

B2B Trust Readiness Navigator

50 Käuferfragen → Unsicherheiten erkennen → 3 nächste Schritte

ORIENTIERUNG • MARKIEREN • RED FLAGS • HANDELN

Sie brauchen heute keine 50 perfekten Antworten.

Sie brauchen Sichtbarkeit: Was ist belastbar, was nur vermutet, was offen — und welche drei Schritte reduzieren das größte Käufer- und Vertrauensrisiko?

20-Minuten-Schnellscan plus Validierung

1 • Schnellscan (20 Min.)

Alle 50 Fragen nur mit B, T, O oder N/A markieren. Noch nicht recherchieren; Notizen nur bei Red Flags.

2 • Validierung (60–120 Min.)

Die drei wichtigsten Lücken mit den zuständigen Rollen prüfen. Aussagen, Verträge, Einstellungen und Nachweise erst jetzt verifizieren.

3 • Handeln

Genau drei nächste Schritte mit verantwortlicher Rolle, Termin, Abnahmekriterium und erwartetem Nachweis festlegen.

Kein Audit, keine Zertifizierung, keine Rechtsberatung und keine Compliance-Garantie. Antworten müssen zu Ihrem realen Produkt und Vertrag passen.

Ihre Orientierungslogik

Status ist keine Schulnote

B — beantwortbar

Konkrete Aussage + aktuelle Basis + Owner.

T — teilweise

Teile stimmen, aber Scope, Beleg oder Freigabe fehlt.

O — offen

Nicht raten. Als Unsicherheit mit nächstem Schritt führen.

N/A

Nur mit kurzer Begründung; bei Produktänderung erneut prüfen.

RED FLAG ≠ VERSAGEN. RED FLAG = KEINE EXTERNE AUSSAGE OHNE KLÄRUNG.

Sofort priorisieren: unbekannter AI-/Datenempfänger; Support/Adminzugriff ohne Begrenzung; Löschversprechen ohne Backup-/Log-Ausnahme; „compliant“, „secure“, „EU-only“ ohne passende Basis; kritischer Provider ohne Ausfallweg.

1. Datenflüsse & Verarbeitung

Warum Käufer fragt	Datenumfang, Zweck und Wege bestimmen Risiko, Vertragsbedarf und Prüfaufwand.
Benötigte Basis	Produkt-/Dateninventar, Architektur, Provider, Umgebungen.
Belastbare Antwort	Zweck + Datenart + System/Ort + Empfänger + Löschung; aktuell und belegbar.
Gefährliche Abkürzung	Nur die Hauptdatenbank nennen; Support, Logs, Backups oder Al-Pfade auslassen.
Späterer Nutzen	Grundlage für Datenflussbild, DPA, Lösch- und Subprocessor-Aussagen.

Fragen markieren

#	Käuferfrage	Status	Notiz
1	Welche Kundendaten verarbeitet Ihr Produkt tatsächlich — und wofür?	☐ B ☐ T ☐ O ☐ N/A	_____
2	Welche Daten sind zwingend erforderlich, welche optional?	☐ B ☐ T ☐ O ☐ N/A	_____
3	Wo entstehen, speichern oder verändern sich personenbezogene Daten?	☐ B ☐ T ☐ O ☐ N/A	_____
4	Welche Daten verlassen die EU oder den EWR?	☐ B ☐ T ☐ O ☐ N/A	_____
5	Gibt es Test-, Demo- oder Supportzugriffe auf echte Kundendaten?	☐ B ☐ T ☐ O ☐ N/A	_____
6	Wie dokumentieren Sie die wichtigsten Datenflüsse für Käufer, Datenschutz und Security Review?	☐ B ☐ T ☐ O ☐ N/A	_____

2. AI-/LLM-Nutzung & Transparenz

Warum Käufer fragt	AI verändert Datenweitergabe, Fehlerbild und Verantwortlichkeit.
Benötigte Basis	Feature-Liste, Modell/Provider, Prompt-Kontext, Training/Retention, Human Gates.
Belastbare Antwort	Pro Feature: Daten hinein, Provider, Ergebnis, Kontrolle, Grenze und Fallback.
Gefährliche Abkürzung	„Wir nutzen AI sicher“ ohne Providerbedingungen oder reale Kontrollpunkte.
Späterer Nutzen	Grundlage für AI Disclosure und sichere Produkt-/Marketingclaims.

