LONIA AI / PALLAS

Transfer Impact Assessment

Assessment of transfers of personal data from the EEA, the UK, and Switzerland to the United States

An assessment of the transfers Pallas carries out, the transfer tool relied on, whether that tool is effective in the destination country, and the supplementary measures adopted, following the six-step methodology of European Data Protection Board Recommendations 01/2020. Every technical safeguard is rendered from the Pallas control inventory with its status, evidence basis, and disclosure text unaltered.

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

Jurisdictions addressed. EU GDPR Chapter V primarily, with the UK GDPR and the Swiss FADP addressed where their obligations diverge. The destination country assessed is the United States. Positions taken by the Irish Data Protection Commission and by the German federal and state supervisory authorities are addressed specifically.

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 assessment is published rather than issued on request, so that an exporting controller can check it before opening a sales conversation. It is the importer's assessment and an input to the exporter's own, not a substitute for it. No counsel has reviewed it; the disclosure at the top of the document says so once.

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

No counsel has reviewed this document. Lonia AI operates without a legal budget. Every part of this document is either rendered from the control inventory or written by the operator. Lonia AI does not hold counsel's opinion on any of the legal questions it addresses, and every characterisation of law in it is the operator's position. Where an exporter's own counsel reaches a different conclusion, that conclusion governs the exporter's assessment and we will engage with it; that is a conversation to have before execution.

1. What this document is, and what it is not

This is a transfer impact assessment carried out by Lonia AI as the data importer, covering transfers of personal data from the European Economic Area, the United Kingdom, and Switzerland to the United States in connection with Pallas.

It follows the six-step methodology in European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools. The six steps are the section structure below, in order, and no step is skipped or merged into another.

Whose assessment this is. Under the Standard Contractual Clauses the obligation to assess a transfer sits on both parties, and Clause 14(a) of the 2021 Clauses records that the parties warrant they have no reason to believe the laws of the destination country prevent the importer from meeting its obligations. The exporter is the party that must be satisfied. This document is therefore the importer's contribution to the exporter's assessment: it describes the transfer, states the destination-country analysis, and sets out the measures in place, so that an exporting controller can carry out its own assessment against a described system rather than against a questionnaire. It does not discharge the exporter's duty and does not purport to.

Version basis. This assessment reflects the 30 August 2026 control inventory pass. Every control rendered below carries the status it held on that date, so a measure that was partial on that date says so here rather than being rounded up.

---

2. Step one: know your transfer

The first step requires the transfer to be mapped: what data, about whom, for what purpose, to whom, and where it comes to rest. A transfer that has not been mapped cannot be assessed, and an assessment that begins at step three is an assessment of an imagined system.

2.1 The parties and the direction of transfer

The exporter is the customer organisation established in the EEA, the United Kingdom, or Switzerland that uses Pallas. The importer is Lonia AI, established in the United States.

For customer organisation data the exporter is the controller and Lonia AI is the processor, which makes this a Module Two transfer, controller to processor. For user profile data and marketing list membership Lonia AI is itself the controller, and the transfer is a controller-to-controller transfer under Module One. The Pallas Data Processing Agreement records the same split, and it is expressed in the database schema rather than only in policy.

Pallas distinguishes the two controller roles in its schema, not only in its policy text. Lonia AI is controller for user profile data; the customer organisation is controller for its own scan and

compliance data. The user export and the organisation export are separate functions, not one filtered by the other.

> Control gdpr-controller-split-documented. 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_export_user_data 039:268 for the individual, pallas_export_org_data 009:13 rebuilt in 032:67 and 037:297 for the organisation.
>
> Verification. app: supabase/migrations/039_gdpr_user_rights.sql, controller split section.

2.2 What is transferred

The data classes Pallas processes are enumerated in the control inventory rather than described loosely here, because a transfer assessment that characterises the data in its own words is an assessment of a different system from the one that runs.

Pallas holds account identity, organisation records, scan findings, generated reports, transiently uploaded source files, audit events, and marketing list membership. It holds no payment card data, no special category data by design, and no health or student records.

> Control data-classes-enumerated. 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. Pallas does not collect special category data as a matter of design, but it scans customer-supplied URLs and accepts customer-uploaded documents. Content a customer submits is outside Pallas control, so the accurate statement is that Pallas does not solicit or intentionally process special category data, not that none can ever transit the system. Uploaded source files carry a 7 day default retention precisely because they are the class most likely to contain something unintended.
>
> Implementation. app: The 29 tables enumerated in tenant-rls-every-table, plus the three Storage buckets in migration 020.
>
> Verification. marketing: src/pages/trust.astro, What Pallas holds and What Pallas never collects.

Summarised for a reader who needs the shape before the detail: authentication assertions from an OAuth identity provider, being name, email address, and where supplied a profile photograph; organisation membership and role; scan configuration, being the URLs and web properties a customer designates; scan results, being accessibility findings against the pages scanned; source files a customer uploads for evaluation; audit ledger entries recording actions taken in the Service; and, for the marketing list, an email address with its consent record.

The class that carries the most transfer risk is the uploaded source file. It is the only class whose contents Pallas does not define. A customer that uploads a document containing personal data beyond the categories above has transferred that data, and no schema constrains what it contains. Section 5.4 returns to this.

2.3 Who the data subjects are

Users of the customer organisation who authenticate to Pallas; individuals named or depicted in content a customer submits for scanning or uploads for evaluation, incidentally rather than by design; and subscribers

to the Lonia AI marketing list, who are data subjects of Lonia AI as controller.

2.4 The purposes

Delivering the Service, being accessibility scanning of customer-designated web properties and the reporting of findings; authenticating users and enforcing organisation and plan boundaries; maintaining a tamper-evident record of actions taken; billing; and, separately and on a separate lawful basis, operating the marketing list.

