GARION

Organizational AI Readiness Intelligence

KI-Reife verstehen, belegen und dokumentieren.

Whitepaper für Unternehmen

Die EU-KI-Verordnung in der Praxis

Ein sachlicher Leitfaden: Pflichten nach der EU-KI-Verordnung, was „ausreichende KI-Kompetenz“ bedeutet und wie eine Organisation ihre KI-Reife nachvollziehbar dokumentiert.

Lokale macOS- und Windows-Anwendung · Deutsch & Englisch · Stand: Juni 2026

prega-design · predrag.gasic@prega-design.de

Inhalt

Hinweis zur Benennung: „EU-KI-Verordnung“ ist die deutsche Bezeichnung für den EU AI Act (Verordnung (EU) 2024/1689). Beide Begriffe meinen dasselbe Gesetz. Dieses Whitepaper dient der Information und stellt keine Rechtsberatung dar.

1. Über dieses Whitepaper

Dieses Whitepaper richtet sich an Organisationen, die Künstliche Intelligenz einsetzen oder bereitstellen und ihre Verpflichtungen aus der EU-KI-Verordnung erfüllen wollen. Es beschreibt sachlich, welche Pflichten für Betreiber entstehen, was „ausreichende KI-Kompetenz“ in der Praxis bedeutet und wie eine Organisation ihren Stand nachvollziehbar erfasst, bewertet und dokumentiert.

Der zweite Teil zeigt, wie die Anwendung GARION diese Arbeit operativ unterstützt — als lokales Werkzeug, das aus Rollen und Nachweisen ein erklärbares Reifebild berechnet, Lücken priorisiert und prüffähige Berichte erzeugt. GARION trifft keine rechtlichen Aussagen und ersetzt keine juristische oder fachliche Prüfung; es schafft die strukturierte Faktengrundlage, auf der eine solche Prüfung aufsetzen kann.

Adressaten dieses Whitepapers sind insbesondere Geschäftsführung und Leitung, KI- und Compliance-Verantwortliche, Datenschutz- und IT-Funktionen sowie Personal- und Weiterbildungsverantwortliche. Es ist so aufgebaut, dass die Kapitel 2 bis 6 die regulatorische Ausgangslage erklären, die Kapitel 7 bis 15 die Funktionsweise des Werkzeugs beschreiben und die Kapitel 16 bis 20 die praktische Umsetzung anleiten. Wer schnell starten möchte, findet in Kapitel 16 den empfohlenen Arbeitsablauf und in Kapitel 20 eine kompakte Checkliste.

Die Darstellung der Verordnung gibt den Stand von Juni 2026 wieder. Laufende Gesetzgebungsprozesse (insbesondere der „Digital Omnibus“) können einzelne Formulierungen und Fristen verändern; die grundsätzliche Pflicht zur dokumentierten KI-Kompetenz bleibt davon unberührt.

2. Die EU-KI-Verordnung im Überblick

Die EU-KI-Verordnung ist das erste umfassende Regelwerk für Künstliche Intelligenz. Sie verfolgt einen risikobasierten Ansatz: Je stärker ein KI-System Rechte, Sicherheit oder Gesundheit von Menschen berühren kann, desto höher die Anforderungen. Die Verordnung unterscheidet vier Risikoklassen:

Risikoklasse	Bedeutung (Überblick)
Inakzeptables Risiko	Verbotene Praktiken (z. B. bestimmte Formen der Manipulation oder des Social Scoring).
Hohes Risiko	Systeme nach Anhang III mit strengen Anforderungen an Risikomanagement, Daten, Aufsicht und Dokumentation.
Begrenztes Risiko	Transparenzpflichten (z. B. Kennzeichnung KI-generierter Inhalte oder von Chatbots).
Minimales Risiko	Der Großteil der Anwendungen; keine spezifischen Pflichten über die Querschnittsregeln hinaus.

Die Verordnung unterscheidet außerdem Rollen: Ein „Anbieter“ entwickelt oder bringt ein KI-System in Verkehr; ein „Betreiber“ (Deployer) setzt ein KI-System unter eigener

Verantwortung ein. Die meisten Unternehmen sind in der Rolle des Betreibers — und genau für diese Rolle ist die Pflicht zur KI-Kompetenz besonders relevant, weil sie unabhängig von der Risikoklasse gilt.

> **Warum Artikel 4 für fast alle gilt**
>
> Kernunterscheidung für die Praxis: Die Hochrisiko-Anforderungen treffen einen klar abgegrenzten Kreis von Systemen. Die Pflicht zur KI-Kompetenz (Artikel 4) trifft hingegen nahezu jede Organisation, die KI überhaupt nutzt.

2.1 Pflichten für Betreiber von Hochrisiko-Systemen

Setzt eine Organisation ein Hochrisiko-System nach Anhang III ein (etwa in den Bereichen Beschäftigung und Personalauswahl, Zugang zu wesentlichen Diensten, Bildung oder kritische Infrastruktur), treffen sie als Betreiber zusätzliche Pflichten. Diese sind organisatorischer Natur und überschneiden sich stark mit dem, was GARION strukturiert dokumentiert:

Pflicht (Betreiber)	Worum es geht
Menschliche Aufsicht	Geeignete Personen mit der nötigen Kompetenz und Befugnis mit der Aufsicht betrauen.
Nutzung nach Anleitung	Das System gemäß der Gebrauchsanweisung des Anbieters betreiben.
Überwachung & Meldung	Den Betrieb beobachten und Vorfälle oder Risiken melden.
Aufbewahrung von Protokollen	Automatisch erzeugte Protokolle für den vorgesehenen Zeitraum aufbewahren.
Information der Betroffenen	Betroffene Personen ggf. über den Einsatz informieren.

Die Schulungs- und Kompetenzanforderung für die menschliche Aufsicht bleibt auch nach den geplanten Änderungen des „Digital Omnibus“ bestehen. Wer die zuständigen Rollen, ihr Risiko und ihre Kompetenznachweise sauber führt, erfüllt zugleich einen wesentlichen Teil dieser Betreiberpflichten.

2.2 Transparenzpflichten bei begrenztem Risiko

Unabhängig von der Hochrisiko-Einstufung gelten Transparenzpflichten: KI-Systeme, die mit Menschen interagieren (etwa Chatbots), müssen als solche erkennbar sein; KI-generierte oder -manipulierte Inhalte (einschließlich „Deepfakes“) sind grundsätzlich zu kennzeichnen. Für die organisatorische Reife heißt das, dass auch Rollen mit Inhaltserstellung oder Kundeninteraktion erfasst und mit Richtlinien hinterlegt werden sollten.

