

AI-ready documents. Without sending identities.

Anonimotor is a local gateway between your staff and cloud AI such as ChatGPT, Claude or Copilot. It pseudonymises personal data before anything leaves your premises, then restores the real data in the answer.

Pseudonymised before sending

Maria Rossi	→	[PERSON_7f3a]
756.xxxx.xxxx.xx	→	[ID_19c2]
maria.rossi@uni.ch	→	[EMAIL_4b1d]
12.03.2026	→	[DATE_8e21]

Example data

→ Cloud AI



The external AI provider receives no identifying data; the key never leaves your premises.

Your data. Your rules. Your control.

The challenge

Researchers, lab teams and administrative staff want cloud AI to summarise reports and draft documents. But those documents contain personal data: names, dates, contact details, ID numbers, health information. Sending them as they are to an external provider raises hard questions.



Who sees the names in our documents?



What about health data and data about minors?



Cloud AI without uploading identities?

How it works

1**Staff work as usual**

Requests to ChatGPT, Claude or Copilot go through Anonimotor, an OpenAI-compatible proxy on your premises.

**2****Identities become placeholders**

Names, emails, phones, IBAN, ID numbers, dates:
Maria Rossi → [PERSON_7f3a].
If it can't check, nothing is sent.

**3****Real data restored**

The cloud AI answers with placeholders; Anonimotor puts the real data back for your user.

Key benefits

**Personal data detection**

Names, emails, phones, IBAN, AHV/AVS, DNI/NIE, dates, licence plates.

**Fail-closed by default**

If Anonimotor can't check a request, nothing is sent.

**Re-identification under your control**

Keys and mappings are managed in your infrastructure.

**Purpose-aware policies**

Strict handling of health data and data about minors.

**Audit without personal data**

Oversight without creating new records of identities.

**Your formats, five languages**

Word, Excel, PowerPoint, PDF, text; OCR optional. ES, DE, FR, IT, EN.

Built for real-world requirements.

On-premise, on standard CPUs, no GPU needed. It sits between your staff and the cloud AI services they already use.

How it differs

	DIY toolkits (e.g. Presidio)	Cloud DLP (Google, AWS, Azure)	Anonimator
Where your data is processed	– Locally (library)	✗ In the provider's cloud	✓ On your premises
Fail-closed gateway in front of cloud AI	✗ No, building blocks to assemble	✗ No built-in AI proxy	✓ Yes: nothing leaves unchecked
Real data restored in the AI answer	– Only if you build it	– Varies by service	✓ Automatic
Re-identification key	– Up to you	✗ Data goes to the provider	✓ Keys and mappings protected under your security policies

Other on-premise tools also keep data local. Anonimator's focus: one ready-to-run, fail-closed gateway with automatic re-identification, not a toolkit you have to assemble.

Typical use cases



Lab & research reports

Study documents, analytical results, clinical texts.



Documentation & correspondence

Applications, records and emails with personal data.



Internal knowledge

SOPs, technical documentation, project reports.



Teaching & administration

University staff using cloud AI with real files.



Pre-release · demo on request

Closed-source, on-premise product by Castellon.CH.

Built around your control

- ✓ Personal data is pseudonymised before anything leaves your premises
- ✓ Keys and mappings are managed in your infrastructure
- ✓ Fail-closed: if it can't check, nothing is sent
- ✓ Audit and oversight without new records of identities
- ✓ Helps with your data-protection obligations; it does not replace them



Anonimator MCP server: coming soon

Ask us to keep you informed.

Contact us / Request a demo

Write to us to request a demo of Anonimator for your lab, life-science company or university.

Email antonio@castellon.ch

 Antonio Castellon · Castellon.CH

 antonio@castellon.ch

 +41 76 689 13 69

 castellon.ch

 Biel/Bienne, Switzerland