

Ovieda Legal Review Packet

Privacy, Terms, DPA, Subprocessors, Retention, AI Disclosure, and Trust/Security Claims

Prepared for lawyer review - June 28, 2026

Purpose

This packet consolidates the Ovieda legal-sensitive drafts and public trust/security claims into one reviewable PDF. Please review for customer-evaluation accuracy, misleading statements, missing legal boundaries, and unsupported claims before these materials are relied on in customer conversations or contracts.

Important: this packet is not legal advice, privileged legal analysis, counsel approval, or final contract language. It is a draft review artifact.

Live policies page	https://vendorly-app.onrender.com/policies
Live trust page	https://vendorly-app.onrender.com/trust
Review packet source	docs/LEVEL2_LEGAL_PRIVACY_SECURITY_REVIEW_READY_20260628.md
Product name	Ovieda

1. Review Instructions

Please review the following questions. The goal is not to make Ovieda enterprise-perfect today. The goal is to confirm that the current draft legal and trust statements are accurate, appropriately limited, and safe for customer evaluation.

- Do the privacy, terms, DPA, subprocessor, retention, and AI statements accurately describe the product?
- Are draft documents clearly labeled as drafts and not final contractual commitments?
- Do any statements overclaim SOC 2, pen testing, SSO, SCIM, MFA enforcement, immutable logging, SLA, service credits, legal advice, or counsel approval?
- Are AI outputs properly described as assistive, with human reviewers owning final decisions?
- Are deletion, retention, audit trail, export, password reset, backup/restore, and subprocessor claims accurate and appropriately bounded?
- What changes are required before these materials can be sent to prospects, attached to a contract, or posted as final public legal documents?

Suggested signoff standard

Reviewer may sign only if the materials are accurate for customer evaluation and contain no known unsupported overclaims. Counsel approval of final contract language is a separate, stronger standard and should not be implied unless explicitly given.

2. Legal Drafts for Review

These sections are the core legal documents and disclosures your lawyer friend should review first.

Privacy Policy Draft

Status: Draft for review

- Ovieda processes account information, tenant-scoped vendor review records, uploaded vendor evidence, AI-assisted findings, reviewer decisions, exports, and audit events.
- Data is used to operate the compliance workspace, generate review assistance, preserve source context, support human decisions, and provide buyer-ready exports.
- Admins can delete active review evidence from the workspace. Deletion actions are recorded in the audit trail.
- Backup retention, legal hold, post-termination deletion, and customer-specific retention commitments require final policy approval before contractual use.

Terms of Service Draft

Status: Draft for review

- Ovieda provides AI-assisted vendor compliance review workflow software; it does not provide legal, insurance, procurement, or security advice by itself.
- Customers remain responsible for final vendor approval, rejection, escalation, accepted-risk decisions, and use of exported materials.
- Users must not upload unlawful content or use Ovieda to make automated vendor approval decisions without human review.
- Availability, support, service credits, indemnity, liability limits, and enterprise identity commitments require approved commercial terms.

Data Processing Addendum Outline

Status: Draft outline

- Processing purpose: operate a tenant-scoped vendor evidence review workspace and related exports.
- Data categories: account data, vendor evidence, findings, source excerpts, decisions, notes, exports, and audit events.
- Security measures: authenticated access, role-based permissions, tenant scoping, password hashing, private evidence storage design, audit logging, and human approval control.
- Open items: approved subprocessors, transfer terms, audit assistance, breach-notification language, retention, deletion, legal hold, and customer return/export obligations.

Subprocessor Disclosure Draft

Status: Deployment-dependent

- Hosting and managed database provider: Render-hosted frontend/API and database services in the current deployed environment.
- Private object storage provider: configured AWS S3 bucket for uploaded vendor evidence; latest storage proof shows region and security posture in retained evidence artifacts.
- AI processing provider: AI-assisted analysis uses the configured AI provider only when assessment features are enabled.
- Final customer-facing subprocessor commitments must include active provider names, regions, roles, transfer posture, and legal review.

Retention and Deletion Draft

Status: Draft for review

- Active workspace review evidence can be deleted by admins through the app when storage deletion succeeds.
- Deletion produces an audit event and deletion receipt so the workspace can prove the action occurred.
- Audit events may remain after active review deletion to preserve security and compliance history.
- Backup purge timing, legal hold exceptions, post-termination deletion, and customer-specific retention windows require final policy approval.

AI and Data-Use Disclosure Draft

Status: Draft for review

- Ovieda uses AI to assist evidence review by extracting signals, drafting findings, identifying gaps, and preserving source context when readable evidence exists.
- AI output is not an approval decision. A human reviewer owns approval, rejection, escalation, accepted-risk, and evidence-request decisions.
- Findings should be reviewed against source evidence; weak or missing source support is labeled for manual verification.
- Provider-specific data-use, model-training, retention, and subprocessor language must be reviewed against the active AI provider terms before contractual reliance.