2.3 KI-Modelle mit allgemeinem Verwendungszweck (GPAI)

Für Modelle mit allgemeinem Verwendungszweck — etwa große Sprachmodelle — gelten eigene Pflichten, die vorrangig die Anbieter dieser Modelle treffen (technische Dokumentation, Urheberrecht, Transparenz). Für die meisten Unternehmen sind sie mittelbar relevant: Sie nutzen solche Modelle als Betreiber und sollten dokumentieren, in welchen Rollen sie eingesetzt werden und welche Kompetenz dafür erforderlich ist.

3. Artikel 4 — die Pflicht zur KI-Kompetenz

Artikel 4 verpflichtet Anbieter und Betreiber, Maßnahmen zu ergreifen, um nach besten Kräften ein ausreichendes Maß an KI-Kompetenz bei ihrem Personal und bei anderen Personen sicherzustellen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind. Dabei sind das technische Wissen, die Erfahrung, Ausbildung und Schulung der Personen sowie der Kontext zu berücksichtigen, in dem die Systeme eingesetzt werden.

In der Praxis bedeutet das zweierlei. Erstens müssen die Personen, die mit KI arbeiten, sie hinreichend verstehen, um sie verantwortungsvoll und im jeweiligen Kontext angemessen zu nutzen. Zweitens muss die Organisation belegen können, dass sie sich darum bemüht hat — „nach besten Kräften“ ist nicht „gar nichts“, sondern verhältnismäßiger, rollengerechter und dokumentierter Aufwand.

3.1 Hinweis zum „Digital Omnibus“

Im Zuge des „Digital Omnibus“ wird die Formulierung von Artikel 4 voraussichtlich abgemildert — von „sicherstellen“ hin zu „die Entwicklung von KI-Kompetenz unterstützen“. Für Betreiber von Hochrisiko-Systemen bleibt die Schulungspflicht zur menschlichen Aufsicht bestehen. Für die operative Vorbereitung ändert sich wenig: Eine Organisation, die Kompetenz und Dokumentation strukturiert nachweist, ist in jedem Fall besser aufgestellt als eine, die es nicht tut.

4. Fristen und Zeitachse

Datum	Was geschieht
2. Februar 2025	Die Pflicht zur KI-Kompetenz (Art. 4) und die Verbote für inakzeptable Praktiken werden anwendbar.
2. August 2025	Pflichten für KI-Modelle mit allgemeinem Verwendungszweck (GPAI) und Governance-Strukturen greifen.
2. August 2026	Die nationalen Marktüberwachungsbehörden erhalten die formalen Durchsetzungsbefugnisse; weitere Pflichten werden anwendbar.
ab 2027	Weitere Anforderungen für Hochrisiko-Systeme greifen schrittweise; der „Digital Omnibus“ kann einzelne Fristen anpassen.

Für die meisten Unternehmen ist der 2. August 2026 der entscheidende Bezugspunkt: Ab diesem Zeitpunkt können Aufsichtsbehörden die KI-Kompetenzpflicht durchsetzen. Wer bis dahin keine belastbare Dokumentation führt, trägt ein vermeidbares Risiko — nicht, weil Kompetenz fehlt, sondern weil sie nicht belegt werden kann.

5. Was „ausreichende KI-Kompetenz“ praktisch bedeutet

„Ausreichend“ ist kein absoluter Maßstab, sondern ein relativer: Er bemisst sich an der Rolle, am Risiko der Nutzung und am Einsatzkontext. Eine Person, die ein KI-System lediglich passiv nutzt, benötigt ein anderes Kompetenzniveau als eine Person, die mit KI rechte- oder sicherheitsrelevante Entscheidungen vorbereitet.

Daraus folgt ein praktischer Grundsatz: Kompetenz lässt sich nicht pauschal, sondern nur rollenbezogen und risikogewichtet bestimmen. Eine sinnvolle Struktur unterscheidet entlang dreier Achsen:

Achse	Beispielhafte Stufen
KI-Nutzung	Keine · Niedrig · Mittel · Hoch · Kritisch
Risikostufe der Nutzung	Niedrig · Moderat · Hoch · Inakzeptabel
Erforderliche Kompetenz	Bewusstsein · Grundlagen · Praktiker · Fortgeschritten · Verantwortungsvolle Nutzung

Eine Rolle mit hoher, risikoreicher KI-Nutzung sollte ein höheres Kompetenzniveau nachweisen als eine Rolle mit geringer Nutzung. Genau diese Logik bildet GARION ab: Es gewichtet die Reife dort, wo das Risiko tatsächlich sitzt.

5.1 Beispiele für angemessene Kompetenzniveaus

Die folgenden Beispiele sind illustrativ und keine verbindliche Vorgabe; die richtige Einstufung hängt vom konkreten Einsatz in der Organisation ab.

Beispielrolle	KI-Nutzung	Risiko	Angemessene Kompetenz
Teammitglied (gelegentliche Nutzung)	Niedrig	Niedrig	Bewusstsein / Grundlagen
Content-Erstellung (Marketing)	Hoch	Moderat	Praktiker (inkl. Quellen- und Markensicherheit)
Kundenservice mit KI-Assistent	Mittel	Hoch	Praktiker
Personalauswahl / Recruiting	Mittel	Hoch	Praktiker bis Fortgeschritten

Beispielrolle	KI-Nutzung	Risiko	Angemessene Kompetenz
Leitung mit Aufsichtsfunktion	Mittel	Moderat	Verantwortungsvolle Nutzung

5.2 Verhältnismäßigkeit

Die Verordnung verlangt keinen einheitlichen Schulungskatalog für alle, sondern angemessene Maßnahmen. Für Rollen mit geringer, risikoarmer Nutzung kann ein Bewusstsein für Chancen, Grenzen und Risiken von KI ausreichen; für Rollen, die mit KI rechte- oder sicherheitsrelevante Entscheidungen vorbereiten, ist ein deutlich höheres Niveau angemessen. Dieser verhältnismäßige Zuschnitt schützt vor zwei Fehlern: zu wenig zu tun und damit ein Risiko zu tragen — oder pauschal zu viel zu verlangen und Ressourcen zu binden, ohne das tatsächliche Risiko zu treffen. GARION unterstützt die Verhältnismäßigkeit, indem es jede Rolle einzeln nach Nutzung und Risiko bewertet.