Fragen markieren

#	Käuferfrage	Status	Notiz
7	Welche AI-/LLM-Funktionen sind Bestandteil des Produkts?	☐ B ☐ T ☐ O ☐ N/A	_____
8	Welche Kundendaten werden an AI-/LLM-Anbieter übermittelt?	☐ B ☐ T ☐ O ☐ N/A	_____
9	Werden Prompts, Dateien, Antworten oder Nutzungsdaten zum Training verwendet?	☐ B ☐ T ☐ O ☐ N/A	_____
10	Wie erklären Sie Käufern den Unterschied zwischen AI-Funktion, Automatisierung und menschlicher Prüfung?	☐ B ☐ T ☐ O ☐ N/A	_____
11	Welche menschlichen Freigaben oder Kontrollpunkte gibt es bei riskanten AI-Ausgaben?	☐ B ☐ T ☐ O ☐ N/A	_____
12	Wie gehen Sie mit Halluzinationen, fehlerhaften Empfehlungen und unsicheren Ergebnissen um?	☐ B ☐ T ☐ O ☐ N/A	_____

3. Zugriff, Rollen & Berechtigungen

Warum Käufer fragt	Unklare Rechte und privilegierte Zugriffe erhöhen Missbrauchs- und Insider-Risiko.
Benötigte Basis	Rollenmodell, IAM-Konfiguration, Joiner/Mover/Leaver- und Supportprozess.
Belastbare Antwort	Rollen, Rechte, Genehmigung, MFA, Review, Logging und Entzug stimmen überein.
Gefährliche Abkürzung	„Nur das Kernteam hat Zugriff“ als Ersatz für technische Begrenzung.
Späterer Nutzen	Grundlage für Zugriffsmatrix, Supportbeschreibung und Käuferfragebogen.

Fragen markieren

#	Käuferfrage	Status	Notiz
13	Welche Rollen und Berechtigungen gibt es im Produkt?	☐ B ☐ T ☐ O ☐ N/A	_____
14	Kann ein Kunde nachvollziehen, wer Zugriff auf welche Daten hat?	☐ B ☐ T ☐ O ☐ N/A	_____
15	Wie wird privilegierter Adminzugriff kontrolliert?	☐ B ☐ T ☐ O ☐ N/A	_____
16	Gibt es MFA für Administrations- und Kundenkonten?	☐ B ☐ T ☐ O ☐ N/A	_____
17	Wie werden ausgeschiedene Mitarbeiter oder Dienstleister aus Systemen entfernt?	☐ B ☐ T ☐ O ☐ N/A	_____
18	Wie wird Supportzugriff begrenzt und protokolliert?	☐ B ☐ T ☐ O ☐ N/A	_____

4. Logging, Nachvollziehbarkeit & Betrieb

Warum Käufer fragt	Ohne Logs und Betriebsweg sind Vorfälle und Zusagen nicht nachvollziehbar.
Benötigte Basis	Logquellen, Aufbewahrung, Alerting, Incidentweg, Status-/SLA-Daten.
Belastbare Antwort	Ereignis, Quelle, Zugriff, Frist, Alarmierung und Verantwortlicher sind benannt.
Gefährliche Abkürzung	Mehr Logging versprechen als ausgewertet oder geschützt werden kann.
Späterer Nutzen	Grundlage für Incident-, Monitoring- und Betriebsantworten.

Fragen markieren

#	Käuferfrage	Status	Notiz
19	Welche sicherheitsrelevanten Ereignisse werden geloggt?	☐ B ☐ T ☐ O ☐ N/A	_____
20	Wie lange werden Logs aufbewahrt?	☐ B ☐ T ☐ O ☐ N/A	_____
21	Können Kunden eigene Aktivitäten oder Exporte nachvollziehen?	☐ B ☐ T ☐ O ☐ N/A	_____
22	Wie erkennen Sie Missbrauch, ungewöhnliche Nutzung oder Datenabfluss?	☐ B ☐ T ☐ O ☐ N/A	_____
23	Wie werden Incidents intern dokumentiert und priorisiert?	☐ B ☐ T ☐ O ☐ N/A	_____
24	Welche Betriebskennzahlen oder Statusinformationen können Käufer erwarten?	☐ B ☐ T ☐ O ☐ N/A	_____

