

LONIA AI / PALLAS

Institutional terms of service

Terms for institutional and enterprise buyers of Pallas by Lonia AI

The terms on which an institutional buyer subscribes to Pallas, covering the service description and its stated limits, acceptable use, ownership of customer data and of the platform, pricing and payment, warranties, liability, indemnification, term and renewal, termination, and what happens to data when the agreement ends.

Version. 1.0. Published 2026-08-30 by Lonia AI.

Jurisdictions addressed. United States primarily. Personal data obligations are governed by the Data Processing Agreement rather than restated here; the Standard Contractual Clauses and the Transfer Impact Assessment are issued separately.

Every control claim in this document is rendered from the Pallas control inventory at `src/data/control-inventory.ts`, with its status, its evidence basis, and its disclosure text unaltered. Appendix A lists every control cited.

This render is informational; signable version issued on request. Request one at support@lonia.ai, giving your legal entity name and the jurisdiction of your establishment.

This document is provided for procurement and vendor-onboarding review. It is not legal advice, and both parties should have any contractual artifact reviewed by counsel before execution. Questions: support@lonia.ai

Contents

Parties and structure of this agreement	3
1. Definitions	3
2. The Service, and what it does not do	3
3. Access, plans, and quotas	5
4. Acceptable use	8
5. Ownership	8
6. Fees, payment, and taxes	9
7. Support, availability, and service levels	9
8. Identity, support, and processing location	11
9. Warranties and disclaimers	11
10. Indemnification	12
11. Limitation of liability	12
12. Personal data	13
13. Confidentiality	13
14. Term, renewal, and termination	13
15. General	15
16. Contact	15
17. Execution	15
Appendix A. Controls cited	16

Parties and structure of this agreement

These terms (the "Agreement") govern the subscription of the customer (the "Customer") to Pallas by Lonia AI (the "Service"), provided by Lonia AI ("Lonia AI"). They apply where the Customer is an institution rather than an individual: a public body, an educational institution, a healthcare organisation, an enterprise, or an agency contracting on behalf of one.

This public render names Lonia AI as the party, leaves the governing law open, and is the template a buyer reviews. Once terms are agreed, the executed version, which states the governing law, is issued on request at support@lonia.ai.

The Agreement comprises these terms, the Data Processing Agreement, and any executed order form. Where they conflict, an executed order form prevails over these terms, these terms prevail over any published web page, and the Data Processing Agreement prevails over all of them with respect to personal data.

Lonia AI publishes consumer-facing terms and a privacy policy at pallas.lonia.ai. Those govern individual self-service use. Where an institutional Customer has executed this Agreement, this Agreement governs instead.

1. Definitions

- **Service** means Pallas by Lonia AI, comprising the marketing site at pallas.lonia.ai, the authenticated application at app.pallas.lonia.ai, and the supporting infrastructure.
- **Customer Data** means all data the Customer or its authorised users submit to, or generate in, the Service, including assets, scans, findings, evidence, comments, reports, uploaded source files, and the Customer's audit records.
- **Authorised User** means an individual the Customer permits to use the Service under the Customer's subscription, holding one of the four organisation roles the Service defines.
- **Plan** means the subscription tier the Customer has purchased.
- **Order Form** means a document executed by both parties that identifies the Plan, the seat count, the term, and the fees.
- **DPA** means the Pallas Data Processing Agreement.

2. The Service, and what it does not do

The Service scans web content against the WCAG 2.2 success criteria, tracks findings to remediation, maintains a tamper-evident record of changes, and produces conformance reports.

What the scanner does and does not do is the term of this Agreement most likely to be read as a warranty, so it is stated as a control rather than as marketing copy. Each row below is rendered from the Lonia AI control inventory with its status and disclosure text unaltered.

The website scanner analyses a single page of static HTML.

Control scan-single-page-static-only. Status: Partial. Demonstrated in the pallas-marketing repository and checked by

a release gate.

Disclosure. The scanner fetches one page, strips scripts, and analyses the resulting static markup. It does not crawl, it does not execute JavaScript, and single-page applications that render their content client side will not be represented in the results. A buyer evaluating Pallas against a client-rendered application should understand that the public scan tool will report on the served shell rather than the rendered page.

Implementation. marketing: `src/lib/scan-report.ts`; app: `pallas-cors-proxy` and `pallas-scanner-sandbox`.

