UNABHÄNGIGES INSTITUT FÜR KI ETHIK

Wissenschaftlicher Whitepaper-Entwurf

Vom Tool-Inventar zum Einsatzfall-Register

Warum KIregister.com einen rechtssystematisch sauberen Startpfad für EU-AI-Act-Readiness bietet

Volltextbasierte Analyse der Verordnung (EU) 2024/1689 und
funktionsbezogene Bewertung der Capture-Architektur von KIregister.com

Zentrale These. Der EU AI Act ist für die Unternehmenspraxis nicht primär ein Tool-Katalogisierungsrecht, sondern ein Kontext-, Rollen- und Nachweisrecht. Dokumentiert werden muss daher zuerst der konkrete KI-Einsatzfall - mit Zweck, Verantwortungsrolle, betroffenen Personengruppen, Datenkontext, Entscheidungsrelevanz und Review-Logik. Genau an dieser Stelle setzt KIregister.com an.

Fallstudie:	KIregister.com
Dokumentenstand:	12. März 2026
Quellenbasis:	amtlicher EU-AI-Act-Text, Kommissionsmaterialien, Produktanalyse

Hinweis: Diese Fassung ist ein redaktioneller wissenschaftlicher Entwurf. Eine tatsächliche externe Autorisierung, institutionelle Freigabe oder Drittbegutachtung ist gesondert herzustellen.

Abstract

Dieses Whitepaper untersucht, ob ein use-case-zentriertes KI-Register dem Regelungsansatz des EU AI Act näher steht als eine bloße Erfassung eingesetzter Tools. Ausgangspunkt ist eine volltextbasierte Auswertung der Verordnung (EU) 2024/1689 in ihrer amtlichen deutschen Fassung, ergänzt um aktuelle Umsetzungsinformationen der Europäischen Kommission und eine funktionsbezogene Analyse der von KIregister.com bereitgestellten Register- und Capture-Architektur.[1]

Die Untersuchung gelangt zu drei Ergebnissen. Erstens werden zentrale Pflichten des AI Act an *Zweckbestimmung*, *Verwendungskontext*, *betroffene Personen*, *menschliche Aufsicht*, *Transparenz* und *Nachweisbarkeit* geknüpft - nicht an eine rein tool-zentrierte Inventarisierung.[2] Zweitens ist die Basiseinheit „KI-Einsatzfall“ deshalb juristisch anschlussfähiger als die Basiseinheit „Tool“. Drittens operationalisiert KIregister.com diese Logik in einer für breite Unternehmensadoption ungewöhnlich niedrigen Eintrittsschwelle: Die freie Basisschicht dokumentiert reale Einsatzfälle, nicht nur Software-Namen, und erzeugt daraus sofort exportierbare, standardisierte Nachweisobjekte.[3]

Der rechtliche Vorteil liegt nicht darin, dass ein Register bereits „Compliance“ im Vollsinn herstellen würde. Der Vorteil liegt darin, dass es die *richtige erste Ordnung der Tatsachen* erzeugt: Organisationen beginnen mit Sichtbarkeit, Zweck, Verantwortung und Kontext - also genau dort, wo der AI Act seine Betreiberlogik verankert.

Transparenzhinweis zur Einordnung. Dieses Whitepaper bewertet die Registerlogik von KIregister.com als *Readiness- und Evidenzinfrastruktur*. Es behauptet ausdrücklich nicht, dass ein Register allein alle Pflichten des AI Act, insbesondere für Anbieter oder Hochrisiko-Konformitätsbewertung, vollständig ersetzt.

Kernaussagen in fünf Punkten

1. Der AI Act klassifiziert und adressiert Risiken in weiten Teilen *anwendungs- und kontextbezogen*; dieselbe Technologie kann je nach Einsatzbereich trivial, transparentpflichtig oder hochriskant sein.[4]
2. Für viele Unternehmen ist nicht die sofortige „End-Compliance“, sondern die belastbare *Erst-Erfassung* der Engpass.
3. Eine tool-zentrierte Liste reicht dafür nicht aus; sie verfehlt Zweckbestimmung, Verantwortungsrolle, betroffene Gruppen und Entscheidungswirkung.
4. KIregister.com dokumentiert den konkreten KI-Einsatzfall über eine Capture-Maske, die Zweck, Owner-Rolle, Wirkung, Datenkontext, Entscheidungsrelevanz, Status und Export strukturiert erfasst.[5]
5. Gerade weil Art. 4 AI-Literacy bereits gilt und die allgemeine Anwendbarkeit des AI Act am 2. August 2026 erreicht ist, sollten Unternehmen die Sichtbarkeits- und Registerarbeit nicht aufschieben.[6]

[1] Vgl. Verordnung (EU) 2024/1689 [1]; Europäische Kommission, „AI Act“ und „Questions & Answers on the AI Act“ [2, 3].
[2] Vgl. insbesondere Art. 3, Art. 4, Art. 12-14, Art. 26, Art. 27, Art. 50 sowie Anhang III AI Act [1].
[3] Vgl. Produktanalyse KIregister.com [6]; KI-Register-Axiome [7].
[4] Vgl. Anhang III sowie Art. 50 AI Act [1].
[5] Vgl. Produktanalyse [6].
[6] Vgl. Art. 4 und Art. 113 AI Act [1]; Europäische Kommission [2, 3, 4, 5].