No purpose in this list involves evaluating a person, profiling, behavioural analytics, advertising, or sale of data to a third party. That matters to a transfer assessment because the categories of processing most likely to attract foreign intelligence interest are absent.

2.5 Where the data comes to rest

The default processing location is the United States. Supabase hosts the database and Storage in us-east-1; Cloudflare serves from its global edge network.

> Control data-location-default-us. 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.
>
> Implementation. vendor: Supabase project region us-east-1; marketing: src/pages/legal/subprocessors.astro.
>
> Verification. marketing: src/pages/trust.astro, Data residency options.

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

> Control data-location-eu-option. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. 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.
>
> Implementation. marketing: src/pages/trust.astro, Data residency options; marketing: src/pages/legal/subprocessors.astro, six operative entries and no planned entry.

This is the single most consequential fact in this assessment and it is stated before any of the legal analysis, because an exporter with a strict residency requirement can stop reading here. There is no European Union deployment of Pallas today. Every transfer this document assesses is an actual transfer to the United States, not a theoretical one, and the EU residency option is an offer to be agreed at Enterprise onboarding rather than a capability that can be switched on for an existing account. An exporter that has been told otherwise has been told something this document contradicts.

2.6 Onward transfers: the subprocessor chain

The full subprocessor list is published, with each provider purpose, data categories, processing location, and published certifications.

> Control subprocessors-published-list. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The 2026-08-30 inventory record names four subprocessors in use: Supabase, Cloudflare, Stripe, and Resend. The published page carries six operative entries, adding Google and Microsoft as OAuth identity providers. Both are accurate about different things: Google and Microsoft receive an authentication assertion at sign-in and store no Pallas customer data. Procurement artifacts should carry all six operative entries, because a buyer assessing identity provider dependency needs to see the two that the four-entry description omits.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Verification. marketing: src/pages/trust.astro, Sub-processors section.

A new subprocessor is published with 30 days advance notice before it processes any customer data.

Control subprocessors-change-notice. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment by the operator, not a technical control. Nothing in either repository enforces the notice period, and no new subprocessor has yet been added under it.

Implementation. marketing: src/pages/legal/subprocessors.astro, Change Notification section.

Certifications listed against each subprocessor are those published by that provider.

Control subprocessors-certifications-are-theirs. 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 holds no SOC 2, ISO 27001, or PCI DSS certification of its own. Every certification named on the subprocessor list belongs to the named provider and covers that provider infrastructure, not the Pallas application built on top of it. A procurement document must never present a subprocessor certification in a way that could be read as a Pallas certification. This is the single most consequential misreading available in this inventory, so the distinction is stated wherever the certifications appear.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Pallas operates no data centre, server cage, office server room, or other facility in which institutional data is held. Physical and environmental security for every system that holds institutional data belongs to Supabase and Cloudflare.

Control physical-security-subprocessor-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. Every physical-security control a questionnaire asks about, including staffed facilities, cages, enclosing barriers, redundant and tested power, cooling, fire suppression, and carrier diversity, belongs to Supabase or Cloudflare. Pallas can neither demonstrate nor test any of them, and does not inherit them as its own controls. Answers to physical-security questions state reliance and name the provider. A buyer who needs evidence should read the provider audit reports; a Pallas assertion is not evidence of a provider control.

Implementation. vendor: Supabase and Cloudflare published data centre physical and environmental security programmes.

Verification. marketing: src/pages/trust.astro, subprocessor list with per-provider processing locations.

Pallas operates no network perimeter, no host, and no network monitoring of its own. Edge filtering, DDoS mitigation, and TLS termination are Cloudflare functions, and the database network boundary

is operated by Supabase.

> Control network-perimeter-subprocessor-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 firewall of its own, no network intrusion detection or prevention system, and no host-based agent, because it operates no hosts. Stateful filtering, DDoS mitigation, and TLS termination happen at the Cloudflare edge and are answered as provider-operated. Intrusion detection, intrusion prevention tuned by Pallas, next-generation persistent threat monitoring, and 24x7 intrusion monitoring are answered no: no such capability is operated by Pallas or configured by Pallas at a provider. A buyer requiring a monitored perimeter under vendor control, or a staffed security operations centre, should treat this as an open item.
>
> Implementation. vendor: Cloudflare edge network, web application firewall and DDoS mitigation; Supabase managed database network boundary.
>
> Verification. marketing: workers/, whose Workers execute on the Cloudflare edge rather than on any Pallas-operated host.

The operative subprocessors and their functions are published and are not restated in different words here. What matters to a transfer assessment is that the chain is disclosed in full, that a change carries advance notice, and that the certifications each provider holds are that provider's own and are not Lonia AI's. An exporter assessing this transfer is assessing the chain, not only its first link.

---

3. Step two: identify the transfer tool relied on

The transfer tool relied on is the European Commission's Standard Contractual Clauses adopted by Implementing Decision (EU) 2021/914, Module Two for controller-to-processor transfers of customer organisation data and Module One for the controller-to-controller transfers described in section 2.1. They are incorporated into the Pallas Data Processing Agreement by reference and are issued in full on request.

For transfers out of the United Kingdom the tool is the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses, issued under section 119A of the Data Protection Act 2018. For transfers out of Switzerland the tool is the Standard Contractual Clauses with the amendments recognised by the Federal Data Protection and Information Commissioner.

Lonia AI does not rely on an adequacy decision for these transfers, and is not self-certified under the EU-US Data Privacy Framework. This is stated plainly because a vendor that is not certified and lets a buyer assume otherwise has misled the buyer about the legal basis of the transfer. Section 4.5 addresses what the Framework does and does not do for a transfer that does not rely on it. An importer relying on the Clauses rather than the Framework carries the full Clause 14 assessment obligation regardless of the adequacy decision's existence.

Derogations under Article 49 are not relied on. Article 49 is for occasional and non-repetitive transfers, and the transfers assessed here are systematic and continuous.

