LEGAL

Data Protection Impact Assessment (DPIA)

This Data Protection Impact Assessment describes the processing Aletheia by Lonia AI carries out, assesses its necessity and proportionality, and sets out the risks to data subjects and the measures that mitigate them. It is written under GDPR Article 35 and the European Data Protection Board WP248 guidelines, for procurement, legal, and data protection teams conducting a review.

Version 1.0. Published: July 15, 2026.

1. Description of Processing

Aletheia is a user-side accessibility tool. It converts documents, images, and web content into accessible forms: optical character recognition, image description, content restructuring, and form labeling, with the result saved to a local library on the user's own device. This assessment covers the personal data processed to provide that service, to bill for it, and to maintain the audit records the service depends on.

- **Nature:** educational and general content translation into accessible formats, accessibility conversion, and audit logging of administrative and privileged actions.
- **Scope:** institutional deployments (Campus and Enterprise) and consumer users (Free, Student, Personal, Family, and Professional).
- **Context:** user-uploaded documents and images processed for translation, aggregate usage telemetry needed to apply plan limits, and institutional administrator identity.
- **Purposes:** providing the accessibility translation service, billing, and audit compliance.

2. Data Flows and Processing Paths

Aletheia has three processing paths. Which paths are available depends on the tier, and the cloud paths are off by default until the user turns them on.

- **On-device (MobileVLM):** processing happens entirely in the user's browser. No content leaves the device and there is no cloud data flow. This path is available on every tier (Free, Student, Personal, Family, Professional, Campus, and Enterprise) and is the always-available baseline.
- **Enhanced AI (Personal and Family only):** a Lonia-mediated cloud path. When the user opts in, the image they choose flows from the browser to a Lonia Cloudflare Worker, then to OpenRouter (United States hosted), and the description returns along the same path. Lonia pays OpenRouter using a Lonia-controlled API key. The image is not stored server-side beyond the synchronous request and response cycle. Enhanced AI is off by default and is capped server-side by an atomic procedure: 500 descriptions per month for Personal, and 1000 per month shared across the family group for Family.
- **Bring-your-own-key Enhanced AI (Professional):** a user-invoked, browser-direct path. The user's image and the user's own API key flow from the browser to the AI provider (Anthropic, OpenAI, or OpenRouter) directly. Lonia never sees the API key or the image content on this path. This path is off until the user configures a key.
- **Institution-managed bring-your-own-key Enhanced AI (Enterprise):** an institution-managed, Lonia-mediated path. The institution's administrator enrolls one API key with Lonia's Enterprise Worker, which holds the key envelope-encrypted at rest and decrypts it in memory at request time to call the AI provider (Anthropic, OpenAI, or OpenRouter) on the institution's behalf. Seats never handle the key, and the key material is never returned to any client. The institution is billed by the AI provider under the institution's own account. On this path the request content transits Lonia's Enterprise Worker to the provider. This path is off until the administrator enrolls a key.

3. Necessity and Proportionality Assessment

The processing is limited to what each purpose requires, consistent with the data minimisation principle. User documents are processed on the device and are not stored on Lonia infrastructure; the personal data Lonia holds is limited to account identity, plan and billing status, the usage counts needed to enforce plan limits, and audit records of administrative and privileged actions. Retention is time-limited: institutional data defaults to 365 days per institution and is configurable per institution. The processing supports the full set of data subject rights: access (Article 15), rectification (Article 16), erasure (Article 17), restriction (Article 18), portability (Article 20), and objection (Article 21).

4. Risks to Data Subject Rights and Mitigations

The risks below are assessed against the processing described above, with the measure that mitigates each.

Risks to data subjects and the measures that mitigate them.

Risk	Mitigation
Confidentiality breach	TLS 1.3 in transit, AES-256 encryption at rest (Supabase-managed), row-level security on every table, write-once read-many audit logging, and OAuth-only authentication with no password storage.
Cross-border transfer (Enhanced AI, Personal and Family)	OpenRouter is United States hosted, so this path transfers data United States-ward for image description. Scoped Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, Module 2) apply to this transit. Supplementary measures: TLS 1.3, no image content logged in the Lonia Worker, and no image persisted server-side beyond the synchronous request and response. See the scoped SCCs at /legal/sccs and the Transfer Impact Assessment at /legal/tia.

