

Data Processing Agreement (DPA)

This is Aletheia's Data Processing Agreement template for institutional customers. It sets out how Lonia AI, as Processor, handles personal data on behalf of a Customer institution, as Controller, when the Customer deploys Aletheia. It is written to be read by procurement, legal, and data protection teams during a security and privacy review.

Template version 1.0. Published: July 14, 2026.

This is a template DPA. Executed DPAs are countersigned per Customer institution. Effective dates, elected options, governing law, and annex details are completed at execution. Nothing on this page is a signed agreement or legal advice. To initiate DPA execution, contact legal@lonia.ai.

1. Preamble

This Data Processing Agreement (the "DPA") is entered into between **Lonia AI** ("Lonia", "Processor") and the customer institution identified in the applicable order or subscription ("Customer", "Controller"). It governs the processing of personal data that Lonia carries out on the Customer's behalf in providing the Aletheia service ("Aletheia" or the "Service"). The effective date of this DPA is the date of the Customer's subscription, or the date of signature where a countersigned copy is executed, whichever the parties elect at execution. This DPA forms part of, and is subject to, the agreement under which the Customer subscribes to Aletheia (the "Principal Agreement"). Where this DPA and the Principal Agreement conflict on the processing of personal data, this DPA governs.

2. Definitions

Terms used in this DPA have the meanings given in the applicable data protection law, in particular the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and, where applicable, the UK GDPR. The following terms apply:

- **Controller, Processor, Data Subject, Personal Data, Processing, and Sub-processor** have the meanings given in the GDPR.
- **Applicable Data Protection Law** means all data protection and privacy laws that apply to the processing under this DPA, which may include the GDPR, the UK GDPR, and United States federal and state privacy laws such as the California Consumer Privacy Act.
- **Aletheia-specific terms:** *Institutional Admin* means a person the Customer designates to manage the Customer's Aletheia account; *End User* means a person to whom the Customer assigns a seat (for example a student in a Campus deployment or an employee in an Enterprise deployment); *User Content* means the documents, images, and web content an End User processes with Aletheia; *Standard Contractual Clauses* or *SCCs* means the clauses approved by the European Commission for transfers of personal data to third countries.

3. Roles of the Parties

The Customer is the **Controller** of the personal data processed under this DPA and determines the purposes and means of that processing. Lonia is the **Processor** and processes personal data only on the Customer's documented instructions. Third parties that Lonia engages to process personal data on its behalf are **Sub-processors**; the current list is maintained at </legal/subprocessors> and summarised in Annex C. Where Applicable Data Protection Law treats a party as an independent controller for a specific processing activity (for example Lonia's processing of billing data as a controller for its own tax and accounting obligations), that activity is governed by Lonia's privacy policy rather than by this DPA.

4. Subject Matter and Duration

The subject matter of the processing is the provision of Aletheia to the Customer and its End Users. This covers accessibility conversion (optical character recognition, image description, content restructuring, and form labeling), audit logging of administrative and privileged actions, and the account operations needed to run the Service. The duration of the processing matches the term of the Customer's active subscription, plus the limited wind-down period described in Section 15 for deletion or return of data.

5. Nature and Purpose of Processing

Lonia processes personal data for the sole purpose of providing and supporting Aletheia in accordance with the Principal Agreement and the Customer's instructions. Because Aletheia processes User Content in the End User's own browser and stores it in a local library on the End User's device, Lonía does not receive or store User Content on its infrastructure. The personal data Lonía processes on its infrastructure is limited to account identity, plan and billing status, usage counts needed to enforce plan limits, and audit records of administrative and privileged actions. Lonía does not use personal data processed under this DPA to train AI models, and does not sell personal data.

6. Types of Personal Data

The categories of personal data processed under this DPA are:

- **Institutional Admin identity:** name, email address, and administrator role.
- **End User identity:** name and email address, as asserted by the Customer's Google Workspace or Microsoft 365 identity provider at OAuth sign-in.
- **User Content:** the documents, images, and web content End Users choose to process. This is handled in the End User's browser and on the End User's device; it is not stored on Lonía infrastructure.

