MODUL 2

Schnellprüfung in 10 Minuten

Kostenlose Kurzfassung

MODUL 2

Schnellprüfung in 10 Minuten

Zehn Fragen, jede mit Ja oder Nein zu beantworten. Sie decken die Fehler ab, die bei KI-gebauten Apps am häufigsten vorkommen und am meisten Schaden anrichten. Jedes Nein ist ein Grund, noch nicht live zu gehen.

DU BRAUCHST

1. Deine veröffentlichte App, nicht die Vorschau der Plattform.
2. Drei E-Mail-Adressen: zwei eigene für die Testkonten **Konto A** und **Konto B**, dazu eine Gmail-Adresse, die nicht in deinem Konto bei Plattform oder Datenbank hinterlegt ist, etwa die eines Bekannten, für das neue Konto in Frage 4 und 6.
3. Dein Handy.
4. Die **Browser-Werkzeuge** in Chrome oder Edge. Das ist ein eingebautes Fenster, das zeigt, was deine App im Hintergrund lädt. Du öffnest es mit F12, am Mac mit Cmd + Option + I.

> Prüfe nur deine eigene App mit deinen eigenen Testkonten.

Fragen mit (Typ A) gelten nur, wenn dein Browser direkt mit der Datenbank spricht, also bei Supabase oder Firebase. Das ist bei Lovable und Bolt fast immer so. So erkennst du es: Browser-Werkzeuge öffnen, Reiter **Netzwerk**, Seite neu laden. Siehst du Adressen mit `supabase.co`, `firestore.googleapis.com` oder `firebaseio.com`, ist deine App Typ A.

> **Wenig Zeit?** Fang mit Frage 1 bis 3 an. Fällt eine davon mit Nein aus, können Fremde an Daten deiner Kunden kommen. Das hat Vorrang vor allem anderen.

---

1 Sind deine geheimen Schlüssel unsichtbar?

☐ Ja ☐ Nein

Ein **Schlüssel** ist eine lange Zeichenkette, mit der deine App sich bei einem Dienst ausweist. Geheime Schlüssel im Browser sind wie ein Generalschlüssel unter der Fussmatte.

SO PRÜFST DU

Logge dich ein und öffne jede Seite deiner App einmal, auch Bezahlseite und Admin-Bereich, sonst findet die Suche nicht allen Code. Dann Browser-Werkzeuge > Reiter **Quellen**, Strg + Shift + F (Mac: Cmd + Option + F) und nacheinander suchen nach: `sb_secret_`, `service_role`, `sk_live_`, `sk-proj-`, `sk-ant-`. Ja heisst: kein einziger Treffer.

BEI NEIN

Schlüssel beim Anbieter sofort neu erzeugen und den alten sperren, dann den Aufruf von der Bau-KI auf den Server verlegen lassen.

IM KIT

Modul 3, Prüfpunkt 3.1

© 2026 Frank Schatz · service@frankschatz.com

2 Typ A Hat jede Tabelle Zugriffsregeln?

☐ Ja ☐ Nein

Datenbankregeln legen fest, wer welche Zeile deiner Datenbank lesen und ändern darf. Bei Supabase heissen sie **RLS** (Row Level Security), bei Firebase **Security Rules**. Fehlen sie, kann jeder alle Daten abrufen.

SO PRÜFST DU

Supabase: Im Dashboard unter **Advisors > Security Advisor** darf keine Meldung "RLS disabled in public" stehen. Lovable Cloud: In der Sicherheitsansicht des Projekts **Run quick scan** starten, keine Meldung zu fehlenden Tabellenregeln. Bolt Database: Datenbank-Symbol > Security darf keine Warnung zeigen. Firebase: Unter Firestore Database > Regeln darf weder `if true` noch ein Ablaufdatum wie `request.time < timestamp.date(...)` stehen.

BEI NEIN

Bau-KI anweisen, für alle Tabellen RLS zu aktivieren und Regeln zu erstellen, sodass jeder Nutzer nur seine eigenen Daten sieht und ändert.

IM KIT

Modul 3, Prüfpunkt 3.2

3 Sieht Konto B nichts von Konto A?

☐ Ja ☐ Nein

SO PRÜFST DU

Mit Konto A einen Eintrag anlegen, öffnen und die Adresse aus der Adresszeile kopieren. In einem privaten Fenster mit Konto B einloggen und die kopierte Adresse öffnen. Ja heisst: Konto B sieht "nicht gefunden" oder eine leere Seite.