5. Subprocessor, Hosting & Lieferkette

Warum Käufer fragt	Dritte bestimmen Standort, Verfügbarkeit, Datenschutz und Konzentrationsrisiko.
Benötigte Basis	Aktuelle Providerliste, Zwecke, Regionen, Verträge, Evidence, Wechselprozess.
Belastbare Antwort	Jeder Provider mit Zweck, Daten, Ort, Kritikalität, Nachweis und Änderungsweg.
Gefährliche Abkürzung	Nur Cloud-Hosting nennen; AI, E-Mail, Analytics und Supporttools vergessen.
Späterer Nutzen	Grundlage für Subprocessor-Liste, Due Diligence und Exit-Prioritäten.

Fragen markieren

#	Käuferfrage	Status	Notiz
25	Welche Unterauftragsverarbeiter setzen Sie ein?	☐ B ☐ T ☐ O ☐ N/A	_____
26	Für welchen Zweck wird jeder Subprocessor genutzt?	☐ B ☐ T ☐ O ☐ N/A	_____
27	Wo befinden sich Hosting, Backups, Logging und AI-Verarbeitung?	☐ B ☐ T ☐ O ☐ N/A	_____
28	Welche AVV-/DPA- oder Sicherheitsnachweise liegen von wichtigen Providern vor?	☐ B ☐ T ☐ O ☐ N/A	_____
29	Wie informieren Sie Kunden über neue oder geänderte Subprocessor?	☐ B ☐ T ☐ O ☐ N/A	_____
30	Welche Provider wären kritisch, wenn sie ausfallen oder kompromittiert werden?	☐ B ☐ T ☐ O ☐ N/A	_____

6. Löschung, Retention & Datenportabilität

Warum Käufer fragt	Kunden müssen wissen, was exportiert, gelöscht oder rechtmäßig behalten wird.
Benötigte Basis	Datenklassen, Systeme, Fristen, Backupzyklen, Export-/Löschtests.
Belastbare Antwort	Frist und Ausnahme je Datenklasse; Owner, Ablauf und Nachweis sind praktisch prüfbar.
Gefährliche Abkürzung	„Alles wird sofort gelöscht“ trotz Backups, Logs oder Aufbewahrungspflichten.
Späterer Nutzen	Grundlage für Offboarding, Retention Schedule und belastbare DPA-Antworten.

Fragen markieren

#	Käuferfrage	Status	Notiz
31	Wie kann ein Kunde seine Daten exportieren?	☐ B ☐ T ☐ O ☐ N/A	_____
32	Wie funktioniert die Löschung nach Vertragsende?	☐ B ☐ T ☐ O ☐ N/A	_____
33	Welche Daten bleiben in Backups, Logs oder Abrechnungssystemen erhalten?	☐ B ☐ T ☐ O ☐ N/A	_____
34	Welche Retention-Fristen gelten für Produktdaten, Supportdaten, Logs und AI-Kontext?	☐ B ☐ T ☐ O ☐ N/A	_____
35	Wie wird Löschung technisch und organisatorisch nachgewiesen?	☐ B ☐ T ☐ O ☐ N/A	_____
36	Gibt es klare Verantwortlichkeiten für Löschanfragen?	☐ B ☐ T ☐ O ☐ N/A	_____

7. Security Baseline & technische Maßnahmen

Warum Käufer fragt	Käufer suchen eine glaubwürdige Mindestbasis, nicht Zertifikatsrhetorik.
Benötigte Basis	Konfiguration, Backup-/Restore-Test, Secrets, Patch- und Vulnerability-Prozess.
Belastbare Antwort	Implementiert + Verantwortlicher + Frequenz + letzter Nachweis + bekannte Grenze.
Gefährliche Abkürzung	Toolnamen oder geplante Maßnahmen als wirksame Kontrolle darstellen.
Späterer Nutzen	Grundlage für Security Overview und priorisierte technische Verbesserungen.