Verification. marketing: `tests/scan-report.test.ts`.

Pallas reports against the WCAG 2.2 success criteria catalogue. Automated detection covers approximately 17 criteria; the remainder require manual review.

Control scan-wcag-coverage. Status: Partial. Demonstrated in the `pallas-marketing` repository and checked by a release gate.

Disclosure. Listing the full WCAG 2.2 catalogue is not the same as detecting all of it. Roughly 17 success criteria are reliably detectable by automated tooling; the rest depend on human judgement about context, purpose, or equivalence and cannot be settled by a rule engine. Any procurement document that presents the catalogue must state the automated subset in the same sentence, not in a footnote.

Implementation. marketing: `src/data/stats.ts`; marketing: `package.json`, `axe-core` dependency.

Verification. marketing: `src/pages/accessibility.astro` and `src/pages/features.astro`.

Section 508 and EN 301 549 results are produced by applying the corresponding axe-core tag presets, not by an independent rule engine for each standard.

Control scan-508-and-en301549-are-tag-presets. Status: Partial. Demonstrated in the `pallas-marketing` repository and checked by a release gate.

Disclosure. Section 508 and EN 301 549 coverage in Pallas is the `axe-core` tag preset for each standard. Pallas has not implemented, and does not claim, an independent rule engine per standard. A buyer procuring against EN 301 549 specifically should read this as WCAG-derived automated coverage mapped to that standard, and should not treat it as a full EN 301 549 conformance assessment, which includes non-web requirements Pallas does not evaluate at all.

Implementation. marketing: `package.json`, `axe-core` dependency, and the tag selection in the scan path.

Verification. marketing: `tests/scan-report.test.ts`.

Pallas publishes a VPAT 2.5 Accessibility Conformance Report for its own product.

Control scan-vpat-published. Status: Implemented. Demonstrated in the `pallas-marketing` repository and checked by a release gate.

Disclosure. PDF content is verifiable in this repository and gated on every release. PDF tagging is not verifiable here and is confirmed by the operator running PAC 2024 against the regenerated file. The build gate can prove the words are right; it cannot prove the tag tree is.

Implementation. marketing: `public/documents/pallas-vpat-2.5-acr.pdf`.

Verification. marketing: `scripts/verify-doc-artifact-freshness.mjs`, check 10; marketing: Validate the regenerated PDF

with PAC 2024, target zero PDF/UA and zero WCAG failures.

Pallas performs no artificial intelligence or machine learning processing on any data. Accessibility findings are produced by deterministic rule evaluation in axe-core, and no model, inference service, or AI provider is present in either repository.

Control ai-no-model-processing. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. The absence of an AI dependency is demonstrable in both repositories by inspection of the dependency sets, and that is the strongest form this claim takes. It is a statement about what is installed, not a runtime proof that no network call ever reaches a third-party model, which no dependency list can establish. A buyer whose control requires attested absence of model processing should ask for it contractually; the answers to the AI worksheet rest on this row and on nothing stronger than it.

Implementation. marketing: package.json dependency set: astro and axe-core at runtime, with no model runtime, inference client, or AI provider SDK; app: package.json dependency set: @supabase/supabase-js, axe-core, pdf-lib, jszip, react and react-router-dom, with no model runtime, inference client, or AI provider SDK.

Verification. marketing: scripts/test-a11y.mjs.

The consequence for the Customer. Automated detection covers approximately 17 of the WCAG 2.2 success criteria. The remainder require human judgement about context, purpose, or equivalence and cannot be settled by a rule engine. Nothing in the Service, and nothing in this Agreement, constitutes a representation that a property scanned by the Service conforms to WCAG 2.2, to Section 508, to EN 301 549, or to any accessibility statute, or that the Customer is compliant with any such statute. Section 8 states this as a disclaimer; it is stated here as well, because a buyer should meet it in the service description rather than in the small print.

Accessibility of the Service itself. Lonia AI publishes a VPAT 2.5 Accessibility Conformance Report for the Service and an internal conformance record naming what is verified by which method and what is not verified at all.

Pallas publishes a VPAT 2.5 Accessibility Conformance Report for its own product.

Control scan-vpat-published. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. PDF content is verifiable in this repository and gated on every release. PDF tagging is not verifiable here and is confirmed by the operator running PAC 2024 against the regenerated file. The build gate can prove the words are right; it cannot prove the tag tree is.