---

4. Step three: is the transfer tool effective in the destination country

The third step is the substance of Schrems II. The question is not whether the Clauses are valid, which the Court of Justice confirmed they are, but whether anything in the law or practice of the destination country prevents the importer from complying with them.

4.1 The question as we understand it

The assessment turns on whether the destination country's public authorities can compel or effect access to the transferred data on terms that go beyond what is necessary and proportionate in a democratic society, and whether a data subject has an effective remedy. The Court's finding in Case C-311/18 concerned two United States authorities specifically, and those two are addressed first.

4.2 FISA Section 702

Section 702 of the Foreign Intelligence Surveillance Act, codified at 50 U.S.C. 1881a, permits the targeting of non-United States persons reasonably believed to be located outside the United States for the acquisition of foreign intelligence information, and permits the compelling of assistance from an electronic communication service provider as that term is defined at 50 U.S.C. 1881(b)(4). The Court of Justice found Section 702 wanting on two grounds: it does not limit collection by reference to the principle of proportionality in the way Union law requires, and it does not confer on non-United States persons a right actionable before a court against the United States authorities.

Whether Lonia AI falls within the definition. We do not claim to be outside it. The definition reaches remote computing service providers and electronic communication service providers, and a software-as-a-service provider holding customer data may fall within it. A vendor that assures a buyer it is out of scope, without counsel's opinion saying so, is offering the buyer a comfort it cannot support. Lonia AI does not offer that comfort.

What we can state as fact rather than as understanding. Lonia AI has never received a request or directive under Section 702, has never received a national security letter, and has never received any order accompanied by a non-disclosure obligation. Section 7.3 records the commitment to keep that statement current.

4.3 Executive Order 12333

Executive Order 12333 governs signals intelligence activity conducted outside the United States. It contains no mechanism by which a United States provider is compelled to assist, and that the concern it raises for a transfer assessment is interception of data in transit rather than compelled production of data at rest.

That is the concern the transport encryption control addresses directly, and it is the one supplementary measure in this assessment whose fit to the threat is exact rather than approximate.

All connections are TLS 1.3, enforced by Cloudflare and Supabase.

> Control encryption-in-transit. 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. TLS termination and version are properties of Cloudflare and Supabase. What this repository

demonstrates is the header set and the build gate that refuses to ship without it, not the negotiated cipher.

Implementation. vendor: Cloudflare edge TLS and Supabase connection TLS; marketing: public/_headers.

Verification. marketing: scripts/csp-hashes.mjs.

4.4 The CLOUD Act

The Clarifying Lawful Overseas Use of Data Act of 2018 amended the Stored Communications Act to confirm that a provider subject to United States jurisdiction must produce data in its possession, custody, or control in response to lawful process, regardless of where the data is stored.

This has two consequences an exporter should weigh. First, the CLOUD Act concerns criminal process, which is issued under a warrant standard requiring judicial authorisation, and is therefore a different instrument from the intelligence authorities in sections 4.2 and 4.3. Second, and more importantly for this assessment, storage location does not by itself defeat it. **An exporter that adopts hosting inside the European Union as its answer to the CLOUD Act has not answered it**, because Lonia AI would remain a United States entity with control over the data. The published trust documentation already makes this distinction between residency and sovereignty, and this assessment repeats it rather than softening it.

What we can state as fact. Lonia AI has never received a CLOUD Act request, a Stored Communications Act warrant, a subpoena, or any other compulsory process from any public authority in any jurisdiction seeking customer personal data.

4.5 Executive Order 14086 and the EU-US Data Privacy Framework

Executive Order 14086 of October 2022 directed that United States signals intelligence activities be conducted only in pursuit of defined legitimate objectives and subject to necessity and proportionality, and established a redress mechanism culminating in the Data Protection Review Court. The European Commission adopted an adequacy decision for the EU-US Data Privacy Framework in July 2023 on that basis, with a UK Extension and a Swiss counterpart following.

The Executive Order's necessity and proportionality constraints and its redress mechanism apply to United States signals intelligence activity generally, and therefore form part of the legal landscape an importer relying on the Clauses assesses under Clause 14, whether or not that importer is certified under the Framework. The adequacy decision itself is available only to certified organisations, and Lonia AI is not one.

The adequacy decision is under challenge and that its durability should not be assumed. This assessment does not rest on it. That is a deliberate structural choice: an assessment whose conclusion depends on an adequacy decision has to be redone if the decision falls, and the transfers here are protected by the Clauses and the measures in section 5 independently of it.

4.6 The practical likelihood, stated honestly

Two facts bear on likelihood and both cut in the same direction. The data classes in section 2.2 contain no communications content, no location data, no device telemetry, and no behavioural record. The customer base is organisations procuring accessibility compliance tooling. This profile is a poor match for the foreign intelligence purposes the authorities in sections 4.2 and 4.3 exist to serve.

That is an argument about likelihood and not about legal effectiveness. It does not answer the Clause 14

question, and this assessment does not present it as though it did. An exporter is entitled to weigh it and entitled to disregard it.

5. Step four: supplementary measures adopted

5.1 Technical measures

Each measure below is rendered from the control inventory. Where a control is partial, it renders as partial, and where its evidence basis is a vendor's assertion rather than something either Pallas repository can demonstrate, it says so. A transfer assessment that presents a vendor assertion as a demonstrated control has misdescribed the protection the exporter is getting.

Encryption.

Data is encrypted at rest with AES-256 through Supabase-managed infrastructure.

> Control encryption-at-rest. 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. Encryption at rest is provided and attested by Supabase. No Pallas code implements it and neither Pallas repository can demonstrate it. A buyer who requires independent evidence should request the Supabase SOC 2 Type II report rather than a Pallas assertion.
>
> Implementation. vendor: Supabase managed PostgreSQL and Storage encryption at rest.
>
> Verification. vendor: Supabase SOC 2 Type II report, available to the operator under NDA.

