INDEPENDENT PRODUCT READINESS

LCMS Legal and Security Review

A GDPR-first, light-SOC-2 review of what must be true before the LCMS is sold as an independent B2B SaaS beta.

DATE	August 12, 2026
CODE REVIEWED	fef65e848e19
STAGE	Independent beta readiness
DECISION	Conditional no-go

Important: product and engineering guidance only. Not legal advice, a penetration test, or an audit opinion.

EXECUTIVE DECISION

Conditional no-go for an independent beta

Do not onboard the first independent beta customer until the ten launch gates in this report are closed. The application has a credible tenant-security foundation, but identity still depends on SolidProfessor services, privacy duties are not operationalized, and telemetry currently exports identifiable context. A SOC 2 report is not a beta prerequisite.

Beta assumptions

- B2B SaaS used only by named business administrators, editors, and reviewers.
- EU and UK organizations may participate; the service may therefore trigger GDPR/UK GDPR duties.
- Children, students, learner records, health/biometric data, and other special-category data are prohibited.
- Payment-card data is not stored or processed inside LCMS.
- The beta is small enough for tested manual privacy operations, but not for missing operations.

Report map

01 / PRODUCT EVIDENCE

A strong application foundation with three independence blockers

Findings are based on the repository at commit fef65e848e19. Production configuration, vendor contracts, access records, and operational evidence were not present in the codebase and remain unverified.

Status	Observed evidence	Beta implication
Strength	Tenant-aware routes, queries, storage prefixes, and Admin/Editor/Viewer roles.	Prove isolation with negative tests and production configuration.
Strength	Encrypted, expiring preview credentials and token hashes rather than raw source tokens in sessions.	Keep; shorten preview lifetime and bind to current user/tenant.
Strength	Multipart uploads use tenant prefixes, validation, lifecycle states, and stale-upload cleanup.	Verify private storage, encryption, malware strategy, and retention.
Blocker	Web/API authentication trusts platform-backend and VAR entry points; no standalone identity lifecycle.	Implement OIDC/SAML or contractually define the shared identity service.
Blocker	Sentry is configured with sendDefaultPii: true.	Disable; implement explicit minimization and scrubbing before any exception.
Blocker	Segment sends IP, user IDs, external UUID, tenant ID, environment, and request ID.	Disable non-essential collection for beta or add lawful controls/consent.
Gap	LaunchDarkly receives user and tenant identifiers and names.	Use private attributes/pseudonymous keys; assess as a subprocessor.
Gap	Legacy reverse-sync and direct legacy database configuration remain.	Remove/isolate from the independent deployment and secrets boundary.
Gap	Retention is undefined for accounts, logs, sessions, soft deletes, uploads, analytics, and backups.	Approve periods and prove automatic/manual enforcement.

Evidence boundary: code controls do not prove that TLS, encryption at rest, MFA, backups, regional hosting, logging, or incident response operate in production. Each needs a configuration export, test record, and owner.

02 / GDPR OPERATING MODEL

LCMS is both controller and processor, depending on purpose

The legal role must be assigned per processing activity. A single blanket description will be inaccurate.

Data / purpose	Likely role	Proposed basis	Beta control
Admin identity and membership	Controller for direct account relationship; sometimes processor for customer-managed accounts	Contract, Art. 6(1)(b), where necessary; otherwise documented legitimate interests, Art. 6(1)(f)	Notice, minimization, access and retention
Customer content and media	Processor; customer normally controller	Documented customer instructions under Art. 28 DPA	Content restriction, private storage, return/delete
Audit, sign-in, IP/device, security events	Controller for service security	Legitimate interests, Art. 6(1)(f), supported by an LIA	Limited fields/access and defined retention
Product analytics	Controller	Consent where storage/access rules require it; otherwise separately documented basis	Off for beta unless consent and vendors are ready
Errors and support diagnostics	Controller and sometimes processor	Legitimate interests for necessary reliability/security; instructions for content	Redaction, no default PII, short retention

Minimum GDPR artifacts

- Data inventory and RoPA: systems, fields, purposes, recipients, locations, transfers, retention, and safeguards (Arts. 5 and 30).
- Privacy notice: controller, purposes, bases, recipients, transfers, retention, rights, complaints, and contacts (Arts. 12-14).
- Processor DPA: instructions, confidentiality, security, subprocessors, rights support, breach support, deletion/return, and audit information (Art. 28).
- Privacy by design: minimization, private content, limited permissions, short retention, and review of every new vendor/data field (Art. 25).
- Transfer assessment: use adequacy, SCCs, or applicable UK mechanism for restricted transfers (Arts. 44-49).