6. Vom Anspruch zum Nachweis: das Dokumentationsproblem

Die meisten Organisationen haben KI organisch eingeführt — ein Werkzeug hier, ein Pilot dort, eine Abteilung, die es still in den Arbeitsalltag integriert. Selten gab es einen Moment, in dem formal festgehalten wurde, wer geschult ist, wer verantwortlich ist und wo sich das Risiko konzentriert. Die Folge ist eine Lücke nicht im Können, sondern im Nachweis.

Diese Lücke wird zum Problem, sobald sie jemand prüft: eine Aufsichtsbehörde, ein Kundenfragebogen, ein Auditor oder die eigene Revision. Unter Druck rekonstruierte Dokumentation ist aufwendig, fehleranfällig und wenig überzeugend. Eine ruhig im Voraus aufgebaute, datierte und auf Belege gestützte Dokumentation ist günstiger zu erstellen und deutlich belastbarer.

> Das Ziel ist daher nicht, „KI-kompetent zu werden“ — das sind viele Organisationen bereits —, sondern die vorhandene Kompetenz sichtbar, strukturiert und prüffähig zu machen.

6.1 Was prüffähige Dokumentation ausmacht

Damit Dokumentation einer Prüfung standhält, sollte sie mehrere Merkmale erfüllen. Sie ist nachvollziehbar (jede Aussage lässt sich auf einen konkreten Beleg zurückführen), aktuell (Stände sind datiert und der Verfall von Nachweisen wird erkannt), vollständig im relevanten Umfang (die wesentlichen Rollen sind erfasst), konsistent (gleiche Begriffe und Maßstäbe über die Organisation hinweg) und reproduzierbar (dieselbe Datengrundlage führt zu demselben Ergebnis).

Diese Merkmale sind kein Selbstzweck. Sie entscheiden darüber, ob eine Geschäftsführung im Prüfungsfall ruhig und belegt antworten kann — oder ob sie unter Druck rekonstruieren

muss. GARION ist entlang genau dieser Merkmale gebaut: deterministische Berechnung, durchgängige Rückführbarkeit auf Nachweise, automatische Statuslogik und ein anfügendes Audit-Protokoll.

7. Was GARION ist

GARION ist eine lokale macOS- und Windows-Anwendung, die verstreute Fakten über Menschen, Rollen Nachweise einer Organisation in ein einziges, erklärbares und prüffähiges Bild der KI-Reife verwandelt. Es ist bewusst kein Lernmanagementsystem, keine HR-Software und keine Compliance-Plattform: Es liefert keine Schulungen und behauptet keine rechtliche Konformität, sondern dokumentiert, dass Reife vorhanden ist, und macht sie nachvollziehbar.

Das Modell ruht auf vier Begriffen:

Begriff	Bedeutung
Organisation	Die bewertete Einheit (eine pro Datenbank).
Rolle	Eine Funktion mit KI-Nutzungsgrad, Risikograd und erforderlichem Kompetenzniveau.
Nachweis	Ein dokumentierter, prüfbarer Beleg: eine Schulung, eine Zertifizierung, eine Richtlinienannahme.
Readiness	Das berechnete Urteil: wie gut Nachweise die Rollen abdecken, gewichtet nach Risiko.

Vier Eigenschaften prägen die Arbeitsweise: GARION ist lokal (alle Daten bleiben auf dem Gerät, keine Cloud, kein Konto), deterministisch (gleiche Eingaben ergeben immer dieselbe Zahl — die KI berechnet den Score nie), prüffähig (jede Kennzahl ist auf Nachweise zurückführbar, jede Änderung wird protokolliert) und zweisprachig (Oberfläche, Berichte und Hilfe in Deutsch und Englisch).

8. Architektur und Funktionsweise

GARION ist eine Einzelplatz-Anwendung ohne Server und ohne Cloud-Datenbank. Eine Oberfläche stellt die Inhalte dar; ein nativer Kern übernimmt die Datenhaltung, die Berechnungen, das Audit-Protokoll und die Erzeugung von Berichten. Der einzige optionale Netzwerkaufruf ist eine ausdrücklich freigegebene Anfrage an einen KI-Dienst, der ausschließlich erklärende Texte formuliert.

Die Reihenfolge, in der GARION arbeitet, folgt einer klaren Doktrin: Readiness → Risiken → Lücken → Empfehlungen → Details. Sie erfassen Rollen und Nachweise; eine deterministische Engine berechnet daraus den Reife-Score; eine zweite Engine leitet priorisierte Lücken ab; und die Berichtsschicht fasst alles in prüffähige Artefakte. Alle Kernfunktionen arbeiten vollständig offline; die optionale KI ist additiv und abschaltbar, ohne dass eine Zahl, eine Lücke oder ein Bericht verloren geht.

8.1 Lokal-first in der Praxis

„Lokal-first“ ist mehr als ein technisches Detail. Es bedeutet, dass die Reife-Daten — die Aussagen darüber, wer in der Organisation wie kompetent ist — das Gerät nicht verlassen. Es gibt genau eine Datenbankdatei; ein Backup ist eine Kopie dieser Datei, eine Wiederherstellung ersetzt sie. Es gibt keinen Server, der ausfallen, und kein Konto, das kompromittiert werden könnte. Für eine Organisation, die sensible Personal- und Governance-Daten verarbeitet, ist diese Architektur die einfachste Form der Datensparsamkeit: Was nie übertragen wird, muss auch nicht abgesichert werden.

9. Das Rollenmodell

Rollen beschreiben, welche Tätigkeiten welches KI-Risiko tragen. Sie sind die Grundlage dafür, dass GARION die Reife dort gewichtet, wo das Risiko sitzt. Damit eine Organisation nicht vor einem leeren System startet, liefert GARION vier zweisprachige Vorlagenpakete mit 24 vordefinierten Rollen (Allgemeine Geschäftsfunktionen, L&D/HR, Vertrieb & Marketing, Management). Jede Rolle ist eine editierbare Vorlage — die Organisation passt sie an ihre Realität an.

Das Profil jeder Rolle umfasst die KI-Nutzung, die Risikostufe, die erforderliche Kompetenz, die erforderlichen Nachweisarten sowie Hinweise zu typischen Risiken und wahrscheinlichen Lücken. Höheres Risiko erhöht das Gewicht der Rolle im Gesamt-Score. Vorlagenrollen sind schreibgeschützt; durch Duplizieren entsteht eine bearbeitbare Kopie.

