Readiness-Checkliste für das europäische Trust Center

Eine Selbstbewertung mit Scoring: Wie gut erfüllt Ihr käuferseitiges Trust Center die europäischen Erwartungen? 58 Prüfpunkte in sechs Stakeholder-Bahnen — Sicherheitsteams, Rechtsteams, Compliance-Teams, Einkauf, Empfänger von Kundenupdates und KI-Agenten. Jeder Punkt wird mit Ja (2) / Teilweise (1) / Nein (0) bewertet und ergibt einen Readiness-Prozentwert sowie eines von drei Bändern.

Dieses PDF ist der Begleiter zum Ausdrucken und Prüfen. Die Arbeitsdatei ist das XLSX (Dropdowns zur Bewertung, automatische Punkteberechnung je Bahn und ein Auswertungsblatt); für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/european-trust-center-readiness-checklist verfügbar — ohne E-Mail-Adresse.

Rechtliche Anker: NIS2 — Richtlinie (EU) 2022/2555 (Art. 21(2)(d); Art. 23: 24 h / 72 h / 1 Monat) · DORA — Verordnung (EU) 2022/2554 (Art. 28–30), anwendbar seit dem 17. Januar 2025 · DSGVO — Verordnung (EU) 2016/679 (Art. 28, Art. 32, Art. 33–34). Diese Checkliste wird ohne Gewähr bereitgestellt und stellt keine Rechtsberatung dar.

Anleitung

Eine Selbstbewertung mit Scoring: Wie gut erfüllt Ihr käuferseitiges Trust Center die europäischen Erwartungen? 58 Prüfpunkte in sechs Stakeholder-Bahnen.

SO BEWERTEN SIE

1. Bewerten Sie von außen: Zählen Sie, was ein externer Prüfer im Trust Center tatsächlich findet (öffentliche und im Self-Service zugängliche Stufen), nicht was intern existiert.

2. Bewerten Sie jeden Prüfpunkt in der Spalte „Bewertung“: Ja = 2 Punkte (veröffentlicht, aktuell, vollständig, auf der richtigen Zugriffsstufe zugänglich); Teilweise = 1 Punkt (vorhanden, aber älter als 12 Monate, unvollständig, schwer auffindbar oder hinter einer Schranke, wo es öffentlich sein sollte); Nein = 0 Punkte (nicht vorhanden oder nicht auffindbar).

3. Die Spalte „Punkte“ und das Blatt „Auswertung“ berechnen die Punktzahl je Bahn, den Gesamtprozentwert und Ihr Readiness-Band automatisch.

READINESS-BÄNDER

Unter 40 % — Foundational: Das Trust Center ist eine Broschüre; Prüfer fallen auf E-Mail-mit-PDF zurück. Bringen Sie zuerst die beiden schwächsten Bahnen in Ordnung.

40–75 % — Developing: Kernnachweise existieren, aber mindestens zwei Bahnen sind unterversorgt; priorisieren Sie Rechtstransparenz und Update-Kanäle.

Über 75 % — Buyer-ready: Alle sechs Bahnen sind Self-Service; die Sicherheitsprüfung läuft parallel zum Deal. Halten Sie den Stand mit vierteljährlicher Neubewertung.

VERANTWORTLICHE JE BAHN (EMPFEHLUNG)

Bahn 1 Sicherheitsteams — Sicherheitsverantwortliche/r / CISO · Bahn 2 Rechtsteams — Recht / Datenschutzbeauftragte/r · Bahn 3 Compliance-Teams — Compliance- / GRC-Leitung · Bahn 4 Einkauf — Vertrieb / RevOps · Bahn 5 Kundenupdates — Customer Success · Bahn 6 KI-Agenten — Engineering / Web-Team. Eine koordinierende Person (meist CISO oder Compliance-Leitung) führt die Auswertung zusammen.

TURNUS

Durchlaufen Sie alle sechs Bahnen vierteljährlich. Bewerten Sie eine einzelne Bahn nach jeder wesentlichen Änderung neu: neues Zertifikat oder Audit, Wechsel eines Subprozessors, Vorfall, Preisänderung, Änderung eines Endpunkts. Subprozessorenlisten und Zertifikatsgültigkeit veralten am schnellsten — prüfen Sie sie monatlich.