DPIA / DPO / representative: under the admin-only beta assumptions, a DPIA and formal DPO are unlikely to be automatically required, but the threshold decisions must be recorded. Counsel should decide whether EU/UK representative rules apply to the actual offering.

03 / RELEASE GATE - PART 1

Ten items required before the first beta customer

Items 1-5 define the independent legal and service boundary.

01	Independent identity and tenant lifecycle Replace the platform/VAR bearer-cookie dependency with standalone OIDC/SAML or a clearly contracted shared identity service. Require MFA, safe provisioning, role assignment, revocation, and offboarding.
02	Signed beta terms and DPA Every customer accepts service terms, acceptable-use rules, privacy allocation, security responsibilities, subprocessor terms, liability framework, and beta limitations before access.
03	Privacy notice and contact routes Publish an LCMS-specific notice plus monitored privacy and security addresses. Do not rely on a generic notice unless it accurately covers this product.
04	Data map, RoPA, lawful bases, and DPIA screen Approve the data inventory and purposes; record controller/processor roles, the LIA, special-data exclusions, and DPIA/DPO/representative decisions.
05	Subprocessors and international transfers Confirm the actual deployment list, data locations, DPAs, transfer mechanisms, security posture, and customer notice/change process.

03 / RELEASE GATE - PART 2

Operational and technical beta controls

Items 6-10 make the contractual promises executable.

06	Retention, export, deletion, and rights runbook Set periods for every data class. Demonstrate account/content export and deletion, explain backup expiry, and establish a one-month request workflow.
07	Telemetry privacy correction Turn off Sentry default PII; redact secrets/content; disable non-essential Segment collection until consent and vendor controls are ready; minimize LaunchDarkly identifiers.
08	Production security baseline Prove TLS, encryption at rest, secrets, least privilege, MFA, private storage, rate limiting, dependency scanning, patch ownership, backups, and a restore test.
09	Tenant-isolation and authorization release tests Test cross-tenant reads/writes/uploads/search/preview/API access and all roles. Exclude sharing modes whose visibility rules are not fully enforced.
10	Incident and breach response Name the incident team, keep a decision log, define containment/forensics/notice, support processor notice without undue delay, and be capable of controller reporting within 72 hours where required.

Acceptable beta compromise: rights requests, export, deletion, subprocessor notices, and incident coordination may be manual if tested, owned, logged, and capable of meeting legal timelines.

04 / LEGAL PACKAGE

Documents required for an independent beta

The beta label reduces product commitments; it does not remove privacy, security, IP, or contracting obligations.

Document	Beta	Required content
Beta terms / order form	Yes	Users, beta limits, support, change/termination, confidentiality, warranty, liability, governing law, suspension, shared duties.
Data Processing Addendum	Yes	Art. 28 processing terms, TOMs, subprocessors, transfers, rights/breach support, return/delete, audit information.
Privacy notice	Yes	LCMS account/security/analytics purposes, bases, vendors, transfers, retention, rights and contacts.
Acceptable Use Policy	Yes	No unlawful content, malware, credential sharing, abusive testing, sensitive/children's data, infringement, or cross-tenant access.
Subprocessor list	Yes	Vendor, service, purpose, country/region, transfer safeguard, and change notification.
Cookie/storage notice	If used	Strictly necessary storage separated from non-essential analytics; prior consent where required.
Security overview / TOMs	Yes	Accurate access, encryption, tenancy, SDLC, vendors, monitoring, backups, incidents, and customer duties.
Vulnerability disclosure	Recommended	Monitored channel, approved safe-harbor language, report contents, and response expectations.

