

PII-ANONYMISIERUNG · SCHWEIZ

# Sovereign Cockpit

Vertrauliche Daten lokal anonymisieren, prüfen, freigeben — der rohe Text verlässt Ihre Kontrolle nie, und Sie können es beweisen.

**Ein kontrollierter Workflow vor Cloud-Modell oder Versand:** vertrauliche Daten werden lokal anonymisiert, jeder Schritt bleibt im Audit-Trail nachweisbar — nur die entschärfte Fassung geht hinaus, auf Ihren Klick.

01

## Lokal ersetzen

Vertrauliche Daten werden auf dieser Maschine erkannt und durch Platzhalter ersetzt — kein Cloud-Versand.

02

## Prüfen & freigeben

Erst Ihr Klick im Human-Gate gibt die anonyme Fassung frei; das Mapping mit Klartext bleibt serverseitig.

03

## Re-identifizieren

Die Antwort des externen Modells fügen Sie zurück ein — die Originalwerte werden wieder eingesetzt.

## WAS ES LEISTET

- **Erzwungenes Human-Gate.** Nichts verlässt den Server ohne Ihre Freigabe.
- **Eigene Standardbegriffe.** Firmenname, Kunden, Produktcodes — einmal erfasst, in jedem Dokument mit-anonymisiert.
- **Verschlüsseltes Mapping.** Re-ID-Schlüssel AES-256-GCM, nach 24 h automatisch gelöscht.
- **Deutsch & Englisch.** Vollständige zweisprachige Oberfläche.
- **Tamper-evidenter Audit-Trail.** HMAC-verkettet, nachweisbar unverändert, PII-frei.
- **CH-Datentypen ab Werk.** AHV, IBAN, CHE-UID, GLN/ZSR und mehr.
- **Offline-fähige Anmeldung.** In-App-Nutzer, bcrypt, ohne externen Dienst.
- **Datenhaltung Schweiz.** On-Prem oder gehostet — Sie wählen.

## BETRIEBSVARIANTEN

### HÖCHSTE SOUVERÄNITÄT

#### On-Premise

App und Namens-Erkennung laufen vollständig bei Ihnen. Kein Datenabfluss, eigene Hardware.

### HYBRID

#### Ihr RZ + CH-Cloud

App in Ihrem Rechenzentrum, Namens-Erkennung über eine Schweizer Cloud-API (Infomaniak).

### GEHOSTET · CH

#### Single-Tenant

Wir betreiben je Kunde eine isolierte Instanz in der Schweiz — eigener Schlüssel, eigener Audit-Trail.

## RICHTPREISE

GEHOSTET (CH)

**ab CHF 250** / Monat · im Jahresabo

Isolierte Instanz, Datenhaltung Schweiz, bis 5 Nutzer. Betrieb durch iConference.

ON-PREMISE

**ab CHF 180** / Monat · im Jahresabo

Betrieb auf Ihrer Hardware (Anforderungen nach Rücksprache), bis 5 Nutzer.

*Richtwerte je Instanz/Firma. Konkretes Angebot nach kurzem Gespräch.*

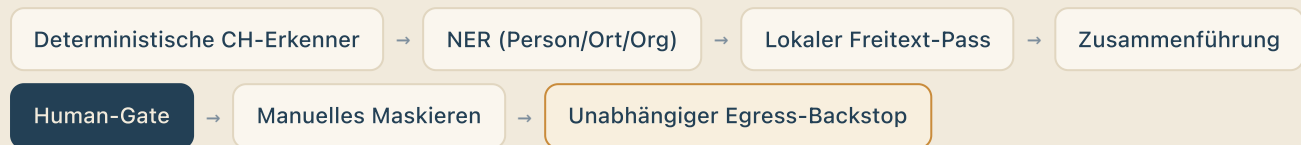
## iConference AG

Grafenastrasse 15 · 6300 Zug · Schweiz  
info@iconference.ch · iconference.ch

**30 Tage kostenlos testen**  
[iconference.ch/ki-produkte](https://iconference.ch/ki-produkte)

## SICHERHEITSARCHITEKTUR

### Mehrere unabhängige Schichten, nicht ein Modell



Der Egress-Backstop ist eine zweite, bewusst breiter angelegte Prüfung vor der Auslieferung – unabhängig vom Haupt-Erkennung, damit eine Lücke nicht zweimal in derselben Schicht steckt.

## WAS GESCHÜTZT BLEIBT

### Mapping verschlüsselt

Re-Identifikations-Schlüssel mit AES-256-GCM. Nach 24 h automatisch gelöscht (Frist konfigurierbar) – danach ist keine Re-Identifikation mehr möglich.

### Fail-closed überall

Scheitert ein Schritt (Erkennung, gescanntes PDF ohne Textebene), bricht der Vorgang ab – statt ungeprüfte Daten weiterzugeben.

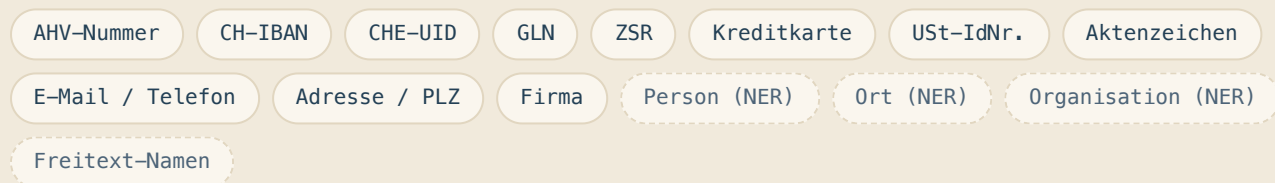
### Audit-Trail fälschungssicher

HMAC-verkettete Protokollkette, PII-frei, jede Änderung nachweisbar.

### Egress-Kontrolle vor Auslieferung

Bleiben schutzwürdige Werte im Klartext, wird die Auslieferung angehalten und Ihnen zur Freigabe vorgelegt; eine bewusste Freigabe wird im Audit-Trail vermerkt.

## ERKANNTE DATENTYPEN (CH-FOKUS)



Eigene Schutzbegriffe lassen sich als **Standardbegriffe** hinterlegen – verschlüsselt, für alle künftigen Dokumente.

## FORMATE & GRENZEN

**Unterstützt:** PDF mit Textebene, Markdown, Text, Excel (XLSX).

Gescannte PDFs ohne Textebene werden bewusst abgewiesen (fail-closed) – OCR ist auf der Roadmap.

Limit 150 000 Zeichen bzw. 25 MB je Upload.

## MODELLE

Namens-Erkennung wahlweise vollständig lokal oder über eine Schweizer Cloud-API.

**Modell-unabhängig:** Der Schutz beruht auf mehreren unabhängigen Prüf-Schichten, nicht auf einem einzelnen Modell – Sie sind an kein bestimmtes KI-Modell gebunden.

## ABGRENZUNG

### Ein Vorstufen-Werkzeug, keine Plattform

Sovereign Cockpit sitzt **vor** jedem Versand nach draussen – Cloud-Modell, E-Mail oder Weitergabe – und ersetzt weder Chatbot, RAG noch DMS. Der Kern: eine erzwungene Freigabe durch einen Menschen im reversiblen Ablauf und ein fälschungssicherer Audit-Trail; Schweizer Identifikatoren erkennt das System ab Werk.