- **Usage telemetry:** counts and metadata needed to apply plan limits and to maintain audit records, such as processing counts and administrative action logs. Aletheia runs no third-party analytics, advertising trackers, or session replay.

The Customer must not instruct Lonia to process special categories of personal data through the account and usage data channels described above except as an incidental part of User Content, which remains on the End User's device.

7. Categories of Data Subjects

- **Institutional Admins** designated by the Customer.
- **End Users** to whom the Customer assigns seats: students in a Campus deployment, employees in an Enterprise deployment, and, where a Customer extends access, other individuals it authorises.

8. Customer Obligations

The Customer, as Controller:

- Ensures it has a lawful basis for the processing it instructs, and that its instructions comply with Applicable Data Protection Law.
- Provides accurate account data and keeps its designated Institutional Admins current.
- Is responsible for the notices and, where required, consents due to its End Users under Applicable Data Protection Law, including notices required under FERPA where the Customer is an educational institution.
- Notifies Lonia without undue delay of a data subject rights request that requires Lonia's assistance, and does not respond on Lonia's behalf.

9. Processor Obligations

Lonia, as Processor:

- **Processes only on instructions.** Lonia processes personal data only on the Customer's documented instructions, including as set out in this DPA and the Principal Agreement, unless required by law, in which case Lonia informs the Customer of that legal requirement before processing unless the law prohibits it.
- **Ensures confidentiality.** Personnel authorised to process personal data are bound by confidentiality obligations.
- **Implements technical and organisational measures.** Lonia maintains the measures described in the [Security Whitepaper](#) and summarised in Annex B, including OAuth-only authentication with no password storage, encryption at rest and in transit, row-level security on every database table, append-only (write-once, read-many) audit logging, and per-institution data retention.
- **Assists with data subject rights.** Taking into account the nature of the processing, Lonia assists the Customer by appropriate technical and organisational measures in responding to data subject rights requests, as described in Section 12.
- **Assists with security and compliance.** Lonia assists the Customer with security incident notification, data protection impact assessments, and prior consultation with supervisory authorities, taking into account the information available to Lonia.
- **Deletes or returns data.** At the end of the Service, Lonia deletes or returns personal data at the Customer's choice, as described in Section 15.
- **Provides audit rights.** Lonia makes available the information necessary to demonstrate compliance with this DPA and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor it mandates, on reasonable prior notice, during normal business hours, and subject to confidentiality, so as not to compromise the security of other customers. Lonia may satisfy an audit request by providing its current documentation, including the Security Whitepaper, in the first instance.

10. Sub-processors

The Customer provides general authorisation for Lonia to engage the Sub-processors listed in Annex C and maintained at </legal/subprocessors>. Lonia imposes data protection obligations on each Sub-processor that are no less protective than those in this DPA, and remains responsible for each Sub-processor's performance. Lonia will give the Customer prior notice of the addition or replacement of a Sub-processor by updating the sub-processor list, and the Customer may object on reasonable data protection grounds within the notice period, in which case the parties will work in good faith to resolve the objection.

11. International Transfers

Aletheia's primary data store (Supabase PostgreSQL) is hosted in a single region in the **United States**, and Lonia's other Sub-processors listed in Annex C are United States providers operating global edge infrastructure. Where personal data of data subjects in the European Economic Area, the United Kingdom, or Switzerland is transferred to the United States or another third country, the transfer is made under an appropriate safeguard recognised by Applicable Data Protection Law, including the **Standard Contractual Clauses** where applicable, which are incorporated by reference in Annex D and completed at execution. The parties will implement any supplementary measures reasonably required for the transfer to be lawful. Lonia's transfer analysis is documented in more detail in the [Data Protection Impact Assessment](#), the scoped [Standard Contractual Clauses](#) covering the Lonia-mediated Enhanced AI image path for the Personal and Family consumer tiers, and the [Transfer Impact Assessment](#) for that path.