9.1 Die vier Vorlagenpakete

Die mitgelieferten Pakete decken typische Organisationsstrukturen ab und lassen sich frei anpassen oder ergänzen:

Paket	Enthaltene Rollen (Beispiele)
Allgemeine Geschäftsfunktionen	Bürokraft, Büroleitung, Kundenservice, Projektkoordination, Teammitglied, Teamleitung
L&D / HR	Personalleitung, Recruiter, Leitung Personalentwicklung, Instructional Designer, Schulungskoordination, HR Business Partner
Vertrieb & Marketing	Marketingleitung, Content-Management, Vertriebsmitarbeiter:in, Vertriebsleitung, Kundenbetreuung, Business Development
Management & Leitung	Geschäftsführung sowie weitere Leitungsfunktionen mit organisationsweiter Wirkung

Insgesamt 24 vordefinierte Rollen sorgen dafür, dass eine Organisation nicht vor einem leeren System startet, sondern unmittelbar ein realistisches, anpassbares Ausgangsbild erhält.

10. Nachweise: Arten, Status und Audit

Ein Nachweis ist ein dokumentierter Beleg der Reife — etwa ein Schulungsabschluss, nicht die Schulung selbst. GARION kennt ein kontrolliertes Vokabular von zehn Nachweisarten: KI-Kompetenzschulung, Zertifizierung, Bewertung, Richtlinienannahme, Managerbestätigung, KI-Tool-Freischaltung, LMS-Abschluss, Workshop, Dokument und Sonstiges. Das hält Datensätze organisationsweit konsistent und auswertbar.

Jeder Nachweis erhält automatisch und deterministisch einen Status, der bei jedem Aufruf neu berechnet wird:

Bedingung	Status
Kein Ausstellungsdatum	Ausstehend
Kein Ablauf oder Ablauf in über 30 Tagen	Gültig
Ablauf innerhalb von 30 Tagen	Läuft ab
Ablauf in der Vergangenheit	Abgelaufen

Jede Aktion — Erstellt, Aktualisiert, Zugewiesen, Archiviert, Abgelaufen — wird sowohl organisationsweit als auch im nachweis-eigenen Verlauf festgehalten. Geht ein Nachweis in „Abgelaufen“ über, wird das automatisch protokolliert. So bleibt das Reifebild ohne manuelle Überwachung ehrlich: Es zeigt Verfall, bevor er zur Beanstandung wird.

11. Der Readiness-Score

Der Readiness-Score ist eine einzelne Zahl von 0 bis 100. Er ist deterministisch, zerlegbar, in vier Bändern benannt und wird von einer Konfidenz begleitet. Die gesamte Berechnung ist in einer Ansicht „Wie wurde das berechnet?“ aufklappbar — mit den Sub-Scores, ihren Gewichten, der Risikogewichtung je Rolle und der Konfidenz-Aufschlüsselung.

11.1 Die acht Komponenten und ihre Gewichte

#	Komponente	Gewicht	Misst
C1	Nachweisabdeckung	22 %	Anteil vorhandener und gültiger erforderlicher Nachweise.
C2	Rollenabdeckung	18 %	Anteil der Rollen, die ihre Schwelle erreichen.
C3	Risikoexposition (invers)	20 %	Unabgedeckte Reife auf Rollen mit höherem Risiko.
C4	Schulungsaktualität	12 %	Anteil frischer (nicht veralteter) Schulungsnachweise.
C5	Verantwortungsabdeckung	10 %	Rollen und Schlüsselnachweise mit zugewiesenem Owner.
C6	Governance-Signale	8 %	Aktualität der Bewertung und strukturelle Vollständigkeit.
C7	Richtlinienannahme	6 %	Anteil eingeholter erforderlicher Richtlinienannahmen.
C8	Bewertungsabschluss	4 %	Ob eine aktuelle Bewertung vorliegt.

Nachweisabdeckung (C1) und risikogewichtete Exposition (C3) tragen zusammen 42 %, weil der Kern „nachweis- und risikoorientiert“ ist. Governance, Richtlinie und Bewertung (C6–C8) sind reale, aber sekundäre Signale und bewusst niedrig gewichtet.

11.2 Risikogewichtung

Innerhalb der rollenbezogenen Komponenten trägt jede Rolle proportional zu einem Risikogewicht bei. Eine Hochrisiko-Rolle ohne Kompetenznachweis senkt den Score rund dreimal stärker als eine Rolle mit geringem Risiko. Dieser Mechanismus bildet den risikobasierten Geist der EU-KI-Verordnung ab, ohne rechtliche Konformität zu behaupten.

11.3 Konfidenz

Die Konfidenz ist vom Score getrennt und beantwortet, wie sehr man der Zahl vertrauen sollte. Sie ergibt sich aus vier Faktoren: Datenvollständigkeit (40 %), Nachweisaktualität (25 %), Quellenqualität (20 %) und Aktualität der Eingabe (15 %), abgebildet auf Niedrig, Mittel oder Hoch. Ein hoher Score aus wenigen Datenpunkten ist nicht dasselbe wie ein hoher Score aus voller Abdeckung; die Konfidenz verhindert falsche Sicherheit.

11.4 Die vier Bänder

Score	Band	Bedeutung
0–39	Gefährdet	Dringender Handlungsbedarf.
40–59	Im Aufbau	Grundlagen vorhanden, Lücken offen.
60–79	In Entwicklung	Solide, gezielt zu schärfen.
80–100	Bereit	Belastbar dokumentiert.

Die Bänder sind beratende Beschreibungen, keine Konformitätsurteile. Die Oberfläche verwendet bewusst nie das Wort „konform“.

11.5 Wie die Berechnung im Kern arbeitet

Der Gesamt-Score ist der gewichtete Durchschnitt der acht Komponenten-Sub-Scores (je 0–100), wobei die rollenbezogenen Komponenten risikogewichtet sind. Beispielhaft: Die Schulungsaktualität ergibt sich als Anteil frischer an allen Schulungsnachweisen (ablaufende zählen anteilig); die Richtlinienannahme als Anteil der eingeholten an den erforderlichen Annahmen, je Rolle risikogewichtet; die Governance-Signale mischen die Aktualität der letzten Bewertung mit der strukturellen Vollständigkeit der Daten.