BEI NEIN

Datenbankregeln oder die Prüfung auf dem Server reparieren lassen, sodass nur der Besitzer seinen Eintrag sieht, dann den Test wiederholen.

IM KIT

Modul 3, Prüfpunkt 3.4

4 Funktioniert dein wichtigster Ablauf auf dem Handy?

☐ Ja ☐ Nein

Gemeint ist der Ablauf, für den Kunden deine App nutzen, etwa Registrieren und Buchen oder Registrieren und Kaufen.

SO PRÜFST DU

Auf deinem Handy die Live-Adresse öffnen und den Ablauf mit einem neuen Konto komplett durchgehen. Danach Seite neu laden und prüfen, ob das Ergebnis gespeichert ist. Ja heisst: alles lesbar ohne Zoomen, kein Fehler, Ergebnis gespeichert.

BEI NEIN

Screenshot und genaue Schrittfolge an die Bau-KI geben, nach der Reparatur den ganzen Ablauf erneut auf dem Handy gehen.

IM KIT

Modul 5, Prüfpunkte 5.1 und 5.4

© 2026 Frank Schatz · service@frankschatz.com

5 Entsteht beim Doppelklick nur ein Eintrag?

☐ Ja ☐ Nein

SO PRÜFST DU

Den Absenden-, Bestellen- oder Speichern-Knopf deines wichtigsten Formulars schnell dreimal hintereinander klicken. Ja heisst: genau ein Eintrag, der Knopf war während des Speicherns gesperrt.

BEI NEIN

Bau-KI anweisen, Knöpfe während der Verarbeitung zu sperren und doppelte Einträge auf dem Server zu verhindern.

IM KIT

Modul 5, Prüfpunkt 5.2

---

6 Kommt die Bestätigungsmail im Posteingang an?

☐ Ja ☐ Nein

SO PRÜFST DU

Ein neues Konto mit der Gmail-Adresse anlegen, die nicht in deinem Plattform- oder Datenbank-Konto hinterlegt ist, und "Passwort vergessen" auslösen. Mit deiner eigenen Adresse ist der Test wertlos: Bei Supabase ohne eigenen Versanddienst bekommen nur Mitglieder deines Projekt-Teams Mails, deine Kunden nicht. Ja heisst: Beide Mails sind innerhalb weniger Minuten im Posteingang, nicht im Spam, und ihre Links führen auf deine Live-Domain und funktionieren.

BEI NEIN

Einen eigenen E-Mail-Versanddienst mit deiner Domain einrichten und die Links in den Mail-Vorlagen auf deine Live-Domain setzen.

IM KIT

Modul 5, Prüfpunkt 5.7

---

7 Lädt deine App vor der Einwilligung keine Tracker?

☐ Ja ☐ Nein

Tracking heisst, das Verhalten deiner Besucher mit Diensten wie Google Analytics oder dem Meta-Pixel zu messen. Das darf erst nach Zustimmung des Besuchers starten.

SO PRÜFST DU

Neues privates Fenster, **zuerst** Browser-Werkzeuge mit Reiter **Netzwerk** öffnen, **dann** deine App laden, im Cookie-Banner nichts anklicken. Im Filterfeld nacheinander `google-analytics`, `googletagmanager`, `facebook` und `fonts.g` eingeben. Ja heisst: keine Treffer. Anfragen an firestore, firebase oder identitytoolkit gehören zu deiner Datenbank und zählen nicht.

BEI NEIN

Tracking-Skripte erst nach Einwilligung laden lassen, Schriften lokal einbinden, oder Tracking ganz entfernen, wenn du es nicht brauchst.

IM KIT

Modul 4, Prüfpunkt 4.8

© 2026 Frank Schatz · service@frankschatz.com

8 Sind Impressum und Datenschutzerklärung überall erreichbar und echt?

☐ Ja ☐ Nein

SO PRÜFST DU

Auf der Startseite, der Login-Seite und einer Seite nach dem Login nach beiden Links suchen, meist ganz unten. Beide öffnen und nach Platzhaltern wie `[Your Company]`, `[Name]`, `Lorem ipsum` oder englischen Mustertexten suchen. Ja heisst: Links auf allen drei Seiten, keine Platzhalter, alles auf Deutsch.

BEI NEIN

Beide Texte mit einem Generator für den deutschsprachigen Raum erstellen und die Links in die Fusszeile aller Seiten setzen lassen.

