREUNDLICHE SCHILDKRÖTE.

NUN GEHT ES WEITER MIT STATION SECHS: DEN PFLICHTEN

6. PFLICHTEN

DAS THEMA RUHIG ANGEHEN!

Zu allererst: Relax! Überall wird von den vielen Pflichten geredet, die jetzt (angeblich) auf alle Akteur-Typen zukommen. An vielen Stellen wird Handlungsdruck aufgebaut, der so wie er von einigen schwarzen Schafen geschäftstüchtig überdramatisiert wird, nur selten besteht bzw. nur wenige betrifft!

Das soll die Wichtigkeit der Pflichten nicht herunterspielen. Im Gegenteil: Wer Pflichten hat, muss diese ernst nehmen und gewissenhaft umsetzen.

Die KI-Verordnung ist aber kein Sprint. Eher ein Langstreckenlauf. Daher muss man sich seine Energie gut einteilen und zu frühe unnötige Sprints meiden – sonst geht viel Energie und Motivation umsonst verloren.

Wichtig ist, sich auf das Wesentliche zu konzentrieren. Also das, was im Hinblick auf die Pflichten unbedingt beachtet werden muss. Dazu gehört auch, dass der EU AI Act eben nicht nur Pflichten, sondern auch wichtige Rechte gewährt. Gerade im Rahmen von komplexen KI-Wertschöpfungsketten, die wir bereits kennengelernt haben.

Insofern eine ernste Empfehlung: Man muss die KI-Verordnung unbedingt beachten, aber alles benötigt auch Zeit – und vor allem Ruhe. Durch Hektik entstehen oft Frustration und unnötige Fehler.

Die einzigen, die schon jetzt wirklich auf der Hut sein müssen, sind T-Rex und Krokodil. Wer sie sieht (oder ein Krokodil das keine Erlaubnis) hat, dann sollte man das sofort einer Behörde melden!

Und ja: Auch der Papagei muss frühzeitig beachtet werden. Aber wir haben ja auf den Seiten davor gelernt, dass die meisten KI-Use-Cases Schildkröten sind. Diese müssen nur ganz wenige Pflichten beachten. Und das ist gut so.

Und was ist mit der nützlichen Äskulap-Schlange? Ok, auf die kommt durchaus noch einiges zu. Aber erst nach und nach. Es gibt nämlich angemessene Übergangsfristen.

Wir sollten das Thema Pflichten daher so angehen: Konzentriert, gelassen und im Wissen, dass die meisten davon gut zu bewältigen sind.

PRIVATE NUTZUNG UND ANDERE AUSNAHMEN

Wieso war unser Akteur auf der Seite zuvor so entspannt? Ach ja: Er hatte gar kein Akteurs-Hütchen auf. Er ist nämlich ein rein privater KI-Nutzer. Damit fällt er unter eine von mehreren Ausnahmen des EU AI Acts.

Wer ein KI-System rein privat nutzt, muss eigentlich gar nichts beachten. Und das ist gut so! Hier ist volle Entspannung angesagt.

Private Nutzung meint aber auch 100% private Nutzung! Wer seinen privaten KI-Account geschäftlich nutzt, ist nämlich Betreiber und muss daher einiges beachten – abhängig davon, ob z.B. ein Fall von Hoch-Risiko-KI vorliegt oder Transparenzpflichten eingehalten werden müssen.

Ähnlich und doch anders ist es bei weiteren Ausnahmen der KI-Verordnung. Zum Beispiel der rein wissenschaftlichen Nutzung von KI-Systemen und GPAI-Modellen:

- Sie fallen auch unter die Ausnahmen des EU AI Acts.
- Aber auch hier muss man darauf achten, dass es wirklich freie Forschung ist.

Ähnliches gilt für die Verprobung von KI-Systemen. Damit gemeint ist das Testen, bevor es in Verkehr gebracht wird.

Schließlich bestehen auch bei quelloffenen KI-Systemen und GPAI-Modellen Ausnahmen.

Doch egal welche Ausnahmen von der KI-Verordnung möglich sind:

- Im Fall von Hochrisiko-KI kann es wieder anders sein. Dann ist z.B. Open Source keine Bereichsausnahme.
- Auch ein Chatbot kann als bunter Papagei das Open-Source-Privileg einschränken.
- Und auch bei der Verprobung von Hochrisiko-KI müssen bestimmte Regeln beachtet werden.

Wie wir jedoch zuvor gelernt haben, sind die meisten Use Cases harmlose Schildkröten. Bei ihnen und allen anderen Anwendungen ist vor allem eines wichtig:

Die Vermittlung von KI-Kompetenz! Gleich erfahren wir, was genau das bedeutet.

DAS HAUS DER KI-KOMPETENZ

Die vielleicht wichtigste Aufgabe aller Anbieter und Betreiber ist es, ausreichend KI-Kompetenz zu vermitteln. Solche, die dabei hilft, dass eine KI-Anwendung von möglichst vielen Anwendern sicher und vertrauensvoll genutzt werden kann.

Dahinter steht die empirische Erkenntnis, dass die falsche Bedienung von KI eine der häufigsten Ursachen dafür ist, dass Risiken von KI-Systemen (und z.T. auch von KI-Modellen) ausgehen.

Erinnern wir uns an das Beispiel mit der Biene: Sie ist ein sehr nützliches Tier, aber wenn man sie ärgert oder anderweitig nicht richtig behandelt, kann sie ihren Stachel ausfahren und empfindlichen pieksen. Wir müssen lernen, sie richtig zu behandeln!

Aber wie erlernt man KI-Kompetenz?

Einerseits ist jedes KI-System bzw. Modell individuell. Andererseits bestehen bei fast allen, die es verwenden, andere Vorkenntnisse und Aufgaben.

Vermittlung von KI-Kompetenz ist daher keine „one-size-fits-all“ Aufgabe. Es geht vielmehr darum, dass alle relevanten Personen ihr individuelles „KI-Kompetenzhaus“ erhalten. Und dieses Gebäude besteht aus unterschiedlichen Bausteinen.

Welche Bausteine dies sind, verdeutlicht das Bild auf der rechten Seite. Je nach Risiko-Klasse, Use Case und Rolle entstehen dann kleine bunte Häuschen, die bei jedem etwas anders aussehen.

Wichtig ist, dass die KI-Verordnung vorsieht, dass bei KI-Systemen jeder Risiko-Klasse auf die Vermittlung von ausreichend KI-Kompetenz zu achten ist. Also auch bei solchen mit geringen Risiken, denn gerade hier kann die falsche Bedienung dazu führen, dass per se wenig riskante KI plötzlich doch kritisch wird.

Zusammengefasst lässt sich sagen, dass es ein sehr wichtiges und zudem recht individuell zu lösendes Thema ist. Aber wenn man die richtigen Klötzchen kennt, kann man auch jedem das passende Häuschen bauen – und lediglich bei Hochrisiko-KI kommt dabei auch mal die Notwendigkeit für ein Kompetenz-Hochhaus heraus.

Nachdem wir nun eine wichtige Grundaufgabe für alle Akteure kennengelernt haben, geht es im nächsten Schritt um den KI-Lebenszyklus.

Doch zuerst merken wir uns:

KI-Kompetenz = buntes Haus

PFLICHTEN: ABHÄNGIG VON RISIKO-KLASSE, ROLLE UND LEBENSZYKLUS

Was muss man über die konkreten Pflichten wissen, die sich aus der KI-Verordnung ergeben? Vor allem, dass sie von vielen verschiedenen Faktoren abhängen. Eine wichtige Rolle spielt zum Beispiel der Lebenszyklus eines KI-Systems.

Der Begriff passt auch zum Symbol des Ei‘s, denn das entwickelt sich ja über die Zeit auch weiter. Auf dem Bild sehen wir typische Phasen der KI-Entwicklung. Und mancher Step, wie die Konformitätsbewertung, betrifft z.B. nur Hochrisiko-KI-Systeme.

Andere Pflichten hängen dafür vom KI-Typ ab sowie der Rolle, die wir an den Hütchen erkennen.

Wichtig ist, dass wir Pflichten nicht als einmalige Anfangsaktivität verstehen. Sie erstrecken sich über den gesamten Lebenszyklus einer KI!

FRISTEN UND SANKTIONEN

Der EU AI Act ist bereits in Kraft getreten. Doch für einige Pflichten (wie z.B. für Hochrisiko-KI) gibt es noch Übergangsfristen. Es gibt zudem einen Schutz für bereits bestehende KI-Systeme, die nicht verändert wurden. Es muss also nicht alles neu gemacht werden, was bereits erfolgreich eingesetzt wird.

Nichts desto trotz ist wichtig, dass vorhandene Pflichten ernstgenommen werden! Insofern kann es empfindlich teuer werden, wenn man sich nicht an die Regeln hält. Und dass man dabei erwischt wird, wenn man die Pflichten nicht umsetzt, ist gar nicht so unwahrscheinlich:

- Die KI-Verordnung enthält einen so genannten Hinweisgeberschutz.
- Ein solcher Hinweisgeber ist die Figur mit der Trillerpfeife.
- Durch sie kann einiges ans Tageslicht kommen, wenn man versucht zu mogeln.

Und wenn man mutwillig gegen ganz besonders wichtige Pflichten verstößt, dann kann ein KI-System auch vom Markt genommen werden …

Also: Das Nichteinhalten von Pflichten ist kein Kavaliersdelikt. Merken wir uns daher die Kasse, die Eieruhr und die Trillerpfeife!

MERKEN WIR UNS ZU STATION SECHS – DEN PFLICHTEN:

1. JA, ES BESTEHEN PFLICHTEN FÜR VIELE AKTEURE. WICHTIG IST JEDOCH, DAS THEMA KONTROLLIERT UND IN RUHE ANZUGEHEN!
2. BEACHTEN WIR, DASS ES RELEVANTE AUSNAHMEN GIBT: PERSÖNLICHE NUTZUNG, WISSENSCHAFT, VERPROBUNG UND OPEN SOURCE.
3. PERSONALISIERUNG VON KI-KOMPETENZ IST IMMER EINE WICHTIGE AUFGABE! MERKEN WIR UNS DAZU DAS KOMPETENZ-HAUS!
4. PFLICHTEN KÖNNEN ENTLANG DES GESAMTEN KI-LEBENSZYKLUS BESTEHEN. SIE SIND ALSO KEINE EINMALIGE AUFGABE!
5. MERKEN WIR UNS BEZÜGLICH PFLICHTEN: DIE EIERUHR (FRISTEN), DIE KASSE (SAKTIONEN) UND DIE TRILLERPFEIFE (HINWEISGEBER)

NUN GEHT ES WEITER MIT STATION SIEBEN: DEN DATEN

7. DATEN

KLEINE DATENPERLEN-KUNDE

Data is the new Oil? Nein: Daten sind Perlen! Denn es gibt sie in ganz unterschiedlicher Form und Farbe. Und zudem gibt es sie auch in variierender Qualität. Gerade bei KI ist die Qualität der Perlen besonders relevant.