Fragen markieren

#	Käuferfrage	Status	Notiz
37	Wie werden Daten bei Übertragung und Speicherung geschützt?	☐ B ☐ T ☐ O ☐ N/A	_____
38	Welche Backup- und Restore-Verfahren existieren?	☐ B ☐ T ☐ O ☐ N/A	_____
39	Wie werden Secrets, API-Keys und Zugangsdaten verwaltet?	☐ B ☐ T ☐ O ☐ N/A	_____
40	Wie werden Abhängigkeiten, Libraries und Schwachstellen überwacht?	☐ B ☐ T ☐ O ☐ N/A	_____
41	Gibt es einen Prozess für Security Updates und kritische Patches?	☐ B ☐ T ☐ O ☐ N/A	_____
42	Welche Mindestmaßnahmen können Sie heute glaubwürdig beschreiben — ohne mehr zu versprechen als umgesetzt ist?	☐ B ☐ T ☐ O ☐ N/A	_____

8. Käuferfragen, Claims & nächste Schritte

Warum Käufer fragt	Widersprüchliche Claims verzögern Sales und erhöhen Haftungs-/Vertrauensrisiko.
Benötigte Basis	Aktuelle Antworten, Claims, vorhandene Dokumente, Deal-Termine und Owner.
Belastbare Antwort	Offenheit wird priorisiert; jede externe Aussage hat Basis, Owner und Freigabestatus.
Gefährliche Abkürzung	Lücken verstecken oder mit „compliant/secure“ überdecken.
Späterer Nutzen	Grundlage für 3 nächste Schritte, sichere Sales-Antworten und Upgrade-Entscheidung.

Fragen markieren

#	Käuferfrage	Status	Notiz
43	Welche Security-Fragen eines B2B-Käufers können Sie heute sicher beantworten?	☐ B ☐ T ☐ O ☐ N/A	_____
44	Welche Fragen müssen Sie ehrlich als offen markieren?	☐ B ☐ T ☐ O ☐ N/A	_____
45	Welche Marketingclaims könnten zu weit gehen?	☐ B ☐ T ☐ O ☐ N/A	_____
46	Welche Unterlagen fehlen für einen ersten Procurement- oder Datenschutz-Review?	☐ B ☐ T ☐ O ☐ N/A	_____
47	Welche drei Lücken sollten vor dem nächsten Käufergespräch geschlossen oder mit einer klaren Zwischenantwort versehen werden?	☐ B ☐ T ☐ O ☐ N/A	_____
48	Welcher nächste Trust-Schritt schafft den größten Verkaufsvorteil bei geringstem Risiko?	☐ B ☐ T ☐ O ☐ N/A	_____
49	Welche Aussage würden Sie einem Enterprise-Käufer schriftlich geben — und welche lieber nicht?	☐ B ☐ T ☐ O ☐ N/A	_____
50	Welche Trust-Materialien sollten vor dem nächsten größeren Sales-Gespräch fertig sein?	☐ B ☐ T ☐ O ☐ N/A	_____

Action Sheet — nächste Schritte

In 15 Minuten von offenen Fragen zu drei machbaren Schritten

Auslöser / nächstes Käufergespräch

Zählfeld B / T / O / N/A

Wichtigstes Muster aus dem Scan

Größte Unsicherheit

Aussage, die wir bis zur Klärung nicht verwenden

Top 3 nächste Schritte

NÄCHSTER SCHRITT 1

Unsicherheit / Red Flag

Warum relevant

Nächste Aktion

Verantwortliche Rolle

Termin

Abnahmekriterium

Ablage / Nachweis

NÄCHSTER SCHRITT 2

Unsicherheit / Red Flag

Warum relevant

Nächste Aktion

Verantwortliche Rolle

Termin

Abnahmekriterium

Ablage / Nachweis

NÄCHSTER SCHRITT 3

Unsicherheit / Red Flag

Warum relevant

Nächste Aktion

Verantwortliche Rolle

Termin

Abnahmekriterium

Ablage / Nachweis

Entscheidungsregel

STOP: Externe Aussage aussetzen, wenn Datenweg, Providerbedingung oder Kontrollnachweis unbekannt ist. CAUTION: offen kennzeichnen und Termin/Owner setzen. GO: nur konkret, aktuell und belegbar antworten.

