



Agreement under Art. 28 GDPR

Data Processing Agreement (DPA)

As of
11 October 2026

Publisher
IonKon GmbH

Contents

	Parties to the contract	3
1	Subject matter and duration of the processing	3
2	Nature and purpose of the processing	3
3	Type of data and categories of data subjects	3
4	Instructions	4
5	Confidentiality of staff	4
6	Measures under Art. 32 GDPR	4
7	Conditions for engaging sub-processors	4
8	Assistance in fulfilling the rights of data subjects	5
9	Support in complying with Art. 32 to 36 GDPR	5
10	Deletion or return after the contract ends	5
11	Evidence and audits	6
12	Liability, term, final provisions	6
	Annex 1 · Technical and organisational measures (TOM)	7

Parties to the contract

The processor is lonKon GmbH, Dessauer Straße 280, 06886 Lutherstadt Wittenberg, Germany. The controller is the customer who commissions an individual language model from lonKon via the customer account; the customer's name and address are set out in the main contract (accepted quote).

1 Subject matter and duration of the processing

The subject matter of this contract is the one-off processing of the documents uploaded by the customer to produce a customer-specific language model by lonKon, its delivery to the customer including the dataset generated from the customer data (return of derived data), and the subsequent deletion of the copies remaining at lonKon. Without booked hosting, lonKon carries out no ongoing processing of customer data after delivery; the delivered model then runs entirely on the customer's own hardware, with no further connection to lonKon. If the customer has booked hosting (§ 17 of the Terms), this contract additionally covers the ongoing operation of the model on a server rented by lonKon for the customer for the duration of the hosting: storage of the documents stored during operation, processing of the users' inputs and outputs, user accounts and the daily encrypted backup. If lonKon delivers a configured server, lonKon sets up the model and dataset on it before delivery; thereafter lonKon carries out no further processing.

This contract applies for the duration of the main contract and ends once lonKon has deleted all copies of the customer data created in the course of the processing. The deletion periods follow from the technical and organisational measures (Annex 1): deletion after the customer confirms receipt of the delivery, at the latest after the technical retention ceiling (default 30 days from delivery, absolute ceiling 180 days from the start of the order).

2 Nature and purpose of the processing

The processing serves exclusively to render the service described in the main contract: extraction and preparation of the documents uploaded by the customer, filtering of personal data, generation of synthetic training examples, the actual training of the customer-specific model, and its packaging for delivery.

For data synthesis, lonKon uses exclusively software it operates itself, running on a GPU instance provisioned solely for the respective order in the EU or Switzerland and deleted afterwards. No external AI provider is ever given access to the customer's documents; this is technically enforced.

3 Type of data and categories of data subjects

The subject matter of the processing is the documents uploaded by the customer as a ZIP file as part of the order, as well as the training and intermediate data derived from them (extracted text, synthetic training examples, model weights). Which personal data the documents contain in detail is determined by the customer through the choice of uploaded content; this may in particular include names, contact details and other information typical of business documents relating to the

customer's employees, customers and business partners. Special categories of personal data under Art. 9 GDPR are contractually excluded: the customer does not upload any such data. If processing special categories is nonetheless intended in an individual case, a separate written agreement with additional safeguards is required before the upload.

Categories of data subjects are the persons whose data is contained in the documents provided by the customer, in particular the customer's employees, customers and business partners.

With booked hosting, the documents stored during operation, the users' inputs and outputs and the user accounts (name, email address, login data) are added; the customer's users are additionally affected.

4 Instructions

lonKon processes the customer's data exclusively on documented instructions from the customer. The customer's acceptance of the quote in the customer account and the content of this contract constitute an instruction. Further or deviating instructions must be given in text form and confirmed by lonKon. If lonKon considers that an instruction from the customer infringes the GDPR or other data protection provisions, lonKon informs the customer without undue delay.

5 Confidentiality of staff

lonKon ensures that the persons authorised to carry out the processing have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and that the customer's data is accessible to them only to the extent required for their respective role.

6 Measures under Art. 32 GDPR

The technical and organisational measures taken by lonKon to ensure a level of security appropriate to the risk are set out in the technical and organisational measures (TOM) attached as Annex 1. The TOM form part of this contract.

