

USER DOCUMENTATION

Sovereign Cockpit

The manual for daily use: anonymise, review, release, re-identify, plus managing standard terms, cases and user accounts.

Contents

- | | |
|--------------------------------------|--------------------------------------|
| 1. The core principle | 8. Releasing and downloading |
| 2. Signing in, language, signing out | 9. Re-identifying a response |
| 3. Anonymising a document | 10. Managing cases |
| 4. Reviewing detected terms | 11. Users and roles (administration) |
| 5. The review page | 12. Security and data storage |
| 6. Masking terms manually | 13. Limitations and tips |
| 7. Standard terms | 14. Messages and help |

1 The core principle

Sovereign Cockpit sits **before** anything is sent outside: to a cloud AI model, by email or as a hand-over. Confidential data is detected and replaced with placeholders such as `<PERSON_1>` or `<AHV_1>`. Only the sanitised version leaves the system, and only through your explicit click in the **human gate**. The link placeholder ↔ original (the **mapping**) stays encrypted on the server; the Cockpit uses it to put the original values back into the AI model's response.

Three principles shape how you work with it:

- **You decide.** Every replacement is visible and can be deselected; every delivery needs your click.
- **Fail-closed.** If a processing step fails, the case stops with a clear message: the system never silently protects less data.
- **Traceable.** Every step (anonymisation, release, deletion) is recorded in a tamper-evident audit trail.

2 Signing in, language, signing out

You reach your Cockpit at your instance's address (e.g. `https://<your-instance>.iconference.ch`). Sign in with your username and password; accounts are created by your administrator (chapter 11).

- **Language:** switch between DE and EN at the top right, at any time, without losing data.
- **Change password:** under **Profile** (at least 10 characters).
- **Sign out:** at the top right. After a longer period of inactivity the session ends automatically.

3 Anonymising a document

On the **Anonymise** start page you have two options:

- **Paste text:** directly into the text field (up to 150,000 characters).
- **Upload a file:** PDF (with a text layer), Word (.docx), Markdown (.md), text (.txt) or Excel (.xlsx), up to 25 MB.

The **label** is optional and helps you recognise the case in the case list; if left empty, the file name (or "Direct entry") plus the date is used.

Scanned PDFs are rejected. A PDF without a text layer (photo/scan) cannot be protected reliably: the Cockpit deliberately stops instead of guessing unsafely. Convert the document to searchable text with an OCR solution first, or use the text source.

- **Excel:** cells, sheet names, comments, headers/footers and text literals in formulas are checked; numbers and formula structure remain untouched. Postal-code and date-of-birth columns are recognised by their column header (e.g. "PLZ", "Date of birth") and offered as maskable values, even though Excel stores them as numbers or dates.
- **Markdown:** passes through with its formatting: headings, lists and markup are preserved, and the downloads again carry the .md extension.
- **Word (.docx):** paragraphs, tables, headers and footers, footnotes, endnotes, comments and text boxes are checked; layout and formatting are preserved, and the downloads again carry the .docx extension. Rejected are documents with active tracked changes, embedded objects, and password-protected or legacy .doc files. Accept or reject the tracked changes, or save as a clean .docx.

While processing runs, the Cockpit shows a live progress indicator with a seconds counter. If the instance's first start takes longer (cold start), a separate notice points this out.

4 Reviewing detected terms

After you start, the Cockpit shows the original text with all detected items. A checklist at the top summarises how many items are masked automatically and how many company, person, date-of-birth and role matches are waiting for review. The suggestions are grouped into four areas:

- **Automatically masked.** A collapsed collection section for unambiguous identifiers (AHV, IBAN, company UID, e-mail/phone, case numbers, property IDs, addresses ...), all pre-selected; the header shows the count per type.
- **Company and person cards.** One card per company or person: every spelling found in the document (Dr., Mr./Mrs., initials, short forms ...) appears on it as an individually deselectable, pre-selected chip. A detected date of birth also appears as a pre-selected chip directly on the person card. Every spelling of the same person or company runs on the same placeholder. Re-identification then consistently inserts the full form, so the anonymised text stays readable and consistent.
- **Roles.** Contract roles (e.g. seller, executor) appear as pure information. They are not masked and are not part of the review decision.
- **Dates & locations / Other.** Two expandable groups for the rest: "Dates & locations" gathers dates, place names and postcode/town entries in one place; "Other" holds the remainder. This group holds only real place names, checked against the official register of towns; generic domain, role and document terms (such as GmbH, annual profit, lawyer, tenancy agreement) that the detection wrongly took for a place, a person or an organisation land in "Other". Neither group is pre-selected.