Inhaltsverzeichnis

Abstract i

Kernaussagen in fünf Punkten i

1 Einleitung und Erkenntnisinteresse 1

2 Methodik und Quellenbasis 1

3 Die regulatorische Logik des EU AI Act 2
3.1 Zielrichtung und Regelungsarchitektur . . . 2
3.2 Rollenmodell: Anbieter, Betreiber, Zweckbestimmung . . . 2
3.3 Zeitliche Anwendbarkeit . . . 2

4 Warum tool-zentrierte Inventare rechtlich zu kurz greifen 4
4.1 Der AI Act ordnet Risiken nach Verwendungskontext . . . 4
4.2 Grundrechte-Folgenabschätzung und Betreiberpflichten sind kontextgebunden . . . 4
4.3 Transparenzpflichten richten sich nicht auf Tools, sondern auf Situationen . . . 5

5 KIregister.com als use-case-zentrierte Dokumentationsarchitektur 7
5.1 Designaxiome und juristische Plausibilität . . . 7
5.2 Die Capture-Maske als juristischer Kern . . . 7
5.3 Verteilte Erfassung: Browser, Menubar, Gastmodus, Access Codes . . . 9
5.4 Freie Basisschicht und standardisierte Outputs . . . 9

6 Juristische Bewertung: Warum dies ein rechtssystematisch sauberer Startpfad ist 9
6.1 Passung zur Normstruktur des AI Act . . . 9
6.2 Manuelle Statusentscheidungen statt automatisierter Schein-Compliance . . . 10
6.3 Warum gerade die freie Basisschicht rechtlich relevant ist . . . 10
6.4 Grenzen des Ansatzes . . . 10

7 Warum Unternehmen jetzt beginnen sollten 11
7.1 Erstens: Art. 4 gilt bereits . . . 12
7.2 Zweitens: Die allgemeine Anwendbarkeit des AI Act ist nah . . . 12
7.3 Drittens: Die größte Lücke liegt meist in der Discovery, nicht im Policy-Dokument . . . 12
7.4 Viertens: Frühzeitige Registerarbeit vermeidet hektische Fehlklassifikation . . . 12
7.5 Fünftens: Ein exportierbares Artefakt ist besser als ein loses Spreadsheet . . . 12

8 Schlussfolgerung 12

Literatur- und Quellenverzeichnis 14

1 Einleitung und Erkenntnisinteresse

Die praktische KI-Governance vieler Organisationen beginnt derzeit mit dem naheliegenden, aber rechtlich oft unzureichenden Reflex, zunächst eingesetzte Tools oder Anbieter zu inventarisieren. Diese Vorgehensweise ist organisatorisch verständlich, regulatorisch jedoch nur begrenzt tragfähig. Denn der EU AI Act fragt nicht zuerst: „Welches Tool wird verwendet?“ Er fragt vielmehr: „Zu welchem Zweck? In welchem Prozess? Gegenüber welchen Personengruppen? Mit welcher Entscheidungswirkung? Unter welcher Aufsicht? Und mit welchem Nachweis?“

Gerade in Unternehmen, die keine eigenen Hochrisiko-Systeme entwickeln, sondern KI vor allem einsetzen, konfigurieren, einkaufen oder in operative Prozesse integrieren, ist dieser Unterschied zentral. Der normative Fokus verschiebt sich vom isolierten Artefakt hin zur verantworteten Nutzung in einem konkreten Organisationskontext. Dies betrifft die Rollenlogik des AI Act ebenso wie spätere Transparenz-, Aufsichts- und Nachweispflichten.

Leitthese der Produktlogik. „Der KI-Einsatzfall ist die kleinste governance-relevante Einheit.“
Quelle: KI-Register Ansatz - Kernannahmen (Axiome) [7].

Dieses Whitepaper prüft, ob diese These mit der Regelungsarchitektur des AI Act übereinstimmt, und ob KIregister.com daraus einen besonders belastbaren Startpfad für Unternehmen ableitet. Bewertet werden dabei ausdrücklich die *freie Basisschicht*, die Capture-Maske und die Art der Dokumentation - also gerade jene Elemente, die in vielen anderen Governance-Werkzeugen entweder gar nicht im Zentrum stehen oder erst in späten, komplexeren Produktstufen zugänglich werden.

2 Methodik und Quellenbasis

Die Analyse folgt einem rechtsdogmatisch-funktionalen Ansatz. Erstens wurde der amtliche deutsche Text der Verordnung (EU) 2024/1689 einschließlich Erwägungsgründen und Anhängen als Primärquelle ausgewertet.[7] Zweitens wurden aktuelle Umsetzungs- und FAQ-Materialien der Europäischen Kommission herangezogen, um den regulatorischen Stand zum 12. März 2026 korrekt abzubilden.[8] Drittens erfolgte eine funktionsbezogene Produktanalyse von KIregister.com anhand der bereitgestellten Quellcodebasis und internen Produktunterlagen.[9]

Die Untersuchung ist damit *volltextbasiert*, ohne zu behaupten, jede einzelne Norm habe für die vorliegende Produktfrage dieselbe dogmatische Tragweite. Vertieft betrachtet werden diejenigen Vorschriften, die für Betreiber-Readiness, Kontextbewertung, Transparenz, Aufsicht, Dokumentation und Nachweislogik besonders relevant sind: Art. 1, Art. 3, Art. 4, Art. 9-14, Art. 26, Art. 27, Art. 50, Art. 113 sowie Anhang III.[10]

Methodisch wichtig ist außerdem eine klare Abgrenzung: Dieses Whitepaper liefert keine Rechtsberatung im Einzelfall und keine vollständige Konformitätsbewertung. Es beantwortet die strukturierende Vorfrage, welches Dokumentationsobjekt und welcher Erfassungsmodus der Systematik des AI Act am ehesten entsprechen.