Wichtig für die Praxis: Importierte Nachweise werden nach der Übernahme identisch zu manuell erfassten bewertet; die Quellenqualität bemisst sich an der Nachweisart, nicht am Eingangsweg. Der Import bestehender Daten erhöht jedoch die Datenvollständigkeit — und hebt damit zugleich Score und Konfidenz. Die Gewichte und Schwellen sind als versionierte Konstanten hinterlegt, sodass eine Anpassung nachvollziehbar und reproduzierbar bleibt.

12. Die Lücken-Engine

Eine Zahl allein genügt nicht; entscheidend ist, was zu tun ist. Die Lücken-Engine ist eine deterministische Regel-Engine, die nach der Readiness läuft und eine nach Wirkung sortierte Liste erzeugt. Sie wendet acht Regeln an; der Basis-Schweregrad wird durch das Risikogewicht der Rolle eskaliert.

Regel	Erkennt
GR1	Fehlender Nachweis: eine erforderliche Nachweisart hat keine gültige Abdeckung.
GR2	Abgelaufener Nachweis, auf den noch vertraut wird.
GR3	Hochrisiko-Rolle unterhalb der erforderlichen Kompetenz.
GR4	Fehlende Verantwortung: Rolle oder Schlüsselnachweis ohne Owner.
GR5	Fehlende Richtlinienannahme.
GR6	Veraltete Schulung (über dem Veraltungshorizont).
GR7	Unvollständige Rollenabdeckung (unzugeordnet oder unter Schwelle).
GR8	Governance-Blindstelle (keine Bewertung seit 90+ Tagen oder Risikostufen unbestimmt).

Jede Lücke trägt einen Schweregrad (Niedrig · Mittel · Hoch · Kritisch), eine Uplift-Schätzung (wie stark sich die Readiness nach Behebung verbessern könnte — eine Schätzung, kein Versprechen) und eine konkrete, vorformulierte Maßnahme. So wird aus einer Diagnose unmittelbar ein priorisierter, nachverfolgbarer Maßnahmenplan; der Lebenszyklus jeder Lücke (offen, in Bearbeitung, behoben) ist steuerbar.

12.1 Typische Maßnahmen je Lückentyp

Lücke	Typische Maßnahme
GR1 Fehlender Nachweis	Den erforderlichen Nachweis erfassen oder die zugehörige Schulung durchführen.
GR2 Abgelaufener Nachweis	Den Nachweis erneuern und das neue Ausstellungsdatum hinterlegen.
GR3 Rolle unter erf. Kompetenz	Gezielte Qualifizierung für die betroffene Rolle, bis das Zielniveau belegt ist.
GR4 Fehlende Verantwortung	Eine verantwortliche Person (Owner) für Rolle oder Nachweis zuweisen.
GR5 Fehlende Richtlinienannahme	Die Annahme der einschlägigen Richtlinie einholen und dokumentieren.
GR6 Veraltete Schulung	Die Schulung auffrischen und den Nachweis aktualisieren.
GR7 Unvollständige Rollenabdeckung	Rollen vollständig zuordnen und fehlende Profile ergänzen.
GR8 Governance-Blindstelle	Eine neue Bewertung durchführen und fehlende Risikostufen setzen.

Weil GARION die Lücken nach einem Prioritäts-Score (nicht allein nach Schweregrad) sortiert, steht die wirksamste Maßnahme zuerst — die Organisation arbeitet von oben nach unten und sieht den Fortschritt nach jeder Neuberechnung.

13. Der EU-KI-Verordnung-Readiness-Check

GARION enthält einen eigenen, rein deterministischen Readiness-Check. Er prüft strukturiert, ob ein Bericht ausreichende Reife-Nachweise und Dokumentationsqualität trägt. Er ist ausdrücklich keine Konformitäts- zertifizierung; die Benennung ist verbindlich „Readiness-Check“, nie „Compliance-Zertifizierung“. Jeder Bereich wird deterministisch bewertet (abgedeckt, teilweise, fehlend) und zu einem Gesamtstatus aggregiert: Stark · Teilweise · Schwach · Nicht genügend Daten.

Geprüft werden zehn Bereiche:

- KI-Kompetenz dokumentiert
- Rollenbasierte KI-Nutzung dokumentiert
- Erforderliche Nachweise zugeordnet
- Richtlinienannahme dokumentiert
- Verantwortung/Owner zugewiesen
- Risikostufe dokumentiert
- Readiness-Lücken identifiziert

- Empfohlene Maßnahmen enthalten
- Audit-Trail verfügbar
- Nicht-rechtlicher Hinweis enthalten

Der Check verschiebt die Frage vom Unzulässigen („Sind wir konform?“) zum Beantwortbaren („Ist unsere Dokumentation stark genug, um sie zu vertreten?“). Die rechtliche Bewertung bleibt ausdrücklich einer fachkundigen Stelle vorbehalten.

14. Berichte und Exporte

Die Berichtsschicht erzeugt prüffähige Artefakte, jeweils mit Herkunfts- und Hinweisblock. Jeder Bericht ist auf Deutsch oder Englisch verfügbar und funktioniert vollständig mit abgeschalteter KI (deterministische Textbausteine statt KI-Erzählung).

Artefakt	Inhalt
Executive One-Pager (PDF)	Einseitige Management-Übersicht: Score, Konfidenz, Top-3-Risiken/Lücken/Maßnahmen, EU-KI-Verordnung-Readiness-Status.
AI-Readiness-Report	Die vollständige, erklärbare Scorecard.
Audit-Readiness-Report	Prüfung, ob ein verteidigbarer Bericht exportierbar ist, mit blockierenden Punkten und Korrekturen.
Rollen-Reports	Detailliert je Funktion.
XLSX-Matrizen / CSV	Rollen-, Nachweis-, Lücken-, Abteilungs- und Audit-Tabellen zur Detailarbeit und Weiterverarbeitung.
.garion-Backup	Portables Paket für Sicherung und Übergabe; enthält keine Geheimnisse (keinen API-Schlüssel).

Jeder Bericht trägt den Hinweis, dass GARION keine rechtliche Konformität zertifiziert und keine rechtliche, regulatorische oder fachliche Beratung ersetzt.