RECHTLICHE ANKER

NIS2 — Richtlinie (EU) 2022/2555 (Art. 21(2)(d) Sicherheit der Lieferkette; Art. 23 Meldepflichten: 24 h / 72 h / 1 Monat) — https://eur-lex.europa.eu/eli/dir/2022/2555

DORA — Verordnung (EU) 2022/2554 (Art. 28–30 Risiko durch IKT-Drittparteien), anwendbar seit dem 17. Januar 2025 — https://eur-lex.europa.eu/eli/reg/2022/2554

DSGVO — Verordnung (EU) 2016/679 (Art. 28 Subprozessoren; Art. 32 Sicherheit; Art. 33–34 Meldung von Datenschutzverletzungen) — https://eur-lex.europa.eu/eli/reg/2016/679

Diese Checkliste wird ohne Gewähr bereitgestellt und stellt keine Rechtsberatung dar. Kostenlos nutz- und anpassbar innerhalb Ihrer Organisation.

Bahn 1 — Sicherheitsteams (11 Prüfpunkte, max. 22 Punkte)

Was ein Sicherheitsprüfer benötigt, um Ihre Kontrolllage ohne Gespräch zu bewerten.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
SEC-01	ISO-27001-Zertifikat veröffentlicht	Zertifikat sichtbar mit Zertifizierungsstelle, Geltungsbereichserklärung, Ausstellungs- und Ablaufdatum — nicht nur ein Logo	PDF oder Nachweiskarte: „ISO/IEC 27001:2022, ausgestellt von [Stelle], gültig bis 01.03.2027, Geltungsbereich: SaaS-Plattform und unterstützende Infrastruktur“	Ja / Teilw. / Nein
SEC-02	Erklärung zur Anwendbarkeit auf Anfrage verfügbar	SoA (oder Kontrollübersicht) über einen Self-Service-Zugang mit ausgewiesener Bearbeitungszeit zugänglich	„Erklärung zur Anwendbarkeit v4.2, 2026-01“ per NDA geschützt in der eingeschränkten Stufe	Ja / Teilw. / Nein
SEC-03	Managementzusammenfassung des Penetrationstests, letzte 12 Monate	Datierte Zusammenfassung mit Prüfunternehmen, Umfang, Methodik, Anzahl der Feststellungen nach Schweregrad und Behebungsstatus	„Externer Pentest durch [Firma], 2026-04; 0 kritisch, 2 hoch (behoben 2026-05)“	Ja / Teilw. / Nein
SEC-04	Lage beim Schwachstellenmanagement	Scan-Turnus, Patch-SLAs und Behebungsfristen für kritische/hohe Feststellungen ausgewiesen	„Wöchentliche Dependency- und Infrastruktur-Scans; kritische Schwachstellen gepatcht ≤ 72 h, hohe ≤ 14 Tage“	Ja / Teilw. / Nein
SEC-05	Verschlüsselungslage dokumentiert	Verschlüsselung im Ruhezustand und bei der Übertragung mit Algorithmen und Zusammenfassung des Schlüsselmanagements	„AES-256 im Ruhezustand, TLS 1.2+ bei der Übertragung, KMS-verwaltete Schlüssel jährlich rotiert“	Ja / Teilw. / Nein
SEC-06	Zusammenfassung des Zugriffsmanagements	Erzwingung von MFA/SSO, Least-Privilege-Modell und Joiner-Mover-Leaver-Prozess beschrieben	„SSO + erzwungene MFA für alle Beschäftigten; vierteljährliche Zugriffsüberprüfungen; RBAC“	Ja / Teilw. / Nein
SEC-07	Sicherer Entwicklungslebenszyklus beschrieben	Code Review, SAST/DAST, Dependency Scanning und Release-Kontrollen zusammengefasst	„Alle Änderungen im Peer Review; SAST + Dependency Scanning in der CI; gestufte Deployments“	Ja / Teilw. / Nein
SEC-08	Mandanten-/Netztrennung erläutert (mandantenfähiges SaaS)	Modell der logischen Trennung zwischen Kundenumgebungen beschrieben	„Mandantentrennung auf Zeilenebene; Verschlüsselungskontexte je Mandant; keine mandantenübergreifenden Abfragen“	Ja / Teilw. / Nein
SEC-09	Zusammenfassung zu Betriebskontinuität / Notfallwiederherstellung	Zusammenfassung des BC-/DR-Plans mit RTO-/RPO-Zielen und Datum des letzten Tests	„RTO 4 h / RPO 1 h; DR-Übung zuletzt durchgeführt 2026-02“	Ja / Teilw. / Nein
SEC-10	Überblick über die Sicherheitsarchitektur	Übergeordnete Architekturbeschreibung oder -grafik (öffentlich oder geschützt) mit Datenflüssen und Grenzen	Geschützter „Überblick über Architektur und Datenflüsse, v3, 2026-03“	Ja / Teilw. / Nein
SEC-11	Weg zur verantwortungsvollen Offenlegung	security.txt und/oder eine veröffentlichte Richtlinie zur Schwachstellenoffenlegung mit Kontakt	„/.well-known/security.txt mit security@-Kontakt und Offenlegungsrichtlinie“	Ja / Teilw. / Nein