[7] Vgl. [1].
[8] Vgl. [2, 3, 4, 5].
[9] Vgl. [6, 7].
[10] Vgl. [1].

3 Die regulatorische Logik des EU AI Act

3.1 Zielrichtung und Regelungsarchitektur

Art. 1 AI Act formuliert den Gegenstand der Verordnung breit: Der Binnenmarkt soll verbessert, eine menschenzentrierte und vertrauenswürdige KI gefördert und zugleich ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte gewährleistet werden.[11] Bereits an dieser Eingangsnorm zeigt sich, dass der AI Act weder als bloße Produktliste noch als reines Technikrecht gelesen werden kann. Er enthält vielmehr ein Bündel aus Markt-, Governance-, Transparenz- und Durchsetzungsregeln.

Aus Unternehmenssicht ist entscheidend, dass diese Architektur unterschiedliche Pflichtencluster erzeugt: verbotene Praktiken, spezifische Anforderungen an Hochrisiko-Systeme, Transparenzpflichten für bestimmte KI-Systeme, Regeln für GPAI-Modelle sowie Governance- und Marktüberwachungsmechanismen.[12] Wer nur Tools erfasst, bildet diese Architektur nicht ab. Wer Einsatzfälle erfasst, nähert sich ihr deutlich stärker an.

3.2 Rollenmodell: Anbieter, Betreiber, Zweckbestimmung

Art. 3 definiert den „Anbieter“ als die natürliche oder juristische Person, die ein KI-System entwickelt oder entwickeln lässt und unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt. Der „Betreiber“ ist dagegen die natürliche oder juristische Person, die ein KI-System in eigener Verantwortung verwendet.[13] Für die Unternehmenspraxis mit Standardsoftware, eingekauften Modellen und eingebetteten KI-Funktionen ist diese Unterscheidung zentral: Viele Organisationen sind primär Betreiber, nicht Anbieter.

Noch wichtiger ist die Legaldefinition der „Zweckbestimmung“. Sie meint die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, „einschließlich der besonderen Umstände und Bedingungen für die Verwendung“.[14] Bereits diese Formulierung zeigt, dass der Rechtsrahmen nicht auf eine abstrakte Softwarebezeichnung verkürzt werden kann. Rechtlich relevant sind besondere Umstände und Bedingungen der Verwendung - also genau jener Kontext, den ein use-case-zentriertes Register zu erfassen versucht.

Hinzu tritt die „vernünftigerweise vorhersehbare Fehlanwendung“. Auch sie ist nutzungsbezogen definiert und verweist auf menschliches Verhalten und Interaktionen mit anderen Systemen.[15] Eine rein tool-zentrierte Liste ist dafür kaum analytisch brauchbar.

3.3 Zeitliche Anwendbarkeit

Art. 113 legt fest: Die Verordnung ist am 1. August 2024 in Kraft getreten, gilt grundsätzlich ab dem 2. August 2026; Kapitel I und II gelten bereits seit dem 2. Februar 2025; bestimmte GPAI- und Governance-Regeln seit dem 2. August 2025; einzelne Pflichten für KI-Systeme in regulierten Produkten ab dem 2. August 2027.[16] Die Kommission bestätigt diese Staffelung in ihrer Hauptseite und in den FAQ ausdrücklich.[17]

[11] Art. 1 AI Act [1].
[12] Art. 1 Abs. 2 AI Act [1].
[13] Art. 3 Nr. 3 und Nr. 4 AI Act [1].
[14] Art. 3 Nr. 12 AI Act [1].
[15] Art. 3 Nr. 13 AI Act [1].
[16] Art. 113 AI Act [1].
[17] Vgl. [2, 3].



Abbildung 1: Zeitliche Staffelung der Anwendbarkeit des EU AI Act. Grundlage sind Art. 113 AI Act sowie die aktuelle Darstellung der Europäischen Kommission.

Die Kommission weist derzeit zugleich darauf hin, dass verzögerte Standards die Umsetzung einzelner Hochrisiko-Anforderungen erschweren und hierzu regulatorische Anpassungen vorgeschlagen wurden.[18] Solange solche Änderungen nicht beschlossen sind, bleibt jedoch Art. 113 die maßgebliche Rechtsgrundlage. Für Unternehmensentscheidungen ist daher Vorsicht geboten: Man kann auf mögliche Erleichterungen nicht seriös „wetten"; man sollte stattdessen die vorbereitenden Register- und Dokumentationsarbeiten jetzt aufbauen.

4 Warum tool-zentrierte Inventare rechtlich zu kurz greifen

4.1 Der AI Act ordnet Risiken nach Verwendungskontext

Eine der stärksten systematischen Beobachtungen ergibt sich aus Anhang III. Die dort genannten Hochrisiko-Fälle werden nicht entlang konkreter Marken oder Tools klassifiziert, sondern entlang *Einsatzbereichen*: Bildung, Beschäftigung, Kreditwürdigkeit, Lebens- und Krankenversicherung, Notruf- und Triage-Kontexte, Strafverfolgung, Migration, Rechtspflege und demokratische Prozesse.[19] Dieselbe technische Basiskomponente kann daher je nach Einsatzfall regulatorisch vollkommen unterschiedlich relevant sein.