14.1 Welcher Bericht wofür

Die Berichte erfüllen unterschiedliche Zwecke. Der Executive One-Pager dient der Leitung als verdichtete Statusübersicht für Berichterstattung und Entscheidungen. Der AI-Readiness-Report liefert die vollständige, erklärbare Grundlage, wenn eine technische oder Compliance-Funktion die Herleitung nachvollziehen möchte. Der Audit-Readiness-Report beantwortet die Frage, ob die Dokumentation aktuell prüffähig ist, und benennt die blockierenden Punkte. Die Matrizen und CSV-Exporte unterstützen die operative Detailarbeit, und das .garion-Backup dient der Sicherung und einer sauberen Übergabe.

Sinnvoll ist es, den Audit-Readiness-Report als internes Frühwarnsystem zu nutzen: Er zeigt, was einer Prüfung heute noch entgegenstünde, und macht die Vorbereitung damit planbar — lange bevor eine externe Anfrage eintrifft.

15. Datenschutz und Sicherheit

Im regulatorischen Umfeld ist die Vertraulichkeit der Daten zentral. GARION ist so gebaut, dass die Reife-Daten das Gerät nicht verlassen:

- **Lokal-first.** Die Anwendung läuft vollständig auf dem Gerät; die Kernfunktionen arbeiten ohne Netzwerk.
- **Schlüsselbund.** Ein optionaler KI-Schlüssel liegt ausschließlich im Schlüsselbund des Betriebssystems — nie in Datenbank, Konfiguration oder Protokollen.
- **Keine Inhalte an die KI.** Es werden keine Dateiinhalte oder Nachweise an die KI gesendet; Aggregation und Schwärzung gelten standardmäßig.
- **Deterministischer Kern.** Scores und Status werden nach festen Regeln berechnet; die KI ist additiv und entfernbar.
- **Append-only-Audit-Log.** Relevante Aktionen und jeder KI-Aufruf werden erfasst und sind exportierbar.

Der genaue Speicherort der lokalen Datenbank wird in den Einstellungen und unter „Über GARION“ angezeigt. Ein Backup ist eine Kopie dieser Datei; eine Wiederherstellung ersetzt sie.

16. Empfohlener Arbeitsablauf

Der folgende Ablauf führt eine Organisation vom leeren Zustand zu einem belastbaren, dokumentierten Reifebild. Eine erste, aussagekräftige Bewertung ist in unter 20 Minuten erreichbar.

1. **Organisation anlegen** und die Arbeitssprache wählen.
2. **Vorlagenpakete installieren** und auf die tatsächlich vorhandenen Rollen kürzen.
3. **KI-Nutzung und Risiko je Rolle setzen** — insbesondere die rechte- oder sicherheitsrelevanten Rollen realistisch einstufen.
4. **Nachweise erfassen oder importieren** (CSV/XLSX) — etwa Schulungsabschlüsse, Zertifizierungen, Richtlinienannahmen.
5. **Readiness berechnen** und einen ersten Snapshot speichern.
6. **Lücken priorisiert abarbeiten** — zuerst die mit dem höchsten Uplift; jede Behebung erfassen.
7. **Berichte exportieren** — Executive One-Pager für die Leitung, Audit-Readiness-Report für die Revision.
8. **Neubewertungs-Rhythmus festlegen** (z. B. quartalsweise), um einen Trend aufzubauen.

16.1 Ein Reifebild lesen — ein neutrales Beispiel

Zur Veranschaulichung ein fiktives Beispiel ohne Bezug zu einer realen Organisation. Nach Anlegen von zwölf Rollen und Import der vorhandenen Schulungsnachweise zeigt GARION einen Score von 61 (Band „In Entwicklung“) bei mittlerer Konfidenz. Die mittlere Konfidenz signalisiert, dass die Datenbasis tragfähig, aber noch nicht vollständig ist — der Wert ist belastbar, aber nicht endgültig.

Die Aufschlüsselung weist die Risikoexposition als schwächste Komponente aus. Im Gap-Center steht oben die Lücke GR3: drei als hochriskant eingestufte Rollen liegen unter der erforderlichen Kompetenz, Schweregrad „Hoch“, geschätzter Uplift +8. Die hinterlegte Maßnahme lautet, für diese Rollen den erforderlichen Kompetenznachweis zu erbringen. Nach Erfassen der entsprechenden Nachweise und einer Neuberechnung steigt der Score sichtbar, die Lücke verschwindet aus der Liste, und der Snapshot dokumentiert die Verbesserung. So wird aus einer Momentaufnahme ein nachvollziehbarer Fortschritt.

17. Rollen und Verantwortlichkeiten im Unternehmen

KI-Reife ist eine Querschnittsaufgabe. Eine klare Zuordnung verhindert, dass sie zwischen Abteilungen verloren geht. Die folgende Aufteilung hat sich in der Praxis bewährt und lässt sich an die Organisationsgröße anpassen:

Funktion	Beitrag
Geschäftsführung / Leitung	Trägt die Gesamtverantwortung; nutzt den Score und den One-Pager für Berichterstattung und Entscheidungen.
KI-/Compliance-Verantwortliche	Pflegt das Reifebild, definiert Rollen und Risiko, steuert die Lückenbehebung.
Abteilungs-/Teamleitung	Bestätigt die reale KI-Nutzung der Rollen und benennt Verantwortliche je Bereich.
HR / L&D	Liefert Schulungs- und Kompetenznachweise; verknüpft Schulungen mit Rollen.
IT / Datenschutz	Verantwortet Gerät, Backup und den lokalen Datenspeicher; prüft die Datenschutz-Konfiguration.

Wichtig ist, dass jede Rolle und jeder Schlüsselnachweis einen Owner hat. GARION macht fehlende Verantwortlichkeiten über die Regel GR4 sichtbar.

18. Governance über die Zeit

Kompetenz ist kein einmaliges Ereignis: Zertifizierungen laufen aus, Richtlinien werden ersetzt, Teams und KI-Nutzung verändern sich. Ein einmaliger Nachweis veraltet daher zwangsläufig. GARION begegnet dem auf zwei Wegen.

Erstens das automatische Ablaufmanagement: Nachweise wechseln 30 Tage vor Ablauf in den Status „Läuft ab“ und geben so einen frühen Anstoß zur Erneuerung. Zweitens der Snapshot-Mechanismus: Jede Neuberechnung speichert einen Stand, und jeder Bericht zeigt die Veränderung gegenüber der letzten Messung. So entsteht ein Trend, der Fortschritt über die Zeit belegt — genau das, was eine fortlaufende, dokumentierte Bemühung „nach besten Kräften“ in der Praxis ausmacht.