Risk	Mitigation
Cross-border transfer (institutional data at rest)	Aletheia's Supabase primary data store is hosted in a single United States region. Migration to an EU region is under consideration but has not been scheduled; any future migration will be announced on this page along with an updated transfer analysis. Institutional data at rest is United States hosted under the Standard Contractual Clauses referenced in the DPA at /legal/dpa.
Cross-border transfer (Professional BYOK)	Professional bring-your-own-key Enhanced AI calls originate from the user's browser using the user's own API key. Aletheia does not intermediate, so no Lonia-driven cross-border transfer occurs on this path.
Cross-border transfer (Enterprise BYOK)	Enterprise bring-your-own-key Enhanced AI is intermediated by Lonia's Enterprise Worker, which calls the institution-selected AI provider on the institution's behalf, so a Lonia-mediated cross-border transfer can occur on this path. That transit runs through Lonia's Cloudflare and Supabase infrastructure and is covered by the Standard Contractual Clauses referenced in the DPA at /legal/dpa. Supplementary measures: TLS 1.3, the institution key held envelope-encrypted at rest and decrypted only in memory for the lifetime of the request, and no image persisted server-side beyond the synchronous request and response.
Unauthorised access	Row-level security, and administrator role separation (primary, secondary, and read-only), with FERPA-privileged access held as a separate audited flag for student-scoped data segmentation rather than a default role.
Third-party AI providers (bring-your-own-key tiers)	On Professional, the call is user-directed under the user's own contract with the provider, and Aletheia does not participate in it. On Enterprise, the institution-selected provider is invoked by Lonia's Enterprise Worker using the institution's enrolled key and is engaged as a Lonia sub-processor for that path; see the Sub-processor list at /legal/subprocessors.

5. Right of Erasure (GDPR Article 17)

Users may request account deletion by writing to privacy@lonia.ai. Aletheia commits to fulfilling erasure requests within 30 days, consistent with GDPR Article 12(3).

In addition, Aletheia's Data Processing Addendum commits to cascade deletion on termination of an institutional subscription, with a 30-day export window for the Customer to retrieve data before final deletion. The server-side behaviour that carries out automated cascade deletion is documented in the Security Whitepaper; it is planned or shipping app-side behaviour and is verified via smoke testing in workstream B29 prior to first customer deployment, rather than a control this assessment independently attests as already exercised in production.

Write-once, read-many audit records are preserved where retention is required by applicable law, even after user deletion. These records hold metadata about actions that occurred, not user-generated content.

6. Right of Data Portability (GDPR Article 20)

Users may export their personal data in a machine-readable format. The in-product export functionality is described in the Privacy Policy. Export scope covers user-generated documents, translation history, and account metadata. As with erasure, the server-side behaviour behind in-product export is planned or shipping app-side behaviour, verified via smoke testing in workstream B29 prior to first customer deployment; this assessment does not attest it as already exercised in production.

7. Consultation

Aletheia's assessment is that residual risk is LOW to MODERATE after the mitigations described above. On that basis, prior consultation with a supervisory authority under GDPR Article 36 is not required. This position is reassessed on each review.

8. Review Cadence

This DPIA is reviewed annually, or on material change, whichever comes first. Material changes include an architecture change, a sub-processor change, a regulatory change, and any future migration of the Supabase primary data store to an EU region. On each review this page and the tagged PDF are regenerated together from the same source.

9. Related Documentation

- Security Whitepaper
- Data Processing Agreement (DPA) template
- Sub-processor list. For the Personal and Family Enhanced AI path, OpenRouter acts as a Lonia sub-processor. On the Enterprise institution-managed bring-your-own-key path, the institution-selected AI provider is invoked by Lonia's Enterprise Worker and is a Lonia sub-processor for that path. On the Professional browser-direct bring-your-own-key path, the AI provider the user configures is the user's own counterparty and is not a Lonia sub-processor.
- Scoped Standard Contractual Clauses (SCCs)
- Transfer Impact Assessment (TIA)
- Privacy Policy

10. Preparation of this DPIA

Preparation and ownership of this assessment.

Prepared by	The Aletheia team.
Publication date	July 15, 2026.
Next review	Annually, or on material change, whichever comes first.
Contact for DPIA inquiries	legal@lonia.ai.

This DPIA is a description of Aletheia's processing and risk assessment. It is not legal advice and is not a signed agreement.