Implementation. marketing: public/documents/pallas-vpat-2.5-acr.pdf.

Verification. marketing: scripts/verify-doc-artifact-freshness.mjs, check 10; marketing: Validate the regenerated PDF with PAC 2024, target zero PDF/UA and zero WCAG failures.

3. Access, plans, and quotas

Lonia AI grants the Customer a non-exclusive, non-transferable, non-sublicensable right for its Authorised Users to access and use the Service during the term, for the Customer's internal business purposes, subject

to the Plan's seat count and quotas.

Plan quotas are enforced in the database rather than in the browser, which matters to a Customer for a reason worth stating: a quota enforced in the interface is a suggestion, and a Customer relying on one to control spend or seat sprawl is relying on the wrong thing.

The per-plan findings cap is enforced in the database, inside the Row-Level Security INSERT policy, not in the browser.

Control plan-finding-cap-rls. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_findings INSERT policy, migration 034:256; app: pallas_check_finding_limit, migration 034:191.

Verification. app: supabase/migrations/034_enforce_finding_limit_and_retention_purge.sql.

Per-plan asset and scan caps are enforced in the database, inside the Row-Level Security INSERT policies.

Control plan-asset-and-scan-caps-rls. Status: Partial. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Migration 045 folds these two caps into the RLS INSERT policies, and its own header states plainly that whether the LIVE database carried limit-bearing policies before it was applied was not confirmed when the file was written. Migration 013 asserted these policies already called the limit functions; a search of the file set found no policy body containing either function name, so 013 was evidently written against a live database that had drifted from the files. Until the operator runs the section 0 pre-check and confirms migration 045 is applied on live, the honest statement to a buyer is that asset and scan caps are enforced in the database by the current migration set, with live application pending operator confirmation. The 2026-08-30 inventory record describes these caps as verified in RLS; that record and migration 045 do not agree, and this row follows migration 045 because it is the more recent and more specific document.

Implementation. app: pallas_assets INSERT policy migration 045:168, pallas_scans INSERT policy migration 045:186; app: pallas_check_asset_limit 017:188, pallas_check_scan_limit 017:246.

Verification. app: supabase/migrations/045_asset_and_scan_cap_policy_alignment.sql section 0 pre-check.

Seat caps are enforced server side, both in the Row-Level Security policy that admits a membership row and in the function that accepts a pending invitation.

Control plan-seat-caps-server-enforced. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. The 2026-08-30 inventory record lists seat caps as client-side only. That is contradicted by the file set: the cap appears in an RLS INSERT policy at migration 034:354 and in the invitation acceptance path at 010:86 and 029:218. This row follows the file set. The inventory record understated the control rather than overstating it, but a control inventory that repeated the understatement would still be inaccurate.

Implementation. app: pallas_organization_users INSERT policy, migration 034:354; app: pallas_org_at_member_limit 010:47 rebuilt 026:146, called from pallas_accept_pending_invites at 010:86 and 029:218; app: pallas_org_invites_today, migration 026:212.

Verification. app: supabase/migrations/026_invitation_seat_accounting.sql.

Per-plan feature access is enforced server side, in the Row-Level Security policy governing report creation and in the audit export function.

Control plan-feature-flags-server-enforced. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. The 2026-08-30 inventory record lists feature flags as client-side only. That is contradicted by the file set at migration 035:296 and 035:380. This row follows the file set. As with seat caps, the inventory record understated rather than overstated the control.

Implementation. app: pallas_reports INSERT policy, migration 035:296; app: pallas_check_feature_access 035:207, also called from pallas_export_audit_events at 035:380 for the 'audit_export' feature.

Verification. app: src/config/plans.ts:12.

Bulk actions (Growth and above) and non-default retention windows (Enterprise and above) are enforced in the database. Bulk updates run through a server-side function that refuses below the plan, and the retention-policy write policies refuse a non-default window below the plan.

Control plan-bulk-actions-and-custom-retention-server-enforced. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Until migration 049 (2026-09-16) both of these were enforced in the browser only: the bulk-actions page had no plan check and issued single-row updates the database could not tell from one-at-a-time edits, and the retention settings page let any organisation administrator on any plan write any window. The site sold both as tier features throughout. The database is now the enforcement point and the browser only hides the controls below the plan; a questionnaire asking whether plan limits are server-enforced can be answered yes for every limit the inventory lists.