Schauen wir zuerst auf die Korallenperlen, denn KI-Modelle sind Polypen oder Korallen. Dieser Datentyp ist daher im KI-Modell enthalten. Aber oft etwas unstrukturiert. Anders daher die Perlen in der Mitte: Sie sind System-Daten und strukturiert.

Und rechts? Das sind wertlose Kieselsteine. Von denen gibt es mehr als einem lieb sein kann!

Wichtig ist, dass wir verschiedene Arten von Daten von Beginn an unterscheiden: Korallen-Perlen und System-Perlen!

ECHTE UND SYNTHETISCHE KORALLENPERLEN

Die Korallenperlen wurden mit großem Aufwand in ein GPAI-Modell oder den einzelnen Polypen eintrainiert. Dabei sind aber nicht immer nur gute Daten integriert worden.

Nicht selten wurden auch Kiesel mit eintrainiert. Sie sorgen dafür, dass in dem Gewusel von Korallen-Perlen noch zusätzliche Unordnung entsteht. Und deshalb sind die oft wilden Korallenperlen auch durchaus mit etwas Vorsicht zu genießen!

Das Gleiche gilt für synthetische Korallenperlen. Das sind Trainingsdaten, die künstlich hergestellt wurden und ähnlich wie echte Korallenperlen aussehen, aber z.B. blau, grün oder gelb eingefärbt sind: Anders also als echte Korallenperlen, die meist rot oder beige sind. Die synthetischen Perlen sind u.a. dann wichtig, wenn zu wenig echte Perlen vorhanden sind. Sie sind hilfreich und plausibel, aber eben nicht echt. Sie können ein Modell daher auch verzerren.

Die Herkunft von Korallenperlen kann ebenfalls ein Problem sein: Weil sie z.B. aus einem Daten-Naturschutzgebiet stammen und Urheberrechtsverletzungen bewirken.

Auch persönliche Daten sollten möglichst nicht als Trainingsdaten integriert sein. Sie sind nur unter großem Aufwand wieder aus dem Modell zu entfernen.

Wer eine Koralle oder ein Korallenriff in sein KI-System integriert, ist daher als nachgelagerter Anbieter (blaues Hütchen) auf Informationen des Anbieters der Koralle angewiesen (gelbes Hütchen): Welche Daten wurden verwendet und wie eintrainiert? Der EU AI Act hat diesbezügliche Transparenzpflichten speziell für Korallen sowie Korallenriffe und deren Perlen definiert.

Ähnlich und doch anders ist es bei Hochrisiko-KI: Hier müssen Qualitätskriterien für Korallenperlen beachtet werden. Dabei sind u.a. Verzerrungen zu prüfen, die zu fehlerhaften Outputs und damit zu Schäden führen können. Entlang des Lebenszyklus sind die Korallenperlen immer wieder neu zu prüfen: Es könnten ja neue Kieselsteine dazugekommen sein … die gilt es zu finden und zu entfernen.

Merken wir uns:

Modelldaten = Korallenperlen

ANGEBUNDENE SYSTEM-PERLEN

Erinnern wir uns an die drei Fächer des Ei‘s: In der Mitte die Intelligenz mit der Koralle. Die haben wir mit den Korallenperlen auf der Seite davor beschrieben.

Im unteren Fach sind es andere Perlen – keine aus Korallen, sondern aus Datenbanken, also besonderen Schmuckkästchen für Perlen. Und die Perlen sind auch nicht so unregelmäßig, sondern schön einheitlich und strukturiert: Eben echte Perlmutt-Perlen.

Auch diese Daten unterliegen bei Hochrisiko-KI strengen Qualitätspflichten. Nehmen wir als Beispiel eine KI, die Bewerber automatisch selektiert und im Hinblick auf die Eignung bewertet. Hier kommen viele Daten aus einer Datenbank, z.B.:

- Das Jobprofil als Anforderungsliste,
- die Priorisierung der Kriterien und
- sonstige Aspekte, die als besonders wichtig oder ggf. auch negativ gelten.

Diese Daten sind keine Korallen-Perlen, die im KI-Modell enthalten sind. Sie kommen aus Datenbanken, die direkt an das System angebunden sind.

Andere Daten sind z.B. Fachinformationen wie Gesetzestexte oder Formularvorlagen. Sie ergänzen die Daten im KI-Modell.

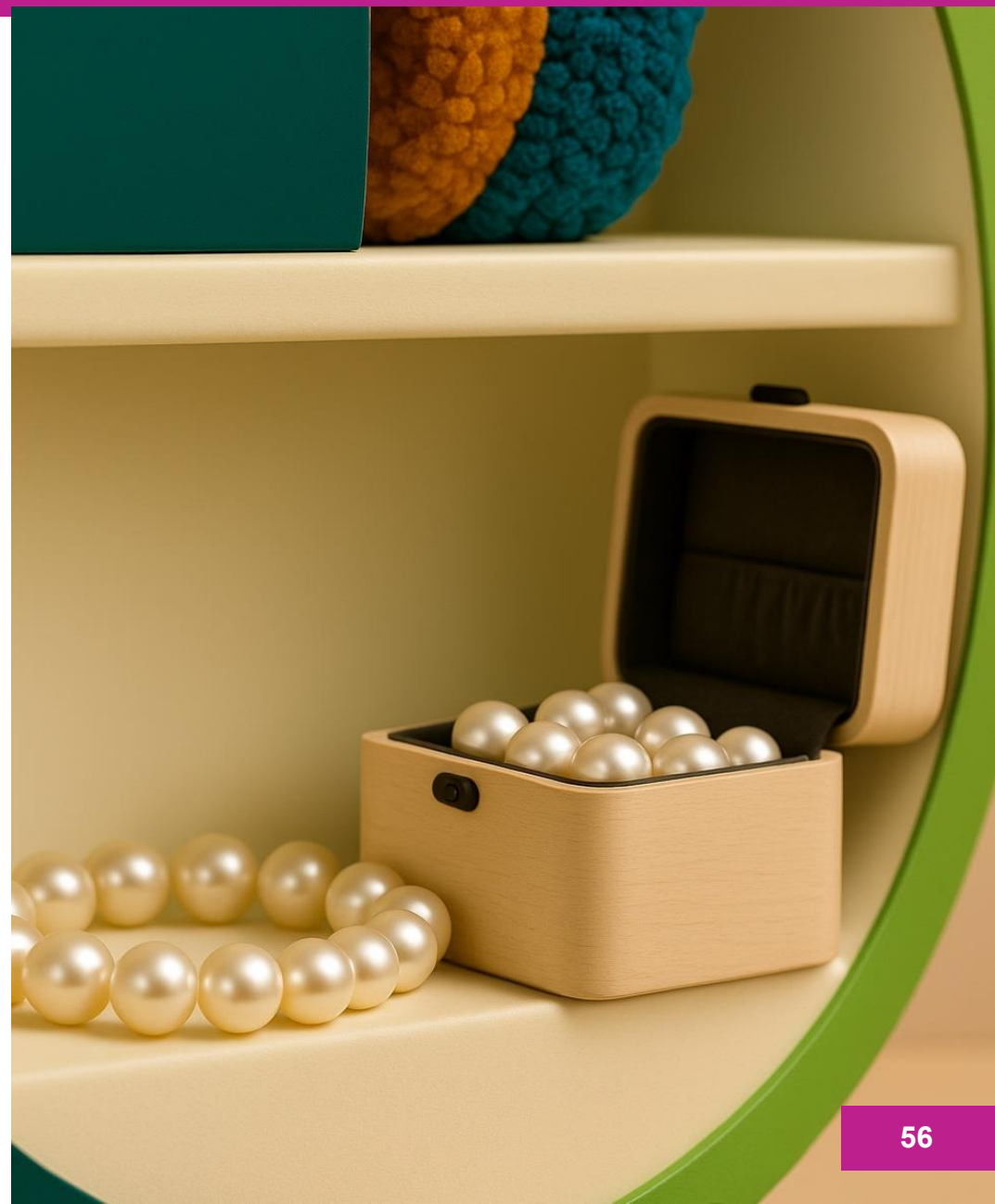
Gerade dann, wenn die exakte Wiedergabe von Informationen von großer Bedeutung ist, sind System-Perlen nämlich deutlich präziser und zuverlässiger als Korallen-Perlen.

Aus regulatorischer Sicht besteht im Hinblick auf System-Perlen jenseits von Hochrisiko-KI auch viel Freiraum. Allerdings ist hier ein anderes Gesetz umso wichtiger: Die DSGVO und damit der Schutz privater Daten. Diese müssen mit Vorsicht und löschbar verwendet werden. Befinden sich System-Perlen in einer Datenbank, lassen sie sich auch meist gut löschen.

Im Hinblick auf die Akteur-Rollen muss beachtet werden, dass ein Betreiber, der eigene Daten so an das System anbindet, dass es zu einer wesentlichen Veränderung führt, selbst zum (Quasi-)Anbieter werden kann.

Achten wir also auf den Unterschied:

Systemdaten = echte Perlen



KIESEL: DATENMÜLL UND SCHLECHTE PROMPTS

Nun ist es leider so, dass viele KI-Anwender glauben, die beste Datenperlen zu besitzen. Doch oft sind es nur Kiesel. Und wenn man dem besten GPAI-Modell (mit feinsten Korallenperlen) Kiesel als Eingabedaten liefert, dann kommen auch keine Datenperlen als Output heraus, sondern ebenfalls Kiesel.

Insofern gilt der englische Merksatz: „Garbage in garbage out“: Wer Datenmüll eingibt, bekommt Datenmüll zurück. Und Kiesel sind in diesem Sinne Datenmüll. Er kann auf unterschiedliche Art entstehen z.B.:

- Durch Tippfehler oder falsche Schreibweisen in Systemdaten,
- durch fehlende oder falsche Werte in Datensätzen, die nicht richtig behandelt werden,
- durch veraltete oder schlecht strukturierte Daten,
- durch falsche Vernetzung von Daten usw.

Besonders kritisch sind Fehler in trainierten Daten, die z.B. bei einer HR-Software zu falschen Vorurteilen führen können. Ähnlich bei fehlerhaft trainierten medizinischen Daten.

