

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 lokal anonymisiert, jeder Schritt im Audit-Trail nachweisbar, Freigabe nur auf Ihren Klick.

01

Lokal ersetzen

Vertrauliche Daten werden lokal 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, überall mit-anonymisiert.
- **Alles verschlüsselt (ruhend).** AES-256-GCM, Schlüssel getrennt vom Daten-Volume, löscherbar per Klick.
- **Deutsch & Englisch.** Vollständige zweisprachige Oberfläche.
- **Deutlich weniger Prüfaufwand.** Eine Karte pro Firma und Person statt langer Kandidatenlisten pro Typ.
- **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, Argon2id, ohne externen Dienst.
- **Datenhaltung Schweiz.** On-Prem oder gehostet (Sie wählen).

BETRIEBSVARIANTEN

HÖCHSTE SOUVERÄNITÄT

On-Premise

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

HYBRID

Ihr RZ + CH-Cloud

App in Ihrem Rechenzentrum, Erkennung via CH-Cloud-API (Infomaniak).

GEHOSTET · CH

Single-Tenant

Isolierte Instanz je Kunde in der Schweiz, eigener Schlüssel und Audit-Trail.

RICHTPREISE

GEHOSTET (CH)

ab CHF 250 / Monat · im Jahresabo

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

ON-PREMISE

ab CHF 180 / Monat · im Jahresabo

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

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

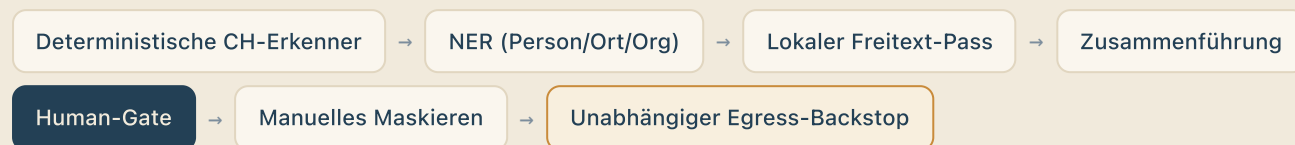
iConference AG

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

30 Tage kostenlos testen
iconference.ch/ki-produkte

SICHERHEITSARCHITEKTUR

Mehrere unabhängige Schichten, nicht ein Modell



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

WAS GESCHÜTZT BLEIBT

Alles verschlüsselt (ruhend)

Sämtliche Vorgangsdaten (Original bis Standardbegriffe) mit AES-256-GCM, nur lokal in Ihrer Instanz; Schlüssel getrennt vom Daten-Volume. Löschung per Klick, nachweisbar in der Audit-Kette.

Audit-Trail fälschungssicher

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

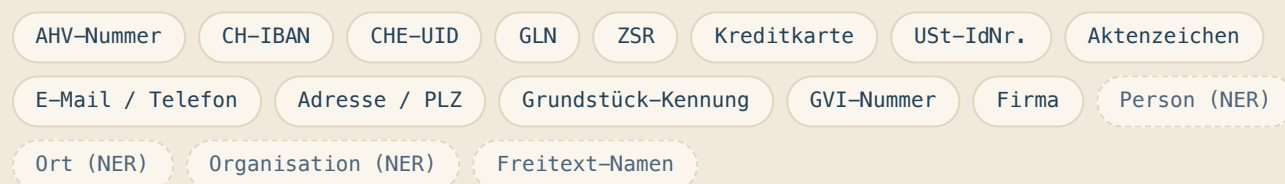
Fail-closed überall

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

Egress-Kontrolle vor Auslieferung

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

ERKANNTE DATENTYPEN (CH-FOKUS)



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

Namen, Orte und Firmen erkennt die NER sprachunabhängig. Länderspezifische Kennungen (z. B. deutsche Steuer-ID, Handelsregisternummer) liefern wir als **Erkennung-Modul für Ihr Land auf Anfrage**.

Neu erkannt werden Aktenzeichen auch im Slash-Format, ein- und zweistellige Datumsangaben sowie romanische Grundbuch-Begriffe wie **foglio** und **particella**. Nachnamen bleiben über alle Schreibvarianten geschützt, auch wenn ein Zeilenumbruch im PDF sie zerreisst.

FORMATE & GRENZEN

Unterstützt: PDF mit Textebene, Word (DOCX), 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.