Direktes Leitmotiv des Verordnungsgebers. Betreiber „können am besten verstehen, wie das Hochrisiko-KI-System konkret eingesetzt wird" und verfügen über eine genauere Kenntnis des Verwendungskontextes sowie der wahrscheinlich betroffenen Personen oder Personengruppen.
Quelle: Erwägungsgrund 93 AI Act [1].

Diese Passage ist für die gesamte Registerfrage hoch aufschlussreich. Sie erklärt, warum die rechtlich relevante Betrachtungseinheit nicht der Software-Name, sondern der konkrete Einsatzkontext ist. Ein Tool-Inventar kann bestenfalls *anzeigen*, dass eine Technologie vorhanden ist. Es kann aber nicht hinreichend erklären, wie sie konkret wirkt, wen sie betrifft und ob daraus besondere Pflichten entstehen.

4.2 Grundrechte-Folgenabschätzung und Betreiberpflichten sind kontextgebunden

Art. 27 AI Act bestätigt diese Logik. Die Grundrechte-Folgenabschätzung - die nur für bestimmte Betreiber und bestimmte Hochrisiko-Fälle vorgeschrieben ist - verlangt unter anderem:

- eine Beschreibung der Verfahren, in denen das System entsprechend seiner Zweckbestimmung verwendet wird,
- eine Beschreibung von Zeitraum und Häufigkeit,
- die Kategorien der betroffenen natürlichen Personen und Personengruppen,
- die spezifischen Schadensrisiken,
- die Umsetzung von Maßnahmen menschlicher Aufsicht sowie
- Maßnahmen für den Fall des Risikoeintritts einschließlich interner Governance und Beschwerdemechanismen.[20]

Keine dieser Kategorien lässt sich belastbar aus einer reinen Tool-Liste ableiten. Die FRIA dient hier nicht als universelle Pflicht für alle Unternehmen, sondern als besonders prägnanter Beleg für

[18] Vgl. [3].
[19] Anhang III AI Act [1].
[20] Art. 27 Abs. 1 lit. a-f AI Act [1].

die Kontextlogik des Gesetzes.

Auch Art. 26 - die Pflichten der Betreiber von Hochrisiko-KI-Systemen - ist eindeutig nutzungsbezogen. Betreiber müssen geeignete technische und organisatorische Maßnahmen treffen, menschliche Aufsicht kompetenten Personen übertragen, auf passende Eingabedaten achten, den Betrieb überwachen und Protokolle aufbewahren.[21] Wer keinen geordneten Registereintrag pro Einsatzfall besitzt, kann diese Pflichten weder systematisch vorbereiten noch effizient nachweisen.

4.3 Transparenzpflichten richten sich nicht auf Tools, sondern auf Situationen

Art. 50 AI Act ist ein weiterer Grund, warum ein bloßes Tool-Inventar zu kurz greift. Transparenzpflichten werden dort an Situationen geknüpft: direkte Interaktion mit natürlichen Personen, synthetische Audio-, Bild-, Video- oder Textinhalte, Emotionserkennung, biometrische Kategorisierung, Deepfakes und bestimmte veröffentlichte Texte.[22] Auch hier ist also nicht primär entscheidend, welches Modell irgendwo im Unternehmen existiert, sondern in welcher Interaktions- oder Veröffentlichungslogik es konkret eingesetzt wird.

Tabelle 1: Dasselbe Tool, unterschiedliche regulatorische Relevanz

Technische Basis	**Konkreter Einsatzfall**	**Mögliche Rechtsrelevanz**	**Warum ein Tool-Inventar nicht reicht**
Generatives Sprachmodell	interne Ideensammlung oder Rohentwürfe ohne Personenbezug	vor allem Dokumentations-, Governance- und ggf. Policy-Fragen	Der Tool-Name sagt nichts über Betroffenheit, Datenkontext oder Entscheidungswirkung.
Dasselbe Modell	Vorauswahl oder Ranking von Bewerber:innen	Anhang III Nr. 4 lit. a; potenziell Hochrisiko-Kontext	Erst der konkrete HR-Einsatz macht die Hochrisiko-Einordnung plausibel.
Dasselbe Modell	Erzeugung veröffentlichter Inhalte über Angelegenheiten von öffentlichem Interesse	Transparenzrelevanz nach Art. 50 Abs. 4	Der regulatorische Trigger ist die Veröffentlichungs- und Nutzungssituation, nicht die Modellfamilie.

Die Folgerung ist klar: Wer regulatorisch sauber beginnen will, muss das *Dokumentationsobjekt* richtig wählen. Nicht jedes Tool ist ein eigener Governance-Fall. Aber jeder wiederholte, wirkungsrelevante Einsatzfall kann ein Governance-Fall sein.

[21] Art. 26 AI Act [1].
[22] Art. 50 AI Act [1].