Aber selbst wenn Trainings- und System-Daten gut sind, so können die Eingabedaten (also die Prompts) so schlecht sein, dass unentwegt neuer Datenmüll entsteht.

Aus regulatorischer Sicht ist das alles durchaus von Relevanz, denn damit wird auch deutlich: Das menschliche Verhalten und fehlende KI-Kompetenz sind oft dafür verantwortlich, dass eine KI schlechte und ggf. auch riskante Ergebnisse liefert.

Und genau deshalb ist die Vermittlung von KI-Kompetenz so wichtig. Ein Element des bereits skizzierten Kompetenz-Hauses ist das Erlernen der richtigen Bedienung – und zwar sowohl beim Trainieren, beim Anbinden von Systemdaten und nicht zuletzt bei der Formulierung von Eingabedaten.

Blicken wir nun auf die drei Daten-Abfalleimer auf der linken Seite: Selbst wenn wir Mülltrennung für Daten betreiben, so bleibt Abfall doch immer Abfall

Merken wir uns:

Kiesel = Datenmüll

OBACHT BEIM NACHTRAINIEREN UND BEI FINETUNING MIT KORALLENPERLEN

Werden spezifische KI-Modelle oder GPAI-Modelle vom Betreiber nachtrainiert oder erfolgt ein Fine-tuning von Inhalten, dann besteht die Gefahr, dass es zum Rollenveränderung kommt. Links ist die normale Rollenverteilung: Der Anbieter hat den orangen Hut, der Betreiber den roten.

In der Mitte fügt der Betreiber dem GPAI-Modell Korallenperlen zu. Damit wird das System als Ganzes wesentlich verändert. Er bekommt einen zusätzlichen orangen Hut. Er ist neben dem Erst-anbieter zum Quasi-Anbieter des GPAI-Systems als Ganzem geworden. Wir haben also zwei Anbieter.

Variante drei ist besonders: Bei Hochrisiko-KI erfolgt bei einer wesentlichen Änderung ein vollständiger Rollentausch. Hier kann es nur noch einen Anbieter geben: Das ist jetzt der Betreiber, der durch das Finetuning zum finalen Anbieter geworden ist. Also:

Obacht beim Nachtrainieren oder bei Finetuning!

DER RICHTIGE UMGANG MIT DATEN IST IMMER WICHTIG

Die KI-Verordnung geht insbesondere an zwei Stellen näher auf Daten und den Umgang mit ihnen ein:

- Bei Hochrisiko-KI ist eine Daten-Governance explizit geregelt.
- Hinzu kommt die Vertraulichkeit von Behörden, wenn sie Daten von Akteuren überprüfen.

Den ersten Punkt sollte man als Anbieter bzw. Betreiber auch dann beachten, wenn ein KI-System zur mittleren oder geringen Risiko-Klasse zählt. Zwar kann in diesem Fall keine Sanktion bei einem Verstoß verhängt werden, es gibt aber generelle Sorgfaltspflichten, die auch ohne den EU AI Act bestehen. Hinzu kommt die Datenschutzgrundverordnung, die immer zu beachten ist.

Es ist daher generell zu empfehlen, die Qualität von Trainingsdaten genau zu kontrollieren (Nr. 1) und diese auch fortwährend zu dokumentieren.

Auch die Genauigkeit und Aktualität von Systemdaten sollte laufend kontrolliert im Hinblick auf Vertraulichkeit klassifiziert werden (Nr. 2): Sie werden vom KI-Modell verarbeitet und gelangen so „nach außen“.

Besondere Vorsicht ist bei personenbezogenen Daten angesagt (Nr. 3). Sie müssen löschbar sein, und ihre Verwendung ist sorgfältig zu protokollieren!

Also: Egal bei welcher Risiko-Klasse – der sorgfältige Umfang mit Daten ist immer von Bedeutung.

MERKEN WIR UNS ZU STATION SIEBEN – DEN DATEN

1. ZU DIFFERENZIEREN SIND DIE MODELLDATEN (KORALLENPERLEN) UND DIE DATEN DES KI-SYSTEMS (SYSTEM-PERLEN)!
2. NACHGELAGERTE ANBIETER (BLAUES HÜTCHEN) HABEN ANSPRUCH AUF TRANSPARENZ BEZÜGLICH DATEN VON GPAI-MODELLEN.
3. SYSTEMDATEN (ECHTE PERLEN) KOMMEN AUS DATENBANKEN. IHRE QUALITÄT MUSS BEI HOCHRISIKO-KI GENAU GEPRÜFT WERDEN.
4. KIESELSTEINE SIND SCHLECHTE DATEN: EGAL OB BEIM TRAINING FÜR KI-MODELLE, ALS SYSTEM-DATEN ODER ALS EINGABEDATEN.
5. NACHTRAINIERN UND FINETUNING KÖNNEN ZU ROLLENTAUSCH FÜHREN. BEI NUTZUNG VON DATEN IST IMMER SORGFALT ANGESAGT!

BEGINNEN WIR NUN MIT EINER KURZEN WIEDERHOLUNG
DANN FOLGEN VERTIEFUNG & ANWENDUNG

8. VERTIEFEN

WHO IS WHO?

Und: Wissen wir noch, welcher Protagonist welches KI-Element ist?

1. Maschinelles EI
2. Drei Fächer
3. Polyp
4. Lila u. pinkes Hütchen
5. Buntes Ei
6. Koralle/Korallenriff
7. Gelb, orange, roter Hut
8. T-Rex & Krokodil
9. Äskulap-Schlange
10. Papagei
11. Schildkröte
12. Persönliches Haus
13. Korallen-Perlen
14. Echte Perlen
15. Kiesel

ZUERST ZUR VERTIEFUNG DER NORMEN

Auf den folgenden fünf Seiten werden die Normen des EU AI Acts zu verschiedenen Symbolen vorgestellt. Die Normen sind so verlinkt, so dass sie in einem Browser direkt geöffnet und nachgelesen werden können.

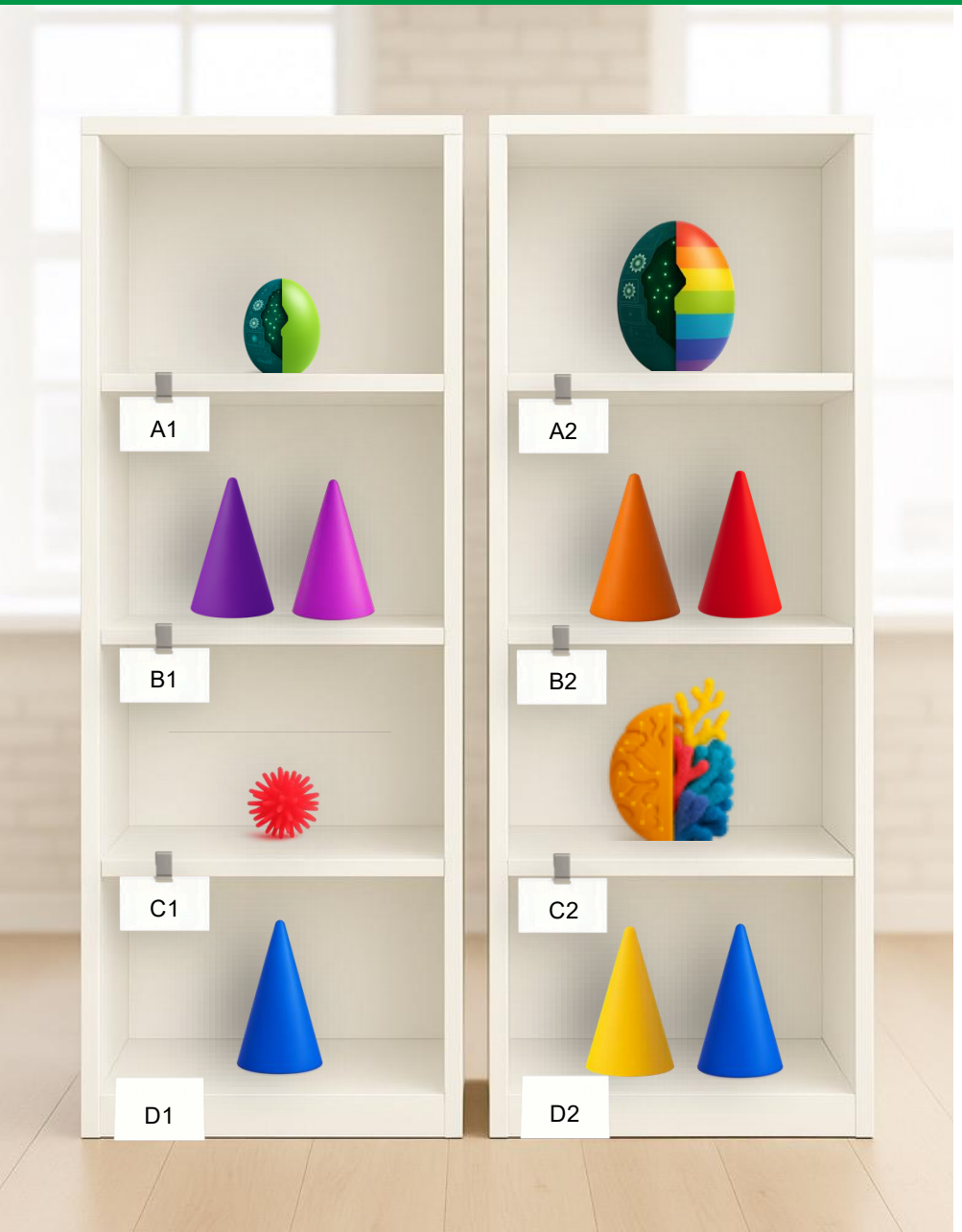
Zu beachten ist, dass viele Definitionen in Art. 3 EU AI Act enthalten und mit Nummern versehen sind. Die Vorschrift für “KI-Modell mit allgemeinem Verwendungszweck“ (= GPAI-Modell) lautet z.B. Art. 3 Nr. 63 EU AI Act. Nach dem Aufrufen des Links von Art. 3 EU AI Act muss daher im Artikel bis zur entsprechenden Ziffer hinuntergescrollt werden.

Das Lesen der Normen im Original empfiehlt sich nicht nur für Juristen: Die fachlich oft sehr anspruchsvollen Formulierungen offenbaren, wie schwer es ist, hoch dynamische KI-Themen zeitlos zu bescheiben. Die Verwendung einer Vielzahl unbestimmter Rechtsbegriffe ist daher fast unvermeidlich.