Additional commercial controls

- Customer retains content ownership and grants only the license needed to host, process, back up, and deliver it.
- Customer warrants it has rights/notices for uploaded materials; provide an infringement/takedown channel.
- Keep payment cards out of LCMS and document the payment-provider boundary.
- Complete an open-source license inventory/SBOM before general availability.
- Screen export controls, sanctions, education-sector rules, accessibility, and local contracting rules as markets expand.

05 / SECURITY BASELINE

Minimum technical controls for beta

Security promises should describe verified deployment reality, not only intended architecture.

Domain	Minimum beta control
Identity and access	MFA for staff/admins; least privilege; separate production access; joiner/mover/leaver process; quarterly review.
Data protection	TLS; at-rest encryption for database, storage, logs and backups; private buckets; expiring URLs; managed secrets.
Application security	Tenant/RBAC negative tests; dependency/secret scanning; upload defenses; rate limits; documented patch deadlines.
Resilience	Central logs; alert ownership; on-call escalation; automated backups; recovery targets; successful restore test.

Repository-specific engineering actions

- Set Sentry sendDefaultPii to false and add explicit event scrubbing.
- Remove IP, external UUID, and raw tenant IDs from Segment unless a necessary approved purpose exists; prefer aggregated beta metrics.
- Mark LaunchDarkly names/tenant attributes private or use pseudonymous keys.
- Remove legacy database credentials and reverse-sync workers from the independent deployment.
- Shorten preview credential duration and bind authorization to current user/tenant plus course/version.
- Apply tenant isolation, deletion propagation, minimization, and vendor controls to search indexes.

> Launch severity rule: no open critical or high vulnerabilities. Medium findings need a named owner, deadline, and beta containment accepted in the release record.

06 / PRIVACY OPERATIONS

Manual is acceptable; undefined is not

A small beta can use human-run workflows if they cover all systems, preserve evidence, and meet required timelines.

Rights and customer request workflow

1. Log the request, date, requester, customer, data scope, and LCMS legal role.

2. Verify identity proportionately without collecting unnecessary identification.

3. When LCMS is processor, route promptly to the customer/controller and act on documented instructions.

4. Search accounts, memberships, content metadata, logs, support, analytics, error monitoring, feature flags, search, and vendors.

5. Export, correct, restrict, object, or delete as directed; record exceptions and backup expiry.

6. Respond within one month under GDPR unless a lawful extension applies; retain completion evidence.

Retention decisions

Set and approve periods for active accounts, customer content, deleted-content recovery, sessions, security/audit logs, support records, multipart uploads, search copies, analytics, error events, and backups. The product must enforce the schedule and explain backup expiry; the agreement must match the implementation.

Breach workflow

Record discovery time, affected tenants/data, containment, evidence preservation, risk assessment, vendors, decisions, and communications. As processor, notify the controller without undue delay. As controller, be capable of supervisory-authority notification within 72 hours where risk triggers it, and direct notification where risk is high.

07 / LIGHT SOC 2

Build evidence habits now; do not buy an audit for beta

SOC 2 is independent assurance over controls, not a product license and not a substitute for GDPR. Do not claim 'SOC 2 compliant' or 'certified.' A CPA firm issues the examination report.

Family	Light beta practice	Evidence
CC1-CC2 Governance	Name security owner; approve short policies; define responsibilities; annual security/privacy training.	Policies, approvals, responsibilities, training records.
CC3 Risk	Maintain product risk register; review for releases and material vendor/architecture changes.	Risks, owners, due dates, treatment decisions, review notes.
CC6 Access	MFA, least privilege, approvals, timely offboarding, quarterly review.	Identity settings, approvals, termination tickets, review exports.
CC7 Operations	Monitor alerts/vulnerabilities, own patch deadlines, run an incident tabletop.	Scans, remediations, alerts, incident/tabletop records.
CC8 Change	Peer review, automated tests, controlled deploys, rollback and emergency-change records.	PR reviews, CI results, deployment logs, change records.
CC9 Vendors	Inventory/tier vendors; review security, privacy, regions, contracts, and exit options.	Vendor register, reviews, DPAs, SOC reports, renewals.