Domain vocabulary from legal and technical fields (e.g. M&A, inheritance law, land register, construction and finance) shows up far less often as a review candidate thanks to this structure. The professional review stays with you; the effort involved drops noticeably.

If a term is missing from the suggestions, add it right here in the "Anything missing?" field: the Cockpit masks it including inflected forms and compound words (example: "WEKO" also covers "WEKO-Vorabklärung").

- **Very short matches** (names, organisations and locations of two characters or fewer, such as initials or abbreviations) are not offered as suggestions. Such abbreviations do not identify anyone on their own and would only clutter the list. If you still want to mask a specific abbreviation, add it as a standard term or mask it manually.

Whatever you leave unticked stays in plain text and leaves the system unmasked. When in doubt, tick it: the review page shows the result, and every decision can still be corrected.

Your standard terms are found here automatically and are always pre-selected.

5 The review page

After confirmation, a **case** with a unique number is created. The review page shows:

- the **anonymised text** with placeholders highlighted,
- the **mapping** (original ↔ placeholder ↔ type): it stays on the server and is not part of the anonymised version,
- the tool for manual masking and the download buttons (human gate).

Proofread the anonymised text before you hand it out. Reviewed does not mean guaranteed complete: what gets replaced is what was detected and ticked.

If you leave the page via the navigation, the Cockpit asks for confirmation. The case is not lost; it remains accessible under **Cases**.

6 Masking terms manually

The safety net for anything the detection missed or that you did not tick in the gate: type the term into the "**Mask terms manually**" field and click "Mask". This is the same field as "Anything missing?" in the gate (chapter 4), including inflected forms and compound words.

- **Several terms** at once: separate them by comma or one per line, each gets its own placeholders.
- **All occurrences** are replaced, regardless of upper/lower case; this includes ss/ß variants ("Strasse" finds "Straße" and "STRASSE") and multi-word terms broken across line breaks.
- **Spelling-faithful**: every spelling found in the text gets its own mapping entry: re-identification restores each one exactly.
- **Clear feedback**: terms that do not occur in the text are reported clearly by the Cockpit ("Not found in the text: ..."), nothing disappears silently.
- **"Remember as standard"**: additionally adds the entered terms to the standard terms. They take effect from the next anonymisation onwards, even if they did not occur in the current document.

7 Standard terms

Standard terms are your instance's personal "always anonymise" list: your own company name, customer names, project and product codes. They are found automatically in **every future document** (regardless of upper/lower case, including joined spellings, e.g. "UCP" also finds "UCPlattform") and are pre-selected in the gate.

- **Adding:** on the **Standard terms** page, several terms by comma or one per line. Or directly while masking manually, via the "Remember as standard" checkbox.
- **Removing:** in the list, with one click. Cases already masked remain unchanged.
- The list is stored encrypted and applies to the whole instance.

8 Releasing and downloading (human gate)

Only when you click a download button does the anonymised version leave the server. Every delivery is sealed in the audit trail with a checksum.

FORMAT	PURPOSE
.txt / .md	Recommended for the return path (re-identification) for text responses. Markdown sources are delivered as .md, otherwise .txt.
PDF	A plain delivery document with a notice footer, not intended for re-identification.
Excel	For Excel sources: the anonymised workbook, cell by cell, with numbers and formulas untouched.
Word	For Word sources: the anonymised document as .docx, with layout preserved: paragraphs, tables, headers and footers.
Mapping (CSV)	Confidential: contains the re-identification keys in plain text. Store it securely only, do not pass it on. The download asks for confirmation as a safeguard.

Residual-risk warning: before delivery, an independent egress check inspects the final version once more. If it still finds critical values in plain text (e.g. AHV, IBAN, CHE-UID, contact details or one of your standard terms), the download stops and lists the affected values individually with context. You can mask each value right there ("mask" or "Mask all"), or deliver the document deliberately as it is; a deliberate release is recorded in the audit trail.

9 Re-identifying a response

The external AI model's response still contains the placeholders. Under **Re-identify**, paste it in, as text or as a file (PDF, Word, Markdown, text, Excel), together with the case number (it is pre-filled if you come from the review page).

- The Cockpit replaces every placeholder with the original value, faithful to the original spelling.
- **Excel responses** (e.g. the model's analysis as a workbook) are re-identified **cell by cell** and returned as an Excel file: columns added by the model are preserved, and postal codes and dates of birth come back as real number and date cells provided they remain in their original position.