Praktisch empfiehlt sich ein fester Rhythmus mit klarer Zuständigkeit: eine verantwortliche Person, ein wiederkehrender Termin (etwa quartalsweise oder bei wesentlichen Änderungen der KI-Nutzung) und ein kurzer, immer gleicher Ablauf — neue Nachweise erfassen, abgelaufene erneuern, Rollen bei veränderter Nutzung anpassen, neu berechnen, Bericht exportieren. Anlässe für eine außerplanmäßige Neubewertung sind die Einführung eines neuen KI-Systems, organisatorische Veränderungen sowie regulatorische Aktualisierungen. Weil der Aufwand pro Durchlauf gering ist, bleibt die Dokumentation dauerhaft aktuell, statt zwischen zwei großen Projekten zu veralten.

19. Grenzen: Was GARION nicht leistet

Eine ehrliche Abgrenzung gehört zu einem belastbaren Werkzeug. GARION leistet ausdrücklich nicht:

- **Keine Rechtsberatung und keine Konformitätszertifizierung.** GARION bewertet die Qualität von Nachweisen und Dokumentation, nicht die rechtliche Konformität.
- **Keine inhaltliche Bewertung von KI-Systemen.** GARION prüft organisatorische Reife, nicht die technische Sicherheit oder Funktionsweise einzelner Systeme.
- **Kein Ersatz für Schulungen.** GARION dokumentiert Kompetenznachweise, vermittelt aber selbst keine Inhalte.
- **Keine automatischen Entscheidungen.** Die KI formuliert nur Erklärungen; die finale Interpretation bestätigt ein Mensch.

Diese Grenzen sind kein Mangel, sondern die Voraussetzung dafür, dass jede Aussage des Werkzeugs verteidigbar bleibt: GARION verspricht nie mehr, als es halten kann.

19.1 Zusammenfassung

Die EU-KI-Verordnung verlangt von Unternehmen nicht in erster Linie, KI-kompetent zu werden, sondern belegen zu können, dass die richtigen Rollen die richtige, dem Risiko angemessene Kompetenz besitzen — und dass dies dokumentiert ist. Diese Pflicht ist seit Februar 2025 aktiv und ab August 2026 durchsetzbar. Wer die Nachweise ruhig, datiert und nachvollziehbar im Voraus aufbaut, ist im Prüfungsfall belegt statt unter Druck. GARION liefert dafür die strukturierte, lokale und prüffähige Faktengrundlage: ein erklärbares Reifebild, priorisierte Lücken mit Maßnahmen und prüffähige Berichte — ohne rechtliche Aussagen zu treffen und ohne dass Daten das Gerät verlassen. Die rechtliche Bewertung bleibt einer fachkundigen Stelle vorbehalten; die Faktengrundlage dafür schafft die Organisation selbst.

20. Umsetzungs-Checkliste

Eine kompakte Liste, die eine Organisation von der Einführung zu einem gepflegten Reifeprogramm führt:

- Organisation angelegt, Arbeitssprache gewählt.
- Rollen vollständig erfasst, KI-Nutzung und Risiko realistisch gesetzt.
- Erforderliche Nachweisarten je Rolle definiert.
- Vorhandene Nachweise erfasst oder importiert; Quellen sauber.
- Owner für Rollen und Schlüsselnachweise zugewiesen.
- Richtlinien hinterlegt und deren Annahme dokumentiert.
- Erster Readiness-Snapshot gespeichert (Baseline).
- Lücken nach Uplift priorisiert und in Bearbeitung.
- Executive One-Pager und Audit-Readiness-Report exportiert.
- Neubewertungs-Rhythmus vereinbart (z. B. quartalsweise).
- Datensicherung als .garion-Paket eingerichtet.

21. Häufige Fragen

Frage	Antwort
Brauchen wir ein Konto oder Internet?	Nein. GARION ist lokal-first; der Kernbetrieb benötigt weder Konto noch Internetverbindung. Nur die optionale KI-Erläuterung benötigt einen Anbieter-Schlüssel und eine Verbindung.
Verändert die KI unsere Werte?	Nein. Alle Kernwerte sind deterministisch. Die KI formuliert nur Erklärungen in verständlicher Sprache und ist abschaltbar.
Zertifiziert GARION die Konformität?	Nein. GARION liefert eine deterministische Readiness-Sicht und ersetzt keine fachliche oder juristische Prüfung.
Wo liegen unsere Daten?	In einer lokalen Datenbank auf dem Gerät. Den genauen Pfad zeigen die Einstellungen und „Über GARION“.
Werden Inhalte an die KI gesendet?	Nein. Es werden keine Dateiinhalte oder Nachweise übertragen; Aggregation und Schwärzung gelten standardmäßig.
Wie oft sollten wir neu bewerten?	Eine quartalsweise Neubewertung hat sich bewährt; sie hält die Dokumentation aktuell und baut einen Trend auf.
Welche Plattform wird unterstützt?	macOS auf Apple Silicon und Windows 10/11 (64-bit). Für den Kernbetrieb ist kein Internet

Hinweis: GARION ist in zwei Editionen mit identischem Kern verfügbar. Die Business Edition bewertet eine einzelne Organisation; die Consultant Edition verwaltet mehrere, strikt voneinander getrennte Mandanten (eigene Datenbank je Mandant, keine mandantenübergreifenden Zugriffe). Für ein einzelnes Unternehmen ist die Business Edition die passende Wahl.

22. Glossar

Begriff	Bedeutung
Readiness-Score	Ein Wert von 0–100 für die organisationale KI-Reife, deterministisch und risikogewichtet.
Konfidenz	Maß dafür, wie sehr dem Score zu vertrauen ist (Datenvollständigkeit, Aktualität, Quellenqualität).
Nachweis	Ein dokumentierter, prüfbarer Beleg der Reife.
Abdeckung	Anteil der erforderlichen Nachweise, der vorhanden und gültig ist.
Lücke	Ein deterministisch erkannter Mangel mit Schweregrad, Uplift und Maßnahme.
Uplift	Geschätzte Reife-Verbesserung nach Behebung einer Lücke — eine Schätzung.
Band	Benannter Bereich eines Scores: Gefährdet / Im Aufbau / In Entwicklung / Bereit.
Snapshot	Ein gespeicherter Reife- und Konfidenzwert zu einem Zeitpunkt; ermöglicht einen Trend.
Audit-Log	Anfügendes Protokoll relevanter Änderungen und jedes KI-Aufrufs.
Betreiber (Deployer)	Wer ein KI-System unter eigener Verantwortung einsetzt.