Implementation. app: pallas_bulk_update_findings, migration 049:151; app: pallas_check_feature_access, migration 035:207, extended 048 and 049:88; app: pallas_retention_policies INSERT and UPDATE policies, migration 049:273 and 049:288.

Verification. app: tests/db/planGates.rls.test.ts.

Plan price strings displayed in the application are literals maintained by hand, separate from the Stripe price identifiers that determine what a buyer is charged.

Control plan-price-display-drift. Status: Partial. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. No automated check in either repository can catch drift between a displayed price and the Stripe price it corresponds to, because asserting they agree requires a live Stripe call that nothing here makes. Changing a price in the Stripe dashboard therefore requires editing src/config/plans.ts in the same batch. This is a documented operational constraint, not an enforced control, and it is listed here so that no generated artifact claims price integrity as a technical control.

Implementation. app: src/config/plans.ts, finding A-12 comment block.

Verification. app: Grep src/config/plans.ts for the currency symbol and reconcile all seven literals.

Seats. The Plan's seat count is the maximum number of Authorised Users with an active membership. Seat

caps are enforced both in the policy that admits a membership row and in the function that accepts a pending invitation. A transactional ceiling of 50 invitations per organisation per 24 hours also applies.

Adding seats. The Customer may add seats mid-term at the then-current per-seat rate for its Plan, pro-rated to the end of the current term. Seats cannot be removed mid-term; a reduction takes effect at renewal.

4. Acceptable use

The Customer will not, and will not permit any Authorised User to:

1. Submit for scanning any property the Customer does not own or is not authorised to test. The Service fetches the URL submitted to it, and that fetch is made in the Customer's interest; the Customer is responsible for having the right to make it.
2. Use the Service to conduct security testing, load testing, denial of service testing, or vulnerability scanning of any property, whether its own or a third party's. The Service is an accessibility tool and is neither designed nor authorised for those purposes.
3. Attempt to circumvent the hostname and address denylist, the response size cap, the rate limits, or the bot challenge, or to induce the Service to fetch an address on a private network.
4. Intentionally submit special categories of personal data within the meaning of GDPR Article 9, criminal conviction data, protected health information, student education records, or payment card data for scanning or upload.
5. Reverse engineer, decompile, or attempt to derive the source code of the Service, except to the extent that restriction is unenforceable under applicable law.
6. Resell, sublicense, or provide the Service as a service bureau to a third party, except where an executed Order Form expressly permits it.
7. Use the Service in a way that interferes with its operation for other customers, or that breaches applicable law.

Lonia AI may suspend access to the Service where continued access presents an immediate risk to the Service, to another customer, or to a third party. Lonia AI will give the Customer notice of a suspension as soon as practicable and will restore access as soon as the cause is resolved.

5. Ownership

Customer Data. As between the parties, the Customer owns all Customer Data and all rights in it. Lonia AI obtains no ownership interest in Customer Data and will not sell it, trade it, use it to train a model, or aggregate it for marketing. Lonia AI processes Customer Data only to provide the Service and only as the DPA permits.

The platform. Lonia AI owns the Service, its software, its interfaces, its documentation, and all intellectual property rights in them. Nothing in this Agreement transfers any of those rights to the Customer. Feedback the Customer provides may be used by Lonia AI without obligation or attribution; feedback is not Customer Data.

Aggregate statistics. Lonia AI may compile aggregate, de-identified statistics about use of the Service, provided those statistics do not identify the Customer, any Authorised User, or any scanned property, and provided they are not derived from the contents of Customer Data.

6. Fees, payment, and taxes

Fees are those stated in the executed Order Form. Where no Order Form states otherwise, list pricing applies. Published list pricing as at the version date of this document, in USD, is:

- Starter: \$149 per month, or \$1,639 billed annually.
- Growth: \$399 per month, or \$4,389 billed annually.
- Enterprise: \$999 per month, or \$10,989 billed annually.

Annual figures are billed at eleven months. These figures are substituted into this document from the single pricing source the site itself renders from, so this document cannot state a price the site does not.

Payment. Fees are payable in advance for the term stated in the Order Form. Lonia AI processes payment through Stripe and holds no payment card data. Where the Customer requires invoicing against a purchase order, that is agreed in the Order Form.

Late payment. Lonia AI will give the Customer at least 15 days written notice before suspending the Service for non-payment, and will not suspend where the Customer is disputing an invoice in good faith and has paid the undisputed portion.