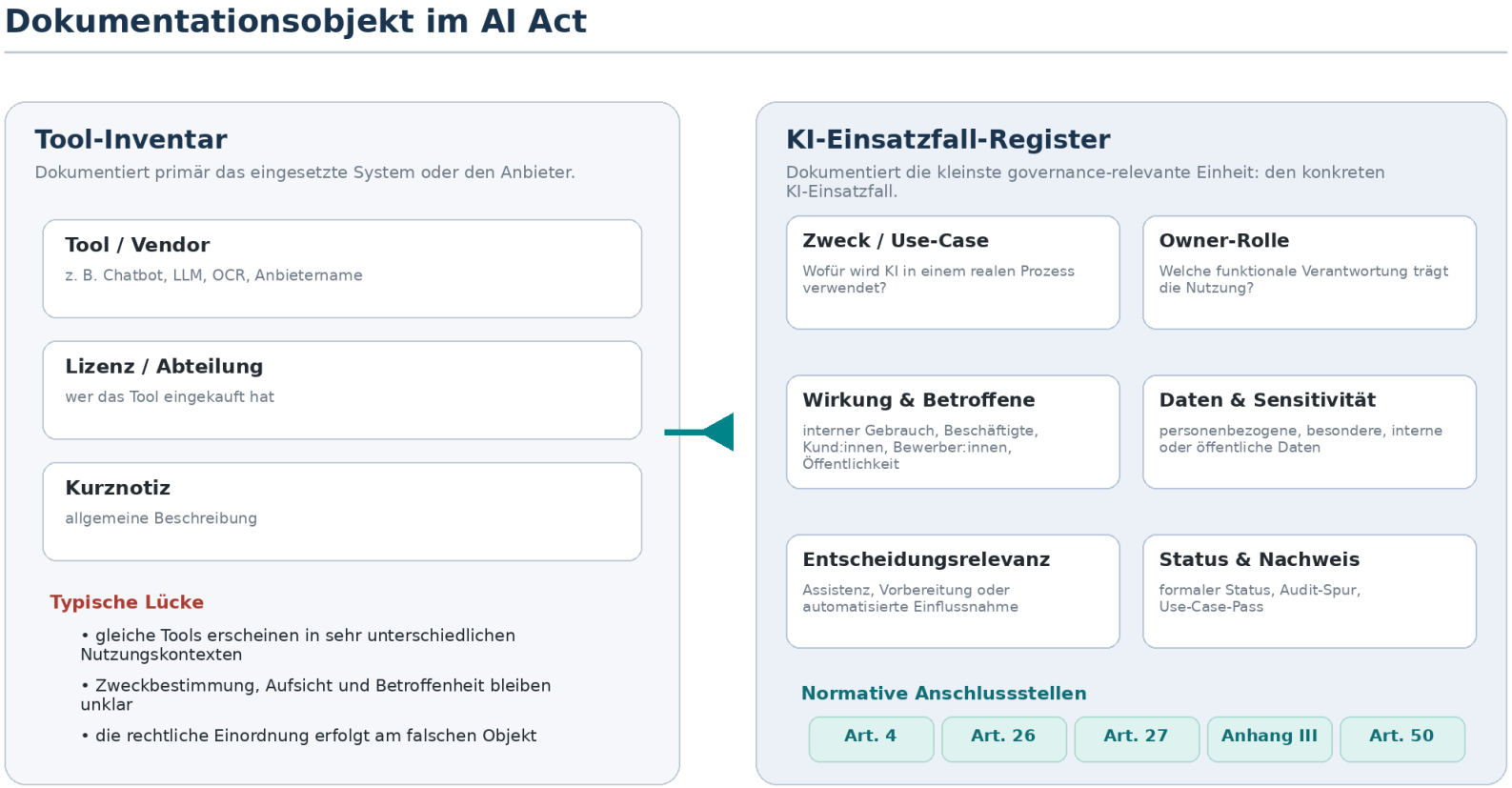


Abbildung 2: Vergleich der Dokumentationsobjekte: Tool-Inventar und use-case-zentriertes Register. Die rechte Seite ist näher an den normativen Anschlussstellen des AI Act.

5 KIregister.com als use-case-zentrierte Dokumentationsarchitektur

5.1 Designaxiome und juristische Plausibilität

Die bereitgestellten Produktunterlagen formulieren die Grundannahme, der AI Act wirke in der Praxis primär als „Organisationsrecht“ und der KI-Einsatzfall sei die kleinste governance-relevante Einheit.[23] Diese Annahme ist aus rechtsdogmatischer Sicht überzeugend, weil sie die oben dargestellte Verbindung von Zweckbestimmung, Verwendungskontext, Betreiberverantwortung und betroffenen Personengruppen präzise aufnimmt.

Ebenfalls überzeugend ist die zweite Designidee: Ein minimaler Datensatz soll zunächst fünf Dinge sichern - Zweck und Kontext, Risikoeinschätzung, verantwortliche Rolle, Maßnahmen/Controls, Review-/Änderungsauslöser.[24] Für eine frühe Registerschicht ist dies sachgerecht, sofern nicht behauptet wird, dieser Minimaldatensatz ersetze bereits sämtliche Detailanforderungen an Hochrisiko-Systeme. Genau diese Überdehnung wird in den Axiomen jedoch ausdrücklich vermieden.

5.2 Die Capture-Maske als juristischer Kern

Die analysierte Capture-Architektur von KIregister.com erfasst nicht bloß einen Software-Namen, sondern eine strukturierte Kombination aus:

- Use-Case-Name,
- Owner-Rolle als funktionale Verantwortungszuordnung,
- optionaler Kontaktperson,
- System/Tool als eingesetztes Mittel,
- Wirkung und betroffene Personengruppen,
- Daten und Sensitivität,
- Entscheidungsrelevanz,
- formaler Status und Exportobjekt.[25]

Gerade die Entscheidung, als Primärfeld nicht den Personennamen, sondern die *Owner-Rolle* zu führen, ist governance-theoretisch stark. Rollen sind stabiler als Personen, besser auditierbar und näher an organisationaler Verantwortungszuweisung. Die optionale Kontaktperson dient dem operativen Rückkanal, ohne die semantische Governance-Einheit zu verwässern.[26]

Ebenso wichtig ist die bewusste Behandlung des Tools als *Attribut* des Einsatzfalls. Das entspricht der Einsicht, dass ein Tool-Wechsel review-relevant sein kann, ohne dass dadurch automatisch eine völlig neue Governance-Einheit entsteht.

