Abnahme-Audit: Prüfbericht

Musterbericht. Auftraggeber, Anwendung und Befunde sind fiktiv.

Auftraggeber	Muster GmbH
Prüfgegenstand	Kundenportal „MeinKonto“, Version 1.4
Technische Basis	Mit KI gebaut (Lovable), Datenbank Supabase, Hosting Vercel
Anlass	Abnahme vor dem Livegang
Prüfzeitraum	03.11. bis 07.11.2026
Auditor	Frank Schatz, unabhängiger Auditor für KI-gebaute Software
Berichtsversion	1.0 vom 10.11.2026

1. Zusammenfassung für die Geschäftsführung

Gesamturteil: Abnahme derzeit nicht empfohlen.

Das Kundenportal funktioniert in den vorgeführten Standardabläufen. Zwei Befunde sind aber kritisch: Es ist nicht nachgewiesen, dass Kunden keinen Zugriff auf Daten anderer Kunden haben, und ein funktionierendes Backup ist ebenfalls nicht nachgewiesen. Beide Punkte können im Ernstfall zu Datenschutzverstößen, Meldepflichten und dem Verlust aller Kundendaten führen.

Werden die beiden kritischen Befunde behoben und nachgewiesen, kann die Abnahme mit Auflagen erfolgen.

Ergebnis in Zahlen

Status	Anzahl
Erfüllt	14
Teilweise erfüllt	5
Nicht erfüllt	6
Geprüfte Punkte gesamt	**25**

Die wichtigsten Befunde

ID	Befund	Risiko
B-01	Schutz vor Zugriff auf fremde Kundendaten nicht nachgewiesen	**Kritisch**
B-02	Backup nie zurückgespielt, Wiederherstellung nicht nachgewiesen	**Kritisch**
B-03	Geheimer API-Schlüssel im Browser-Code sichtbar	**Hoch**
B-04	Kein Weg zurück bei fehlgeschlagenem Update	**Hoch**
B-05	Keine automatisierten Tests	**Mittel**

2. Prüfauftrag und Umfang

Geprüft wurde:

- Das Kundenportal in der Version 1.4 auf der Testumgebung
- Die zugehörige Datenbank und ihre Zugriffsregeln
- Dokumentation, Betriebsabläufe und vorgelegte Nachweise

Nicht Bestandteil des Audits:

- Die interne Verwaltungsoberfläche (nicht Teil des Auftrags)
- Die Infrastruktur des Hosting-Anbieters selbst
- Eine Prüfung des Quellcodes (Code-Review)
- Eigene Tests oder Sicherheitstests durch den Auditor, insbesondere kein Penetrationstest. Sicherheitsthemen werden ausschließlich anhand vorgelegter Nachweise bewertet.

Vorgehen:

- Fragenkatalog nach Prüfliste, vorab an den Auftraggeber übergeben
- Interviews mit Geschäftsführung und Entwicklungsdienstleister
- Sichtung der vorgelegten Nachweise
- Vorführung ausgewählter Abläufe durch den Entwicklungsdienstleister im Beisein des Auditors

Prüfgrundlagen:

- Qualitätsmerkmale nach ISO/IEC 25010 (Funktionalität, Zuverlässigkeit, Sicherheit, Wartbarkeit, Benutzbarkeit)
- Testvorgehen in Anlehnung an ISO/IEC/IEEE 29119
- DSGVO, soweit für den Betrieb relevant
- Prüfliste Frank Schatz, Version 2026-11

---

3. Bewertungsmaßstab

Nachweisstufen

Stufe	Bedeutung	Bewertung
Behauptet	Nur mündlich zugesagt	**Nicht erfüllt**
Dokumentiert	Schriftlich beschrieben, aber nicht belegt	**Teilweise erfüllt**
Nachgewiesen	Protokoll, Beleg oder Vorführung liegt vor	**Erfüllt**

Risikostufen

Stufe	Bedeutung
Kritisch	Kann zu Datenverlust, Datenschutzverstoß oder Ausfall führen. Muss vor dem Livegang behoben sein.
Hoch	Erhebliches Risiko für Betrieb oder Sicherheit. Sollte vor dem Livegang behoben sein, spätestens kurz danach.

Stufe	Bedeutung
Mittel	Erschwert Betrieb oder Weiterentwicklung. Innerhalb von drei Monaten beheben.
Niedrig	Verbesserung, kein akutes Risiko.

