A-R-C Andreas Rühl Consulting

50 Fragen, die AI-/SaaS-Founder von B2B-Kunden gestellt bekommen

Käuferfragen zu Security, Datenschutz, AI-Nutzung und Beschaffbarkeit sichtbar machen.

Für wen? Solo-/Micro-SaaS-Founder, AI-Tool-Builder, frühe B2B-SaaS-Teams und Agenturen.	Nutzung Jede Frage als beantwortbar, teilweise beantwortbar, offen oder nicht relevant markieren. Schriftliche Aussagen müssen belastbar sein.

Datenflüsse & Verarbeitung

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

AI-/LLM-Nutzung & Transparenz

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

Zugriff, Rollen & Berechtigungen

13. Welche Rollen und Berechtigungen gibt es im Produkt?
14. Kann ein Kunde nachvollziehen, wer Zugriff auf welche Daten hat?
15. Wie wird privilegierter Adminzugriff kontrolliert?
16. Gibt es MFA für Administrations- und Kundenkonten?
17. Wie werden ausgeschiedene Mitarbeiter oder Dienstleister aus Systemen entfernt?
18. Wie wird Supportzugriff begrenzt und protokolliert?

Logging, Nachvollziehbarkeit & Betrieb

19. Welche sicherheitsrelevanten Ereignisse werden geloggt?
20. Wie lange werden Logs aufbewahrt?
21. Können Kunden eigene Aktivitäten oder Exporte nachvollziehen?
22. Wie erkennen Sie Missbrauch, ungewöhnliche Nutzung oder Datenabfluss?
23. Wie werden Incidents intern dokumentiert und priorisiert?
24. Welche Betriebskennzahlen oder Statusinformationen können Käufer erwarten?

Subprocessor, Hosting & Lieferkette

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

Löschung, Retention & Datenportabilität

31. Wie kann ein Kunde seine Daten exportieren?
32. Wie funktioniert die Löschung nach Vertragsende?
33. Welche Daten bleiben in Backups, Logs oder Abrechnungssystemen erhalten?
34. Welche Retention-Fristen gelten für Produktdaten, Supportdaten, Logs und AI-Kontext?
35. Wie wird Löschung technisch und organisatorisch nachgewiesen?
36. Gibt es klare Verantwortlichkeiten für Löschanfragen?

Security Baseline & technische Maßnahmen

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

Käuferfragen, Claims & nächste Schritte

43. Welche Security-Fragen eines B2B-Käufers können Sie heute sicher beantworten?
44. Welche Fragen müssen Sie ehrlich als offen markieren?
45. Welche Marketingclaims könnten zu weit gehen?
46. Welche Unterlagen fehlen für einen ersten Procurement- oder Datenschutz-Review?
47. Welche Top-10-Lücken sollten in den nächsten 30/60/90 Tagen geschlossen werden?
48. Welcher nächste Trust-Schritt schafft den größten Verkaufsvorteil bei geringstem Risiko?
49. Welche Aussage würden Sie einem Enterprise-Käufer schriftlich geben — und welche lieber nicht?
50. Welche Trust-Materialien sollten vor dem nächsten größeren Sales-Gespräch fertig sein?

Typische Red Flags

• Unklar, ob Kundendaten an AI-/LLM-Provider gehen.
• Subprocessor sind bekannt, aber nicht dokumentiert.
• Marketing verspricht mehr Sicherheit/Compliance als umgesetzt ist.
• Support- oder Adminzugriffe sind möglich, aber nicht beschrieben oder geloggt.
• Löschung, Backups und Retention sind intern unklar.

Nächster sinnvoller Schritt

Wenn mehrere Fragen offen bleiben: Starten Sie mit dem Trust Starter Kit oder einem kurzen Readiness Call. Ziel ist nicht Perfektion, sondern eine belastbare, ehrliche Grundlage für Käufergespräche.

Pragmatisch in der Umsetzung, compliant im Ergebnis.