[23] Vgl. [7].
[24] Vgl. [7].
[25] Vgl. [6].
[26] Vgl. [6].



Abbildung 3: Die Capture-Maske von KIregister.com bildet jene Felder ab, die für Zweckbestimmung, Kontext, Betreiberpflichten, Aufsicht und spätere Nachweise besonders relevant sind.

5.3 Verteilte Erfassung: Browser, Menubar, Gastmodus, Access Codes

Aus funktionaler Sicht ist nicht nur *was* erfasst wird relevant, sondern auch *wie*. Die freie Basisschicht von KIregister.com erlaubt Quick Capture im Browser, in einer Browser-Erweiterung, in einer macOS-Menüleisten-App sowie im Gastmodus.[27] Gast-Einträge werden nach der analysierten Produktlogik lokal im Browser gespeichert, solange keine direkte Registerspeicherung erfolgt. Das senkt Hemmschwellen und unterstützt eine privacy-sensible Erstaufnahme.

Besonders relevant ist außerdem die verteilte Erfassung über Zugangslinks bzw. Access Codes. Teams oder Lieferanten können Einsatzfälle ohne Login in dieselbe Capture-Sprache einspeisen.[28] Diese Architektur adressiert ein reales Governance-Problem: *Shadow AI*. Die größte Lücke vieler Organisationen liegt nicht in fehlenden Policies, sondern in fehlender Sichtbarkeit. Ein niederschwelliger, standardisierter Erfassungszugang ist daher nicht bloß ein Usability-Merkmal, sondern ein rechtlich hochrelevanter Adoptionshebel.

5.4 Freie Basisschicht und standardisierte Outputs

Nach der analysierten Produktlage umfasst die freie Basisschicht insbesondere:

- Einrichtung des Registers und Erfassung erster Einsatzfälle,
- Festhalten der Owner-Rolle,
- Use-Case-Pass als PDF- oder JSON-Ausgabe,
- Erfassungslink für Team oder Lieferanten,
- Quick Capture im Browser, in der Menubar oder als Gast,
- reduzierte Detailansicht mit minimaler Statusdokumentation und Audit-Spur.[29]

Diese Kombination ist aus Compliance-ökonomischer Sicht bemerkenswert. Die *erste Dokumentationsebene* - also das Sichtbarmachen realer KI-Nutzung - wird nicht als fortgeschrittene Enterprise-Funktion behandelt, sondern als frei zugängliche Basisschicht. Das ist kein rein kommerzielles Detail, sondern berührt die rechtliche Qualität des Startpfads. Je niedriger die Hürde der Ersterfassung, desto eher entsteht ein vollständigeres Tatsachenbild der KI-Nutzung im Unternehmen.

6 Juristische Bewertung: Warum dies ein rechtssystematisch sauberer Startpfad ist

6.1 Passung zur Normstruktur des AI Act

Die juristische Stärke von KIregister.com liegt in der hohen Strukturgleichheit zwischen Produktlogik und Rechtslogik. Die Plattform fragt zuerst nach dem *konkreten Einsatzfall*, nicht zuerst nach dem *abstrakten Tool*. Damit knüpft sie an dieselben semantischen Achsen an, entlang derer der AI Act Pflichten verteilt: Zweckbestimmung, Verwendungskontext, betroffene Personen, Aufsicht, Datenkontext, Transparenzsituation und Nachweisfähigkeit.

In diesem Sinne ist der Ansatz *sauberer* als tool-zentrierte Alternativen - nicht weil er mehr Schlagworte sammelt, sondern weil er näher am regulatorischen Objekt dokumentiert. Die Dokumentation wird dort angesetzt, wo spätere Rechtsfragen tatsächlich entstehen.

[27] Vgl. [6].
[28] Vgl. [6].
[29] Vgl. [6].

6.2 Manuelle Statusentscheidungen statt automatisierter Schein-Compliance

Die analysierte Governance-Logik trennt formale Statusdokumentation von der bloßen Pflege der Stammdaten und sieht keine automatisierte Compliance-Freigabe vor; Statuswechsel sind als manuelle, dokumentierte Entscheidungen angelegt.[30] Das ist juristisch klug. Denn Governance-Systeme sollten Verantwortung sichtbar machen, nicht unsichtbar automatisieren.