7 Conditions for engaging sub-processors

lonKon engages the following sub-processors to perform this contract; the customer hereby grants general authorisation for their use. All providers named process the customer's data exclusively within the European Union or Switzerland; the European Commission has established an equivalent level of data protection for both.

STRATO GmbH (Germany): operation of the web server and database.

DataCrunch Oy, cloud brand “Verda” (Finland): GPU compute for training and data synthesis, a dedicated instance per order, deleted afterwards; processed in Finland.

Akenes SA, trading as “Exoscale” (Switzerland): encrypted object storage for the uploaded documents and, with booked hosting, for the daily backup in Frankfurt am Main, and GPU compute for training and data synthesis, a dedicated instance per order, deleted afterwards; processed in Frankfurt, Zagreb or Zurich. IonKon selects the region per order according to available capacity.

Hetzner Online GmbH (Germany): only with booked hosting; rental of the server on which the customer’s model is operated, in data centres in Germany (Nuremberg, Falkenstein) or Finland (Helsinki), location as stated in the quote.

BuchhaltungsButler GmbH (Germany): invoicing and payment reconciliation; receives only master data, no training documents.

If IonKon intends to replace a sub-processor or engage an additional one, IonKon informs the customer in advance in text form; the customer may object to the change for good cause within 14 days of receiving the notice in text form. If the customer does not object within this period, the change is deemed approved. IonKon contractually obliges every sub-processor to the same data protection obligations as set out in this contract.

8 Assistance in fulfilling the rights of data subjects

IonKon assists the customer, where possible, with appropriate technical and organisational measures in fulfilling its obligation to respond to requests from data subjects to exercise their rights under Chapter III of the GDPR (in particular access, rectification, erasure, restriction of processing, data portability and objection). If a data subject contacts IonKon directly with such a request, IonKon forwards the request to the customer without undue delay.

9 Support in complying with Art. 32 to 36 GDPR

IonKon supports the customer with the security of processing, with notifying the supervisory authority and the data subject of a personal data breach, and with data protection impact assessments and prior consultation of the supervisory authority. If IonKon becomes aware of a breach of the protection of personal data affecting the customer’s data, IonKon notifies the customer without undue delay, at the latest 48 hours after becoming aware of it, via the contact address info@ionkon.de; the notification includes at least the nature of the breach, the affected categories of data, the likely consequences and the measures taken, so the customer can meet its own 72-hour notification deadline under Art. 33 GDPR.

10 Deletion or return after the contract ends

The dataset generated from the customer data and the model are handed over to the customer with the delivery (return of derived data). After the processing ends, IonKon deletes all copies of the customer data held by it (uploaded documents, training data generated from them and its own model copies) at the latest after the technical retention ceiling expires (default 30 days from delivery, absolute ceiling 180 days from the start of the order). Once deletion has taken place, IonKon

automatically issues the customer with proof of deletion. Returning the source documents is not necessary, as the customer already holds the originals of the documents it uploaded. With booked hosting, § 17 (2) of the Terms applies to the server and the data stored during operation: the documents are made available for download on request within 30 days after the end of the contract, after which the server including the backups is deleted and proof of deletion is issued.

11 Evidence and audits

On request, lonKon demonstrates to the customer that it complies with the obligations set out in this contract and enables the customer, or an auditor engaged by the customer, to carry out audits, in particular by providing suitable evidence. The customer may audit compliance with this contract once a year and on specific cause; the customer gives 14 days' notice of on-site audits. Audits take place during lonKon's usual business hours, while preserving lonKon's trade and business secrets and the confidentiality and security of other customers' data, without unreasonably disrupting lonKon's operations. lonKon may instead provide the required evidence through current certificates or audit reports. The customer bears the cost of an on-site audit, except where the audit finds a material breach by lonKon.

12 Liability, term, final provisions

The liability provisions of the General Terms and Conditions apply, unless this contract provides otherwise. This contract begins upon its conclusion, at the latest before the customer's data upload, and ends once the customer data has been fully deleted. In the event of conflict between this contract and the main contract, this contract takes precedence in matters of data protection. The law of the Federal Republic of Germany applies.

Annex 1

Technical and organisational measures (TOM)

Overview

Annex 1 to the data processing agreement under Art. 28(3)©, Art. 32 GDPR. The processor is lonKon 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, lonKon 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; lonKon 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.