Taxes. Fees are exclusive of taxes. The Customer is responsible for any sales, use, value added, or withholding tax arising from the subscription, other than taxes on Lonia AI's income. Where the Customer is exempt, it will supply a valid exemption certificate.

Price changes. Lonia AI may change list pricing on renewal with at least 60 days written notice before the renewal date. A price change does not take effect during a term the Customer has already paid for.

7. Support, availability, and service levels

Availability. Lonia AI targets 99.9 percent monthly availability for the application and its API, on commercially reasonable efforts. Lonia AI runs no uptime monitor and publishes no measured availability history. Maintenance windows are announced at least 48 hours in advance and are scheduled outside 08:00 to 18:00 US Eastern on business days wherever possible. Where an underlying provider is the cause of an outage, Lonia AI's recovery is bounded by that provider's.

What that target is, and is not. For Starter, Growth, and Enterprise the availability target is an operating target provided on commercially reasonable efforts. It is not a contractual service level and carries no service credit.

Support response targets. First response means a human acknowledging the request and stating what happens next, not a resolution. Targets apply during business hours, 09:00 to 17:00 US Eastern, Monday to Friday, excluding US public holidays.

- Starter: email, 2 business days.
- Growth: email, 1 business day.
- Enterprise: email, 4 business hours.

Security reports to support@lonia.ai are triaged ahead of the queue on every Plan.

Recovery objectives. Lonia AI publishes no recovery time objective and no recovery point objective, and states why rather than leaving the field blank.

Application data is held in Supabase managed PostgreSQL with provider-operated automated backups and point-in-time recovery. The recoverable window is set by the provider tier.

Control backup-provider-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no backup schedule of its own. The backup posture is entirely the Supabase provider tier posture, and the operator has not customised it.

Implementation. vendor: Supabase automated backups and point-in-time recovery.

Verification. marketing: [src/pages/trust.astro](#), Backup and disaster recovery questionnaire answer.

Pallas does not publish a recovery time objective or a recovery point objective.

Control backup-no-published-rto-rpo. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No RTO or RPO is published, because a number that cannot be evidenced from a restore test is worth nothing on a questionnaire. No restore test has been performed. A negotiated RTO and RPO with service credits is an Enterprise onboarding item. Any questionnaire field asking for an RTO or RPO must be answered as not published rather than filled with an estimate.

Verification. marketing: [src/pages/trust.astro:126](#).

Pallas has not performed a documented restore test.

Control backup-no-restore-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No restore test has been carried out, so the recoverability of the backups is a provider assertion rather than a demonstrated property. This is a genuine gap and it is listed as one. A buyer for whom tested recoverability is a control requirement should treat this as an open item, and the operator should schedule a restore test into a non-production project as the remediation.

Pallas does not maintain a business continuity plan or a disaster recovery plan that is documented, assigned to a named owner, and exercised annually.

Control continuity-no-tested-bcp-drp. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. There is no annually tested BCP or DRP with a named owner. Continuity rests on the managed platform underneath: Supabase provider backups with point-in-time recovery, and Cloudflare for edge and Pages hosting. Because no restore test has been performed, recoverability is a provider assertion rather than a demonstrated property. A questionnaire item asking for a documented and tested plan is answered no, not answered yes from the existence of provider backups.

Verification. marketing: [src/pages/trust.astro](#), Backup and disaster recovery questionnaire answer.

Detection and monitoring. A Customer whose procurement process asks about 24 by 7 monitoring, a security information and event management system, or a tested incident response plan should read the following before answering the question on Lonia AI's behalf.

Worker observability and logging are enabled on every deployed Worker so that failures surface

rather than passing silently.

Control incident-detection-monitoring. Observability is enabled and logs are collected. There is no security information and event management system, no alerting pipeline, no on-call rotation, and no documented incident response runbook with named roles. Detection today means an operator reading the Cloudflare dashboard. Any questionnaire asking about 24 by 7 monitoring, SIEM, or a tested incident response plan must be answered no. Pallas is operated by a single operator and a procurement document that implied a staffed security operations centre would be false.

8. Identity, support, and processing location

Sign-in. The Service authenticates through Google Workspace and Microsoft Entra ID OAuth. Multi-factor authentication, conditional access, and session revocation are therefore the Customer's own identity provider policies rather than Service features the Customer must trust. Federation against an arbitrary institutional identity provider and automated user provisioning are **not** available on any Plan and are not roadmap commitments in this Agreement. A Customer whose procurement requires them should treat this as a gap.