Auch die Art, wie z.B. die Risiken strukturiert sind, ist aufschlussreich. Unmittelbar rechtlich geregelt sind z.B. nur die Hochrisiko-Themen, darunter die Voraussetzungen und Pflichten. Mittlere und geringe Risiken sind nicht explizit geregelt. Sie ergeben sich aber aus der Systematik der KI-Verordnung.

Die Vertiefung der rechtlichen Normen sollte auf jeden Fall erfolgen, damit wichtige Artikel der KI-Verordnung bekannt sind.

8. VERTIEFUNG – KI-SYSTEM, GPAI-MODELL UND AKTEURE



Normen im EU AI Act	Erläuterung
A1) KI-System (generell): • Art. 3 Nr. 1 EU AI Act Link zur Norm **A2) GPAI-System (allgem. Verwendungszweck):** • Art. 3 Nr. 66 EU AI Act Link zur Norm	Die KI-Verordnung differenziert zwei Arten von KI-Systemen: Das generelle KI-System (meist spezifisch) und das GPAI-System (KI-System mit allgemeinem Verwendungszweck). Für beide gibt es jeweils eigene Legaldefinitionen.
B1) Anbieter u. Betreiber (allgemein): • Art. 3 Nr. 3 & Nr. 4 EU AI Act Link zur Norm **B2) Anbieter u. Betreiber (GPAI-System):** • Art. 3 Nr. 3 & Nr. 4 EU AI Act Link zur Norm	Die Rollen von Anbieter und Betreiber sind für beide KI-System-Varianten gleich. Die farbliche Trennung ist gleichwohl sinnvoll: Pflichten i.S.v. Art. 50 EU AI Act betreffen z.B. oft GPAI-Systeme. Hochrisiko-Pflichten dagegen häufiger spezifische KI-Systeme.
C1) KI-Modell (allgemein): • Keine Definition **C2) GPAI-Modell (allgem. Verwendungszweck):** • Art. 3 Nr. 63 EU AI Act Link zur Norm	Wichtig ist: Für die KI-Modelle von spezifischen KI-Systemen gibt es keine Legaldefinition. Dies ist u.a. dem technologieneutralen Ansatz der KI-Verordnung geschuldet. Daher bezieht sich die Definition für GPAI-Modelle auch explizit auf die Vielseitigkeit.
D1) Anbieter (nachgelagert): • Art. 3 Nr. 3 & Nr. 68 EU AI Act Link zur Norm **D2) Anbieter (GPAI-Modell & nachgelagert):** • Art. 3 Nr. 3 & Nr.68 EU AI Act Link zur Norm	Die Rolle des Anbieters ist nur für GPAI-Modelle definiert. Gleichwohl gibt es für beide Modellvarianten (spezifisch und allgemeiner Verwendungszweck) den nachgelagerten Anbieter. Dieser ist u.a. im Rahmen der KI-Wertschöpfungskette von Bedeutung.

8. VERTIEFUNG – DATEN

Normen im EU AI Act	Erläuterung
E) Verbotene Praktiken: • Art. 5 EU AI Act Link zur Norm • Konkretisierend: Anhang II Link zu Anhang II	Die verbotenen Praktiken werden grundsätzlich in Art. 5 EU AI Act geregelt. Die besonderen Auflagen für staatliche Akteure sind in Anhang II enthalten. Dieser Anhang gilt also nur für die „Krokodile“. Nicht für die „T-Rex-Verbote“. Letztere sind immer verboten, bentigen daher auch keine (strafrechtlichen) Ausnahmen.
F) Hochrisiko-KI: • Art. 6 EU AI Act Link zur Norm • Konkretisierend: Anhang I / III Link zu Anhang I, Link zu Anhang III • Pflichten ab Art. 8 u. ab Art. 71 ff. EU AI Act Link zur Art. 8; Link zur Art. 71;	Hochrisiko-KI hat mehrere Varianten: Solche, die in Bezug auf Produkte in Anhang I aufgelistet sind und weitere Use Cases, die in Anhang III konkretisiert werden. Die Pflichten ergeben sich aus den Art. 8 ff. EU AI Act sowie aus Art. 72 ff. EU AI Act. Wichtig ist, dass Hochrisiko-KI eine Konformitätserklärung benötigt (Art. 47 i.V.m. Anhang V).
G) KI mit mittleren Risiken: • Keine Definition für mittlere Risiken • Aber Transparenzpflichten für Anbieter u. Betreiber von GPAI-Systemen • Art. 50 EU AI Act • Link zur Norm	Zu beachten ist, dass die mittlere Risiko-Klasse nicht explizit als solche im EU AI Act erwähnt wird. Aus Art. 50 ergibt sich aber ihre Existenz. Darin werden unterschiedliche Pflichten für „bestimmte“ KI-Systeme vorgeschrieben. Dies sind meist GPAI-Systeme. Wichtigste Pflichten sind die Transparenzpflichten von Art. 50 und die Vermittlung von KI-Kompetenz, Art. 4.
H) KI mit geringen Risiken: • Keine Definition für geringe Risiken • Aber Pflichten für Anbieter u. Betreiber zur Vermittlung von KI-Kompetenz • Art. 4 und 3 Nr. 56 EU AI Act • Link zu Art. 4, Link zu Art. 3	Ähnlich auch hier: Diese Risiko-Klasse wird auch nicht explizit in der KI-Verordnung als solche benannt. Sie ergibt sich aber aus der Vorschrift von Art. 4. Demnach ist bei allen KI-Use-Cases ausreichend KI-Kompetenz zu vermittelt – also auch bei KI-Systemen mit geringen Risiken. Erfolgt dies nicht, kann es eine Sorgfaltspflichtverletzung darstellen.

8. VERTIEFUNG – AKTIVITÄTEN

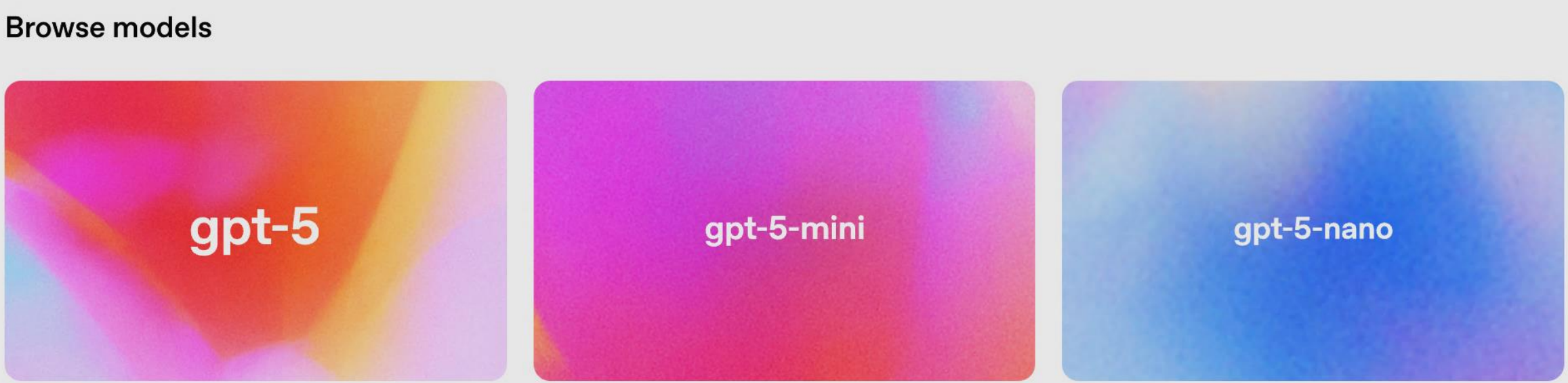
Normen im EU AI Act	Erläuterung
I) Inverkehrbringen: • Art. 3 Nr. 9 EU AI Act Link zur Norm • Erweiterung um Definition für die Bereitstellung auf dem Markt, Art. 3 Nr. 10 • gilt für KI-Systeme/GPAI-Systeme als auch für GPAI-Modelle	Das Inverkehrbringen ist ein Prozess, der von Anbietern eines KI-/GPAI-Systems oder eines GPAI-Modells ausgeführt wird. Wichtig ist das Bereitstellen am Markt, das ergänzend zur Definition in Art. 3 Nr. 9 in Nr. 10 geregelt ist. Danach reicht bereits die Übergabe an den Vertrieb aus, um die Inbetriebnahme zu bewirken. Die entgeltliche oder unentgeltliche Bereitstellung muss im Rahmen einer Geschäftstätigkeit erfolgen.
J) Inbetriebnahme: • Art. 3 Nr. 11 EU AI Act Link zur Norm • gilt nur für KI-Systeme/GPAI-Systeme	Die Inbetriebnahme steht in direktem Zusammenhang mit der Betreiberrolle, die durch die Inbetriebnahme begründet wird: Entweder beim Anbieter, wenn dieser selbst ein KI-/GPAI-System in Betrieb nimmt oder durch Übergabe des Systems an einen Dritten, der dadurch Betreiber wird. Der “Erstgebrauch“ ist dabei die Schwelle, ab der das System in einem realen Kontext wirksam betrieben wird. Pflichten aus der Zweckbestimmung sind ab diesem Zeitpunkt zu beachten
K) Zweckbestimmung: • Art. 3 Nr. 12 EU AI Act Link zur Norm • Art. 3 Nr. 11 EU AI Act Link zur Norm • Bezug für Hochrisiko-KI u.a. bei Art. 7, 8, 10 und 25 EU AI Act • Relevanz ggf. auch für Anbieterwechsel	Die Zweckbestimmung ist in mehrfacher Hinsicht von Bedeutung: Zunächst bezieht sie sich auf die Inbetriebnahme eines KI-Systems „entsprechend der Zweckbestimmung“. Wird ein KI-System jenseits von ihr betrieben, kann dies u.a. dazu führen, dass sowohl die Risiko-Klasse neu beurteilt werden muss, aber auch, dass ein Betreiber durch die modifizierte Zweckbestimmung bzw. Nutzung selbst zum Anbieter wird.