All connections are TLS 1.3, enforced by Cloudflare and Supabase.

> Control encryption-in-transit. 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. TLS termination and version are properties of Cloudflare and Supabase. What this repository demonstrates is the header set and the build gate that refuses to ship without it, not the negotiated cipher.
>
> Implementation. vendor: Cloudflare edge TLS and Supabase connection TLS; marketing: public/_headers.
>
> Verification. marketing: scripts/csp-hashes.mjs.

Production secrets are held in the platform secret store and never in either repository. Worker configuration files carry variable names only.

> Control encryption-no-secrets-in-repo. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.
>
> Disclosure. Two Cloudflare KV namespace identifiers are committed, at workers/pallas-scan-email/wrangler.toml and in the pallas-app Workers. A KV namespace id is an identifier rather than a credential: reaching the namespace still requires authenticated access to the Cloudflare account. This is recorded as a deliberate decision, with the note that the ids should move to deploy-time values if either repository is shared with a buyer, an auditor, or a contractor.
>
> Implementation. marketing: workers/pallas-scan-email/.dev.vars.example and

workers/pallas-email-gate/.dev.vars.example; marketing: .gitignore.

Verification. marketing: Rule sweep for key, token, price identifier, and webhook secret strings.

Finding comments, evidence descriptions and code snippets, and evidence files are encrypted at rest by the database and storage provider under a key the provider holds, and in transit by TLS. They are not client-side encrypted: every member of the organization can read them, they are included in the organization's data export, and the Processor can read them as any SaaS operator can.

Control encryption-member-prose-provider-held-key. 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: docs/DATABASE_ENFORCEMENT.md:86, What is and is not encrypted; app: src/audit/auditMetadataKeys.ts, AUDIT_METADATA_KEYS.

Verification. app: tests/audit/auditMetadataKeys.test.ts.

Tenant isolation. Isolation is not a transfer measure in the Schrems II sense, because it does not defend against a compelled disclosure directed at Lonia AI. It is included because it bounds the scope of any single disclosure to one organisation's data rather than the estate, which is a consequence an exporter should be able to see.

Row-Level Security is enabled on every Pallas application table. Twenty-nine tables carry it in the migration file set.

Control tenant-rls-every-table. Status: Implemented. 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. Twenty-nine tables carry RLS in the migration file set (twenty-four before migrations 057 and 059 added the digest-run and rule-override tables on 2026-09-16, twenty-six before migration 067 added the two crawl-state tables on 2026-09-17, and twenty-eight before migration 072 added the API-token table). Two of them, pallas_subscribers and pallas_subscriber_suppression, were created directly on the live database on 2026-08-30 and captured into migration 046 only afterwards, so any count taken before that migration was written disagrees with this one. The 2026-08-30 inventory pass recorded twenty-two on the live project. That difference has not been reconciled against the live database, because code in these repositories does not execute SQL. Before this claim is stated to a buyer with a number attached, the operator should run a live count of pg_tables joined to pg_class.relrowsecurity for tables matching pallas_%, and either correct this row or correct the 2026-08-30 inventory record. Until then the safe published form of this claim omits the count and states only that RLS is enabled on every application table.

Implementation. app: ENABLE ROW LEVEL SECURITY on 29 tables across migrations 001, 002, 005, 010, 017, 021, 024, 029, 034, 041, 046, 057, 059, 067, 072.

Verification. app: Search supabase/migrations/*.sql for ENABLE ROW LEVEL SECURITY and compare the count against CREATE TABLE.

Every tenant-scoped policy resolves membership through two SECURITY DEFINER helpers with a pinned search_path, rather than by re-entering the membership table under its own RLS.

Control tenant-org-scoping-helpers. 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_user_has_org_access, migration 002:8, hardened in 031:54; app: pallas_user_org_role, migration 002:17, hardened in 031:68.

Verification. app: supabase/migrations/031_low_severity_hardening.sql.

The evidence, source-files, and reports Storage buckets are private and carry per-organisation RLS policies on storage.objects, with read, write, update, and delete scoped to organisation role.

Control tenant-storage-per-org. 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: supabase/migrations/020_storage_bucket_rls.sql; app: pallas_storage_org_access, migration 020:50.

Verification. app: supabase/migrations/020_storage_bucket_rls.sql header.

Server-side operator functions run under service credentials that bypass Row-Level Security by necessity. Their scope is limited, they are versioned in source, and their actions are covered by the audit trail.

Control tenant-service-role-bypass-disclosed. 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. Service-role credentials bypass Row-Level Security. This is a property of PostgreSQL and Supabase, not a Pallas design choice, and it means tenant isolation for service-role code paths rests on the correctness of those code paths rather than on the database refusing them. The mitigating controls are that the paths are few, versioned, and audit-logged, not that they are constrained by RLS.

Implementation. app: pallas-app-api; app: supabase/functions/enforce-retention/index.ts.

Verification. marketing: src/pages/trust.astro, Security posture, Tenant isolation.

Tamper-evident audit record. Its relevance to a transfer assessment is narrow and specific: it makes access to data visible after the fact and makes silent alteration of the access record detectable.

Every audit event appends an entry to a SHA-256 hash chain. Each entry is hashed together with the previous entry hash, so modification, deletion, or reordering of historical events breaks the chain and is detectable.

Control audit-sha256-ledger. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: supabase/migrations/041_audit_tamper_evidence.sql; app: hashing helpers inside migration 041; row_hash and prev_row_hash columns on pallas_audit_events; app: insert trigger on pallas_audit_events, migration 041.

Verification. app: pallas_verify_audit_chain, migration 041; app: pallas_verify_audit_row, migration 041.

The ledger table is append-only in the strong sense: Row-Level Security is enabled with zero policies, and INSERT, UPDATE, DELETE, and TRUNCATE are revoked from every role including service_role. Only SECURITY DEFINER trigger functions can write to it.