Pallas authenticates users through Google and Microsoft OAuth only. It stores no passwords, offers no password login, and has no password reset flow.

Control auth-oauth-only. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: src/contexts/AuthContext.tsx:172 and :181; app: src/pages/Onboarding.tsx:123.

Verification. app: Search src/ for signInWithPassword and signUp(.

Support. Support on every Plan is by email to support@lonia.ai, handled by the operator. Lonia AI is operated by a single operator, and no staffed account management function exists.

Processing location. The position as at the version date of this document is stated below rather than characterised.

Processing takes place in the United States only. No European Union hosting exists and none is offered.

Control data-location-eu-option. No customer data is processed in the European Union and no EU infrastructure subprocessor is engaged or planned. Any procurement document, questionnaire response, or sales conversation must present United States processing as the only option and must not present EU hosting as available, on request, or on a roadmap.

Negotiated service levels. Uptime commitments, response commitments, service credits, an end-to-end breach notification window that does not depend on subprocessor performance, and recovery objectives are not terms of this Agreement and are agreed, where at all, in an executed Order Form.

9. Warranties and disclaimers

Lonia AI warrants that it will provide the Service with reasonable skill and care; that the Service will perform materially in accordance with its published documentation; that it has the right to grant the rights it grants in Section 3; and that it will comply with the DPA in its processing of personal data.

Lonia AI does not warrant, and expressly disclaims, that use of the Service will result in conformance

with WCAG 2.2, Section 508, EN 301 549, the Americans with Disabilities Act, the European Accessibility Act, the AODA, or any other accessibility statute or standard; that the Service will detect every accessibility barrier present in a scanned property; that the Service will be uninterrupted or error free; or that a report produced by the Service constitutes a legal opinion or a defence to a claim.

Accessibility conformance is a property of the Customer's own web content and of the manual review the Customer carries out alongside automated scanning. The Service is a tool for that work. It is not a substitute for it, and no Lonia AI representation, on any surface, may be read as saying otherwise.

Except as expressly stated in this Section, the Service is provided as is, and Lonia AI disclaims all other warranties, whether express, implied, statutory, or otherwise, including implied warranties of merchantability, fitness for a particular purpose, and non-infringement, to the maximum extent permitted by applicable law.

10. Indemnification

By Lonia AI. Lonia AI will defend the Customer against any third-party claim alleging that the Service, as provided by Lonia AI and used in accordance with this Agreement, infringes that third party's patent, copyright, trademark, or trade secret, and will indemnify the Customer against damages and costs finally awarded or agreed in settlement of such a claim.

This obligation does not apply to a claim arising from Customer Data, from the Customer's use of the Service in breach of this Agreement, from modification of the Service by anyone other than Lonia AI, or from combination of the Service with anything not supplied by Lonia AI where the claim would not have arisen but for the combination.

If the Service becomes, or Lonia AI reasonably believes it may become, the subject of such a claim, Lonia AI may at its option procure the right for the Customer to continue using the Service, modify the Service so that it is non-infringing while remaining materially equivalent, or terminate the affected subscription and refund fees prepaid for the unused portion of the term.

By the Customer. The Customer will defend Lonia AI against any third-party claim arising from Customer Data or from the Customer's submission of a property for scanning that the Customer was not authorised to submit, and will indemnify Lonia AI against damages and costs finally awarded or agreed in settlement of such a claim.

Procedure. The indemnified party will notify the indemnifying party promptly, give it sole control of the defence and settlement, and provide reasonable cooperation at the indemnifying party's expense. A settlement that imposes a non-monetary obligation on the indemnified party requires that party's consent, not to be unreasonably withheld.

11. Limitation of liability

Cap. Except for the excluded matters below, each party's total aggregate liability arising out of or related to this Agreement, whether in contract, tort, or otherwise, will not exceed the fees paid or payable by the Customer under this Agreement in the 12 months preceding the event giving rise to the liability.

Excluded from the cap. The Customer's obligation to pay fees; either party's indemnification obligations under Section 10; either party's breach of confidentiality; and any liability that cannot be limited or excluded

under applicable law, including liability for death or personal injury caused by negligence, for fraud, and to a data subject under GDPR Article 82.