8. VERTIEFUNG – RISIKO-KLASSEN

Normen im EU AI Act	Erläuterung
L) Trainingsdaten von GPAI-Modellen: • Art. 3 Nr. 63 EU AI Act Link zur Norm • Transparenzpflichten, Art. 53 EU AI Act Link zur Norm • Bei Hochrisiko: Art. 10 u. Art. 72 EU AI Act Link zu Art. 10; Link zu Art. 72	Die KI-Verordnung erwähnt Trainingsdaten für GPAI-Modelle in Art. 3 Nr. 63 eher indirekt. Diese Daten sind meist sehr umfangreich („große Menge“) und ermöglichen einen allgemeinen Verwendungszweck. Insbesondere bei lokal genutzten oder auf VPS genutzten GPAI-Modellen kann ein Nachtrainieren erfolgen. Das Nachtrainieren führt aber (anders als bei KI-Systemen) nicht zur Quasi-Anbieterschaft eines GPAI-Modells. Zu beachten sind die Transparenzpflichten v. Art. 53
M) System-Daten: • Art. 3 Nr. 29 ff. EU AI Act Link zur Norm • u.a. Trainingsdaten, Validierungsdaten, Eingabedaten, personenbezogene Daten • Bei Hochrisiko: Art. 10 u. Art. 72 EU AI Act Link zu Art. 10; Link zu Art. 72	Im Hinblick auf System-Daten differenziert die KI-Verordnung verschiedene Typen. So kann z.B. bei einem KI-System dessen internes KI-Modell trainiert werden. Dann ist dieses KI-Modell jedoch systembezogen. Werden z.B. Nutzerpräferenzen in einer Datenbank gespeichert, sind dies i.d.R. keine Trainingsdaten, sondern auf Eingabedaten beruhende personenbezogene Daten. Sie werden oft in einer Datenbank gespeichert und sind i.d.R. löschbar.
N) Schlechte Daten: • Keine Definition • Bei Hochrisiko: Art. 10 u. Art. 72 EU AI Act Link zu Art. 10; Link zu Art. 72 • Aber: Allgemeine Sorgfaltspflicht für alle beachten	Schlechte Daten werden nicht explizit als solche bezeichnet. Weder bzgl. der KI-Modelle, noch im Hinblick auf Systemdaten. Die Datenqualität ist aber u.a. Teil von Art. 10 für Hochrisiko-Systeme. Sie ist z.B. bei der Annotation u. der Bereinigung wichtig. Wesentlich ist, dass die Datenqualität als grundsätzliche Sorgfaltspflicht für alle KI-Systeme zu beachten ist, also nicht nur bei Hochrisiko-KI. Dort kann das Nichtbeachten jedoch sanktioniert werden.

8. VERTIEFUNG – MONITORING, STÖRFÄLLE & KODIZES

Normen im EU AI Act	Erläuterung
O) Monitoring nach dem Inverkehrbringen • Pflicht nach Art. 72 EU AI Act Link zur Norm • bei Hochrisiko: Art. 10 u. Art. 72 EU AI Act Link zu Art. 10 • betrifft primär Anbieter • potenzielle allgemeine Sorgfaltspflicht	Anbieter von Hochrisiko-KI-Systemen müssen über ein System zur Überwachung nach dem Inverkehrbringen verfügen (Art. 72). Es wertet relevante Daten regelmäßig aus und dokumentiert diese (vgl. Art. 10) . Auch öffentliche Daten zu (neuen) Risiken sind auszuwerten. Diese Pflicht kann in reduziertem Umfang auch als allgemeine Sorgfaltspflicht für KI-Systeme aller Risiko-Klassen interpretiert werden.
P) Meldung schwerer Vorfälle: • Pflicht Art. 73 EU AI Act bei Hochrisiko Link zur Norm • Definition v. schwerwiegend: Art. 3 Nr. 49 Link zu Art. 3 • betrifft Anbieter und Betreiber	Die Pflicht zur Meldung schwerer Vorfälle ist sowohl für Anbieter als auch Betreiber von Hochrisiko-KI-Systemen zu beachten. Was ein schwerer Vorfall i.S.v. Art. 73 ist, wird in Art. 3 Nr. 49 näher definiert. Es sind Gefahren für Gesundheit, kritische Infrastrukturen, Grundrechte sowie schwere Sach- und Umweltschäden. Zu beachten ist, dass die Meldepflichten an Fristen gebunden sind – auch für Maßnahmen der Meldebehörden.
Q) Freiwillige Verhaltenskodizes: • Förderung nach Art. 95 Link zu Art. 95 • Freiwillige Übernahme von Pflichten für Hochrisiko-KI auch für mittlere u. geringe Risiko-Klasse	Aus Art. 95 lässt sich der Rückschluss ziehen, dass auch bei KI-Systemen der mittleren und geringeren Risiko-Klassen die Anforderungen für Hochrisiko-KI von Relevanz sein können. Freiwillige Anwendung bedeutet, dass ein Unterlassen nicht sanktioniert werden kann. Zugleich wird verdeutlicht, dass diverse Risiken von Hochrisiko-KI genereller Natur sind. Entsprechende Vorkehrungen können daher auch als allgemeine Sorgfaltspflicht interpretiert werden.



OPENAI: EIN REALER BEISPIELSFALL

Nachfolgend wird ein Fall skizziert, der in der Praxis häufig vorkommt:

- Unternehmen U möchte einen eigenen Chatbot im Intranet betreiben.
- U lässt von der Software-Firma S ein Interaktionsinterface für den Chatbot erstellen, das im Intranet integriert werden kann.
- Fragen von Mitarbeitern zu Fachinhalten von U's Business und vielen weiteren Themen sollen über das Interface beantwortet werden.
- Die für den Chatbot erforderlichen KI-Services bezieht U mit eigener Lizenz direkt bei OpenAI.
- S entscheidet sich für zwei KI-Services: Ein Large Language Model sowie einen KI-Service, der Fundstellen im Internet berücksichtigt (gpt-5 und gpt-4o-search-preview).
- S erstellt nur die Interaktionsoberfläche und verbindet diese mit den für U lizensierten Services.
- Beide KI-Services werden mit dem gleichen API-Key von OpenAI an den Chatbot angeschlossen.

Nun stellt sich die Frage, wie die KI-Services im Sinne der KI-Verordnung zu bewerten sind, und welche Rollen die Akteure diesbezüglich haben.

Werfen wir dazu zunächst einen Blick auf die Website von OpenAI, um die von U genutzten KI-Services näher zu prüfen.

OpenAI ist ein Beispielanbieter. Es geht um das Prinzip.

KI-SYSTEM ODER GPAI-MODELL?

OpenAI bietet ebenso wie google, Antrophic oder Mistral auf seiner Plattform viele verschiedene KI-Services an. Diese remote-Services werden auf den Plattformen häufig nur als “Models“ bezeichnet. Dies ist in den USA kein Problem, aber in Sinne der KI-Verordnung potenziell irreführend.

Remote angeboten werden in undifferenzierter Form:

- KI-Systeme i.S.v. Art. 3 Nr. 1 EU AI Act,
- GPAI-Modelle i.S.v. Art. 3 Nr. 63 EU AI Act,
- GPAI-Systeme i.S.v. Art. 3 Nr. 66 EU AI Act.

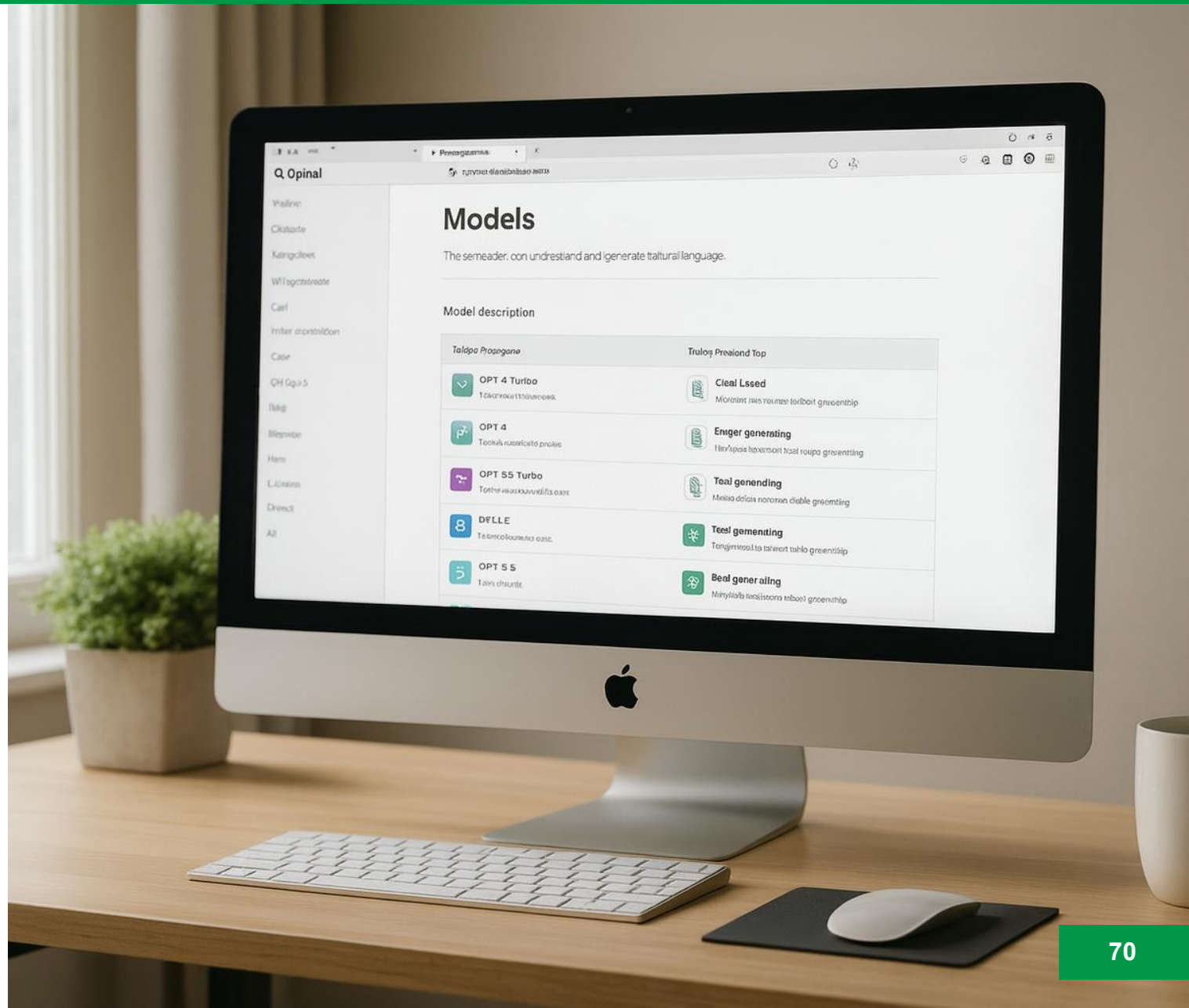
Nur wer entsprechende Angebote zutreffend einstuft, kann die rechtlichen Folgen korrekt bestimmen:

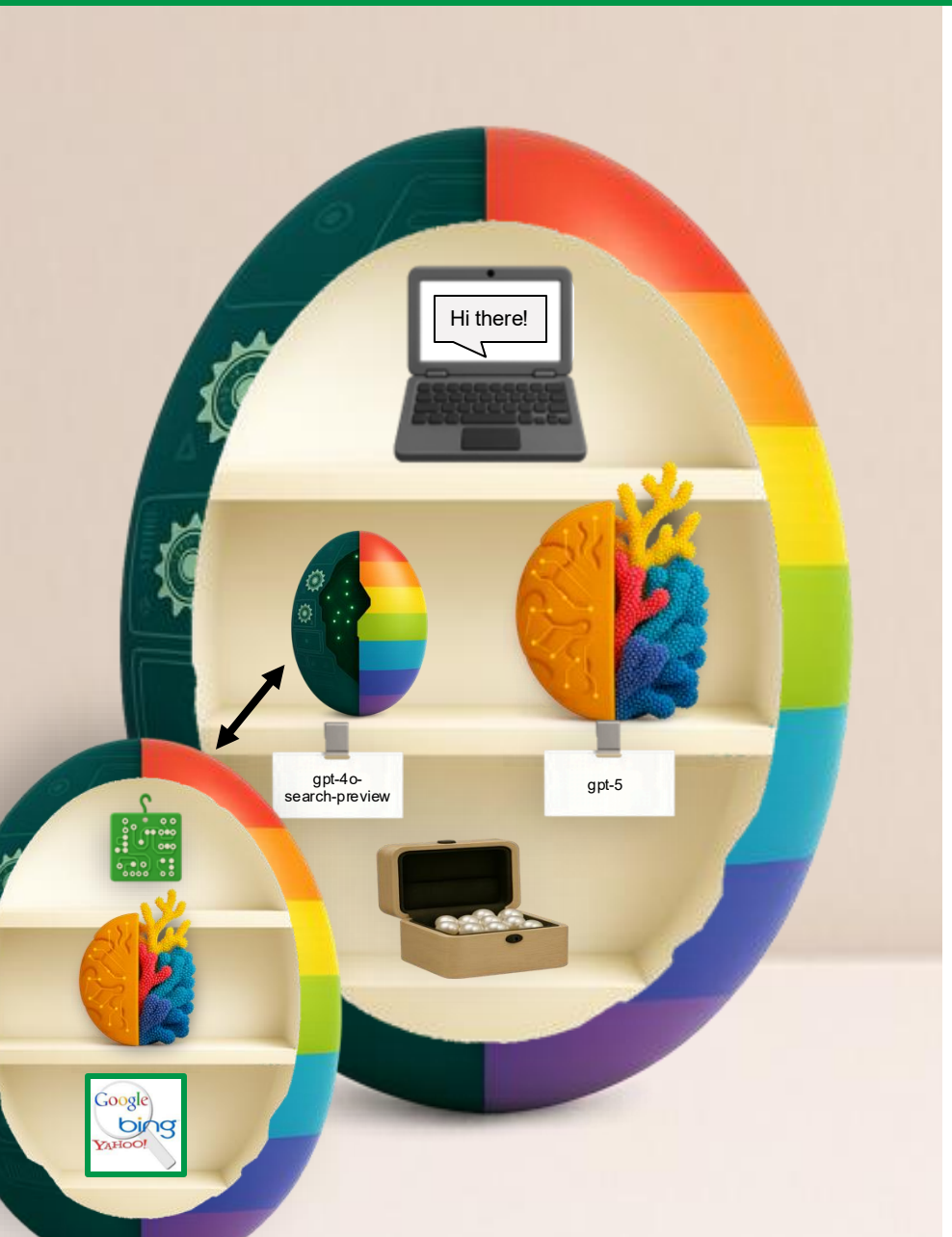
- Die Rollen (Akteur, Betreiber, Nutzer),
- die Risikoklassen (Verbot, High-, Medium, Low-Risk)
- sowie die Pflichten, Sanktionen und Fristen.

Verwenden wir nun die Symbole des Playbooks, um den Fall anschaulich zu lösen. Es geht um zwei Services: Ein Large Language Model und einen Internet-Suchservice:

- **Im Fall ist das Large Language Model „gpt-5“**
- **Der Websearch-Service ist „gpt-4o-search-preview“.**

Link zu den openAI-Services: https://platform.openai.com





DER CHATBOT VON INNEN

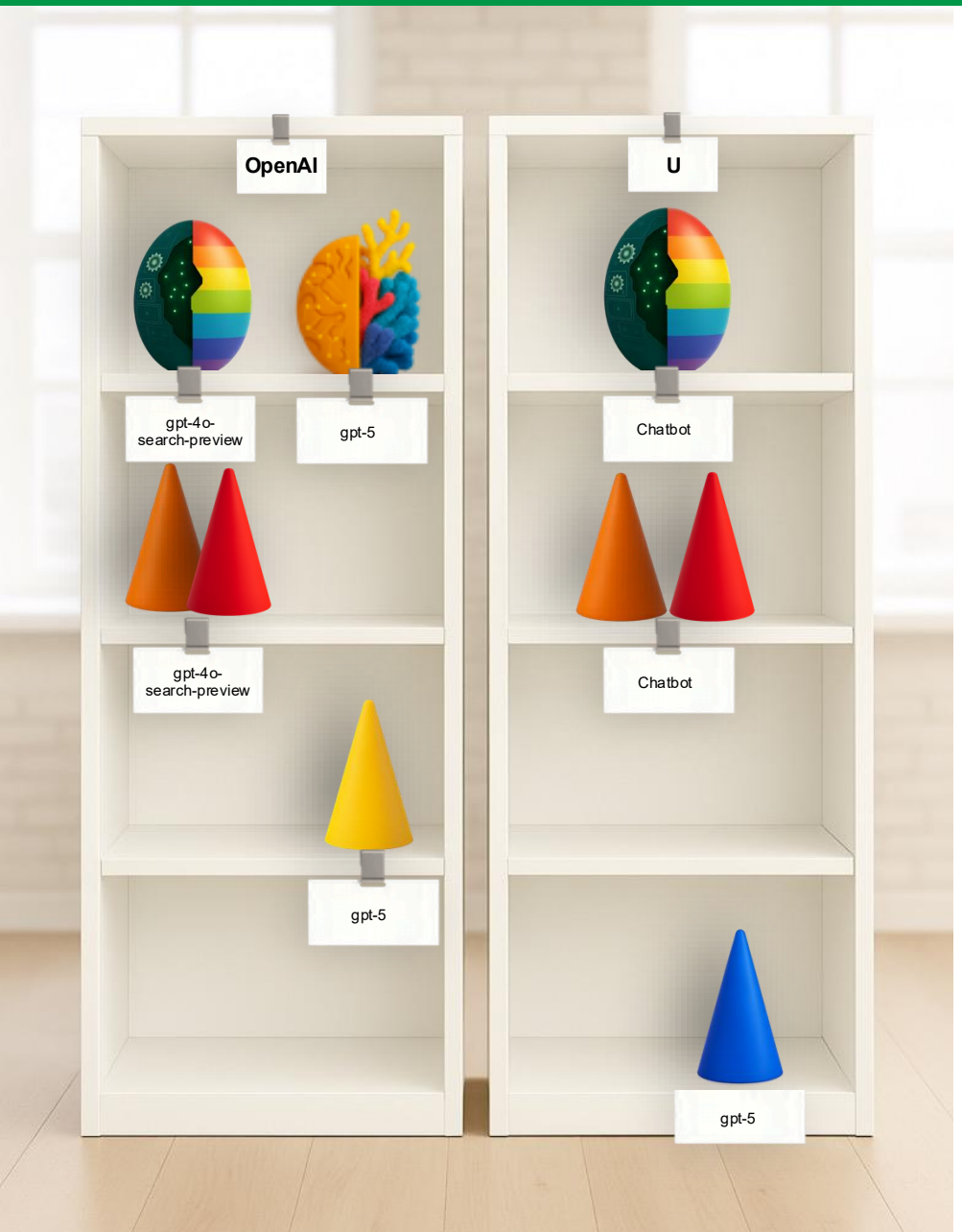
U‘s Chatbot ist ein GPAI-System, da dieser für viele verschiedene Zwecke genutzt werden kann. Daher ist das Symbol ein buntes Ei. So wie es auf Seite 21 erklärt wurde.

- Es enthält ein Interaktionsinterface. Hier als Laptop im oberen Fach dargestellt. Im Interface können User den KI-Service wählen: Entweder ein Large Language Model (gpt-5) oder einen Web-Suchservice (gpt-4o-search-preview). Die Nutzer-Oberfläche bleibt dabei immer gleich.
- Im mittleren Fach – der Intelligenz – enthält das EI daher rechts ein GPAI-Modell (hier das Symbol für das LLM gpt-5)
- Links enthält das mittlere Fach ein GPAI-System. Es wird ebenfalls remote über einen API-Key angebunden.
- Dieses GPAI-System ist der Web-Suchservice gpt-4o-search-preview. Er ist unten links noch einmal genauer als separates buntes Ei dargestellt:
  - Es enthält in der Mitte eine bunte Koralle, nämlich das GPAI-Modell „4o“.
  - Hinzu kommt oben im oberen Fach eine Schnittstelle, damit es Suchanfragen des Chatbots erkennen und beantworten kann. Hier dargestellt als eine kleine Platine.
  - Am wichtigsten ist jedoch das unterste Fach: Es enthält die Anbindung von Suchdaten aus dem Internet (google, bing, yahoo). Damit können z.B. aktuelle Realtime-Outputs erfolgen, die gpt-4o mit den Modell-Daten vermengt.
  - Somit kommen die Antworten auch nicht mehr nur aus einem GPAI-Modell, sondern aus einem GPAI-System im GPAI-System (Matrjoschka-Prinzip, Seite 16).

Der Chatbot enthält in der Regel noch einen Speicher für die Sessions. Zudem sind Fachdaten angebunden. Beides wird durch die Schatulle im unteren Fach symbolisiert.

Das Besondere ist hier, dass das linke Ei auf dem Portal von OpenAI als „Modell“ bezeichnet wird, obwohl es faktisch ein „System“ im Sinne der KI-Verordnung ist.

Dies wirkt sich auf die mit dem Chatbot verbundenen Akteur-Rollen und die sich daraus ergebenden Pflicht aus!



DIE VERTEILUNG DER ROLLEN

Zunächst zur Rolle von S. Als Software-Dienstleister hat S nur die Interaktionsoberfläche erstellt – ohne selbst Lieferant der Intelligenz zu sein. S hat damit keine Rolle i.S.d. KI-Verordnung. S ist lediglich Dienstleister von U.