4. Ergebnisübersicht

ID	Prüfpunkt	Bereich	Nachweis	Status	Risiko
B-01	Datenzugriff nur auf eigene Daten	Sicherheit	Behauptet	Nicht erfüllt	Kritisch
B-02	Backup mit nachgewiesener Wiederherstellung	Zuverlässigkeit	Behauptet	Nicht erfüllt	Kritisch
B-03	Keine geheimen Schlüssel im Browser	Sicherheit	Vorführung	Nicht erfüllt	Hoch
B-04	Rollback bei fehlgeschlagenem Update	Zuverlässigkeit	Behauptet	Nicht erfüllt	Hoch
B-05	Automatisierte Tests vorhanden	Wartbarkeit	Keine	Nicht erfüllt	Mittel
B-06	Fehlerprotokollierung im Betrieb	Zuverlässigkeit	Dokumentiert	Teilweise erfüllt	Mittel
B-07	Verständliche Fehlermeldungen für Nutzer	Benutzbarkeit	Vorführung	Teilweise erfüllt	Niedrig
B-08	Technische Dokumentation	Wartbarkeit	Dokumentiert	Teilweise erfüllt	Mittel
B-09	Trennung Test- und Produktivumgebung	Sicherheit	Nachgewiesen	Erfüllt	
B-10	Verschlüsselte Verbindung (HTTPS)	Sicherheit	Nachgewiesen	Erfüllt	
B-11	Passwort zurücksetzen funktioniert	Funktionalität	Vorführung	Erfüllt	
B-12	Datenschutzerklärung und Impressum vorhanden	Recht	Nachgewiesen	Erfüllt	
B-13	Schutz vor wiederholten Fehlanmeldungen	Sicherheit	Vorführung	Nicht erfüllt	Mittel
...	weitere Prüfpunkte				

5. Befunde im Detail

B-01: Schutz vor Zugriff auf fremde Kundendaten nicht nachgewiesen

Bereich	Sicherheit
Risiko	**Kritisch**
Status	**Nicht erfüllt**
Nachweis	**Behauptet**
Bedingung für die Abnahme	Ja

Beobachtung

Laut Aussage des Entwicklungsdienstleisters sieht jeder Kunde nur seine eigenen Daten. Dokumentierte Zugriffsregeln je Datenbanktabelle liegen nicht vor. Ein Berechtigungstest oder Penetrationstest wurde nach eigener Aussage nicht durchgeführt. Im Interview wurde bestätigt, dass die Zugriffsregeln der Datenbank bei der Erstellung mit dem KI-Werkzeug nicht gesondert eingerichtet wurden.

Auswirkung auf das Geschäft

Fehlen die Zugriffsregeln, kann jeder angemeldete Kunde mit wenig technischem Wissen Namen, Adressen und Rechnungsbeträge anderer Kunden einsehen. Das wäre eine meldepflichtige Datenschutzverletzung nach Art. 33 DSGVO und ein erhebliches Haftungs- und Rufrisiko. Bei KI-gebauten Anwendungen mit dieser Datenbank ist dieser Fehler häufig.

Was erreicht werden muss

Jeder Kunde darf ausschließlich seine eigenen Datensätze lesen und ändern. Das gilt für alle Tabellen mit personenbezogenen Daten.

Erwarteter Nachweis für die Nachprüfung

Dokumentierte Zugriffsregeln je Tabelle und das Protokoll eines Berechtigungstests oder Penetrationstests durch einen Sicherheitsspezialisten. Empfehlung: Penetrationstest beauftragen.

B-02: Backup nie zurückgespielt

Bereich	Zuverlässigkeit
Risiko	**Kritisch**
Status	**Nicht erfüllt**
Nachweis	**Behauptet**
Bedingung für die Abnahme	Ja

Beobachtung

Laut Aussage des Entwicklers werden täglich automatische Backups erstellt. Ein Protokoll über eine erfolgreiche Wiederherstellung liegt nicht vor. Eine Wiederherstellung wurde nach eigener Aussage noch nie durchgeführt.

Auswirkung auf das Geschäft

Ob im Ernstfall Daten wiederhergestellt werden können, wie lange das dauert und welche Daten dabei verloren gehen, ist unbekannt. Ein Backup, das nie zurückgespielt wurde, ist kein Backup.

Was erreicht werden muss

Eine vollständige Wiederherstellung auf einer separaten Umgebung, mit dokumentierter Dauer und Prüfung, ob alle Daten vollständig sind. Danach regelmäßige Wiederholung, mindestens vierteljährlich.

Erwarteter Nachweis für die Nachprüfung

Protokoll der Wiederherstellung mit Datum, Dauer, Datenstand und Ergebnis.

B-03: Geheimer API-Schlüssel im Browser-Code

Bereich	Sicherheit
Risiko	**Hoch**
Status	**Nicht erfüllt**
Nachweis	Vorführung der Konfiguration am 04.11.2026
Bedingung für die Abnahme	Nein, aber Behebung vor dem Livegang empfohlen

Beobachtung

Bei der Vorführung der Konfiguration durch den Entwicklungsdienstleister zeigte sich, dass der Schlüssel für den E-Mail-Versanddienst als Variable für den Browser-Code hinterlegt ist. Damit wird er an jeden Besucher ausgeliefert.

