DATA PROCESSING AGREEMENT (DPA)

Processing of personal data

This agreement governs the processing of personal data by iConference AG on behalf of the Customer when operating the Sovereign Cockpit service, in accordance with the Swiss Federal Act on Data Protection (revFADP / revDSG) and, where applicable, Art. 28 GDPR.

Template — legal review required. This is a working template reflecting the technical facts of the Sovereign Cockpit service. Before signing it must be reviewed by qualified legal counsel and completed with the customer-specific details marked *in italics*.

1. Parties

CONTROLLER

Customer

Company name
Address
Represented by

PROCESSOR

iConference AG

Grafenaustrasse 15
6300 Zug · Switzerland
info@iconference.ch

2. Subject matter and duration

The Processor processes personal data solely to provide the Sovereign Cockpit service: anonymisation / pseudonymisation of documents uploaded by the Customer, secure storage of the re-identification mapping, and re-identification on the Customer's instruction. Processing lasts for the term of the underlying service agreement and ends with its termination.

3. Nature, purpose and categories

The **nature and purpose** of processing is the detection and masking of personal data within Customer documents so that only a sanitised version leaves the Customer's control. The **categories of data subjects and personal data** are determined by the Customer through the documents it uploads and are specified in Annex 1.

4. Instructions

The Processor processes personal data only on documented instructions from the Customer, including the operation of the service as configured. The Processor informs the Customer if, in its opinion, an instruction infringes applicable data protection law. Human-in-the-loop release: data leaves the system only upon an explicit release action recorded in the audit trail.

5. Confidentiality

The Processor ensures that persons authorised to process the personal data are bound to confidentiality and are trained accordingly. Access to a Customer instance is limited to named, authenticated user accounts.

Within the Customer's own team, a case is accessible only to the user who created it and to administrators, so that the Customer controls access among its own users.

6. Security of processing (technical & organisational measures)

The Processor implements appropriate technical and organisational measures. The measures in place for the Sovereign Cockpit are listed in Annex 2. They include, in particular: single-tenant isolation (one container per customer), encryption at rest of all case artefacts (AES-256-GCM; master key held separately from the data volume), auditable deletion of entire cases by the customer, a tamper-evident HMAC-chained audit trail, an enforced egress check before any release, transport encryption, authenticated access with per-case ownership, and hardening against denial-of-service.

7. Sub-processors

The Customer authorises the use of the sub-processor listed in Annex 3. The Processor imposes the same data-protection obligations on any sub-processor and informs the Customer of any intended change, allowing the Customer to object. For an on-premise deployment there is no sub-processor; name detection then runs locally.

SUB-PROCESSOR	PURPOSE	LOCATION
Infomaniak Network SA	AI API for name/entity detection (free-text NER) — hosted deployment only	Switzerland

8. Data location and international transfers

All processing takes place **in Switzerland** — either on the Customer's premises or on a Swiss-hosted single-tenant instance operated by the Processor. In the service as delivered there is **no transfer of personal data abroad** and no involvement of providers outside Switzerland.

9. Assistance to the Controller

The Processor assists the Customer, taking into account the nature of processing, in responding to data-subject requests and in meeting the Customer's obligations regarding security, breach notification and, where applicable, data protection impact assessments.

10. Personal data breach

The Processor notifies the Customer without undue delay after becoming aware of a personal data breach affecting the Customer's data, providing the information the Customer needs to meet its own notification duties.

11. Deletion and return

On termination the Processor deletes or returns the personal data at the Customer's choice, unless retention is required by law. All case artefacts are encrypted at rest and are deleted together with the rest of the case file on termination.

12. Audits

The Processor makes available the information necessary to demonstrate compliance with this agreement and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by it, subject to reasonable notice and confidentiality.

13. Governing law and language

This agreement is governed by Swiss law. Place of jurisdiction is *Zug, Switzerland* unless mandatory law provides otherwise.

This English version and the German version are equivalent in content. The contract shall designate *one language version as authoritative*.

ANNEXES

ANNEX	CONTENT
Annex 1	Categories of data subjects and personal data — completed by the Customer per contract (defined by the documents the Customer uploads)
Annex 2	Technical and organisational measures — see below
Annex 3	Approved sub-processors (see clause 7)

ANNEX 2

Technical & organisational measures

The measures below are in place for the Sovereign Cockpit as delivered. They implement the security obligations under clause 6.

AREA	MEASURE
Data location	All processing in Switzerland — on-premise or on a Swiss-hosted single-tenant instance. No transfer of personal data abroad.
Tenant isolation	One isolated container instance per customer, with its own encryption key and its own audit trail. No shared storage between customers.
Encryption at rest	All case artefacts — original, anonymised and re-identified version, source file, re-identification mapping, case metadata, user list, standard terms — are encrypted with AES-256-GCM and remain exclusively within the customer instance. The master key is held separately from the data volume and from the data backups, one per instance. The audit trail contains no document content, but does contain user names and case metadata in clear text. Cases are retained until deleted by the customer; deletion removes the entire record and is recorded in the tamper-evident audit chain. *Master-key responsibility: in hosted operation the Processor holds the key escrow; in on-premise operation the Customer (loss of the key means total loss of the data). — Draft, legal review pending.*
Encryption in transit	TLS is enforced for the web interface and for any call to the Swiss name-detection API (hosted deployment).
Access control	Named, authenticated user accounts (bcrypt password hashing, works offline). Within the customer's team a case is accessible only to its creator and to administrators; role checks are read fresh on every request.
Egress control	Data leaves the system only on an explicit human release. A fail-closed egress check holds the release if protected values would remain in plain text; a deliberate release is recorded.
Auditability	Tamper-evident, HMAC-chained and PII-free audit log; reordering, rewriting or injected entries are detected.
Web hardening	Content-Security-Policy with per-request nonce, HSTS, X-Frame-Options DENY, CSRF protection on all state-changing requests, login rate limiting; public API documentation disabled in production.
Resource protection	Container memory limit and request concurrency limit; upload size and decompression limits — a single request cannot exhaust the host (denial-of-service hardening).
Deletion	On termination personal data is deleted or returned at the customer's choice. The customer can fully delete any case at any time; every deletion is recorded in the audit chain.

Measures reflect the service as delivered and may be updated to equivalent or stronger measures over time. This annex is part of the DPA and is subject to legal review before use.

Customer (Controller)
Name, date, signature

iConference AG (Processor)
Name, date, signature

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