Bahn 2 — Rechtsteams (10 Prüfpunkte, max. 20 Punkte)

Was Rechtsprüfer und Datenschutzbeauftragte prüfen, bevor ein AVV unterzeichnet wird. Anker: DSGVO Art. 28 und 32.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
LEG-01	AVV reibungslos verfügbar	Aktuelle AVV-Vorlage ohne Registrierung oder Vertriebsgespräch herunterladbar	„AVV v5.1 (2026-01), PDF, öffentlicher Download“	Ja / Teilw. / Nein
LEG-02	Öffentliche Subprozessorenliste	Jeder Subprozessor mit Name, Zweck, verarbeiteten Datenkategorien und Hosting-Standort aufgeführt — öffentlich, nicht per NDA geschützt (DSGVO Art. 28)	„AWS (eu-central-1, Frankfurt) — Infrastruktur-Hosting — Kundeninhalte“	Ja / Teilw. / Nein
LEG-03	Mechanismus zur Änderungsmitteilung bei Subprozessoren	Abonnierbarer Benachrichtigungskanal sowie ausgewiesene vertragliche Mitteilungsfrist (typischerweise ca. 15 Tage; in größeren Deals 30–60 Tage verhandelt)	„Subprozessor-Updates abonnieren; AVV §9 gewährt eine Mitteilungs- und Widerspruchsfrist“	Ja / Teilw. / Nein
LEG-04	Mechanismen für internationale Datenübermittlungen dokumentiert	Standardvertragsklauseln / Angemessenheitsbeschluss je Übermittlung benannt; Transfer-Folgenabschätzung auf Anfrage verfügbar	„Übermittlungen an [Anbieter] auf Basis der SCC (2021/914 Modul 2) + TIA unter NDA verfügbar“	Ja / Teilw. / Nein
LEG-05	Zusagen zum Datenstandort in Schriftform	Wo Kundendaten (sowie Metadaten/Backups) je Dienst gespeichert werden, als schriftliche Zusage	„Kundeninhalte werden ausschließlich in EU-Regionen gespeichert und verarbeitet; Backups in derselben Region“	Ja / Teilw. / Nein
LEG-06	Rechtsraum des Anbieters offengelegt	Betreibende Rechtseinheit, Gründungsort und Exposition gegenüber Herausgabeanordnungen außerhalb der EU (z. B. US CLOUD Act) ausgewiesen	„Betrieben von [Einheit] GmbH mit Sitz in Deutschland; keine US-Muttergesellschaft“	Ja / Teilw. / Nein
LEG-07	Self-Service-NDA-Flow für geschützte Dokumente	Ein NDA per Klick-Unterschrift mit Audit-Trail gibt eingeschränkte Dokumente in Minuten frei, nicht in Tagen	„Zugang anfragen → NDA im Browser unterzeichnen → Dokument freigeschaltet; Unterschrift protokolliert“	Ja / Teilw. / Nein
LEG-08	Aufbewahrungs- und Löschbedingungen veröffentlicht	Was bei Vertragsende mit den Kundendaten geschieht, mit Fristen	„Kundendaten werden innerhalb von 30 Tagen nach Vertragsende gelöscht; Löschbescheinigung auf Anfrage“	Ja / Teilw. / Nein
LEG-09	Zusammenfassung der technischen und organisatorischen Maßnahmen (TOM)	Maßnahmen nach DSGVO Art. 32 als strukturierte Zusammenfassung veröffentlicht und im AVV referenziert	„TOM-Anlage v3 (2026-02): Zugriffskontrolle, Verschlüsselung, Resilienz, Testturnus“	Ja / Teilw. / Nein
LEG-10	Offenlegung zur KI-Datennutzung	Ob Kundendaten KI-Modelle trainieren; welche KI-Subprozessoren Zugriff haben; Weg zum Opt-out	„Kundendaten werden nicht zum Training von Modellen genutzt; KI-Subprozessoren: [Liste], in der EU gehostet“	Ja / Teilw. / Nein

