

PII ANONYMISATION · SWITZERLAND

Sovereign Cockpit

Anonymise, review and release confidential data locally: the raw text never leaves your control, and you can prove it.

A controlled workflow before any cloud model or dispatch: confidential data anonymised locally, every step provable in the audit trail, release only on your click.

01

Replace locally

Confidential data is detected locally and replaced with placeholders: nothing is sent to the cloud.

02

Review & release

Only your click at the human gate releases the anonymised version; the mapping with the original values stays on the server.

03

Re-identify

Paste the external model's response back in: Sovereign Cockpit restores the original values.

WHAT IT DELIVERS

- **Enforced human gate.** Nothing leaves the server without your release.
- **Your own standard terms.** Company name, clients, product codes: entered once, anonymised everywhere.
- **Everything encrypted at rest.** AES-256-GCM, key held separately from the data volume, deletable per click.
- **German & English.** Fully bilingual interface.
- **Noticeably less review effort.** One card per company and person instead of long candidate lists per type.
- **Tamper-evident audit trail.** HMAC-chained, provably unaltered, PII-free.
- **Swiss data types built in.** AHV, IBAN, CHE-UID, GLN/ZSR and more.
- **Offline-capable sign-in.** In-app users, Argon2id, no external service.
- **Data kept in Switzerland.** On-premise or hosted (your choice).

DEPLOYMENT OPTIONS

HIGHEST SOVEREIGNTY

On-premise

App and name detection run entirely on your side, your own hardware.

HYBRID

Your DC + Swiss cloud

App in your data centre, detection via a Swiss cloud API (Infomaniak).

HOSTED · CH

Single-tenant

Isolated instance per customer in Switzerland, own key and audit trail.

INDICATIVE PRICING

HOSTED (CH)

from CHF 250 / month · annual plan

Isolated instance, data kept in Switzerland, 5 users included. Operated by iConference.

ON-PREMISE

from CHF 180 / month · annual plan

Runs on your hardware (requirements on consultation), 5 users included.

Indicative per instance/company. Concrete quote after a short conversation.

iConference AG

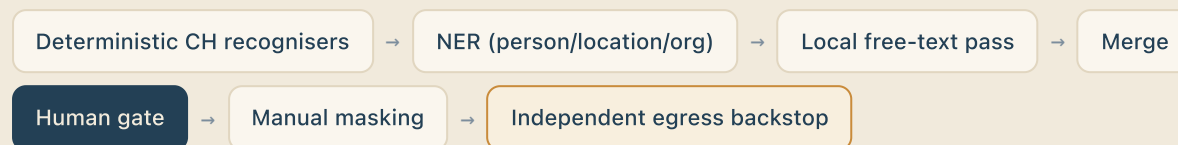
Grafenastrasse 15 · 6300 Zug · Switzerland
info@iconference.ch · iconference.ch

Try 30 days free

iconference.ch/ki-produkte

SECURITY ARCHITECTURE

Several independent layers, not one model



The egress backstop is a second, deliberately broader check before release, independent of the main recogniser, so a gap does not sit twice in the same layer.

WHAT STAYS PROTECTED

Everything encrypted at rest

All case data (original through standard terms) with AES-256-GCM, kept locally in your instance only; key held separately from the data volume. Deleted per click, verifiable in the audit chain.

Tamper-evident audit trail

HMAC-chained log, PII-free, every change provable.

Fail-closed everywhere

If a step fails (detection, scanned PDF without a text layer), the case aborts, rather than passing on unchecked data.

Egress control before release

If protected values remain in plain text, release is held and put to you for approval, recorded in the audit trail.

DETECTED DATA TYPES (SWISS FOCUS)



Your own protected terms can be stored as **standard terms**: encrypted, for all future documents.

Names, places and companies are detected language-independently by NER. Country-specific identifiers (e.g. German tax ID, commercial-register number) are available as a **recogniser module for your country on request**.

Newly detected: case numbers also in slash format, one- and two-digit date entries, and Romance-language land-register terms such as **foglio** and **particella**. Surnames stay protected across every spelling variant, even when a line break in the PDF splits them apart.

FORMATS & LIMITS

Supported: PDF with a text layer, Word (DOCX), Markdown, text, Excel (XLSX).

Scanned PDFs without a text layer are deliberately rejected (fail-closed). OCR is on the roadmap.

Limit 150,000 characters or 25 MB per upload.

MODELS

Name detection either fully local or via a Swiss cloud API.

Model-independent: protection rests on several independent check layers, not on a single model. You are not tied to any particular AI model.

POSITIONING

A pre-stage tool, not a platform

Sovereign Cockpit sits **in front of** anything you send out (a cloud model, email or handover) and replaces neither chatbot, RAG nor DMS. At its core: an enforced release by a human in the reversible flow and a tamper-evident audit trail; Swiss identifiers are recognised out of the box.