12. Data Subject Rights

Taking into account the nature of the processing and the information available to it, Lonia provides technical mechanisms to help the Customer meet data subject rights requests under the GDPR:

- **Access (Article 15):** Lonia can provide the account-level personal data it holds for an identified data subject.
- **Rectification (Article 16):** account identity data can be corrected; End User identity is refreshed from the Customer's identity provider at sign-in.
- **Erasure (Article 17):** account termination triggers cascade deletion of the account-level data Lonia holds. User Content is on the End User's device and is not held by Lonia. Append-only audit records are retained where retention is required by law or the applicable retention policy.
- **Restriction (Article 18):** a seat can be suspended so that processing is restricted while a dispute or verification is resolved.
- **Portability (Article 20):** an End User can export their local library from the product at any time, and account-level data can be provided in a structured, commonly used format.
- **Objection (Article 21):** the Customer can suspend or remove a seat to give effect to a valid objection to processing.

13. Security Incidents

Lonia notifies the Customer without undue delay, and in any event within **72 hours**, after becoming aware of a personal data breach affecting personal data processed under this DPA, consistent with GDPR Article 33. The notification describes, to the extent known, the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed. Lonia cooperates with the Customer and takes reasonable steps to mitigate and remediate the breach. Security concerns can be reported to security@lonia.ai.

14. Term and Termination

This DPA takes effect on its effective date and remains in force for as long as Lonia processes personal data on the Customer's behalf under the Principal Agreement. It terminates automatically when the Principal Agreement terminates, subject to the

survival of provisions that by their nature should survive, including confidentiality and the deletion and return obligations in Section 15.

15. Data Deletion and Return

On termination or expiry of the Service, the Customer may elect, within the wind-down period stated in the Principal Agreement, for Lonia to **delete** or **return** the account-level personal data Lonia holds. On deletion, account identity, plan, billing status, and usage records are removed by cascade. User Content requires no action by Lonia because it resides on End User devices and is not held by Lonia; End Users can export their local libraries from the product before their seats are removed. Lonia may retain personal data to the extent, and for as long as, required by law, and may retain append-only audit records for compliance; such retained data remains subject to the confidentiality and security obligations of this DPA.

16. Governing Law and Jurisdiction

This DPA is governed by the law and subject to the jurisdiction elected by the parties at execution, which is the Customer's choice within the reasonable constraints of the Principal Agreement. Absent an election, this DPA is governed by the laws of the State of New Jersey, United States, without regard to its conflict of laws principles, consistent with Aletheia's privacy policy, except that the Standard Contractual Clauses in Annex D are governed by the law they specify where they apply to a transfer.

17. Signatures

This template is executed by authorised representatives of each party at the time of contracting. The signature block below is completed at execution.

Signature block, completed at execution.

Field	Processor (Lonia AI)	Controller (Customer)
-------	----------------------	-----------------------

Field	Processor (Lonia AI)	Controller (Customer)
Signature	_____	_____
Name	_____	_____
Title	_____	_____
Date	_____	_____

Annex A: Processing Details

Annex A. Details of the processing.

Subject matter	Provision of Aletheia to the Customer and its End Users.
Duration	The term of the Customer's active subscription, plus the wind-down period in Section 15.
Nature and purpose	Accessibility conversion (OCR, image description, content restructuring, form labeling), audit logging, and account operations, solely to provide and support the Service.
Types of personal data	Institutional Admin identity (name, email, role); End User identity (name, email); User Content (on device, not held by Lonia); usage telemetry.
Categories of data subjects	Institutional Admins and End Users (students in Campus, employees in Enterprise, and other individuals the Customer authorises).
Frequency	Continuous for the duration of the subscription.