Bahn 3 — Compliance-Teams (11 Prüfpunkte, max. 22 Punkte)

Was GRC-Prüfer bei regulierten Kunden für ihre eigenen NIS2-/DORA-/DSGVO-Akten benötigen.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
COM-01	Frameworks mit Geltungsbereich und Daten dargestellt	Jede Zertifizierung/Attestierung zeigt Geltungsbereich, ausstellende Stelle, Auditdatum und Gültigkeit — keine Logoleiste	„ISO 27001 (gültig bis 2027-03), ISO 27701 (gültig bis 2027-03), Geltungsbereichserklärungen verlinkt“	Ja / Teilw. / Nein
COM-02	NIS2-Lage gemappt	Sicherheitsmaßnahmen den Kategorien nach NIS2 Art. 21(2) zugeordnet, damit wesentliche/wichtige Kunden sie in ihrer eigenen Lieferkettenakte referenzieren können	„NIS2-Readiness-Seite: Art. 21(2)(a)–(j) auf Kontrollen und Nachweise gemappt“	Ja / Teilw. / Nein
COM-03	Zusage zur Vorfallskommunikation im Einklang mit den NIS2-Fristen	Zusage, betroffene Kunden so rechtzeitig zu benachrichtigen, dass diese ihre Meldepflichten von 24 h / 72 h / 1 Monat erfüllen können (NIS2 Art. 23)	„Wir benachrichtigen betroffene Kunden unverzüglich, damit sie die Fristen nach Art. 23 einhalten können“	Ja / Teilw. / Nein
COM-04	DORA-Datenpunkte zu IKT-Drittparteien verfügbar	Die vertraglichen und operativen Datenpunkte, die Finanzunternehmen nach DORA Art. 28–30 benötigen (Leistungsbeschreibung, Datenstandorte, Unterauftragnehmer, Ausstiegsunterstützung), sind bereitgestellt	„DORA-Informationsblatt: Felder des Informationsregisters für Kunden vorbefüllt“	Ja / Teilw. / Nein
COM-05	Zertifikatsverlängerungen laufen nie stillschweigend aus	Verlängerungs-/Ablaufdaten sichtbar; erneuerte Nachweise werden vor Ablauf veröffentlicht	„Zertifikatskarte zeigt das Datum „gültig bis“; Verlängerung wird 2 Wochen vor Ablauf veröffentlicht“	Ja / Teilw. / Nein
COM-06	Nachweise nach Framework und Kontrolle gegliedert	Navigierbare Struktur (Framework → Maßnahme → Nachweis), kein flacher PDF-Ordner	„Navigation nach ISO 27001 / NIS2 / DORA / DSGVO; jede Kontrolle verlinkt ihre Nachweise“	Ja / Teilw. / Nein
COM-07	Jedes Dokument versioniert und datiert	Versionsnummer und Datum der letzten Aktualisierung bei jedem Nachweis	„Informationssicherheitsrichtlinie v6.0 — aktualisiert am 14.05.2026“	Ja / Teilw. / Nein
COM-08	Zugangsweg zu Auditberichten ausgewiesen	Wie Kunden Auditberichte Dritter erhalten (unter NDA) und ob Prüfrechte unterstützt werden	„ISO-Auditbericht unter NDA verfügbar; Prüfrechtsklausel für regulierte Kunden unterstützt“	Ja / Teilw. / Nein
COM-09	Schwachstellenbehandlung & Advisories (CRA-bewusst)	Für Produkte mit digitalen Elementen: dokumentierte Schwachstellenbehandlung und ein Kanal für Sicherheitshinweise	„Advisory-Seite mit CVE-Historie und Prozess der koordinierten Offenlegung“	Ja / Teilw. / Nein
COM-10	Erklärung zu Ausstieg und Datenportabilität	Datenexportformate, Übergangsunterstützung und Unterstützung bei Vertragsende beschrieben (unterstützt die DORA-Anforderungen an Ausstiegsstrategien)	„Vollexport in offenen Formaten binnen 30 Tagen; Klausel zur Übergangsunterstützung verfügbar“	Ja / Teilw. / Nein
COM-11	Framework-übergreifende Nachweisnutzung	Derselbe Kontrollnachweis wird einmal auf NIS2, DORA und DSGVO gemappt statt drei paralleler Antwortsätze	„Verschlüsselungskontrolle referenziert von ISO A.8.24, NIS2 Art. 21(2)(h), DORA, DSGVO Art. 32“	Ja / Teilw. / Nein

