Subprocessor & International Processing Notice

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T06 · Version 1.0.0

Provider roles, required disclosures, integration-specific boundaries and controlled changes to processing locations.

On this page

1. Purpose and scope
2. What the active schedule must disclose
3. Named integration — UIDAI OVSE / Aadhaar App
4. Named integration — DigiLocker
5. Named integration — Leegality
6. AI, infrastructure and other recipients
7. Selection, contracts and oversight
8. Processing locations and changes
9. Incidents, deletion and enquiries

▶ On this page

1. Purpose and scope

1.a — Operator. Vidyaluma is a product of KRAVIA PRIVATE LIMITED. This Notice explains how external recipients are selected, disclosed and controlled, including infrastructure, AI, communications, payments, identity and agreement-execution services. L01 covers individuals' information and L09 governs instructed school processing.

1.b — Role accuracy. A recipient may be a processor, subprocessor, independent service provider, government system or another legally relevant role depending on the actual arrangement. UIDAI, DigiLocker, a signing authority and a payment merchant must not all be described as ordinary KRAVIA subprocessors without assessing their functions and contracts.

1.c — Register status. This review version sets the required provider terms and the three named integration purposes discussed for Vidyaluma. It is not a certified complete inventory of active production recipients. The

verified active-provider schedule is a mandatory publication prerequisite and must be completed from current deployment and contractual evidence, not filled with guessed providers or regions.

2. What the active schedule must disclose

2.a — Required fields. Each active entry identifies the provider's legal entity and service, relevant Vidyaluma feature, processing role, purpose, necessary data categories, primary processing/storage locations, applicable support or backup access, retention basis and material provider-change date. Appropriate public privacy/security references are included without exposing credentials or internal connection details.

2.b — Actual rather than possible processing. A provider's catalogue of capabilities is not the Vidyaluma data inventory. The schedule must describe what is enabled in the contracted service tier and configuration. A test integration, unused SDK or planned fallback is not described as live, and a live undeclared recipient must be investigated rather than omitted.

2.c — Separate schedules. Different app packages, school functions, public website analytics and adult onboarding may use different recipients. Their schedules must be scoped so a parent can understand what happens to student data without assuming that every public-site or signing provider receives it.

3. Named integration — UIDAI OVSE / Aadhaar App

3.a — Defined purpose. The recorded Vidyaluma purpose is offline identity verification of an authorized adult school representative during onboarding. It is not student KYC, biometric attendance, school accreditation or legal authority to sign. The current registered scope, permitted claims and technical mode require verification before production claims.

3.b — Consent and alternatives. The representative receives a purpose-specific explanation and the permitted information request. Appropriate consent and a viable permitted alternative must be provided. A general subscription clause is not authorization to collect more Aadhaar-related information or share it onward for unrelated purposes.

3.c — Evidence and restrictions. Only necessary permitted outcomes and references are retained. Raw payloads, Aadhaar numbers, unnecessary copies and tokens must not enter analytics, AI or ordinary logs. Withdrawal/deletion is governed by the stricter applicable OVSE requirements and law; a generic audit-retention clause cannot be used to evade them.

4. Named integration — DigiLocker

4.a — Defined purpose. DigiLocker is used in the recorded scope for consent-based retrieval and verification of selected permitted onboarding documents for adult school representatives. It is not routine teacher login, student attendance, unrestricted locker browsing or default e-Aadhaar retrieval.

4.b — User interaction. The representative authenticates with the provider, selects or consents to relevant access and returns through the approved transaction flow. Vidyaluma does not collect the provider password or OTP. Scopes, document types and integrity requirements must match the actual approved Requester arrangement.

4.c — Separate decisions. A retrieved document does not establish authority to bind a school, execute a contract or activate a tenant. Mismatches and uncertain authority need separate review. Temporary access and document copies must be minimized, cleaned up and handled under the applicable provider conditions.

5. Named integration — Leegality

5.a — Defined purpose and role. Leegality, operated by Grey Swift Private Limited according to its published notice, is the discussed agreement-execution provider. The actual Vidyaluma arrangement must identify the chosen signing method and relevant signing-service/certifying-authority roles. This statement does not assert every Leegality feature is enabled.

