

Annex 1 to the data processing agreement

Technical and organisational measures (TOM)

As of
11 October 2026

Publisher
IonKon GmbH

Contents

Overview	3
1.1 Physical access control	3
1.2 System access control	3
1.3 Access control (authorisation)	3
1.4 Separation control	4
1.5 Pseudonymisation and data minimisation	4
2.1 Transfer control (transport)	4
2.2 Storage encryption	4
2.3 Input control	5
3 Availability and resilience	5
4.1 Development and change process	5
4.2 Deletion concept	6
4.3 Sub-processor oversight	6

Overview

Annex 1 to the data processing agreement under Art. 28(3)©, Art. 32 GDPR. The processor is IonKon GmbH, Dessauer Straße 280, 06886 Lutherstadt Wittenberg, Germany.

Subject matter of the processing: one-off processing of the documents provided by the customer to produce a customer-specific language model, delivery on a local AI server, subsequent deletion. After delivery, IonKon carries out no ongoing processing of customer data; the model runs entirely at the customer's premises.

1.1 Physical access control

- Customer data is processed and stored exclusively in data centres of infrastructure partners within the EU or Switzerland; IonKon does not operate its own servers holding customer data on its business premises.
- Physical security of the data centres is the partners' responsibility; the register of sub-processors used, with registered office and purpose, is set out in Section 7 of the DPA and Section 4.3 of this TOM.
- Device policy: staff work devices are secured with full-disk encryption and automatic screen lock.

1.2 System access control

- Access to production systems is restricted to a minimal group of people documented by name; the list is disclosed on request.
- Programmatic access to the training API requires secret API keys (at least 32 bytes of randomness); keys are never kept in source code, only as environment variables or from a secret store. An automated hardening check refuses to start production with placeholder or short keys.
- Integration interface for our own customer management system: access only with credentials issued per purpose and limited to individual permissions (reading orders, reading customer data, activation, order control).
- Customer portal: password-based accounts (scrypt), email verification before ordering, one-time tokens (hashed, single-use) for sign-in and reset links, brute-force limiting per email/IP combination.

1.3 Access control (authorisation)

- The integration interface checks the issued permission on every call; every access is logged with time, outcome and the record concerned.
- Database access follows the least-privilege principle: the application's runtime credential has no schema rights (DDL); migrations run through a separate credential in a dedicated, one-off migration step. A versioned check script enforces the rights assignment fail-closed.
- The audit log is append-only; retroactive changes are excluded by database permissions.

1.4 Separation control

- Strict per-customer silo separation: every order produces its own model built exclusively from that one customer's documents. Mixing training data or models between customers is not provided for in the process and is technically prevented through order-bound storage paths and order-bound encryption contexts.
- Each training order spins up its own dedicated GPU instance, which is destroyed after completion on every outcome (success, failure, abort); unencrypted intermediate state on the instance is deleted.
- The website database (accounts, orders, payment status) is fully separated from the processing database; customer documents never reach the website layer (upload goes directly into object storage, see 2.1).

1.5 Pseudonymisation and data minimisation

- Before training datasets are generated, the extracted text passes through its own PII filtering stage of the pipeline.
- The integration interface exposes only minimised order, customer and state data; uploaded customer documents are not reachable through it.
- No payment instrument data (e.g. card numbers) is stored; invoicing and payment reconciliation run through BuchhaltungsButler GmbH.

2.1 Transfer control (transport)

- All external connections are transport-encrypted (TLS/HTTPS); in production the application enforces HTTPS for public base and callback URLs fail-closed.
- Document upload uses short-lived, pre-signed forms (valid for 1 hour) directly into EU object storage, without passing through application servers.
- Status updates between processing and the website are HMAC-SHA-256-signed per message; messages with an invalid signature are discarded without side effects. Callback targets are checked against an allowlist (protection against SSRF), in production HTTPS-only to public targets.

2.2 Storage encryption

- Artefacts in object storage (corpus, datasets, model checkpoints, delivery packages) are encrypted on the application side with AES-256-GCM, using an envelope scheme: a separate data key per artefact, itself stored encrypted under the master key; the format is versioned and bound to the order context (no exchange between orders).
- The master key is kept separately from the encrypted artefacts and is subject to the same production hardening check as all secrets.

2.3 Input control

- Order state transitions are recorded with versioned timestamps (monotonic event sequence, protection against stale or ambiguous facts).
- Access through the integration interface is recorded with actor, action, resource and outcome in the append-only audit log.
- Uploads are validated on the server before acceptance; anything outside the agreed limits is rejected.

3 Availability and resilience

- Processing is orchestrated as a short-lived, resumable workflow (Temporal); aborted runs can be resumed deterministically or brought to a controlled failed state.
- Production containers run without root privileges with a read-only filesystem, with healthchecks, restart policies and resource limits; container images are pinned immutably by digest and are script-checked before rollout.
- A reconciliation job detects stuck orders and orphaned resources and follows up on them.
- Data backup: the two databases (training pipeline and website) are backed up via documented pg_dump exports; artefacts in object storage are held redundantly at Exoscale (Frankfurt am Main). The master key is kept separately from both backups, so that a single compromised component alone is not enough to decrypt anything.
- Because customer data is retained only for the duration of production (see 4.2), the damage from a total loss is structurally limited: the customer holds the source documents, and IonKon can repeat production.

4.1 Development and change process

This TOM is reviewed and updated as needed by IonKon's management at least once a year and whenever the processing changes materially.

- Changes go through version control with continuous integration: automated tests (web and backend), static analysis and a secret scanner (Gitleaks) before every merge.
- Security-relevant configuration defaults to fail-closed; test and development switches are technically ineffective in production (double guards against misconfiguration).
- Adversarial security reviews (red-team exercises) are carried out as needed, and their findings are demonstrably remediated.

4.2 Deletion concept

- Training data and IonKon's own model copies are deleted after the customer confirms receipt of the delivery; if the customer does not confirm despite two reminders, the contractual deemed-acceptance provision applies and deletion takes place at that point. Proof of deletion is provided automatically once deletion has taken place.
- Independently of this, a technical retention ceiling applies (default 30 days from delivery, absolute ceiling 180 days from the start of the order), after which artefacts are cleaned up automatically.
- Contact enquiries are automatically deleted after 365 days at the latest; deleting a customer account cascades to remove all associated personal data records at the website level.

4.3 Sub-processor oversight

- Complete register of sub-processors, each engaged under a data processing agreement: STRATO GmbH (Germany), operation of the web server and the database; DataCrunch Oy, cloud brand "Verda" (Finland), GPU compute for training and data synthesis; Akenes SA, trading as "Exoscale" (Switzerland), object storage in Frankfurt am Main and GPU compute for training and data synthesis in Frankfurt, Zagreb or Zurich according to available capacity; Hetzner Online GmbH (Germany), only with booked hosting, the customer's server in Germany or Finland; BuchhaltungsButler GmbH (Germany), invoicing and payment reconciliation. Processing of customer documents takes place only within the EU or Switzerland. No external AI provider is used; the substantive processing runs solely on the instance provisioned for the order.
- Instruction rights, audit rights and notification channels for data protection incidents are governed by the DPA (Section 9): IonKon notifies the customer of a breach of the protection of personal data without undue delay, at the latest 48 hours after becoming aware of it, via the contact address info@ionkon.de.