Bahn 4 — Einkauf (9 Prüfpunkte, max. 18 Punkte)

Was der Einkauf benötigt, um das Lieferanten-Onboarding ohne Discovery-Call abzuschließen.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
PRO-01	Veröffentlichte, transparente Preise	Preise (oder mindestens Preismodell und Stufen) öffentlich — keine „Vertrieb kontaktieren“-Schranke	„Preisseite mit Funktionen je Stufe und Jahres-/Monatspreisen“	Ja / Teilw. / Nein
PRO-02	Lieferantenprofil	Unternehmensdaten an einem Ort: Rechtseinheit, Registernummer, Hauptsitz, Eigentümerstruktur, wichtige Kontakte	„Lieferantenprofil: [Einheit], HRB [Nummer], Berlin; Kontakte für Sicherheit und Datenschutz“	Ja / Teilw. / Nein
PRO-03	Nachweis der Cyberversicherung	Cyber-Haftpflichtversicherung mit Deckungshöhe bestätigt (Nachweis auf Anfrage)	„Cyberversicherung: 5 Mio. € Deckung; Nachweis unter NDA verfügbar“	Ja / Teilw. / Nein
PRO-04	Verfügbarkeits- und Uptime-Historie	Öffentliche Statusseite und historische Uptime-Kennzahlen	„status.[unternehmen].com — Uptime über 12 Monate 99,97 %“	Ja / Teilw. / Nein
PRO-05	Signale zur Betriebskontinuität	Für den Einkauf relevante Kontinuitätsnachweise: Escrow, Nachfolge, Finanzierungs-/Bestandssignale, soweit angebracht	„BC-Zusammenfassung + kundengerichtete Kontinuitätszusagen“	Ja / Teilw. / Nein
PRO-06	Support- und Eskalationsmodell	Supportstufen, Reaktions-SLAs und ein Eskalationspfad dokumentiert	„Support-SLA: P1-Reaktion ≤ 1 h; benannter Eskalationsweg“	Ja / Teilw. / Nein
PRO-07	Bedingungen für On-/Offboarding und Datenausleitung	Was das Onboarding erfordert und was das Offboarding zurückgibt, einschließlich etwaiger Egress-Kosten	„Keine Egress-Gebühren; Export-Werkzeuge im Self-Service; Offboarding-Checkliste veröffentlicht“	Ja / Teilw. / Nein
PRO-08	Bearbeitungszeit für Dokumentenanfragen ausgewiesen	Ein ausgewiesenes SLA für die Bearbeitung von Dokumentenanfragen im Rahmen der Due Diligence	„Geschützte Dokumente werden ≤ 1 Arbeitstag nach dem NDA freigegeben“	Ja / Teilw. / Nein
PRO-09	Wesentliche Abhängigkeiten offengelegt	Wesentliche Vierte Parteien / Konzentrationsabhängigkeiten benannt (Cloud-Anbieter, kritische Lieferanten)	„Kritische Abhängigkeiten: AWS eu-central-1; [Zahlungsanbieter]; [Authentifizierungsanbieter]“	Ja / Teilw. / Nein