Later path: consider Type 1 when control design and the system description are stable. Pursue Type 2 only after controls have operated long enough to produce consistent evidence, commonly at least several months. Security is the required Trust Services Category; add others only when customer commitments justify scope.

08 / DELIVERY PLAN

30/60/90-day path to a controlled beta

The plan starts by shrinking scope, then proves controls, then operates the beta with evidence.

Window	Outcome	Work
Days 0-30	Define and shrink	Name owners; data map/roles; choose identity; disable PII telemetry; vendor inventory; draft terms/DPA/notices/AUP/TOMs/retention/rights/incident; create risk register.
Days 31-60	Implement and prove	Deliver identity/tenant lifecycle; remove legacy path; configure encryption/MFA/secrets/backups; deletion/export; tenant/RBAC tests; vendor DPAs/transfers; scan and restore test.
Days 61-90	Run named beta	Sign documents; readiness sign-off; incident tabletop and request rehearsal; monitor support/security; access/vendor review; collect change/deployment evidence; reassess scope before expansion.

Go decision

Product, Security, and Legal should sign a one-page release record listing every gate, evidence link, residual risk, accepting owner, and customer restriction. An open blocker keeps the decision at no-go. Medium residual risks require written acceptance, a deadline, and beta-specific containment.

What is not required for beta

- A SOC 2 Type 1 or Type 2 report.
- ISO 27001 certification.
- A full self-service privacy portal, if the manual workflow is tested and timely.
- A formal DPO when the documented Art. 37 threshold is not met.
- A global legal package for every country before selling only to named beta customers in approved locations.

09 / LAUNCH EVIDENCE

What the reviewer should be able to open

A launch gate is closed only when the evidence exists and matches production.

Evidence	Owner	Pass condition
Data map, RoPA, lawful-basis/LIA, DPIA screen	Privacy / Product	Approved, dated, matches production fields/vendors.
Terms, DPA, notice, AUP, TOMs, subprocessors	Legal / Privacy	Approved versions and signed customer acceptance.
Identity, MFA, access, tenant-isolation proof	Engineering / Security	Configuration, negative tests, access review.
Telemetry fields and redaction proof	Engineering / Privacy	No default PII; only approved fields/vendors.
Encryption, secrets, backups, restore result	Platform	Production configuration and successful restore.
Vulnerability/dependency results	Security / Engineering	No critical/high; lower findings owned and dated.
DSAR/delete/export rehearsal	Support / Privacy	Completed within target across systems/vendors.
Incident tabletop and breach log	Security / Legal	Scenario, decisions, gaps, owners, closure dates.
Beta release sign-off	Product / Security / Legal	All gates closed or contained and accepted.

10 / SOURCES

Primary legal and assurance references

The report uses official regulatory and professional sources. Legal applicability still depends on the actual entity, customers, data, deployment, and contracts.

- EU General Data Protection Regulation - official text
- EDPB Guidelines 07/2020 on controller and processor concepts
- EDPB Guidelines 9/2022 on personal-data-breach notification
- European Commission rules on international data transfers
- European Commission Standard Contractual Clauses
- ICO guidance on controller-processor contracts
- ICO guidance on data protection by design and default
- ICO guidance on cookies and storage/access technologies
- AICPA Trust Services Criteria

Repository evidence

Reviewed: resources/js/app.ts; SegmentTracker; LaunchDarklyContext; EntryPointAuthenticator; SyncPlatformSession; PreviewToken; multipart-upload services/tests; tenancy and permission configuration; routes; CI; migrations; and dependency manifests at fef65e848e19.

> Important: This report is product and engineering guidance, not legal advice, a penetration test, or an audit opinion. Qualified privacy and commercial counsel should approve the legal documents and jurisdiction decisions before launch. A security professional should validate production controls.

Review limitations

No production environment, vendor agreement, subprocessor portal, cloud console, identity provider, support process, policy set, incident history, penetration-test report, or customer contract was inspected. Items dependent on those sources are readiness requirements, not confirmed deficiencies.