Control audit-ledger-append-only. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: pallas_audit_chain, created by migration 041 with Row-Level Security enabled; app: SECURITY DEFINER trigger functions inside migration 041.

Verification. app: pallas_audit_chain, migration 041; the table answers permission denied to the anon role through the API.

Lawful removal of an audit row, whether under a retention policy or under GDPR Article 17, appends a redaction entry recording the sequence number, the hash before, the hash after, the reason, and the timestamp. The ledger outlives the row it describes, so a reviewer can distinguish a lawful purge from a concealment.

Control audit-lawful-redaction-recorded. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Disclosure. The delete allowlist is a declaration, not an authorisation control. Anything holding service_role and a SQL connection can set the redaction reason. The control is not that setting it is hard; the control is that setting it does not buy silence, because the redaction entry lands in a table that role cannot subsequently edit or truncate. An audit row can be deleted. It cannot be deleted quietly. This distinction is stated here because a reviewer will press on it, and a document that presented the flag as an access control would be overclaiming.

Implementation. app: pallas_audit_delete_reason_allowed, migration 041; the redaction hash is computed inside the same migration; app: update and delete triggers on pallas_audit_events, migration 041.

Verification. app: migration 041, which carries the update and delete allowlists.

A daily anchor snapshot of the chain tip is taken at 06:00 UTC and retained. Any anchor can be exported for independent verification on request.

Control audit-daily-anchors. 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. Anchor creation is automated. External publication of anchors is an operator action and not an automated feed, so Pallas does not claim an automated external anchoring service. Until external publication begins, an anchor proves the chain was in a given state at a given time only to a party who trusts the Pallas database clock. Additionally, the cron job schedules itself inside a DO block that catches its own exception: if pg_cron was not enabled at migration time, the job was never created and the migration still reported success. Whether the job exists on the live database is an operator check against cron.job, not a fact this repository can assert.

Implementation. app: pg_cron job at '0 6 * * *', scheduled by migration 041; app: pallas_create_audit_anchor, pallas_verify_audit_anchors, pallas_list_audit_anchors, pallas_mark_audit_anchor_exported, migration 041; app: pallas-app-api, POST /audit-chain/anchor, /anchors, /verify-anchors, /anchor-exported.

Verification. app: pallas_verify_audit_anchors, migration 041.

Access control and authentication.

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(.

Sessions are JWT-based through Supabase Auth, and refresh tokens rotate on use.

Control auth-session-jwt. 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. Token rotation behaviour is a property of Supabase Auth. Pallas configures it and relies on it; no Pallas code implements it, and neither Pallas repository can demonstrate it independently.

Implementation. vendor: Supabase Auth refresh token rotation.

Verification. marketing: src/pages/trust.astro, Security posture, Session security.

Organisation membership carries one of four roles: org_admin, manager, contributor, viewer. Read is available to any member; write and update require contributor or above; delete requires org_admin.

Control access-org-roles. 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_organization_users.role, migration 001:30; app: supabase/migrations/020_storage_bucket_rls.sql, role model section.

Verification. app: pallas_user_org_role, migration 002:17 hardened 031:68.

Authenticated endpoints carry per-user rate limits. Endpoints that move or expose data fail closed when the limiter is unavailable; read-only endpoints degrade to load.

Control access-rate-limiting-authenticated. 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. Cloudflare Workers KV is eventually consistent across colocations, so a KV-backed counter is a burst guard rather than a hard ceiling: concurrent requests can each read the same value before any write lands. Where a hard ceiling was required, the limit is transactional in PostgreSQL instead, as with the 50 invitations per organisation per 24 hours enforced by pallas_org_invites_today. Pallas does not claim KV-backed limits are exact.

Implementation. app: pallas-app-api, checkRateLimit() over the RATE_LIMIT_KV namespace.

Verification. app: workers/pallas-app-api/wrangler.toml, rate limiting comment block.

5.2 Contractual measures

The Standard Contractual Clauses themselves are the primary contractual measure, and Clause 15 of the 2021 Clauses imposes on the importer the obligations that matter most to this section: to notify the exporter of a public authority's request where permitted, to challenge a request it considers unlawful, and to provide the minimum permissible in response.

A limitation stated rather than glossed. The Pallas Data Processing Agreement as currently published incorporates the Clauses by reference and does not itself contain a standalone public-authority-disclosure clause. Until the Clauses are executed with a given exporter, the Clause 15 obligations are incorporated rather than executed. Section 9 records this as an action arising. It is recorded here rather than presented as

a measure already in force, because a measure that will be in force is not a measure that is in force.

The commitments Lonia AI makes in this document. Where a public authority request is received, Lonia AI will notify the affected customer before disclosure unless legally prohibited from doing so; will seek to have any prohibition lifted or narrowed; will challenge process it considers unlawful or overbroad; and will disclose only the minimum the process compels. These are operator commitments made in this document. **They carry no control-inventory row, no code enforces them, and neither Pallas repository can demonstrate them.** They are stated in these terms rather than presented alongside the technical controls above, because the difference between a control a release gate checks and a promise a person makes is exactly the difference this assessment exists to preserve.

Beyond the Clauses, the Data Processing Agreement carries the breach notification and subprocessor obligations an exporter relies on when a disclosure does occur.

Pallas notifies affected customers without undue delay and in any event within 72 hours of becoming aware of a breach affecting their data. The clock starts on awareness, not on confirmation.

> Control incident-72-hour-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. This is a contractual commitment. No technical control enforces it and no artifact in either repository can demonstrate it has been met, because no breach has occurred. A buyer should treat it as a term to be captured in the Data Processing Agreement rather than as a verified capability.
>
> Implementation. marketing: src/pages/trust.astro, Breach commitments, Customer notification; marketing: src/pages/legal/dpa.astro.