Bahn 5 — Empfänger von Kundenupdates (8 Prüfpunkte, max. 16 Punkte)

Ob Bestandskunden über einen strukturierten Kanal von Änderungen erfahren — und nicht per Überraschungs-E-Mail.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
UPD-01	Abonnierbare Trust Updates	Kunden können Sicherheits-/Compliance-Updates des Trust Centers abonnieren	„Abonnieren-Schaltfläche; Updates per E-Mail mit Archivseite“	Ja / Teilw. / Nein
UPD-02	Strukturierte Vorfallsmitteilungen	Vorfallskommunikation wird über das Trust Center mit Schweregrad, Auswirkung und Status veröffentlicht — keine improvisierten E-Mail-Verläufe	„Vorfallsmitteilung 2026-03: Schweregrad, betroffene Dienste, Zeitleiste, aktueller Status“	Ja / Teilw. / Nein
UPD-03	Subprozessor-Änderungsmitteilungen mit Widerspruchsfrist	Änderungen werden vor Beauftragung angekündigt, mit Verweis auf den Mitteilungs- und Widerspruchsmechanismus des AVV	„Mitteilung 2026-05: Aufnahme von [Anbieter] als Subprozessor, wirksam ab [Datum]; Widerspruchsweg gemäß AVV“	Ja / Teilw. / Nein
UPD-04	Ankündigungen zum Zertifizierungslebenszyklus	Verlängerungen, Änderungen des Geltungsbereichs und neue Zertifizierungen werden angekündigt	„Update: ISO 27001 rezertifiziert 2026-03, Geltungsbereich unverändert“	Ja / Teilw. / Nein
UPD-05	Sicherheitshinweise / CVE-Feed	Advisories zu Produktschwachstellen werden über einen eigenen, verlinkbaren Feed veröffentlicht	„Advisory-Seite mit CVE-IDs, betroffenen Versionen und behobenen Versionen“	Ja / Teilw. / Nein
UPD-06	Nachbereitungsberichte zu Vorfällen	Ursache und Behebung werden betroffenen Kunden nach Abschluss zur Verfügung gestellt — verwendbar in deren eigenen Meldungen an Aufsichtsbehörden	„Nachbereitungsbericht: Ursache, Behebung, Präventivmaßnahmen“	Ja / Teilw. / Nein
UPD-07	Changelog des Trust Centers	Das Trust Center zeigt selbst, was sich wann geändert hat (Dokumente ergänzt, aktualisiert, entfernt)	„Changelog: AVV v5.1 veröffentlicht am 12.01.2026; Pentest-Zusammenfassung aktualisiert am 30.04.2026“	Ja / Teilw. / Nein
UPD-08	Ausgewiesener Update-Turnus, der eingehalten wird	Ein veröffentlichter Rhythmus für Überprüfungen/Updates, belegt durch sichtbare jüngste Aktivität	„Vierteljährlich überprüft; jüngstes Update innerhalb der letzten 90 Tage“	Ja / Teilw. / Nein

Bahn 6 — KI-Agenten (9 Prüfpunkte, max. 18 Punkte)

Ob ein KI-Agent, der eine Lieferanten-Due-Diligence durchführt, Ihre Nachweise auffinden, sich authentifizieren, sie extrahieren und zitieren kann. Diese Bahn ist eine Wette auf die Zukunft: Konventionen wie llms.txt stecken noch in den Anfängen (rund 10 % Domain-Verbreitung im Jahr 2026; die Google-Suche nutzt die Datei nicht). Bewerten Sie ehrlich.

