

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 is anonymised locally, every step stays provable in the audit trail — only the sanitised version goes out, on your click.

01

## Replace locally

Confidential data is detected on this machine 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 in every document.
- **Encrypted mapping.** Re-ID keys AES-256-GCM, auto-deleted after 24 h.
- **German & English.** Fully bilingual interface.
- **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, bcrypt, 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. No data egress, your own hardware.

### HYBRID

#### Your DC + Swiss cloud

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

### HOSTED · CH

#### Single-tenant

We run an isolated instance per customer in Switzerland — own key, own audit trail.

## INDICATIVE PRICING

HOSTED (CH)

**from CHF 250** / month · annual plan

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

ON-PREMISE

**from CHF 180** / month · annual plan

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

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

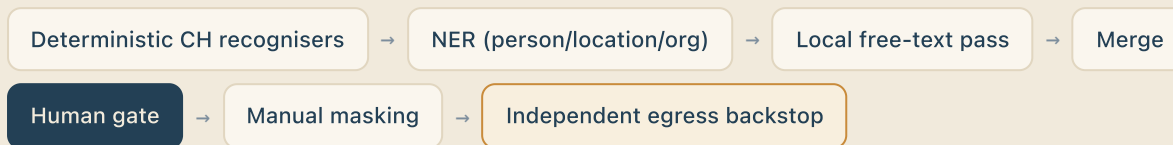
## iConference AG

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

Try 30 days free  
[iconference.ch/ki-produkte](https://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

### Mapping encrypted

Re-identification keys with AES-256-GCM. Auto-deleted after 24 h (window configurable) — after that re-identification is no longer possible.

### Fail-closed everywhere

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

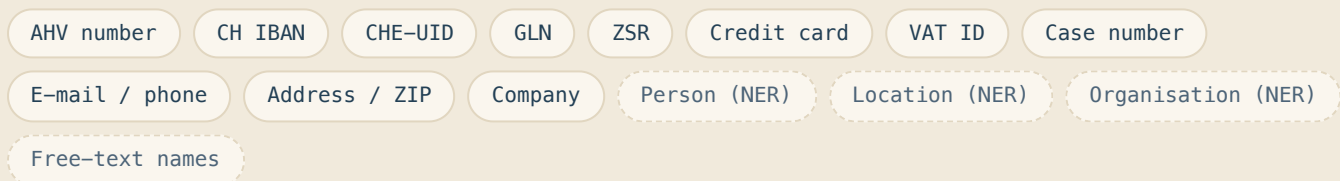
### Tamper-evident audit trail

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

### Egress control before release

If protected values remain in plain text, release is held and put to you for approval; a deliberate release is 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.

## FORMATS & LIMITS

**Supported:** PDF with a text layer, 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.