U hat die Rollen als Anbieter und Betreiber des Chatbots (Art. 3 Nr. 3 & 4, orange/rot). U hat den Chatbot z.T. entwickeln lassen und durch Verwendung eigener API-Key zusätzlich den Chatbot auch noch mit erstellt. Erst durch Anbindung eines Intelligenz-Service (remote) entsteht im Fall der Chatbot als ein GPAI-System (Art. 3 Nr. 1, & Nr. 66).

U hat den Chatbot in Verkehr gebracht und zudem in eigener Verantwortung in Betrieb genommen (Art. 3 Nr. 9 - 11).

Dass der Chatbot zwei unterschiedliche KI-Services nutzt (einmal LLM, einmal Such-Service) ändert nichts. Es führt aber dazu, dass U im Hinblick auf das LLM nachgelagerter Anbieter i.S.v. Art. 3 Nr. 68 ist (blau) und damit gegenüber OpenAI einen Anspruch auf Transparenz bzgl. des LLM hat (hier gpt-5). Dieser Anspruch besteht nicht im Hinblick auf den Suchservice!

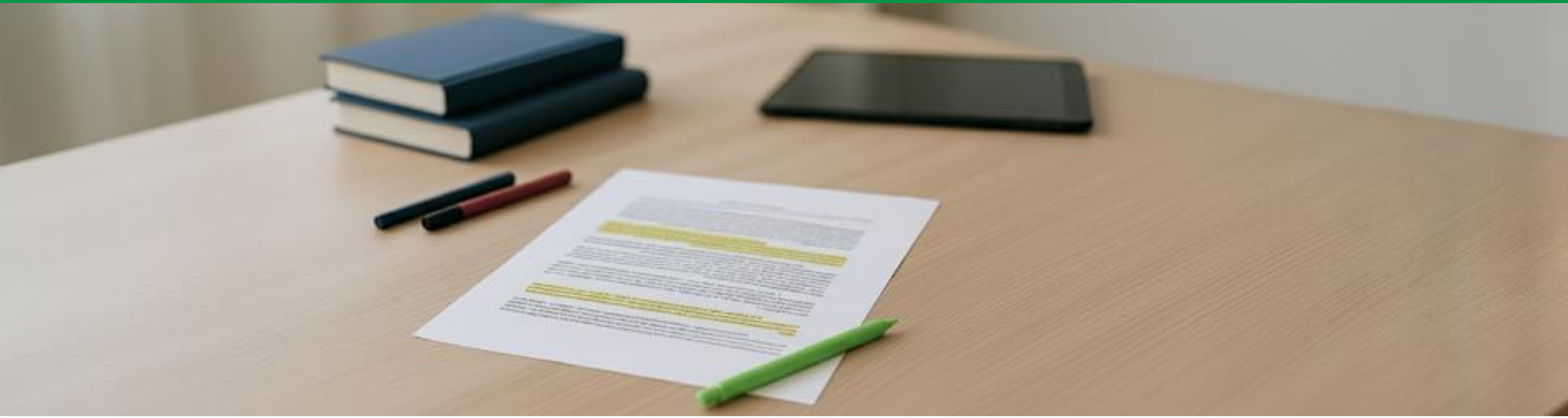
Schauen wir nun auf die linke Seite des Regals: OpenAI bietet sowohl den Suchservice gpt-4o-search-preview (Ei) als auch das LLM gpt-5 (Koralle/Korallenriff) an.

- Bezüglich des Suchservice ist OpenAI sowohl Anbieter als auch Betreiber von gpt-4o-search-preview.
- Und im Hinblick auf das LLM (gpt-5) ist OpenAI zusätzlich Anbieter.

Kommen wir nun zu den Learnings, die sich aus dem Fall ergeben:

- Es kommt nicht darauf an, wie KI-Services benannt werden (z.B. als Model), sondern auf den tatsächlichen Charakter.
- Man muss als Anbieter/Betreiber selbständig beurteilen, welchen Charakter KI-Services haben, die man integriert.
- Die Darstellung mit den Symbolen kann helfen, ähnlich klingende Begriff klar erkennbar abzugrenzen!

Das Beispiel zeigt: Die Verwendung von plakativen „serious play“ Methoden hat einen ernsthaften und praxisbezogenen Hintergrund!



NUN ZU INHALTEN UND RANDNUMMERN DES SKRIPTS

Im Skript **Grundwissen KI-Recht** werden viele wichtige Aspekte der zuvor dargestellten Themen in rechtlich vertiefender Form dargestellt.

Die rechtliche Vertiefung ist selbst im Hinblick auf eine endgültige Bewertung von Sachverhalten wie dem zuvor geschilderten Beispielsfall wichtig. Für den individuellen Einzelfall gilt das erst Recht, denn dieser muss mit dem „klassischen juristischen Werkzeugkoffer“ gelöst werden.

Nachfolgend werden einige Beispiele aus dem Skript skizziert, um den Bezug zwischen Playbook und Skript zu verdeutlichen.

Dabei sollte betont werden, dass das Skript auch ein Nachschlagewerk ist, in dem man spezifische Themen bearbeitet, ohne gleich den gesamten Inhalt des Skripts lesen zu müssen.

Insofern erfolgt auf den folgenden Seiten auch die Angabe von Randnummern des Skripts, welche die hier im Playbook verwendeten Symbole und sonstigen Inhalte durch Text, Prüfungsschemata und Übersichten ergänzen.

Exemplarisch dargestellt werden nachfolgend fünf Themenbereiche des Skripts, die im Kontext des Playbooks als besonders wichtig empfunden werden.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de

	KI-Modell	KI-System
Definition	Rechnerische Einheit zur Verarbeitung von Daten und Generierung von Ergebnissen	Umfassendes maschinengestütztes System mit autonomem Betrieb
Fokus	Spezifische Aufgaben (Vorhersagen, Klassifikationen etc.)	Erreichung verschiedener Ziele
Komplexität	Teil eines größeren Systems	Umfasst mehrere Komponenten, darunter KI-Modelle
Interaktion mit Nutzern	Indirekt	Kann direkt oder indirekt mit Nutzern interagieren
Adaptivität	Kann sich durch Updates und Neutraining weiterentwickeln	Ist adaptiv und kann sich an verschiedene Situationen anpassen

KI-SYSTEME UND KI-MODELLE

Der im Playbook skizzierte Unterschied von einfarbigen mechanischem Ei, buntem Ei, Polyp, Koralle und Korallenriff hilft bereits, wesentliche Unterschiede verschiedener Varianten von KI-Systemen und KI-Modellen zumindest grob zu verstehen.

Der Beispielsfall macht aber auch deutlich, dass es im Einzelfall auf viele Details ankommt. Erschwerend kommt hinzu, dass die KI-Verordnung zwar KI-Systeme, GPAI-Systeme und GPAI-Modelle definiert – nicht aber den Begriff des KI-Modells.

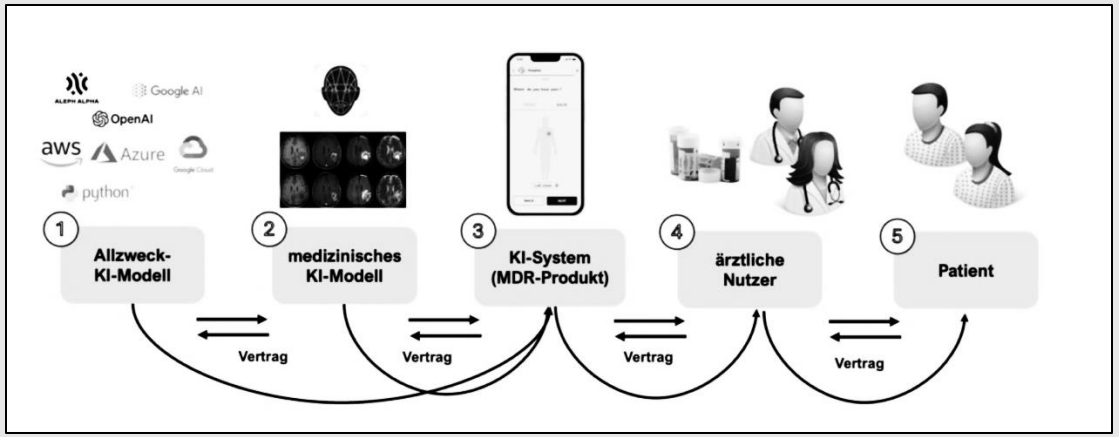
Diese Lücke systematisch und fachlich korrekt zu schließen, ist u.a. dadurch möglich, dass man sich die vergleichbaren Definitionen der OECD oder der UNSECO für KI-Modelle und KI-Systeme anschaut.

Diesbezüglicher Lesetipp zu Station 2 & 3:

Das Skript thematisiert ab **Randnummer 87** ausführlich, welche Bedeutung die Unterscheidung von KI-Systemen und KI-Modellen in unterschiedlichen Kontexten besitzt. Zum Beispiel bei der Frage, ob der sachliche Anwendungsbereich der KI-Verordnung erfüllt ist.

Zu diesem Zweck stellt das Skript unter **Randnummer 92** ein Prüfungsschema für KI-Systeme vor, das auf den diesbezüglichen Leitlinien der EU beruht. Es verdeutlicht u.a., welche Kriterien der Definition von Art. 3 Nr. 1 zwingend zu beachten sind und welche Kann-Kriterien sind.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de



KI-WERTSCHÖPFUNGSKETTE

In diesem Playbook wird die vielleicht wichtigste und mitunter anspruchvollste Thematik nur angedeutet: Es ist die Aufteilung von Rechten und Pflichten in der KI-Wertschöpfungskette.