Auswirkung auf das Geschäft

Jeder kann den Schlüssel auslesen und über das Konto der Muster GmbH E-Mails verschicken. Möglich sind Spam im Namen des Unternehmens, Sperrung des Kontos beim Anbieter und Kosten.

Was erreicht werden muss

Geheime Schlüssel dürfen nur auf dem Server liegen. Der bisherige Schlüssel muss beim Anbieter ungültig gemacht und durch einen neuen ersetzt werden.

Erwarteter Nachweis für die Nachprüfung

Vorführung der geänderten Konfiguration, Bestätigung des Schlüsselwechsels durch den Anbieter.

Die weiteren Befunde folgen im selben Aufbau.

---

6. Vorgeführte Abläufe

Die folgenden Abläufe wurden vom Entwicklungsdienstleister auf der Testumgebung im Beisein des Auditors vorgeführt.

Nr.	Ablauf	Ergebnis
V-01	Registrierung mit gültigen Daten	**In Ordnung**
V-02	Registrierung mit bereits verwendeter E-Mail	In Ordnung, verständliche Meldung
V-03	Anmeldung mit falschem Passwort, fünfmal hintereinander	Keine Sperre, keine Verzögerung, siehe B-13
V-04	Passwort zurücksetzen	**In Ordnung**
V-05	Rechnung als PDF herunterladen	**In Ordnung**

Nr.	Ablauf	Ergebnis
V-06	Formular mit Sonderzeichen und sehr langen Eingaben	Technische Fehlermeldung sichtbar, siehe B-07
V-07	Bedienung auf dem Smartphone	**In Ordnung**
V-08	Wiederherstellung aus Backup	Konnte nicht vorgeführt werden, siehe B-02
V-09	Rücknahme eines Updates	Konnte nicht vorgeführt werden, siehe B-04

7. Auflagen und Maßnahmen nach Priorität

Vor der Abnahme zwingend:

1. B-01: Zugriff auf eigene Daten beschränken und durch Berechtigungstest oder Penetrationstest nachweisen
2. B-02: Wiederherstellung durchführen und protokollieren

Vor dem Livegang empfohlen:

3. B-03: Schlüssel vom Browser auf den Server verlagern und erneuern
4. B-04: Rollback-Verfahren festlegen und einmal erproben

Innerhalb von drei Monaten:

5. B-05: Automatisierte Tests für die Kernabläufe
6. B-06: Fehlerprotokollierung im Betrieb vervollständigen
7. B-08: Technische Dokumentation ergänzen
8. B-13: Sperre oder Verzögerung nach wiederholten Fehlanmeldungen einrichten

Bei Gelegenheit:

9. B-07: Verständliche Fehlermeldungen statt technischer Texte

8. Freigabe-Empfehlung

Option	Bedingung
☐ Abnahme empfohlen	
☐ Abnahme mit Auflagen empfohlen	Nach Nachweis von B-01 und B-02
☒ **Abnahme derzeit nicht empfohlen**	

Eine Nachprüfung der kritischen Befunde ist nach Vorlage der Nachweise möglich.

9. Anhang

A. Angeforderte und erhaltene Nachweise

Nachweis	Angefordert	Erhalten
Zugang zur Testumgebung	Ja	Ja
Vorführung der Konfiguration	Ja	Ja
Dokumentierte Zugriffsregeln je Tabelle	Ja	**Nein**
Protokoll Berechtigungstest oder Penetrationstest	Ja	**Nein**
Protokoll letzte Backup-Wiederherstellung	Ja	**Nein**
Beschreibung Rollback-Verfahren	Ja	**Nein**
Technische Dokumentation	Ja	**Teilweise**
Testprotokolle	Ja	**Nein**

B. Erklärung zur Unabhängigkeit

Der Auditor war an Entwicklung und Betrieb des Prüfgegenstands nicht beteiligt und steht in keiner geschäftlichen Beziehung zum Entwicklungsdienstleister. Die Prüfung erfolgte nach bestem Wissen auf Grundlage der vorgelegten Unterlagen, der geführten Interviews und der vorgeführten Abläufe im genannten Prüfzeitraum. Der Bericht beschreibt den Stand zum Prüfzeitpunkt. Die Freigabe-Empfehlung ist eine Empfehlung; die Entscheidung über die Abnahme trifft der Auftraggeber.

Dieser Bericht ist ausschließlich für den Auftraggeber bestimmt. Eine Weitergabe an Dritte bedarf der schriftlichen Zustimmung des Auditors.

Cala Ratjada, 10.11.2026

Frank Schatz
Unabhängiger Auditor für KI-gebaute Software