

Dokcheck

Data-processing agreement

UNSIGNED REVIEW DRAFT - 21 October 2026

This template is not an executed agreement or a certification. Complete the annexes and obtain appropriate review before processing real client data. The English template does not replace any required local-language contract.

1. Parties and scope

Provider / processor: **Fibuag AG**, Oberneuhofstrasse 5, 6340 Baar, Switzerland, operating Dokcheck by Krascorp. Customer: [legal name, address, authorised representative and privacy contact]. Effective date: [date]. Main service agreement: [reference]. Where the customer acts for its own clients, it confirms authority to appoint a subprocessor.

The processor handles personal data only to provide the instructed document intake, security checks, reading, company/period matching, filing, archive search, document requests, staff collaboration and invoice-draft features. The customer defines approved requirements, contacts, access and billing rules. All suggestions are not accounting or tax advice. Invoice approval remains with an authorised person.

2. Instructions and confidentiality

Documented instructions comprise the completed service agreement, this agreement and authenticated workspace instructions from authorised customer staff. The processor shall notify the customer if an instruction appears unlawful, unless prohibited by law. Access is limited to authorised persons bound by confidentiality, including personnel supporting the service. The customer remains responsible for its lawful basis, transparency notices and the accuracy of instructions.

3. Security obligations

The processor shall maintain appropriate technical and organisational measures, considering the nature and risk of the processing. Annex B records the current measures and operational limits. Material changes shall not reduce the agreed overall protection without notice and agreement where required. The customer shall manage user access, set an appropriate MFA policy, protect credentials and review uncertain matches.

4. Assistance and incidents

Taking account of the service and available information, the processor shall assist with data-subject requests, security assessments and regulatory obligations. Requests received directly shall be referred to the customer unless legally required otherwise. The processor shall notify the customer without undue delay after becoming aware of a personal-data breach, provide available nature, impact and mitigation details, and update the notice as facts emerge. Customer incident contact and notification channel: [complete].

Instructions and safeguards

5. Subprocessors and international transfers

The customer authorises only the subprocessors and processing activities listed in completed Annex C. The processor shall impose appropriate data-protection obligations and remain responsible for their contracted processing obligations. Proposed additions or replacements require prior notice of at least [agreed number] days and an agreed objection/remedy process. Do not sign while subprocessor legal entities, countries and transfer safeguards remain unspecified.

EU restrictions on the R2 original-file bucket do not establish an EU-only boundary for the complete application, metadata, support, email or AI processing. International transfers require the applicable assessment and safeguards under the Swiss FADP and, where applicable, the GDPR. Specify applicable adequacy decisions or contractual safeguards, including any Swiss adaptations, in Annex C. No Swiss-only processing, zero provider retention or unverified residency arrangement is promised.

6. Evidence and audits

The processor shall make available information reasonably necessary to demonstrate its obligations and allow appropriate agreed audits or inspections, protecting other customers and system security. Workspace audit history covers filing, changes and approvals; it is not represented as a complete log of every file read. Audit scope, scheduling and allocation of costs: [complete].

7. Return, deletion and retention

On termination, the processor shall return or delete personal data as the customer chooses, unless applicable law requires retention. Agree an export window, deletion deadline, backup expiry and treatment of issued invoices in Annex D. Backups remain protected during their lifecycle and restored data must again follow applicable deletion instructions. No retention period is accepted by leaving these fields blank.

8. Priority, term and signatures

This agreement applies for the duration of instructed personal-data processing. Mandatory law prevails; this agreement governs data protection where it conflicts with the main service agreement. Governing law, venue and liability terms follow the reviewed main agreement, subject to mandatory data-protection rules. Both parties must complete the annexes and approve the final document before signature.

Customer: [name / position / date / signature]

Fibuag AG: [authorised representative / date / signature]

Processing annexes

Annex A - Data and people

Purpose: document organisation, requested-document collection and invoice preparation. Duration: service term plus agreed export/retention periods. People may include customer staff, client contacts, suppliers, customers, employees and other people named in uploaded records. Data may include business/contact information, email content and attachments, invoices, bank transactions, payroll, financial and tax records. Special-category or otherwise sensitive records: [identify, justify and agree handling before upload]. Customer-approved mailbox folders/labels and historical-import scope: [complete].

Annex B - Current technical and organisational measures

Private EU-jurisdiction R2 bucket for original files; HTTPS and storage encryption; authenticated access checked by workspace and client; configurable authenticator MFA and owner-enforced policy; malware quarantine and retries without bypass; preserved originals and reviewed filing changes; encrypted backups with isolated recovery checks and original-file checksums; activity history for filing, edits and approvals; scoped AI retrieval and staff approval for invoices. Confirm availability targets, retention, restore objectives, administrator access and support procedures in the final agreement.

Current operational limitation: private scanning and large-document preparation run on an operator-managed workstation that must remain online. Its physical location, responsible operator, access controls, deletion of temporary files and always-on hosting arrangement must be completed here before production client-data processing. No independent security certification or external security review is claimed.

Annex C - Provider and transfer register (complete before signature)

Cloudflare: Application/metadata hosting and EU R2 original storage. Contracting entity, all relevant processing/support countries, DPA and transfer mechanism: [confirm]. A Western Europe database location hint is not a residency guarantee.

OpenAI: Relevant authorised document content, pages or records for AI assistance. API requests use store:false. API data is not used for training by default unless the account opts in. Standard abuse-monitoring content retention may be up to 30 days with documented exceptions; other feature retention may apply. Contracting entity, account sharing settings, countries, retention controls and transfer mechanism: [confirm].

Resend: Transactional email delivery to approved recipients, using necessary contact/message data. Contracting entity, processing locations, retention, DPA and transfer mechanism: [confirm].

Microsoft / Google: Customer-selected mailbox services under the customer connection and permissions. Identify tenant/provider, folder/label, shared-mailbox scope, applicable contracts and respective controller/processor roles: [complete].

Before signature and rollout

Annex D - Required commercial and retention decisions

Complete: customer and provider signatories; main agreement; privacy and incident contacts; customer processing purposes and data categories; sensitive-record handling; approved mailbox scope; processing workstation location; provider legal entities and subprocessors; international-transfer assessment and safeguards; subprocessor notice period; MFA policy; support-access procedure; incident escalation; availability and recovery objectives; export format/window; deletion deadline; backup retention/expiry; statutory invoice-retention treatment; audit arrangements.

Reference documents for review

[Swiss FDPIC: cloud processing](#)

[Swiss FDPIC: outsourcing](#)

[Cloudflare: R2 location](#)

[Cloudflare: R2 data security](#)

[OpenAI: API data controls](#)

The references describe provider policies, not a confirmation of this customer account configuration. Verify the final contractual and technical state before signing. This document deliberately leaves unconfirmed terms visible rather than treating them as agreed.