Eine häufige Fehlentwicklung digitaler Compliance-Tools besteht darin, aus heuristischen Scorings den Eindruck eines „automatischen“ Rechtsurteils zu erzeugen. KIregister.com vermeidet diesen Kurzschluss im analysierten Produktstand. Das entspricht der Grundidee menschlicher Aufsicht und dokumentierter Verantwortungsübernahme, wie sie insbesondere Art. 14 und Art. 26 AI Act voraussetzen.[31]

6.3 Warum gerade die freie Basisschicht rechtlich relevant ist

Viele Governance-Produkte dokumentieren vor allem das Tool oder monetarisieren die erste Erfassungsebene so stark, dass Unternehmen die Sichtbarkeitsarbeit aufschieben. Aus juristischer Perspektive ist das problematisch. Denn die schwierigste Vorfrage lautet regelmäßig nicht: „Wie baue ich einen perfekten Kontrollworkflow?“ Sie lautet: „Welche KI-Einsatzfälle habe ich überhaupt, und wer trägt dafür Verantwortung?“

Art. 4 AI Act verlangt bereits seit dem 2. Februar 2025 Maßnahmen zur Sicherstellung ausreichender KI-Kompetenz. Der Gesetzgeber nennt dabei ausdrücklich „den Kontext, in dem die KI-Systeme eingesetzt werden sollen“, sowie „die Personen oder Personengruppen“, bei denen sie eingesetzt werden sollen.[32] Eine Organisation kann diese Pflicht schwer sinnvoll operationalisieren, solange sie ihre realen Einsatzfälle nicht strukturiert sichtbar gemacht hat.

> **Direktes Zitat aus Art. 4 AI Act.** Maßnahmen zur KI-Kompetenz müssen „den Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen“ berücksichtigen, bei denen sie eingesetzt werden sollen.
> *Quelle: Art. 4 AI Act [1].*

Genau deshalb ist die freie Registerschicht nicht bloß „nice to have“, sondern regulatorisch vernünftig: Sie erzeugt früh jene Kartierung der Organisation, auf der spätere Schulung, Policy-Zuordnung, Review-Zyklen und ggf. vertiefte Risikoanalysen überhaupt erst aufsetzen können.

6.4 Grenzen des Ansatzes

Wissenschaftliche Sauberkeit verlangt eine klare Begrenzung der These. KIregister.com ist im hier analysierten Sinn kein vollständiges AI-Act-Managementsystem für alle denkbaren Konstellationen. Insbesondere ersetzt die Plattform nicht:

- die technische Dokumentation eines Anbieters nach Art. 11,
- die spezifische Daten-Governance und Testlogik für Hochrisiko-Systeme nach Art. 10,
- ggf. Konformitätsbewertung, Qualitätsmanagement oder Post-Market-Monitoring auf Anbieterseite,

[30] Vgl. [6].
[31] Vgl. Art. 14 und Art. 26 AI Act [1].
[32] Art. 4 AI Act [1].

- die materiell-rechtliche Prüfung, ob ein bestimmter Einsatzfall tatsächlich unter Anhang III oder Art. 50 fällt.

Aber genau in dieser begrenzten, präzisen Einordnung liegt ihre Stärke. Das Register ist keine Überbehauptung von Compliance, sondern eine robuste *Vorstufe belastbarer Compliance-Arbeit.*

Tabelle 2: Freie Basisschicht von KIregister.com und ihr rechtlicher Mehrwert (Stand der Produktanalyse)

Freies Feature	**Funktionsbeschreibung**	**Rechtlicher bzw. governance-seitiger Mehrwert**
Register und Quick Capture	strukturierte Erst-Erfassung je Einsatzfall	schafft Sichtbarkeit und ordnet Dokumentation am richtigen Objekt an
Owner-Rolle	funktionale Verantwortungszuordnung statt bloßer Personennennung	unterstützt Rechenschaft, Review und stabile Verantwortungsarchitektur
Wirkung, Betroffene, Datenkontext, Entscheidungsrelevanz	Capture der wesentlichen Kontextdimensionen	ermöglicht spätere Prüfung entlang von Art. 4, Art. 26, Art. 27 und Anhang III
Erfassungslink für Teams oder Lieferanten	verteilte Einspeisung ohne Vollzugriff	reduziert Shadow AI und verbessert Vollständigkeit des Registers
Gastmodus / lokale Zwischenspeicherung	niederschwellige Erstaufnahme ohne unmittelbare Kontobindung	senkt Adoption und erleichtert privacy-sensible Discovery
Use-Case-Pass als PDF/JSON	menschen- und maschinenlesbares Artefakt	stärkt Nachweisfähigkeit, Exportierbarkeit und spätere Weiterverarbeitung
Minimaler Status + Audit-Spur	dokumentierte formale Einordnung statt bloßer Notizsammlung	erzeugt belastbarere Governance-Historie als lose Spreadsheets

7 Warum Unternehmen jetzt beginnen sollten

Die Frage ist nicht, ob jedes Unternehmen heute schon einen Hochrisiko-Fall im engeren Sinn nachweisen kann. Die Frage ist, ob ein Unternehmen ohne strukturierte Registerarbeit seriös *ausschließen* kann, dass solche Fälle vorliegen oder entstehen. Gerade deshalb sollten Unternehmen mit KI-Nutzung jetzt beginnen.

7.1 Erstens: Art. 4 gilt bereits

Seit dem 2. Februar 2025 gelten die Kapitel I und II, also auch Art. 4 zur KI-Kompetenz.[33] Die Kommission hat inzwischen eigens FAQ und ein Repository praktischer AI-Literacy-Maßnahmen veröffentlicht.[34] Das signalisiert deutlich: AI Literacy ist keine entfernte Zukunftspflicht, sondern eine bereits operative Erwartung.

Wer KI-Kompetenz ernsthaft aufbauen will, muss wissen, welche Einsatzfälle existieren, in welchen Funktionen sie genutzt werden und welche Personengruppen betroffen sind. Ein Register ist dafür die naheliegende Infrastruktur.