Authority notification follows the jurisdiction: Ireland DPC, UK ICO, and EU supervisory authorities within 72 hours; Canada OPC under PIPEDA; Australia OAIC under the Notifiable Data Breaches scheme.

> Control incident-authority-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. A contractual and regulatory commitment rather than a technical control. Pallas has not been required to make such a notification, so there is no track record to evidence.
>
> Implementation. marketing: src/pages/trust.astro, Breach commitments, Authority notification.

A subprocessor breach triggers the same 72 hour notification cascade, from the subprocessor to Pallas to the customer.

> Control incident-subprocessor-cascade. Status: Partial. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. The Pallas leg of this cascade is a commitment Pallas controls. The subprocessor leg depends on each provider notifying Pallas, which is governed by that provider terms and is outside Pallas control. The end-to-end 72 hours is therefore contingent on subprocessor performance, and a buyer requiring a guaranteed end-to-end window should raise it during Enterprise contracting rather than rely on this statement.
>
> Implementation. marketing: src/pages/trust.astro, Breach commitments.

5.3 Organisational measures

Any signed-in user can export the personal data Pallas holds about them, across every organisation they belong to. This serves GDPR Article 15 and Article 20, CCPA and CPRA right to know, PIPEDA Principle 9, and Australian Privacy Principle 12.

Control gdpr-art15-art20-user-export. 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_export_user_data, migration 039:268, extended to ten collections in migration 042; app: pallas-app-api, POST /export-user-data, 3 per hour per user, fails closed.

Verification. app: supabase/migrations/039_gdpr_user_rights.sql header, controller split section.

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.

Retention is configured per organisation, with defaults of 365 days for scan data, 7 days for uploaded source files, 730 days for reports, and 2555 days (seven years) for the audit log.

Control retention-per-org-policies. 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_retention_policies, migration 002:374.

Verification. app: uq_pallas_retention_org, migration 002:385.

A scheduled job applies retention policies daily at 03:00 UTC for every organisation with automatic deletion enabled.

Control retention-daily-sweep. Status: Implemented. 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. The job is scheduled by a DO block that catches its own exception, so a database on which pg_cron was not enabled at migration time has no job and the migration still reported success. Whether the job exists and is running on the live database is an operator check against the cron.job and cron.job_run_details tables. This repository can show what was intended to be scheduled; it cannot show what is scheduled.

Implementation. app: pallas-daily-retention, '0 3 * * *', scheduled at migration 021:238; app:

pallas_apply_retention_policies, migration 021:197, rebuilt 029:629, migration 041, and migration 042.

Verification. app: supabase/migrations/042_restore_retention_sweeps_and_gaps.sql.

Archived audit events past their retention window are purged nightly at 04:00 UTC, and each purge run is logged.

Control retention-audit-purge. Status: Implemented. 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. Scheduled by the same self-catching DO block pattern as the 03:00 UTC sweep. Existence of the live job is an operator check against cron.job.

Implementation. app: pallas_nightly_retention_purge, '0 4 * * *', scheduled at migration 034:581; app: pallas_purge_expired_retained_audit_events, migration 034:460; app: pallas_retention_purge_log, migration 034:405, RLS enabled 034:416.

Verification. app: supabase/migrations/034_enforce_finding_limit_and_retention_purge.sql section 9.

Uploaded source files are purged from Storage daily at 05:00 UTC by a Supabase Edge Function invoked from the database.

Control retention-source-file-purge. 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. This job does no work unless two database settings are present: app.settings.functions_base_url and app.settings.cron_secret. When either is missing the job raises a warning and returns, so source files are NOT purged and nothing fails loudly. Migration 035:619 states this in the job body. The operator must confirm both settings are set on the live database before this control is claimed to a buyer. Separately, the 2026-08-30 inventory record describes this credential as being held in Supabase Vault under the name pallas_enforce_retention_bearer. No file in either repository references Vault or that name; the mechanism on disk is a Supabase Edge Function secret named CRON_SECRET plus a database setting named app.settings.cron_secret. The inventory description and the file set disagree, and the file set is what these repositories can show.

Implementation. app: pallas_daily_source_file_retention, '0 5 * * *', scheduled at migration 035:609; app: supabase/functions/enforce-retention/index.ts.

Verification. app: supabase/functions/enforce-retention/index.ts:239 to :252.

Retention settings cause actual deletion rather than being stored as a preference. The sweep issues DELETE statements against the tables it governs.

Control retention-deletion-actually-deletes. 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_apply_retention_policies, migration 042.

Verification. app: migration 041, which enumerates the three code paths that lawfully remove audit rows.

Retention is a transfer measure in a sense that is easy to overlook: data that has been deleted cannot be disclosed. The retention controls are therefore listed here in full, including the two whose live enforcement is not provable from source and the one that is partial, because an exporter relying on deletion as a bound on exposure needs to know which of those two positions each control is in.

5.4 What these measures do not do

The Recommendations require that supplementary measures be assessed for whether they actually address the identified problem. This subsection states where they do not.

- **Encryption at rest does not defeat compelled disclosure.** Lonia AI, or a subprocessor acting on its instruction, holds the ability to decrypt data in the ordinary operation of the Service. Encryption at rest defends against physical media compromise. It does not put the data beyond the reach of process served on the party that holds the key. An assessment claiming otherwise would be claiming that Pallas cannot read its own database.
- **No end-to-end encryption under exporter-held keys is offered.** The measure the Recommendations describe as most robust, encryption where the importer never holds the key, is not available in Pallas, because the Service reads and evaluates the content it processes. This is a design consequence rather than an omission that could be remedied by configuration.
- **Pseudonymisation of the kind the Recommendations contemplate is not applied.** User identity is functional to the Service: an audit ledger that cannot attribute an action is not an audit ledger, and organisation membership is what the isolation model is built on.
- **Residency is not sovereignty.** Restated from section 4.4 because it is the most common misunderstanding this document exists to correct.
- **Uploaded source files are unbounded in content.** The measures above apply to them equally, but no measure constrains what a customer chooses to upload. An exporter concerned about the transfer of a data category it has not authorised should control this at its own end.
- **No independent assurance stands behind any of it.**

Pallas holds no SOC 2, ISO 27001, or other independent security certification.