Review-Termin: _____ Entscheider/Freigabe: _____ Käuferantwort aktualisiert am: _____

Ausgefülltes fiktives Beispiel — CloudKite AI

FIKTIV — kein reales Unternehmen

Auslöser / nächstes Käufergespräch	Vendor Review mit MedicoWorks, 30.07.2026
Zählfeld B / T / O / N/A	18 / 17 / 13 / 2
Wichtigstes Muster aus dem Scan	Datenflüsse zu LLM-Provider und Supportzugriff sind nicht zusammengeführt.
Größte Unsicherheit	Ob Prompt-/Output-Retention beim aktuellen Providervertrag deaktiviert ist.
Aussage, die wir bis zur Klärung nicht verwenden	„EU-only processing“

Top 3 nächste Schritte

NÄCHSTER SCHRITT 1

Unsicherheit / Red Flag	AI-Retention im aktuellen Providervertrag unklar
Warum relevant	Eine falsche Aussage zur Nutzung von Prompts kann den Vendor Review stoppen.
Nächste Aktion	DPA und Adminsetting gemeinsam prüfen; freigabefähige Aussage formulieren.
Verantwortliche Rolle	Mira / CTO
Termin	17.07.2026
Abnahmekriterium	Aussage durch CTO geprüft und im Antwortbestand aktualisiert.
Ablage / Nachweis	DPA v3.2 + datierter Screenshot des Adminsettings.

NÄCHSTER SCHRITT 2

Unsicherheit / Red Flag	Supportzugriff nicht durchgängig protokolliert
Warum relevant	Unbelegter privilegierter Zugriff ist ein konkreter Käufer- und Incident-Risikopunkt.
Nächste Aktion	JIT-Zugriff mit Ticket-ID in Staging testen und Arbeitsanweisung ergänzen.
Verantwortliche Rolle	Jonas / Engineering
Termin	22.07.2026
Abnahmekriterium	Test erfolgreich; Ticket-, Freigabe- und Logkette nachvollziehbar.
Ablage / Nachweis	TEST-LOG-014 + Arbeitsanweisung SUP-02 v0.3.

NÄCHSTER SCHRITT 3		
Unsicherheit / Red Flag		Löschung in Backups nicht erklärt
Warum relevant		Ein pauschales Löschversprechen wäre ohne Backup-Ausnahme nicht belastbar.
Nächste Aktion		Backupzyklen und Ausnahmen dokumentieren; Käuferantwort begrenzen.
Verantwortliche Rolle		Mira / CTO
Termin		24.07.2026
Abnahmekriterium		Retention-Antwort freigegeben und in DPA-FAQ übernommen.
Ablage / Nachweis		Retention-Tabelle v0.1 + Reviewnotiz 2026-07-24.

Entscheidungsregel

STOP: Externe Aussage aussetzen, wenn Datenweg, Providerbedingung oder Kontrollnachweis unbekannt ist. CAUTION: offen kennzeichnen und Termin/Owner setzen. GO: nur konkret, aktuell und belegbar antworten.

Ergebnis nach 30 Tagen: AI-Disclosure v0.1, protokollierter Supportzugriff und belastbare Retention-Antwort; kein Compliance-Claim.

Wenn Sie weitergehen möchten

Freiwillige Orientierung: Wenn Ihre drei Schritte vor allem Scope, Verantwortlichkeiten und belastbare Arbeitsstrukturen betreffen, ist das ISMS Scope & Governance Starter Kit mit einem vorgesehenen Preis von 199 EUR möglicherweise ein passender Self-Service-Schritt. Dieser VERSION 1.0-Review-Kandidat behauptet keine aktuelle Verfügbarkeit. Das Kit strukturiert den Einstieg, ersetzt aber weder fachliche Einzelfallprüfung noch Beratung.

Vor dem Teilen

- Nur bestätigte Aussagen extern verwenden.
- Offene Punkte sichtbar lassen; nicht kosmetisch schließen.
- Vertrauliche Architektur-, Kunden- und Zugangsdaten redigieren.
- Owner und Aktualisierungsdatum ergänzen.

A-R-C Andreas Rühl Consulting · SaaS Enablement Consulting · a.ruehl@a-r-c.me · www.a-r-c.me