IM KIT

Modul 4, Prüfpunkt 4.7

9 Hat dein KI-Anbieter eine harte Ausgabengrenze?

☐ Ja ☐ Nein

Gilt nur, wenn deine App eine eingebaute KI-Funktion hat. Ohne KI-Funktion beantwortest du die Frage mit Ja.

SO PRÜFST DU

Im Konto deines KI-Anbieters, etwa OpenAI oder Anthropic, die Einstellungen zu Limits und Abrechnung öffnen. Ja heisst: Es gibt eine Obergrenze, die Kosten stoppt, oder du zahlst über vorab gekauftes Guthaben ohne automatische Aufladung.

BEI NEIN

Grenze sofort setzen und automatische Aufladung abschalten oder mit niedrigem Höchstbetrag versehen.

IM KIT

Modul 6, Prüfpunkt 6.3

10 Sind dein E-Mail-Postfach und deine Bau-Plattform mit Zwei-Faktor-Anmeldung geschützt?

☐ Ja ☐ Nein

Zwei-Faktor-Anmeldung heisst, dass zum Passwort ein zweiter Nachweis kommt, meist ein Code aus einer App auf dem Handy. Wer dein E-Mail-Postfach übernimmt, kann bei allen anderen Diensten das Passwort zurücksetzen.

SO PRÜFST DU

In den Sicherheitseinstellungen deines E-Mail-Postfachs und deiner Bau-Plattform nachsehen. Ja heisst: Bei beiden ist die Zwei-Faktor-Anmeldung aktiv.

BEI NEIN

Jetzt einschalten, das E-Mail-Postfach zuerst, und die Wiederherstellungscodes an einem sicheren Ort ausserhalb des Handys ablegen.

IM KIT

Modul 6, Prüfpunkt 6.7

© 2026 Frank Schatz · service@frankschatz.com

Dein Ergebnis

Zehnmal Ja: Die häufigsten und teuersten Fehler hat deine App nicht. Fertig ist sie damit noch nicht.

Mindestens ein Nein: Behebe diesen Punkt, bevor echte Kunden deine App nutzen, und wiederhole danach die betroffene Frage. Sagt die KI beim Reparieren "erledigt", glaubst du ihr erst, wenn deine Frage wieder Ja ergibt.

Was die Schnellprüfung nicht sieht

Die Schnellprüfung prüft zehn Dinge, die du von aussen sehen kannst. Einige der teuersten Fehler liegen aber dort, wo du ohne Hilfe nicht hinschaust: in Server-Funktionen, die jeder ohne Login aufrufen kann, in einer Löschfunktion, die nur den Login entfernt und alle Daten behält, in Zahlungen, die im Testmodus laufen und im Live-Modus still scheitern, oder in einer KI-Funktion ohne Grenze pro Nutzer.

Dafür gibt es das vollständige Vibecode-Testing-Kit. Es prüft deine App in 47 Prüfpunkten in vier Bereichen: Sicherheit, Daten und DSGVO, Funktion aus Kundensicht sowie Betrieb und Kosten. Was du nicht selbst sehen kannst, prüft die KI für dich, mit 34 fertigen Prüf-Prompts und je einer Gegenprüfung. Am Ende entscheidest du nicht nach Gefühl, sondern über eine Ampel für jeden Bereich und eine klare Regel, wann deine App live darf.

79 € einmalig. Buchst du innerhalb von 30 Tagen nach dem Kauf mein Vibe-Code-Review, werden die 79 € voll angerechnet.

Zum Vibecode-Testing-Kit: frankschatz.com/vibecode-testing-kit

© 2026 Frank Schatz · service@frankschatz.com

HERAUSGEBER

Frank Schatz

C/ Magallanes 27b
07590 Cala Ratjada
Spanien

NIE: X6965317C

Web: frankschatz.com
Support: service@frankschatz.com

Stand: Oktober 2026. Plattformen wie Lovable, Bolt, Cursor, Replit, Supabase und Firebase ändern Menüs, Namen und Funktionen laufend. Menüpfade und Angaben wurden im Oktober 2026 mit den offiziellen Dokumentationen der Anbieter abgeglichen.

Das Vibecode-Testing-Kit ist eine Prüfanleitung. Es ersetzt keinen Penetrationstest durch Sicherheitsfachleute und keine Rechtsberatung. Prüfe nur deine eigene App mit deinen eigenen Testkonten.

© 2026 Frank Schatz. Diese kostenlose Kurzfassung darfst du unverändert und kostenlos weitergeben, etwa an andere, die mit KI Apps bauen. Verkauf, Veränderung und Veröffentlichung unter eigenem Namen sind nicht erlaubt.