

ABOUT THIS PAGE · ADDED BY STRUKTÜRS, NOT PART OF THE DOCUMENT

Effective date

14 October 2026

Version

v=2026-10-14

Status

In force

Contracting party

Yorkville Advisors B.V., trading as Struktürs

This DPA forms part of the Terms of Service, so accepting the Terms accepts it. No separate signature is needed.

DOCUMENT TEXT

Effective date: 2026-10-14

# Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Terms of Service (the "**Terms**") between **Yorkville Advisors B.V.** (KvK 87502151), trading as Struktürs, Platinaweg 25, 2544 EZ The Hague, the Netherlands ("**Struktürs**", "**Processor**"), and the Customer named in the Terms ("**Customer**", "**Controller**"). It applies whenever Struktürs processes Customer Personal Data in providing the Service. Terms defined in the Terms have the same meaning here.

## 1. Definitions

- "**Data Protection Law**" means all laws on the processing of personal data that apply to the processing under this DPA, including the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK GDPR and Data Protection Act 2018, and the South African Protection of Personal Information Act, 2013 ("**POPIA**").
- "**Customer Personal Data**" means personal data within Customer Data that Struktürs processes on the Customer's behalf.
- "**Sub-processor**" means a third party engaged by Struktürs that processes Customer Personal Data.
- "**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

- "controller", "processor", "data subject", "personal data" and "processing" have the meanings given in the GDPR. Under POPIA, "controller" means "responsible party", "processor" means "operator", and "data subject" includes juristic persons where POPIA so provides.

## 2. Roles and scope

2.1 The Customer is the controller of Customer Personal Data and Struktürs is its processor. Annex I describes the processing.

2.2 This DPA does not apply to personal data for which Struktürs is a controller, such as account, billing, support and website data. Struktürs is an independent controller of Users' account and membership records and of its central audit record. That processing is described in the Privacy Policy.

2.3 The Customer is responsible for having a lawful basis for the processing it instructs, and for the accuracy of Customer Personal Data and the notices it gives to data subjects.

## 3. Instructions

3.1 Struktürs processes Customer Personal Data only on the Customer's documented instructions, including with regard to transfers to a third country, unless required to do otherwise by Union or Member State law or, for data subject to UK or South African law, the law of that country, in each case to which Struktürs is subject, in which case Struktürs will inform the Customer before processing unless the law prohibits it. The Terms, this DPA and the Customer's use and configuration of the Service are the Customer's complete instructions, together with any further instructions the parties agree in writing.

3.2 Struktürs will immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Law.

3.3 Struktürs does not sell Customer Personal Data, does not use it to train machine-learning models, and does not combine it with personal data from other customers or sources except as needed to provide the Service to the Customer.

## 4. Confidentiality

Struktürs ensures that every person it authorises to process Customer Personal Data is bound by a duty of confidentiality. Struktürs grants no routine human access to Customer Workspaces; access to Customer Data by Struktürs personnel is limited to break-glass access that is logged, or to access the Customer requests for support.

## 5. Security

5.1 Struktürs implements and maintains the technical and organisational measures in **Annex II** to protect Customer Personal Data.

5.2 Struktürs may update those measures, provided that the update does not reduce the overall level of protection.

## 6. Sub-processors

6.1 **General authorisation.** The Customer gives general authorisation for Struktürs to engage Sub-processors. The Sub-processors in use are listed in the **Sub-processor List** at [strukturs.ai/legal/sub-processors](https://strukturs.ai/legal/sub-processors) (**Annex III**).

6.2 **Notice and objection.** Struktürs will give at least **14 days' notice** before engaging a new or replacement Sub-processor, by updating the Sub-processor List and notifying the Customer by email. Where a change is needed urgently for security, to comply with law or to keep the Service running, Struktürs may make it at once and will notify the Customer as soon as practicable. The Customer may object on reasonable data protection grounds within 14 days of the notice. The parties will discuss the objection in good faith; if it cannot be resolved, the Customer may terminate the Terms and receive a pro-rata refund of prepaid fees for the unused period. Where a Sub-processor notifies Struktürs that it is appointing a new sub-processor of Customer Personal Data, Struktürs will pass on that notice as soon as practicable.

6.3 **Flow-down.** Struktürs engages each Sub-processor under a written contract that imposes data protection obligations meeting the requirements of Article 28(3) of the GDPR and the equivalent requirements of Data Protection Law, and remains liable to the Customer for each Sub-processor's performance of those obligations.

## 7. Data location and international transfers

**7.1 Storage.** Customer Data in the Workspace (files, figures and database) is stored in the region the Customer selects for its Workspace, except as set out in Annex I §6.

**7.2 Processing outside the selected region.** Some processing takes place outside that region, as set out in Annex I §6 and the Sub-processor List, in particular processing by AI Features.