> Control vuln-no-independent-certification. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. Pallas holds no certification of its own. Certifications named anywhere in Pallas materials belong to subprocessors. Where a buyer requires a converted assurance rather than an assertion, the mechanism is a contractual term in the Institutional Terms of Service, the signable agreement, not a certificate Pallas can produce. There is no separate master services agreement.
>
> Verification. marketing: src/pages/trust.astro, Compliance frameworks, Planned.

Pallas has not commissioned an independent penetration test.

> Control vuln-no-penetration-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. No third party penetration test has been performed and no report exists. Security review to date has been internal, through repeated structured audits recorded in this repository. Any questionnaire field asking for the date of the last penetration test or for a report must be answered as none performed. This is a real gap for institutional buyers and it should be presented as one rather than deflected to the internal audit history.
>
> Verification. marketing: src/pages/trust.astro, questionnaire answers section.

---

6. Step five: formal procedural steps

The Recommendations require that the formal steps arising from the assessment be taken and recorded.

1. **Execution of the Clauses.** The Clauses are incorporated by reference into the Pallas Data Processing Agreement. A signable Data Processing Agreement is issued to a named counterparty on request, and the Clauses are executed as part of it, with Annexes populated for that exporter.
2. **Annex population.** Annex I identifies the parties, the categories of data subjects and personal data, the frequency and nature of the transfer, and the competent supervisory authority. Annex II sets out the technical and organisational measures, which are the controls rendered in section 5.1 rather than a separately worded list. Annex III lists the subprocessors, which are the published list rather than a subset.
3. **No supervisory authority authorisation is required.** Transfers made under the Clauses without modification to the mandatory text require no prior authorisation, and Lonia AI is not in a position to modify the mandatory text in any event.
4. **Documentation.** This assessment is published and versioned, and is referenced from the Data Processing Agreement so that an exporter can find it without asking.

---

7. Step six: re-evaluate at appropriate intervals

7.1 The commitment

Lonia AI will review this assessment at least annually, and will review it without waiting for the annual cycle on any of the following triggers.

- A change in the law or practice of the United States material to section 4.
- A judgment of the Court of Justice of the European Union, or a decision of a competent supervisory authority, bearing on transfers to the United States.
- A change in the subprocessor chain, which carries its own advance notice.
- A change to any control rendered in section 5, including a status change from implemented to partial.
- Receipt of any request from a public authority for personal data, which would make section 4.2 and section 4.4 factually inaccurate as written and would require immediate correction.

7.2 How the review is actually triggered by the build

The control renderings in section 5 are not copied into this document. They are read from the control inventory at render time, and a release gate fails the build when the inventory has changed since this document was last rendered. A control whose status changes therefore cannot silently leave a stale claim in a published assessment: the release chain stops until the document is regenerated. That is the mechanism behind the fourth trigger above, and it is the only one of the five that does not depend on someone remembering.

The build command itself runs every gate: a type check, the typography and published-document freshness checks, the six written-claim verification gates, the unit test suite over the security and

validation code, the build, an automated accessibility test against every built page, a Turnstile configuration check against the built artifact, and a sweep of the built output for forbidden claims. The hosting platform runs that command on every push, so a non-zero exit at any step fails the build and nothing deploys; the failing guards remove the dist directory so a failed build leaves nothing to deploy.

> Control appsec-release-gate-fails-closed. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.
>
> Implementation. marketing: package.json, the build script.
>
> Verification. marketing: scripts/test-a11y.mjs, scripts/test-turnstile.mjs, scripts/check-dashes.mjs, scripts/verify-doc-artifact-freshness.mjs.

7.3 The transparency statement

The factual statements in sections 4.2 and 4.4, that no request from any public authority has ever been received, are true as at the version date of this document. They are reviewed on the same cycle. Lonia AI publishes no periodic transparency report, and does not operate a warrant canary. An exporter that requires either should raise it at onboarding.

---

8. Supervisory authority positions addressed

8.1 Ireland

The Irish Data Protection Commission's position following its inquiry in the Schrems matter is that an exporter may not rely on the Clauses where the importer is subject to legislation that prevents compliance with them, and that the assessment must be evidence-based and specific to the transfer rather than generic. Two consequences follow for how this document is written.

- The destination-country analysis in section 4 addresses named statutory authorities and states, for each, whether Lonia AI claims to be outside its scope. Section 4.2 records that we do not claim to be outside Section 702.
- The measures in section 5 are stated with their limitations in section 5.4 rather than as an unqualified list, because a list of measures without an assessment of whether they address the identified problem is the generic form the Commission's position rules out.

Ireland is named as the competent supervisory authority and as the governing forum in the Clauses issued by Lonia AI, which aligns the assessment and the instrument.

8.2 Germany

The German federal and state supervisory authorities, individually and through the Datenschutzkonferenz, have taken a stricter line than most on United States transfers, and that the recurring themes in their published positions are three: that supplementary measures must be effective against the specific access identified rather than merely present; that encryption is a sufficient measure only where the importer cannot access the plaintext; and that transfers should be assessed for whether a European alternative would avoid

the transfer altogether.

This assessment addresses all three directly and, on two of them, concedes.

- **Effectiveness.** Section 5.4 states which measures do not address compelled disclosure, rather than leaving the reader to infer it.
- **Encryption sufficiency.** Conceded. Section 5.4 states that Lonia AI holds the ability to decrypt, and therefore that encryption at rest is not a sufficient measure under this test. We do not argue the point.
- **European alternative.** Conceded as a live question. There is no EU deployment today, as section 2.5 states without qualification. A German public sector or higher education buyer for whom this is dispositive should treat it as dispositive rather than as something to be negotiated around.