Rechtlicher Hinweis & Quellen

GARION liefert eine beratende Einschätzung der organisatorischen KI-Bereitschaft. Es handelt sich nicht um eine Rechtsberatung und nicht um eine Zertifizierung der Konformität mit der EU-KI-Verordnung (EU AI Act) oder einer anderen Regulierung. Der Readiness-Check bewertet die Qualität von Nachweisen und Dokumentation, nicht die rechtliche Konformität. Alle Score-Werte sind deterministisch; KI-generierte Texte sind als beratend gekennzeichnet und ersetzen keine fachliche oder juristische Prüfung. Die finale Interpretation ist durch einen Menschen zu bestätigen. Angaben zur EU-KI-Verordnung geben den Stand von Juni 2026 wieder und können sich durch laufende Gesetzgebungsprozesse (u. a. „Digital Omnibus“) ändern.

- EU-KI-Verordnung — Artikel 4 (KI-Kompetenz): https://artificialintelligenceact.eu/article/4/
- AI Act Service Desk (Europäische Kommission) — Artikel 4: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4
- Europäische Kommission — AI Literacy, Fragen & Antworten: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
- Gibson Dunn — EU AI Act Omnibus Agreement: https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/

ERGÄNZUNG · STAND JUNI 2026

Neu in GARION: NIS2-Governance-Sichtbarkeit und kontrollierter Datenimport

GARION bleibt, was es ist: ein System für Organizational AI Readiness Intelligence. Seit der Erstausgabe dieses Whitepapers ist die Plattform um zwei Bereiche gewachsen, die hier sachlich beschrieben werden: ein NIS2-Governance-Modul für die Sichtbarkeit von Cyber-Risiken und ein kontrollierter Import bestehender Organisationsdaten. Beschrieben wird ausschließlich, was implementiert ist — keine Roadmap, keine Versprechen.

NIS2-Governance-Sichtbarkeit

Vorstände und Sicherheitsverantwortliche brauchen eine Antwort auf die Frage „Was ist jetzt wichtig?“ — in Sekunden, nicht nach Wochen der Tabellen-Konsolidierung. Das NIS2-Modul verbindet Cyber-Risiko-Daten zu einer lesbaren Governance-Kette:

Risiko → Behandlung → Nachweis → Frist → Executive-Überblick

- Risiko-Register: strukturierte Cyber-Risiken mit Titel, Auswirkung, Eintrittswahrscheinlichkeit, Verantwortlichem und Lebenszyklus-Status — lokal im eigenen Workspace.
- Behandlungen: jedes Risiko verknüpft mit einer oder mehreren Maßnahmen samt Verantwortlichem, Status und nachvollziehbarer Entscheidung.
- Nachweis-Verknüpfung: Behandlungen binden an reale Nachweis-Einträge (primär, erforderlich, unterstützend) — Beleg und Handlung gehören zusammen.
- Fristen-Governance: Behandlungen tragen Frist-Fenster mit eindeutigen Zuständen — ausstehend, gefährdet, eingehalten, überschritten — deterministisch in UTC ausgewertet. Eine eingehaltene oder überschrittene Frist ist ein Fakt, kein Interpretationsspielraum.
- Executive-Überblick: eine Governance-Zusammenfassung mit reinen Zählständen — Risiken, offene Risiken, Behandlungen, Nachweise, Frist-Zustände. Orientierung in unter zehn Sekunden, zweisprachig (DE/EN).

Bewusste Abgrenzung — sie ist Absicht, nicht Lücke: Das NIS2-Modul erzeugt keine Scores, keine Diagramme und keine KI-Interpretation. Es ist keine Rechtsberatung, keine NIS2-Zertifizierung und kein Incident-Management. GARION zeigt, wo Sie stehen — wie Sie handeln, entscheiden Sie.

Kontrollierter Datenimport

Niemand möchte eine Organisation von Hand abtippen. GARION importiert bestehende Daten per CSV — Rollen, Nachweise, Abteilungen, Workforce-Identitäten, Rollen-Zuordnungen und Trainingsnachweise — über eine einzige, kontrollierte Pipeline:

- Vorschau vor dem Schreiben: Jede Datei wird geprüft und vollständig angezeigt, bevor irgendetwas gespeichert wird. Erst die ausdrückliche Freigabe schreibt Daten — keine stillen Schreibvorgänge, kein automatischer Import.
- Deterministische Validierung: fehlende Pflichtfelder, Duplikate, unbekannte Verweise und ungültige Statuswerte blockieren die Übernahme, bis sie behoben sind. Der Freigabe-Knopf ist bei blockierenden Fehlern technisch deaktiviert.
- Pseudonym per Architektur: Workforce-Daten werden ohne Klarnamen importiert — nur opake Kennungen. Verbotene Spalten wie Vorname, Geburtsdatum oder Gehalt führen zur

Ablehnung der gesamten Datei, bevor etwas gespeichert wird. Datenminimierung ist hier Schema, nicht Richtlinie.

• Audit und Aufbewahrung: jeder Import wird mit Bediener, Datei, Zählständen und Ergebnis unveränderlich protokolliert; Zwischendaten werden nach erfolgreicher Übernahme gelöscht und verfallen spätestens nach sieben Tagen.

• Demo und Produktiv sauber getrennt: Beim ersten Start wählt die Organisation ausdrücklich zwischen Demo-Workspace (Beispieldaten „Aurora Industries“) und produktivem Workspace — produktive Workspaces starten leer, ohne Demo-Daten und ohne Aufräumarbeit.

Was das für Ihre Organisation bedeutet

Der Start wird leichter und der Blick wird breiter: Bestehende Organisationsdaten gelangen per kontrolliertem Import in GARION, statt manuell erfasst zu werden — pseudonym, geprüft und auditierbar. Und neben der KI-Kompetenz-Dokumentation nach der EU-KI-Verordnung beantwortet GARION nun auch die Cyber-Governance-Frage der Geschäftsführung: Welche Risiken sind offen, welche Maßnahmen laufen, welche Nachweise existieren, welche Fristen stehen an — auf einen Blick, lokal, ohne Cloud.

Alle genannten Funktionen sind lokal, lizenzgeschützt und zweisprachig (Deutsch/Englisch). Vollständige Leistungs- und Abgrenzungsübersichten stellen wir auf Anfrage bereit. Kontakt: office@garion-ai.de