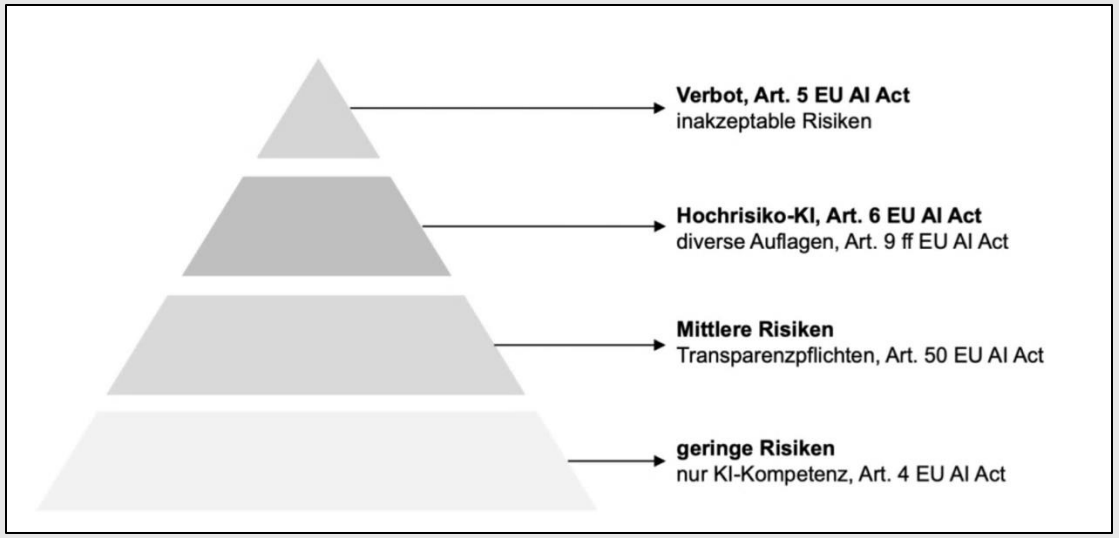
Explizite Regeln für diesbezügliche Verantwortlichkeiten finden sich dafür in der KI-Verordnung insbesondere in Art. 25. Die dort getroffenen Wertungen sind nicht nur aufsichtsrechtlich, sondern auch zivilrechtlich und sogar strafrechtlich von Bedeutung: Pflichtverletzungen können nämlich von jedem einzelnen Akteur erfolgen. Dies führt u.a. zu Fragen der Beweisbarkeit.

Diesbezüglicher Lesetipp zu Station 4:

Das Skript erläutert ab **Randnummer 453 u. 467** praxisrelevante Fragen der Zurechnung und Verantwortung von Handlungen bzw. Unterlassungen in der KI-Wertschöpfungskette. Hier insbesondere im strafrechtlichen Kontext. Dort gilt (anders als im Zivilrecht) der Grundsatz *in dubio pro reo* – im Zweifel für den Angeklagten.

Im Ergebnis kann aufgrund eine KI-typische Beweisnot dazu führen, dass im Zweifel niemand entlang einer komplexen KI-Wertschöpfungskette strafrechtlich zur Rechenschaft gezogen werden kann.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de



VERBOTS- & RISIKO-PYRAMIDE

Die verbotenen KI-Praktiken und die drei Risiko-Klassen bilden zusammen eine vierstufige Pyramide. Sie wird, entsprechend der links dargestellten Übersicht, in vielen Fachveröffentlichungen zur KI-Verordnung auch auch als solche symbolisch dargestellt und entsprechend bezeichnet.

Aufgrund der großen Verbreitung von immer leistungsfähigeren multimodalen KI-Chatbots, die nicht nur Texte generieren, sondern auch Bilder und Videos in Deep-Fake-Qualität erstellen können, ist die Kenntnis der Pflichten für KI-/GPAI-Systeme der mittleren Risiko-Klasse besonders wichtig.

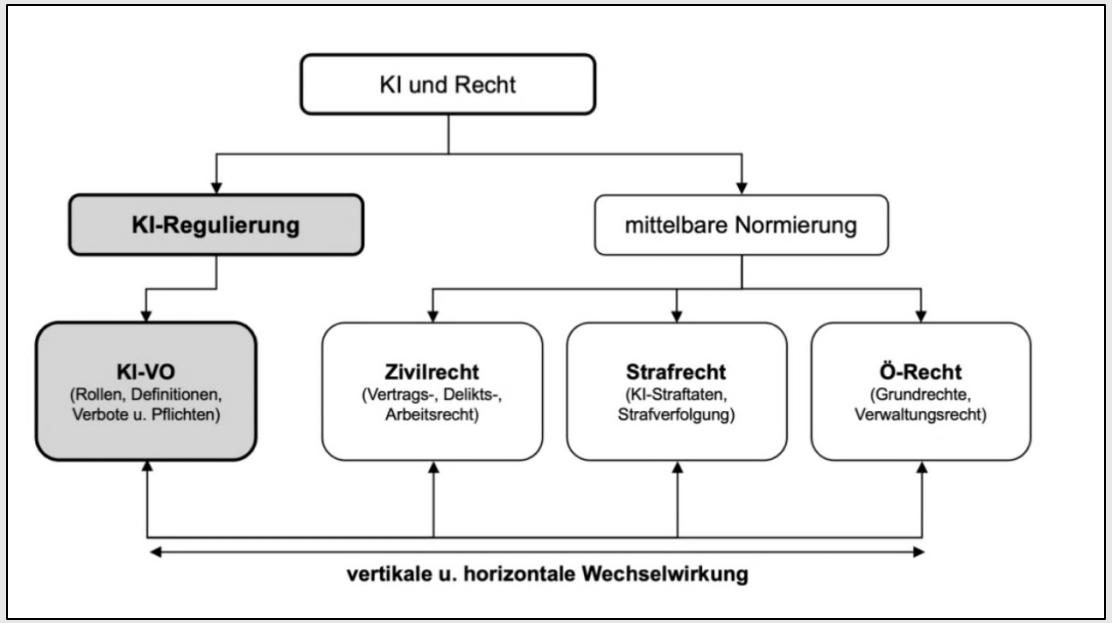
Diesbezüglicher Lesetipp zu Station 5:

Das Skript erläutert ab **Randnummer 199** ausführlich die verschiedenen Pflichten nach Art. 50 für KI-Systeme der mittleren Risiko-Klasse. Dabei ist einerseits zwischen generellen Kennzeichnungspflichten für KI und besonderen Transparenzpflichten für Deepfakes zu unterscheiden.

Wichtig ist aber auch, dass sich die Pflichten nach Art. 50 mal auf die Anbieter und mal auf die Betreiber von KI-Systemen beziehen, die mit Menschen interagieren oder besondere Fähigkeiten besitzen.

Davon abzugrenzen sind die Pflichten für Anbieter von GPAI-Modellen gegenüber nachgelagerten Anbietern. Diese werden u.a. unter den **Randnummer 187, 217 f. u. 315 ff.** dargestellt.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de



DIREKTE U. MITTELBARE REGULIERUNG

Eine geläufige Annahme ist, dass die KI-Verordnung alles regelt, was man als Anbieter oder Betreiber von KI-Systemen beachten muss. Dies ist nur bedingt zutreffend:

- Die KI-Verordnung enthält spezifische Definitionen, Regeln und Pflichten. Werden die bestehenden Pflichten nicht eingehalten, dann sind Sanktionen möglich (z.B. bei einer Hochrisiko-KI).
- Für ein KI-System der mittleren oder geringen Risikoklasse sind aber ebenfalls Sorgfaltspflichten zu beachten. Werden diese nicht beachtet, kann zwar keine Sanktionierung erfolgen. Es ist aber möglich, dass im Fall eines Schadens Haftungsansprüche entstehen, weil allgemeine Sorgfaltspflichten nicht eingehalten wurden.

Diesbezüglicher Lesetipp zu Station 6:

Im Skript wird unter **Randnummer 23 ff.** dargestellt, dass eine Wechselwirkung von KI-Verordnung und den allgemeinen Gesetzen besteht.

Die **Randnummern 388 ff.** widmen sich dabei den Fragen deliktischer Haftung. Hier ist zu beachten, dass die Verletzung von Normen der KI-Verordnung einerseits eine Schutzgutverletzung i.S.v. § 823 II BGB darstellen kann. Es kann aber auch im Fall einer allgemeinen Sorgfaltspflichtverletzung eine Haftung nach § 823 I BGB in Betracht kommen.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de

BEACHTUNG VON SORGFALTSPFLICHTEN

Oft unterschätzt wird die (mittelbare) Indizwirkung, die spezifische Sorgfaltspflichten z.B. für Hochrisiko-KI auch für alle anderen Risiko-Klassen haben kann. Fällt z.B. eine KI aufgrund einer Bereichsausnahme nicht unter die KI-Verordnung, dann bedeutet das nicht, dass man keine Sorgfaltspflichten zu beachten hat.

Welche Sorgfaltspflichten generell im Hinblick auf KI-Systeme zu beachten sind, lässt sich u.a. im Rückschluss aus den explizit im EU AI Act verankerten Pflichten entnehmen.

Diesbezüglich stationsübergreifender Lesetipp:

Diese u.a. unter **Randnummer 407 und 580** skizzierte Thematik ist in der Praxis deshalb von großer Bedeutung, weil sich Sorgfaltspflichten dynamisch verändern können.

Anbieter und Betreiber sind durchaus angehalten, sich regelmäßig darüber zu informieren, welche Risiken von KI-Systemen ausgehen können, für die sie Mitverantwortung tragen. So können neue Warnungen oder Veröffentlichungen zu bislang unbekannten Risiken zur Notwendigkeit führen, Gegenmaßnahmen zu treffen – ganz egal, welcher Risiko-Klasse ein KI-System angehört.

Da sich KI-Systeme häufig weiterentwickeln und auch laufend neue Erkenntnisse bezüglich der Risiken entstehen, muss geprüft werden, welche Sorgfaltspflichten zu welchem Zeitpunkt zumutbar (gewesen) sind.

zum Grundwissen-Skript:
http://www.grundwissen-ki-recht.de

ANHANG

Sichere Verwendung von Stehleitern






Verwendung der Baustellenkreissäge






Sonnenschutz bei Bauarbeiten






IMPRESSUM

EU AI ACT Playbook
Version 1.1, Stand 21. September 2025

Autor:
Ass. Iur. & AI Officer (AIO)
Oliver M. Merx
83229 Aschau

Kontakt:
https://www.linkedin.com/in/oliver-m-merx-83777b/

Internet:
https://cair4.eu
https://grundwissen-ki-recht.de/
https://grundwissen-ki-recht.de/playbook/

Bildrechte:
Alle Bilder wurden mittels lizensierter generativer KI und vom Autor erstellt.

Hinweis:
Das Bild auf der vorherigen Seite zeigt die Sicherheitstafel einer Baustelle.
Das Original befindet sich an einer neu zu erstellenden Autobahnbrücke für die A8.
Nach Fertigstellung des Skripts “Grundwissen KI-Recht“ wurde der Autor
bei einer E-Bike-Tour auf die in der Tafel verwendete Symbolsprache aufmerksam.
Sie ist für Bauarbeiter unterschiedlicher Herkunft in ähnlicher Form verständlich.
Es war der Geburtsmoment für die Idee der Symbolsprache dieses Playbooks.