7.2 Zweitens: Die allgemeine Anwendbarkeit des AI Act ist nah

Der 2. August 2026 ist keine abstrakte Fernmarke mehr, sondern die allgemeine Anwendungsgrenze der Verordnung.[35] Organisationen, die bis dahin erst mit der Entdeckung ihrer KI-Nutzung beginnen, verlieren wertvolle Monate an Inventarisierung, Zuständigkeitsklärung und Priorisierung.

7.3 Drittens: Die größte Lücke liegt meist in der Discovery, nicht im Policy-Dokument

In der Praxis existiert KI-Nutzung oft verteilt: Fachbereiche, Pilotprojekte, Assistenten, eingekaufte SaaS-Funktionen, Browser-Plug-ins, einzelne Teams, Lieferanten und Agenturen. Die formale Policy hinkt dann der Realität hinterher. Ein niedrigschwelliges, use-case-zentriertes Register ist deshalb kein „später Governance-Luxus“, sondern die notwendige Vorbedingung aller weiteren Governance.

7.4 Viertens: Frühzeitige Registerarbeit vermeidet hektische Fehlklassifikation

Wer zu spät beginnt, neigt zu groben Vereinfachungen: Alles wird pauschal als „unkritisch“ oder umgekehrt als „hochriskant“ markiert. Beides ist ineffizient. Eine strukturierte Capture-Logik erlaubt stattdessen ein differenziertes Vorgehen: zuerst Sichtbarkeit, dann Priorisierung, dann vertiefte Prüfung dort, wo Anhang III, Art. 26, Art. 27 oder Art. 50 tatsächlich berührt sein könnten.

7.5 Fünftens: Ein exportierbares Artefakt ist besser als ein loses Spreadsheet

Viele Organisationen arbeiten anfangs mit Tabellen, Chat-Protokollen oder unverbundenen Einzelformularen. Diese Formate sind für Discovery nützlich, aber schwach in Verantwortungslogik, Statushistorie und exportierbarer Evidenz. Ein standardisierter Use-Case-Pass in PDF und JSON ist deshalb mehr als Komfort. Er markiert den Übergang von bloßer Sammlung zu prüffähiger, wiederverwendbarer Dokumentation.[36]

8 Schlussfolgerung

Das zentrale Ergebnis dieses Whitepapers lautet: Für Unternehmen, die KI-Anwendungsfälle identifizieren, dokumentieren und regulatorisch vorbereiten wollen, ist ein use-case-zentriertes Register der rechtssystematisch sauberere Ausgangspunkt als ein bloßes Tool-Inventar.

[33] Art. 113 lit. a AI Act [1]; Europäische Kommission [2, 3].
[34] Vgl. [4, 5].
[35] Art. 113 AI Act [1].
[36] Vgl. [6, 7].

Diese Aussage stützt sich nicht auf Produktmarketing, sondern auf die Struktur des AI Act selbst. Der Verordnungsgeber denkt in Zweckbestimmung, Verwendungskontext, betroffenen Personengruppen, menschlicher Aufsicht, Transparenzsituationen und nachweisfähigen Pflichten. Genau deshalb ist der KI-Einsatzfall die sinnvollere Basiseinheit der Dokumentation.

KIregister.com operationalisiert diese Logik in einer Weise, die für die frühe Unternehmenspraxis besonders relevant ist:

- Die Capture-Maske erfasst die juristisch relevanten Kontextfelder.
- Die Owner-Rolle schafft belastbarere Verantwortung als eine reine Personenliste.
- Die freie Basisschicht senkt die Hürde der Ersterfassung.
- Verteilte Capture-Wege reduzieren Shadow AI.
- Statusdokumentation, Audit-Spur und Use-Case-Pass schaffen frühe Nachweisfähigkeit.[37]

Der Ansatz ist damit nicht „vollständige Compliance aus einem Klick“. Aber er ist aus wissenschaftlich-juristischer Sicht ein besonders belastbarer Startpfad in Richtung EU-AI-Act-Readiness. Für Unternehmen mit realen KI-Einsatzfällen ist gerade jetzt der richtige Zeitpunkt, diese Basisschicht aufzubauen.

[37] Vgl. [6].

Literatur- und Quellenverzeichnis

Literatur

[1] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 12.7.2024.

[2] European Commission. *AI Act*. Offizielle Übersichtsseite der Europäischen Kommission zum AI Act, mit Umsetzungszeitplan. Abruf: 12.03.2026.

[3] European Commission. *Questions & Answers on the AI Act*. Offizielle FAQ der Europäischen Kommission. Abruf: 12.03.2026.

[4] European Commission. *AI literacy questions & answers*. Offizielle Erläuterungen der Kommission zu Art. 4 AI Act. Abruf: 12.03.2026.

[5] European Commission. *Living repository to foster learning and exchange on AI literacy*. Offizielles Repository der Kommission zu AI-Literacy-Praktiken. Abruf: 12.03.2026.

[6] KIregister.com. Bereitgestellte Quellcodebasis und interne Produktdokumentation, insbesondere zur freien Registerschicht, Quick Capture, Access-Code-Erfassung, Statusdokumentation, Audit-Trail und Use-Case-Pass. Funktionsanalyse durch OpenAI im Zeitraum 12.03.2026.

[7] *KI-Register Ansatz - Kernannahmen (Axiome)*. Vom Auftraggeber bereitgestellte PDF-Unterlage, Stand der ausgewerteten Fassung: 12.03.2026.