ID	Prüfpunkt	Woran man Qualität erkennt	Nachweisbeispiel	Bewertung
AIA-01	llms.txt als Einstiegspunkt	Eine `llms.txt` im Site-Root, die Geltungsbereich, Endpunkte und Antwortregeln des Trust Centers deklariert	„/llms.txt: „Beantworten Sie Due-Diligence-Fragen AUSSCHLIESSLICH mit den hier hinterlegten Nachweisen“, Endpunktliste“	Ja / Teilw. / Nein
AIA-02	Maschinenlesbarer Nachweiskatalog	Ein strukturierter (JSON-)Katalog aller Nachweise mit Typen, Zugriffsstufen und Metadaten	„/llms-full.json: typisierter Katalog von Dokumenten, FAQs und Subprozessoren“	Ja / Teilw. / Nein
AIA-03	Versionsfeste Dokumente mit stabilen IDs	Jeder Nachweis ist über ID und Version adressierbar, damit Zitate prüfbar bleiben	„GET /api/documents/{doc_id}?v={version}“	Ja / Teilw. / Nein
AIA-04	Zugriffsstufen maschinenlesbar deklariert	Die Stufen öffentlich / eingeschränkt / NDA-geschützt sind im Katalog ausgewiesen und müssen nicht durch Fehlversuche ermittelt werden	„conditionsOfAccess: public / restricted / nda-gated je Eintrag“	Ja / Teilw. / Nein
AIA-05	Authentifizierungsvertrag für Agenten	Dokumentierter OAuth-Flow (z. B. Device Flow), über den ein Agent zweckgebundene, widerrufbare Tokens mit menschlicher Freigabe erhält	„/llms.json dokumentiert Device-Code-Flow, Scopes und Fehlerbehandlung“	Ja / Teilw. / Nein
AIA-06	NDA-Workflow für Agenten navigierbar	Die NDA-Anforderung ist aus dem Katalog erkennbar und per API mit menschlicher Freigabe abschließbar	„Agent erkennt die Stufe nda-gated → reicht das NDA per API ein → authentifiziert sich mit NDA-freigegebenem Scope neu“	Ja / Teilw. / Nein
AIA-07	Extrahierbare, semantische Inhalte	Nachweise ohne JavaScript-Ausführung lesbar: semantisches HTML/Markdown, echter Text (keine reinen Bildzertifikate), stabile Anker	„Die Subprozessorenliste ist eine HTML-Tabelle, kein Screenshot; Überschriften sind echte h2/h3“	Ja / Teilw. / Nein
AIA-08	Ausgabe-/Zitationsvertrag veröffentlicht	Vorgegebenes Antwortformat, das Agenten verpflichtet, Dokument-ID + Version zu zitieren und „unzureichend“ zurückzugeben, wenn Nachweise fehlen	„Antwortvertrag in der llms.txt: Jede Aussage zitiert Dokument-ID + Version“	Ja / Teilw. / Nein
AIA-09	Aktualitäts-Metadaten an den Nachweisen	Metadaten dateModified / ETag / zuletzt überprüft, damit Agenten Nachweise nach Aktualität gewichten können	„Katalogeinträge tragen dateModified; HTTP-Antworten senden ETags“	Ja / Teilw. / Nein

Auswertung

Bahn	Prüfpunkte	Maximalpunkte	Ihre Punkte	% der Bahn
1. Sicherheitsteams	11	22		
2. Rechtsteams	10	20		
3. Compliance-Teams	11	22		
4. Einkauf	9	18		
5. Kundenupdates	8	16		
6. KI-Agenten	9	18		
GESAMT	58	116		

Readiness-Band: Gesamtpunkte ÷ 116 → < 40 % Foundational · 40–75 % Developing · > 75 % Buyer-ready.

Nach der Bewertung: Notieren Sie die beiden schwächsten Bahnen, überführen Sie jedes „Nein“ in diesen Bahnen in ein Ticket mit Verantwortlichem und Datum und bewerten Sie die Bahnen neu, sobald die Korrekturen umgesetzt sind. Wiederholen Sie die vollständige Bewertung vierteljährlich.