8.3 The other first-wave jurisdictions

- **United Kingdom.** The transfer tool is the International Data Transfer Agreement or the Addendum, and the assessment above is the transfer risk assessment that accompanies it. The Information Commissioner's Office permits either its own transfer risk assessment methodology or the European Data Protection Board approach, and this document uses the latter.
- **Switzerland.** The Clauses apply with the amendments recognised by the Federal Data Protection and Information Commissioner, including that references to the GDPR are read as references to the FADP and that the Commissioner is the competent authority.
- **Canada, including Quebec.** Not a Chapter V transfer, and assessed under the accountability principle in PIPEDA and the Law 25 requirement to assess before transferring outside Quebec. The published Quebec position is unchanged by this assessment and is not restated here.
- **Australia.** Australian Privacy Principle 8 governs cross-border disclosure. The technical and organisational measures in section 5 are the reasonable steps relied on.

---

9. Conclusion, residual position, and actions arising

Conclusion. The transfers described in section 2 may proceed under the Standard Contractual Clauses with the supplementary measures in section 5, and that nothing in the law or practice of the United States has been identified that prevents Lonia AI from complying with its obligations under the Clauses. This conclusion is Lonia AI's, it is reached without counsel's opinion, and an exporter whose own assessment reaches a different conclusion is not contradicting a fact.

Residual position: medium, and structural. It is medium for the same reason the corresponding risk in the published Data Protection Impact Assessment is medium, and the two documents are deliberately consistent: the absence of an EU deployment means every transfer is a real transfer, and no measure available to Pallas places the data beyond the reach of process served on a United States entity. Neither is fixable by a code change.

Actions arising.

1. Execute the Clauses with each exporter that requires them, with Annexes populated, rather than relying on incorporation by reference alone. Section 5.2 records why this matters.
2. Carry the public-authority-disclosure commitments in section 5.2 into the Data Processing Agreement text, so that they bind before the Clauses are executed rather than only after.

3. Review on the cycle and the triggers in section 7.1.

10. Limitations of this assessment

1. It is not legal advice, and no counsel has reviewed it.
2. It is the importer's assessment. The exporting controller remains responsible for its own, and this document is an input to it.
3. Controls whose evidence basis is a vendor assertion cannot be demonstrated by either Pallas repository. Controls whose basis is live-unverifiable are true of the migration file set and are resolved by the named operator pre-check. Both are rendered with that basis visible in section 5.
4. No independent audit, penetration test, or certification stands behind the controls, as section 5.4 records from the inventory.
5. The assessment addresses transfers to the United States. It does not assess transfers by an exporter to any party other than Lonia AI.

11. Contact

Questions about this assessment, requests for the Standard Contractual Clauses with Annexes populated for your organisation, and requests for the signable Data Processing Agreement: support@lonia.ai. General enquiries: support@lonia.ai.

An exporter whose own transfer risk assessment reaches a different conclusion from section 9 is invited to send it to the same address. A vendor that only hears from buyers who agree with it learns nothing.

Appendix A. Controls cited

This document cites 38 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.
- **auth-session-jwt** (Authentication). Implemented.
- **tenant-rls-every-table** (Multi-tenancy isolation). Implemented.
- **tenant-org-scoping-helpers** (Multi-tenancy isolation). Implemented.
- **tenant-storage-per-org** (Multi-tenancy isolation). Implemented.
- **tenant-service-role-bypass-disclosed** (Multi-tenancy isolation). Implemented.
- **audit-sha256-ledger** (Tamper-evident audit chain). Implemented.
- **audit-ledger-append-only** (Tamper-evident audit chain). Implemented.
- **audit-lawful-redaction-recorded** (Tamper-evident audit chain). Implemented.
- **audit-daily-anchors** (Tamper-evident audit chain). Partial.
- **gdpr-art15-art20-user-export** (Data subject rights). Implemented.
- **gdpr-art17-user-erasure** (Data subject rights). Implemented.
- **gdpr-controller-split-documented** (Data subject rights). Implemented.

- **retention-per-org-policies** (Retention and deletion). Implemented.
- **retention-daily-sweep** (Retention and deletion). Implemented.
- **retention-audit-purge** (Retention and deletion). Implemented.
- **retention-source-file-purge** (Retention and deletion). Partial.
- **retention-deletion-actually-deletes** (Retention and deletion). Implemented.
- **encryption-at-rest** (Encryption). Implemented.
- **encryption-in-transit** (Encryption). Implemented.
- **encryption-no-secrets-in-repo** (Encryption). Implemented.
- **encryption-member-prose-provider-held-key** (Encryption). Implemented.
- **access-org-roles** (Access control). Implemented.
- **access-rate-limiting-authenticated** (Access control). Implemented.
- **appsec-release-gate-fails-closed** (Application security). Implemented.
- **data-classes-enumerated** (Data classes and processing location). Implemented.
- **data-location-default-us** (Data classes and processing location). Implemented.
- **data-location-eu-option** (Data classes and processing location). Not implemented.
- **subprocessors-published-list** (Subprocessors). Implemented.
- **subprocessors-change-notice** (Subprocessors). Implemented.
- **subprocessors-certifications-are-theirs** (Subprocessors). Implemented.
- **physical-security-subprocessor-operated** (Subprocessors). Implemented.
- **network-perimeter-subprocessor-operated** (Subprocessors). Implemented.
- **incident-72-hour-notification** (Incident response). Implemented.
- **incident-authority-notification** (Incident response). Implemented.
- **incident-subprocessor-cascade** (Incident response). Partial.
- **vuln-no-penetration-test** (Vulnerability management). Not implemented.
- **vuln-no-independent-certification** (Vulnerability management). Not implemented.