Consequential damages. Neither party is liable for indirect, incidental, special, consequential, or exemplary damages, or for loss of profits, revenue, goodwill, or anticipated savings, whether or not the possibility of such damage was known. This exclusion does not apply to the matters excluded from the cap above.

Allocation of risk. The Customer acknowledges that the fees reflect this allocation of risk and that Lonia AI would not provide the Service on these fees without it.

12. Personal data

All processing of personal data under this Agreement is governed by the DPA, which is incorporated by reference and prevails over this Agreement with respect to personal data. This Agreement does not restate the DPA's terms.

The DPA covers the categories of data and data subjects, the security measures relied on, the subprocessor chain and the objection right, breach notification including the 72-hour commitment, assistance with data subject rights, international transfers and the Standard Contractual Clauses, audit rights, and the return or deletion of personal data at termination.

The DPA, the Standard Contractual Clauses, and the Transfer Impact Assessment are published at pallas.lonia.ai/trust; the executed version of the DPA is issued on request at support@lonia.ai once terms are agreed.

13. Confidentiality

Each party will protect the other's confidential information with at least the care it applies to its own, and will not disclose it except to personnel and advisers who need it and are bound by equivalent obligations.

Confidential information does not include information that is or becomes public without breach, was known to the receiving party without obligation, is independently developed, or is rightfully received from a third party.

A party may disclose confidential information where compelled by law, provided it gives the other party notice sufficient to seek protective treatment unless prohibited from doing so.

Customer Data is the Customer's confidential information. The Service's source code, security architecture beyond what Lonia AI publishes, and pricing agreed in an Order Form are Lonia AI's confidential information.

14. Term, renewal, and termination

Term. The initial term is 12 months from the effective date stated in the Order Form, unless the Order Form states otherwise.

Renewal. The Agreement renews automatically for successive 12-month terms unless either party gives written notice of non-renewal at least 60 days before the end of the then-current term. Lonia AI will give the Customer written notice of an upcoming automatic renewal, and of any price change taking effect on renewal, at least 60 days before the renewal date, so the Customer's decision window and its notice period are the same window.

Termination for cause. Either party may terminate for the other's material breach on 30 days written notice, if the breach is not cured within that period. Either party may terminate immediately on the other's insolvency, liquidation, or assignment for the benefit of creditors.

Termination for convenience. The Customer may terminate for convenience effective at the end of the then-current term by giving the 60 days notice described above. Fees paid for a term are not refundable on termination for convenience. Where the Customer terminates because it objected to a new subprocessor and the objection could not be resolved, or because Lonia AI exercised its option under Section 10 to terminate an affected subscription, Lonia AI will refund fees prepaid for the unused portion of the term.

Effect of termination. The Customer's right to access the Service ends. The Customer may export Customer Data during the 30 days following termination. After that period, Customer Data is deleted or returned in accordance with the DPA and the Customer's configured retention policies.

Two exceptions apply. Audit records carry a seven-year retention floor that neither party can configure below. Erasure of an individual user does not erase the organisation content that user created.

Audit rows carry a seven-year (2555 day) retention floor enforced by a database CHECK constraint. An administrator cannot configure a shorter audit retention than the regulatory minimum.

Control audit-seven-year-floor. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: chk_audit_log_retention_min_2555 on pallas_retention_policies, migration 016:34; app: pallas_apply_retention_policies, migration 042.

Verification. app: supabase/migrations/016_audit_retention_floor_check.sql.

Any signed-in user can erase their own account. This serves GDPR Article 17, CCPA and CPRA right to delete, and PIPEDA withdrawal of consent.

Control gdpr-art17-user-erasure. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Erasure of a user does not erase the organisation content that user created. Findings, comments, and evidence belong to the organisation as a separate controller with its own retention obligation. The identity link is severed and the audit trail keeps the attribution snapshot. A data subject asking for erasure receives this explanation rather than a silent partial deletion. The request also returns HTTP 409 rather than proceeding if the caller is the sole org_admin of any organisation, because completing it would leave that organisation unadministrable.

Implementation. app: pallas_delete_user_account, migration 039:506; app: pallas-app-api, POST /delete-user-account, requires the X-Confirm-Deletion header, 3 per hour per user, fails closed.

Verification. app: supabase/migrations/040_user_fk_set_null.sql.