Annex B: Technical and Organisational Measures

Lonia maintains the technical and organisational measures described in full in the [Security Whitepaper](#). In summary:

- **Identity:** OAuth single sign-on only (Google Workspace and Microsoft 365), zero password storage, and least-privilege administrator roles with FERPA-privileged access as a separate, audited flag.
- **Encryption:** AES-256 encryption at rest for the managed database; TLS 1.3 in transit with HSTS; on Professional, browser-held bring-your-own-key material encrypted with AES-GCM-256 using a non-extractable key; on Enterprise, institution-managed bring-your-own-key material envelope-encrypted with a master key and stored encrypted at rest, decrypted by Lonia's Enterprise Worker only in memory at request time and never returned to any client.
- **Isolation:** row-level security on every database table, with institutional data scoped by institution identifier.
- **Audit:** append-only (write-once, read-many) audit logs with no update or delete policy, emitted through server-side procedures on privileged operations.
- **Retention and deletion:** per-institution retention (default 365 days) enforced by a scheduled deletion job, and cascade deletion of account data on termination.

Annex C: Sub-processors

The current Sub-processors are listed below and maintained at

[/legal/subprocessors](#). Bring-your-own-key AI providers are treated per tier. On the Professional tier the End User's browser calls the provider directly and no key or content passes through Lonia, so the provider is not a Lonia Sub-processor. On the Enterprise tier the institution's key is enrolled with Lonia's Enterprise Worker, which relays Enhanced AI request payloads to the institution-selected provider on the institution's behalf; for that path the provider receives content via Lonia infrastructure and is engaged as a Lonia Sub-processor, listed below and disclosed under the update-on-change policy.

Annex C. Current Sub-processors, region, and purpose.

Sub-processor	Region	Purpose
Supabase	United States	Managed PostgreSQL database, authentication, and account storage.
Cloudflare	Global edge, United States account	Static hosting (Pages), serverless compute (Workers), and bot protection (Turnstile).
Google	United States	OAuth sign-in (identity only).
Microsoft	United States	OAuth sign-in (identity only).
Stripe	United States	Payment processing and subscription billing.
OpenRouter (Enhanced AI on Personal and Family tiers)	United States	AI model routing for the opt-in Enhanced AI image description path on the Personal and Family consumer tiers only, mediated through Lonia's own OpenRouter account and covered by the scoped Standard Contractual Clauses at /legal/sccs . This entry covers only the Lonia-mediated consumer path; the Enterprise institution-managed bring-your-own-key path is listed separately below.
AI provider for Enterprise bring-your-own-key (institution-selected: Anthropic, OpenAI, or OpenRouter)	User-selectable per institutional enrollment	On the Enterprise tier only, the institution-selected provider receives Enhanced AI request payloads relayed by Lonia's Enterprise Worker using the institution's own enrolled key, decrypted in memory at request time. Engaged as a Lonia Sub-processor for this path; the transit through Lonia's Cloudflare and Supabase infrastructure is covered by the Standard Contractual Clauses referenced in Annex D. Disclosed under the update-on-change policy at /legal/subprocessors .

Annex D: Standard Contractual Clauses

Where a transfer of personal data of data subjects in the European Economic Area, the United Kingdom, or Switzerland requires an appropriate safeguard, the European Commission Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), together with the UK International Data Transfer Addendum and the Swiss addendum where applicable, are incorporated into this DPA by reference. The modules, options, and annexed details are completed at execution to reflect the Controller-to-Processor relationship in this DPA, with Annex A of this DPA supplying the description of processing and Annex B supplying the technical and organisational measures.

Contact

To initiate DPA execution or ask a question about this template, contact legal@lonia.ai.

Review cadence

Last review date: July 14, 2026. Next review: annually, or on material change, whichever comes first. Material changes include an architecture change, a sub-processor change, a regulatory change, and contract execution practice. The review is owned by legal@lonia.ai, and on each review this page and the tagged PDF are regenerated together from the same source.

Related documents

- [Data Processing Agreement template \(tagged PDF\)](#)
- [Institutional Terms of Service template](#)
- [Sub-processor list](#)
- [Data Protection Impact Assessment \(DPIA\)](#)
- [Scoped Standard Contractual Clauses \(SCCs\)](#)

- [Transfer Impact Assessment \(TIA\)](#)
- [Cookies and tracking statement](#)
- [Security whitepaper](#)
- [Privacy policy](#)
- [VPAT accessibility report](#)