- **Word responses** are uploaded as .docx and returned **structure-preserving**, re-identified as a Word file.
- **Unknown placeholders** (e.g. altered by the model) are marked in red rather than guessed.
- Download the re-identified version as .txt/.md, PDF, Excel or Word.

Opening an already re-identified case: a case that has already been re-identified can be opened directly from the case list and immediately shows the re-identified version for download, without any further input.

The case is then complete: after re-identification no further masking is possible. The manual-masking tool is then hidden, "Back to review" is dropped, and opening the review page redirects to the re-identified version. To mask something else, start a new run.

10 Managing cases

The **Cases** page lists all runs of the instance, newest first. Clicking the label reopens the case, including the review page, manual masking and downloads. The **case ID** is shown in the list and can be copied with a click, for example to paste it into the re-identification form. All timestamps in the list (created, last changed) are shown in Swiss local time.

COLUMN	MEANING
Status	anonymised, delivered, re-identified.
Integrity	A check against the tamper-evident audit trail: "intact" means the original, the anonymised version and the mapping are unchanged.
Cloud-NER tokens	Usage of the Swiss name-detection API for this case (hosted operation only).
Actions	Re-identify, Mapping (CSV) (with confirmation), Delete (with confirmation).

Retention: cases stay stored until you delete them. Deletion removes the entire record (original, anonymised version, mapping) and remains verifiable as an event in the audit trail. **Access:** a case is visible only to its creator and to administrators.

11 Users and roles (administration)

Administrators find user management at the top right under **Users**. Each instance keeps its own accounts, no external service, and it works offline too.

ROLE	PERMISSIONS
user	Anonymise, view/further-mask/re-identify/ delete their own cases, maintain standard terms, change their own password.
admin	In addition: view and manage all cases of the instance, create and remove users.

- **Creating users:** username + initial password (at least 10 characters) + role. A maximum of **5 users** per instance.
- **Passwords** are stored only as Argon2id hashes; hand the initial password to the new user through a secure channel. They change it under **Profile**.

- **Roles are checked afresh on every request:** revoking a role takes effect immediately.
- **The last remaining admin** cannot be deleted or demoted; the Cockpit reports this with a notice, so the instance is never left without administration.
- For separate companies or clients, the rule is: **one dedicated instance per company**, not shared accounts. Talk to us.

12 Security and data storage

- **Everything encrypted at rest:** all case artefacts (original, anonymised and re-identified version, source file, mapping, metadata) are encrypted with AES-256-GCM and never leave the instance; the master key is held separately from the data volume. The audit trail contains no document content, but does contain user names and case metadata in clear text.
- **Retention:** cases are kept until you explicitly delete them; deletion is complete and is recorded.
- **Audit trail:** HMAC-chained and PII-free: reordering, rewriting or inserting entries is detected.
- **Egress control:** a second, independent check before every delivery (see chapter 8).
- **Operation:** on-premise at your site or as an isolated single-tenant instance in Switzerland, operated by iConference. Details: datasheet and DPA.

13 Limitations and tips

- **Not 100% automatic:** detection works in several layers, but it is not infallible. Protection relies on the interplay with you: proofread, apply further masking, maintain standard terms.
- **Not supported:** scanned PDFs without a text layer (OCR is on the roadmap) and Word documents with active tracked changes or embedded objects. Accept or reject the tracked changes, or save a clean .docx.
- **Limits:** 150,000 characters per text, 25 MB per upload.
- **Plan the return path:** use the .txt/.md version for text responses. The PDF is purely a delivery format. Excel analyses can be uploaded as .xlsx and come back re-identified cell by cell, Word documents as .docx structure-preserving.
- **Large documents:** the free-text detection works in sections; for very long documents the analysis can take a few minutes.

14 Messages and help

MESSAGE

MEANING AND REMEDY

"Free-text pass failed"

The free-text detection was unreachable or reported an error: the case deliberately stops (fail-closed); nothing was processed unsafely. Wait briefly and try again; if the problem persists, contact support.

"No extractable text found — the PDF is probably scanned"

The PDF has no text layer. Provide the source as text/Markdown or convert it with OCR first.

"Format ... not supported"

Allowed formats are PDF (text layer), Word (.docx), Markdown, text and Excel (.xlsx).

"File too large"

The limit is 25 MB: split or reduce the file.

"Not found in the text: ..."

The term to be masked does not occur in the text. Check the spelling in the document (typo? written separately?).

"This case has already been re-identified or completed"

Completed cases allow no further masking. Start a new run.

Placeholder marked in red

The placeholder in the response is unknown to this case (often altered by the AI model). Check against the original and carry the passage over by hand.

Support: iConference AG · info@iconference.ch · iconference.ch