**7.3 Transfer mechanisms.** Where processing involves a transfer of Customer Personal Data that requires a transfer mechanism under Data Protection Law, the parties rely on:

- (a) an adequacy decision or adequacy regulations covering the destination, where one applies (including the UK's adequacy regulations for transfers from the UK to the EU);
- (b) for onward transfers by Struktürs to Sub-processors in countries without adequacy, the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 ("**SCCs**"), Module Three (processor to processor), the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner (the "**UK Addendum**"), or the EU-US Data Privacy Framework and its UK Extension, as set out in Struktürs' contract with each Sub-processor (§6.3);
- (c) where Struktürs, as a processor established in the EU, returns or makes Customer Personal Data available to a Customer in a country without adequacy, the SCCs, Module Four (processor to controller), incorporated by reference with the elections in §7.4;
- (d) for transfers subject to POPIA, section 72(1)(a) of POPIA: each recipient is subject to binding agreements (this DPA, and Struktürs' agreements with its Sub-processors) that Struktürs has assessed as providing an adequate level of protection substantially similar to the conditions for lawful processing in POPIA. Where the Service asks a User to confirm a transfer, that confirmation is an additional basis under section 72(1)(b), to the extent the person confirming is, or may consent for, the data subject.

**7.4 SCC elections.** For the SCCs incorporated under §7.3(c): Clause 7 (docking clause) applies; Clause 11 optional language does not apply; Clauses 17 and 18: the law and courts of the Netherlands; Annexes I and II of the SCCs are completed by Annexes I and II of this DPA.

## **8. Assistance**

**8.1 Data subject requests.** Struktürs will, taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures to respond to requests from data subjects. If Struktürs receives a request directly, it will refer the data

subject to the Customer without responding substantively, unless the law requires otherwise.

**8.2 Impact assessments and consultation.** Struktürs will provide reasonable information to help the Customer carry out data protection impact assessments and prior consultations with supervisory authorities, in relation to the Service.

## 9. Security Incidents

9.1 Struktürs will notify the Customer **as soon as it becomes aware** of a Security Incident affecting Customer Personal Data, whatever the Customer's country. This also meets section 21(2) of POPIA where POPIA applies. Struktürs' procedure is set out in its incident response runbook and is available on request.

9.2 The notification will describe, to the extent known, the nature of the incident, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Struktürs will provide further information as it becomes available. The contact point for a Security Incident is [security@strukturs.ai](mailto:security@strukturs.ai).

9.3 Struktürs will take reasonable steps to contain, investigate and mitigate the Security Incident. Notification is not an acknowledgement of fault or liability.

## 10. Return and deletion

10.1 On termination, Struktürs makes Customer Data available for export and then deletes it, as set out in section 16 of the Terms, unless the law referred to in §3.1 requires Struktürs to retain it. Residual copies held by Sub-processors, including in backups, are erased under their terms (for Google Cloud, within 180 days).

10.2 Struktürs retains an audit record of operations performed in the Service for the periods set out in Annex I §5: seven years for governance actions, and between 90 days and five years for other operational event records, depending on the type. The audit record contains identifiers, timestamps and outcomes. It does not contain the contents of Customer documents.

## 11. Audits

11.1 Struktürs will make available the information reasonably necessary to demonstrate compliance with this DPA, including responses to security questionnaires and its documentation of the measures in Annex II.

11.2 If that information is not sufficient to demonstrate compliance, or a supervisory authority requires it, the Customer may carry out an audit, at its own cost, no more than once in any twelve months, on at least 30 days' written notice, during business hours, through an independent auditor bound by confidentiality, and without access to other customers' data.

## 12. Liability

Each party's liability under this DPA is subject to the limitations and exclusions in the Terms, except where Data Protection Law does not allow them.

## 13. Term and precedence

13.1 This DPA lasts for as long as Struktürs processes Customer Personal Data.

13.2 If this DPA conflicts with the Terms, this DPA prevails in relation to the processing of Customer Personal Data. If the SCCs or the UK Addendum conflict with this DPA, they prevail.

---

## Annex I — Description of the processing

**1. Parties.** Controller: the Customer, contact as set out in its account. Processor: Yorkville Advisors B.V., trading as Struktürs, Platinaweg 25, 2544 EZ The Hague, the Netherlands; contact [privacy@strukturs.ai](mailto:privacy@strukturs.ai).

**2. Subject matter and duration.** Provision of the Service under the Terms, for the term of the Terms and until deletion under section 10 of this DPA.

**3. Nature and purpose.** Hosting, storage, structuring, verification, analysis, indexing and retrieval of Customer Data; generation of statements, explanations, answers, knowledge articles and board packs, including with AI models; export and deletion; support; security and audit logging.