An organisation administrator can delete the organisation. Deletion cancels the Stripe subscription, wipes Storage under the organisation prefix, and removes the database rows, archiving a defined subset of audit actions first.

Control gdpr-org-deletion. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_delete_org, migration 008:70, rebuilt 022:71, 024:702, 025:245, and again in migration

041; app: pallas-app-api, POST /delete-org, org_admin plus a typed confirmation phrase, deliberately not rate limited;
app: pallas_retained_audit_events, migration 021:119.

Verification. app: pallas_record_post_delete_failure, migration 025:337.

Survival. Sections 5, 6 as to accrued fees, 9, 10, 11, 12, 13, and 15 survive termination.

15. General

Governing law. This Agreement is governed by the laws of the customer's jurisdiction unless otherwise agreed in an executed order form. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

Assignment. Neither party may assign this Agreement without the other's written consent, except to a successor in connection with a merger, acquisition, or sale of substantially all assets, on written notice.

Notices. Notices to Lonia AI, including notices concerning personal data, go to support@lonia.ai. Notices to the Customer go to the administrative contact stated in the Order Form. Notice is effective on delivery.

Publicity. Neither party may use the other's name or marks in publicity without prior written consent. A Customer's consent to be named as a reference is separate from this Agreement and may be withdrawn.

Force majeure. Neither party is liable for a failure to perform, other than a payment obligation, caused by an event beyond its reasonable control, provided it notifies the other party and resumes performance as soon as practicable.

Entire agreement. This Agreement, the DPA, and any executed Order Form are the entire agreement between the parties on their subject matter and supersede all prior understandings. No amendment is effective unless in writing and signed by both parties, except that Lonia AI may update the published version of these terms for future terms on the notice described in Section 6.

Severability and waiver. If a provision is held unenforceable, the rest remains in effect and the provision is modified to the minimum extent necessary to make it enforceable. A failure to enforce a provision is not a waiver of it.

Independent contractors. The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, or employment relationship.

16. Contact

Commercial questions and Order Forms, support and general notices, personal data, the DPA, the Standard Contractual Clauses, the Transfer Impact Assessment, and security reports: support@lonia.ai.

17. Execution

Lonia AI. Lonia AI

- Signature: _____
- Name: _____
- Title: _____

- Date: _____

Customer. _____

- Signature: _____

- Name: _____

- Title: _____

- Date: _____

The signature lines above are reproduced so that a reviewer can see the shape of the instrument they would be asked to sign. This render is the public template; the executed version is issued once terms are agreed, on request at support@lonia.ai.

Appendix A. Controls cited

This document cites 21 of the 84 rows in the Pallas control inventory. Each is listed below with the status and evidence basis it carried at the 2026-08-30 inventory pass. A row absent from this list is not claimed by this document.

- **auth-oauth-only** (Authentication). Implemented.
- **audit-seven-year-floor** (Tamper-evident audit chain). Implemented.
- **gdpr-art17-user-erasure** (Data subject rights). Implemented.
- **gdpr-org-deletion** (Data subject rights). Implemented.
- **plan-finding-cap-rls** (Plan and quota enforcement). Implemented.
- **plan-asset-and-scan-caps-rls** (Plan and quota enforcement). Partial.
- **plan-seat-caps-server-enforced** (Plan and quota enforcement). Implemented.
- **plan-feature-flags-server-enforced** (Plan and quota enforcement). Implemented.
- **plan-bulk-actions-and-custom-retention-server-enforced** (Plan and quota enforcement). Implemented.
- **plan-price-display-drift** (Plan and quota enforcement). Partial.
- **scan-single-page-static-only** (Scanning engine capability). Partial.
- **scan-wcag-coverage** (Scanning engine capability). Partial.
- **scan-508-and-en301549-are-tag-presets** (Scanning engine capability). Partial.
- **scan-vpat-published** (Scanning engine capability). Implemented.
- **ai-no-model-processing** (Scanning engine capability). Implemented.
- **data-location-eu-option** (Data classes and processing location). Not implemented.
- **incident-detection-monitoring** (Incident response). Partial.
- **backup-provider-operated** (Backup and recovery). Implemented.
- **backup-no-published-rto-rpo** (Backup and recovery). Not implemented.
- **backup-no-restore-test** (Backup and recovery). Not implemented.
- **continuity-no-tested-bcp-drp** (Backup and recovery). Not implemented.