5.b — Data. The signing workflow may require relevant adult signatory contact details, the agreement, execution timestamps, signature/certificate data and a necessary audit trail. Extra location, photo/video, liveness, biometric or messaging options must be assessed and disclosed only when actually enabled. They must not be turned on merely to imitate a provider demonstration.

5.c — Boundaries. Provider credentials and OTPs are entered only through the authorized provider process, not collected by support. Signed agreements and audit artifacts have controlled access, integrity checks and justified retention. Signing consent is distinct from document-retrieval consent, and a signature cannot cure missing school-authority evidence.

6. AI, infrastructure and other recipients

6.a — AI providers. Each active AI provider requires evidence of the actual service tier, no-training terms, retention, human-review practices, data locations and onward processing. An unreviewed provider cannot receive private school content, including as an automatic fallback. T03's prohibitions apply to prompts, outputs and retrieval material.

6.b — Hosting and communications. The register must identify actual cloud/database/storage, delivery, email/SMS/push, support and anti-abuse services used by the released build. Logs, metadata and remote support matter as well as database content. A publicly named hosting company is not proof of every backend or region.

6.c — Payments and analytics. School-fee payments and KRAVIA subscriptions identify their actual merchant, processor and receiving entity. Optional website analytics require separate consent and a verified inventory under L03. Neither a payment gateway nor an analytics tool is authorized to use school data for unrelated advertising by default.

7. Selection, contracts and oversight

7.a — Due diligence. KRAVIA reviews necessity, security, confidentiality, data minimization, children-related restrictions, transfer requirements, incident handling and deletion support before engaging a relevant provider. Credentials and account access are limited to authorized staff and revoked when the relationship ends.

7.b — Contractual controls. Actual processors/subprocessors receive appropriate purpose, confidentiality, security, assistance, incident and exit duties. Independent providers' own roles and legally required activities are disclosed accurately. A general provider privacy link does not replace the agreement needed for KRAVIA's arrangement.

7.c — Accountability. KRAVIA remains accountable for its selection, configuration, integration, oversight and applicable processor obligations. A provider failure requires assessment and reasonable mitigation. The Notice does not shift all operational or privacy responsibility to an external company.

8. Processing locations and changes

8.a — India-first direction. Indian data regions are preferred for core school records. This is not an absolute assurance that public-site delivery, support, AI processing, metadata or backups never leave India. Actual regions and relevant remote-access locations must be verified and disclosed with applicable safeguards and restrictions.

Skip to content

8.b — Material changes. A new recipient, service tier or material location/data-use change requires review before activation and appropriate notices under the applicable agreement and law. Where required, affected schools have a meaningful objection route. No unsupported universal notice interval is created by this Policy.

8.c — Objection and exit. KRAVIA examines a substantiated concern, considers a suitable alternative or affected-feature restriction and discusses applicable exit/remedy options when the concern cannot be resolved. An objection is not automatically answered by changing the policy after transfer has already occurred.

9. Incidents, deletion and enquiries

9.a — Incident coordination. Provider agreements and applicable legal duties may have different notification deadlines and recipients. KRAVIA tracks these separately, preserves evidence and coordinates school/user communications as appropriate. Registration or an old dashboard test is not evidence of a functioning incident-response path.

9.b — End of access. Tokens, credentials and authorized access are revoked when no longer needed. Eligible data deletion/return propagates to relevant recipients, with verified exceptions and backup schedules. A provider termination must not leave a live unmonitored integration account.

9.c — Questions and publication. Raise provider or transfer questions through /privacy-request or support@vidyaluma.in. The verified register is public and versioned; confidential contracts and security evidence may use controlled access. All policy/register changes require authorized source review and deployment, never editing through Vidyaluma's website or portals.

Related documents
L01 — Privacy PolicyL03 — Cookie & Tracking Technologies PolicyL07 — Billing, Subscription, Cancellation & Refund PolicyL09 — Data Processing AgreementL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT03 — Responsible AI PolicyT07 — Data Retention, Export & Deletion Policy

The current published version is shown. Earlier review copies do not create customer acceptance or contractual terms.

Vidyaluma

VidyaLuma

Clear school work, calmer daily decisions, and trusted records in one connected place.

Book a walkthrough

Contact support

Skip to content

Explore

School support

Trust

Legal

Copyright 2026 Vidyaluma. All rights reserved.