SO ARBEITE ICH SICHER AN IHREN AUTOMATISIERUNGEN

Datenschutz & Sicherheit bei codefeeder

Wie ich KI-Automatisierungen — etwa eine Schnittstelle von Excel zu Ihrem Rechnungsprogramm — aus der Ferne umsetze, ohne dass Ihre echten Daten je Ihr Haus verlassen.

LEITPRINZIP

Ich entwickle ausschließlich mit anonymisierten Testdaten. Ihre echten Kunden-, Umsatz- und Rechnungsdaten bleiben zu jedem Zeitpunkt auf Ihren Systemen. Die fertige Automatisierung läuft anschließend lokal und **ohne KI-Dienst im Datenpfad**.

Drei Sicherheitsebenen

1

Vertraglich

Geheimhaltungsvereinbarung (NDA), Dienstleistungsvertrag mit klarem Leistungsumfang und — sobald personenbezogene Daten berührt werden — ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO.

2

Datenfluss

Entwicklung gegen synthetische Testdaten. Sie liefern *Struktur* (Spalten, Schema, anonyme Beispiele) — nicht Ihren Echtbestand. Keine echten Personendaten in KI-Systemen.

3

Technischer Zugriff

Bevorzugt gar kein Fernzugriff: Sie führen aus, ich leite an. Falls nötig, nur zeitlich befristete Zugänge nach dem Prinzip der Datensparsamkeit (Least Privilege), verschlüsselt und protokolliert.

Wo fließen Daten mit KI hin?

ZWEI GETRENNTE EBENEN — WICHTIG ZU UNTERSCHEIDEN

a) Während der Entwicklung hilft mir Claude (Anthropic), den Code zu schreiben. Dabei fließen nur Code und Datenstruktur — keine echten Personendaten. Genutzt wird der kommerzielle Zugang: **kein Training auf Ihren Daten**, Auftragsverarbeitung vertraglich abgesichert (DPA), auf Wunsch mit Zero-Data-Retention.

b) Zur Laufzeit arbeitet die fertige Schnittstelle **deterministisch und offline** (z. B. Python + openpyxl + API Ihres Rechnungsprogramms). Kein KI-Dienst wird im Betrieb aufgerufen — nachweisbar und prüfbar.

Der Ablauf in der Praxis

01 **NDA unterzeichnen** — Vertraulichkeit vor dem ersten Detailgespräch.

02 **Discovery** — Sie beschreiben Excel-Struktur & Ziel-API; ich erhalte Schema und anonyme Beispiele.

03 **Angebot & Vertrag** — Dienstleistungsvertrag mit klarem Scope; AVV beigefügt, falls Personendaten betroffen sind.

04 **Synthetische Testdaten** — reproduzierbar erzeugt, realistisch, aber vollständig erfunden.

05 **Entwicklung** — gegen Testdaten, kommerzieller KI-Zugang ohne Training.

06 **Übergabe** — Skript, Dokumentation und Testsuite; Zugangsschlüssel legen Sie selbst an (eng gefasst).

07 **Gemeinsamer Testlauf** — Sie bedienen, ich leite an; erster Echtlauf auf kleinem Ausschnitt.

08 **Abnahme & Cleanup** — Testdaten gelöscht, Zugänge widerrufen, Löschung bestätigt.

09 **Wartung optional** — als separater Vertrag mit eigenem, minimalem Zugriffsmodell.

Meine Zusagen an Sie

- ✓ Echtdaten verlassen nie Ihr System
- ✓ Kommerzieller KI-Zugang, kein Training
- ✓ Least-Privilege & befristete Zugänge
- ✓ Keine Personendaten in Klartext-Logs
- ✓ Keine Personendaten in KI-Chats
- ✓ Zugangsdaten legen Sie an, nicht ich
- ✓ Verschlüsselung in Transit & at Rest
- ✓ Nachweisliche Löschung nach Projektende

codefeeder · KI-Automatisierung für den Mittelstand
Marco Fütterer Management Holding GmbH
marco@codefeeder.ai · 0179 503 12 14

Hinweis: Dieses Dokument ist ein sorgfältig ausgearbeitetes Muster für den Geschäftsbetrieb der Marke codefeeder und dient als Verhandlungs- und Arbeitsgrundlage. Es stellt keine Rechtsberatung im Einzelfall dar. Für rechtsverbindliche Vereinbarungen — insbesondere bei besonderen Datenkategorien, hohen Auftragswerten oder Drittlandsbezug — wird eine anwaltliche Prüfung empfohlen. Mit `[...]` markierte Felder sind vor Vertragsschluss auszufüllen.