#### 4. Data subjects and categories of personal data.

| Data subjects                                                                                                           | Personal data                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Customer's Users                                                                                                    | Sign-offs and declarations (name, role, date), and actions recorded in the Workspace's own audit trail                                                                                                    |
| Individuals named in Customer Data, such as employees, directors, shareholders, customers and suppliers of the Customer | Whatever the Customer includes in uploaded records, documents, questions and knowledge articles: typically names, roles, and amounts attributable to them (for example payroll or director loan accounts) |
| Meeting attendees, if the Customer uses meeting capture                                                                 | Name and role (not email)                                                                                                                                                                                 |

Special categories: none are required for the Service. The Customer should not upload special-category data unless it is necessary and lawful.

#### 5. Retention.

| Data                                                                                                                                                                                                                          | Retention                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Customer Data in the Workspace                                                                                                                                                                                                | Until deletion under section 16 of the Terms              |
| Audit record of governance actions (approvals and admissions, privacy requests, offboarding and encryption-key events; central, metadata only: identifiers, timestamps, outcomes; Users identified by an internal identifier) | 7 years                                                   |
| Other operational event records (for example processing, indexing and usage metering; metadata only)                                                                                                                          | Between 90 days and 5 years, depending on the type        |
| Exports of a Workspace's own audit trail held in retention-locked storage, where applicable. The Customer instructs Struktürs to keep them until their retention period ends                                                  | Until the retention period (7 years from creation) ends   |
| Service request logs                                                                                                                                                                                                          | 30 days                                                   |
| Residual copies in Sub-processors' backups                                                                                                                                                                                    | Erased on their schedules (Google Cloud: within 180 days) |

**6. Location of processing.** As set out in section 6 of the Privacy Policy. In summary:

|                                                 | United Kingdom Workspaces                                        | South Africa Workspaces                                          |
|-------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------|
| Customer Data at rest                           | London, UK                                                       | Johannesburg, South Africa                                       |
| AI generation                                   | Belgium (EU) (Claude via Vertex AI), London fallback (Gemini)    | Belgium (EU) (Claude via Vertex AI), London fallback (Gemini)    |
| AI embeddings and search indexes                | London, UK                                                       | London, UK                                                       |
| Document text extraction                        | EU (Document AI)                                                 | Not used                                                         |
| Service logs                                    | London, UK                                                       | Johannesburg, South Africa                                       |
| Audit record                                    | London, UK                                                       | London, UK                                                       |
| Onboarding, billing and administration services | London, UK                                                       | London, UK                                                       |
| Sign-in and email                               | United States (Clerk, Resend)                                    | United States (Clerk, Resend)                                    |
| Support correspondence                          | As set out in the Sub-processor List (HubSpot, Google Workspace) | As set out in the Sub-processor List (HubSpot, Google Workspace) |

**7. Frequency.** Continuous, for the term.

**8. Competent supervisory authority.** For the SCCs: the Autoriteit Persoonsgegevens (Netherlands).

## Annex II — Technical and organisational measures

### Isolation

- Each Customer has a dedicated Google Cloud project, with its own storage bucket and database. Isolation between customers is by architecture, not by shared-database access rules.
- Every service that serves a region checks that a Workspace belongs to that region, and refuses requests for Workspaces in another region.

## Encryption

- Customer Data at rest is encrypted with encryption keys that Struktürs manages in Cloud KMS (CMEK), held in the Workspace's region.
- Data in transit is encrypted with TLS.

## Access control

- Users authenticate through Clerk; every request to the platform carries a verified token, and the Workspace and user identity are derived from it.
- Internal services accept only authenticated service-to-service calls (Cloud Run IAM). The services that must accept requests from the internet check each one before any Customer Data is reached: the browser-facing services verify the user's Clerk sign-in, and payment notifications are verified by Stripe's signature.
- No service-account keys are issued; services use workload identities.
- Staff have no routine access to Customer Workspaces. Emergency (break-glass) access is temporary, logged and reviewed.
- Storage buckets enforce uniform access and public-access prevention.

## Logging and audit

- Operations in the Service are recorded in an append-only audit record, held centrally for the periods in Annex I §5, with Users identified by an internal identifier.
- Infrastructure and deployments are defined as code; deployments use immutable, versioned images and are recorded.

## AI safeguards

- AI providers are reached only through Google Cloud Vertex AI in fixed, configured regions; a service whose region is missing or wrong refuses to send the request instead of falling back to another region.
- Prompts are minimised to what a request needs; responses that stream to Users pass through an egress filter designed to redact credentials and personal contact details.

## Data lifecycle

- Exit export with a SHA-256 manifest; deletion of the Customer project, storage, database and platform records under an authorised, logged procedure.
- Data subject requests are logged and tracked against a 30-day deadline.

## Organisation

- Named owners for data protection ([privacy@struktors.ai](mailto:privacy@struktors.ai)) and security ([security@struktors.ai](mailto:security@struktors.ai)).
- Personnel with access to production are bound by confidentiality obligations.

## Annex III — Sub-processors

The Sub-processor List in force at [struktors.ai/legal/sub-processors](https://struktors.ai/legal/sub-processors), currently version v=2026-10-14.