3. Trust and Security Claims for Review

These are legal-sensitive public claims. They are not formal legal documents, but a lawyer should check them because buyers may rely on them.

Current public posture statement

Core workflow, password-reset delivery, and backup/restore proof exist. Broad enterprise commitments still require final legal/security review.

Verified Product Controls

- Authenticated workspace access with role-based admin, reviewer, and viewer permissions.
- Tenant-scoped reviews, findings, users, operational evidence, exports, and audit events.
- Human approval control: AI-assisted findings do not automatically approve vendors.
- Source-backed findings where document text is readable, with manual-verification language when evidence is weak or unavailable.
- Blocked approval behavior when unresolved high-risk blockers or required review notes remain.
- Exportable review reports, evidence requests, audit logs, deletion receipts, access-review proof, and operational-evidence packets.
- Admin-only evidence deletion with audit trail events.
- Operational evidence tracking for monitoring, backup/restore, incident response, storage smoke tests, access review, legal review, and security process readiness.

Live Proof Retained

- Live Render app and API gate passed against the deployed environment.
- Credential-backed six-PDF workflow regression passed against the live app.
- Performance smoke proof retained for public app load, API health, authenticated sign-in, and authenticated review-list load.
- Password-reset delivery and backup/restore proof are retained in Level 2 evidence artifacts.
- Backend alert proof and uptime-monitor proof retained.
- Security regression and hardening marker checks are part of the repository quality workflow.

Boundaries and Non-Claims

- Ovieda is AI-assisted review software, not legal, insurance, procurement, or security advice.
- A human reviewer remains responsible for approval, rejection, escalation, and accepted-risk decisions.
- SOC 2, penetration testing, contractual SLA/service-credit terms, SSO/SAML/SCIM, and counsel-approved legal terms are not claimed as complete unless separately evidenced.
- Legal/privacy review, final public claims, and broad recovery/SLA commitments require retained proof and review before broad enterprise commitments.

Data and AI Handling

- Customer workspace records are scoped by tenant.
- Uploaded vendor evidence is processed to create findings, source excerpts, review decisions, and exports.
- Admins can delete active review evidence from the workspace; backup retention and legal-hold behavior require final policy language.
- AI output is treated as reviewer assistance and should be verified against source evidence before reliance.

Vulnerability Disclosure Process

- Report suspected vulnerabilities through the published security.txt contact path or to the accountable Ovieda workspace owner during evaluation.
- Include the affected URL, reproduction steps, observed impact, and a safe proof artifact; do not include unrelated personal data, secrets, or customer evidence.
- Ovieda triages reports by severity, records remediation work in release evidence, and verifies fixes before broad deployment.
- Critical and high-severity reports are targeted for first review within one business day during customer evaluation; contractual response times require final support terms.

4. Known Non-Claims and Open Legal Items

These are intentionally not claimed as complete unless separately reviewed and evidenced.

- Completed SOC 2 audit or SOC 2 certification.
- Third-party penetration test completion.
- Contractual uptime SLA, service credits, or final support terms.
- SSO/SAML, SCIM, or MFA enforcement as completed enterprise identity controls.
- Immutable or external audit logging guarantee.
- Counsel-approved privacy policy, terms, DPA, or final subprocessor commitments.
- Customer-specific retention, legal-hold, post-termination deletion, or backup purge guarantees.
- AI provider data-use or model-training guarantees beyond reviewed provider terms and account settings.

Proof items already retained

- Password-reset delivery proof:
output/ovieda-level2-password-reset-check/ovieda-password-reset-delivery-test-20260628-083502.json
- Backup/restore proof: output/ovieda-level2-backup-restore-proof/ovieda-backup-restore-proof-20260628-084524.json
- Latest live Level 2 gate bundle: output/github-level2-live-gate-run-28319941135/ovieda-level2-live-gate-report/

5. Reviewer Signoff Checklist

Use this page after review. If any item is not true, list required edits in the follow-up section instead of signing off.

Item	Reviewed?	Notes
Privacy policy draft reviewed for customer-evaluation accuracy.	☐	
Terms draft reviewed for customer-evaluation accuracy.	☐	
DPA outline reviewed for customer-evaluation accuracy.	☐	
Subprocessor/data-flow position reviewed for customer-evaluation accuracy.	☐	
Retention/deletion language reviewed for customer-evaluation accuracy.	☐	
Trust/security page reviewed for customer-evaluation accuracy.	☐	
AI disclosure and human-review language reviewed for customer-evaluation accuracy.	☐	
Customer-facing claims match the live product.	☐	
Contractual-use boundary is documented.	☐	
No known unsupported overclaims remain.	☐	

Reviewer name	
Reviewer role	
Review date	
Signature / approval	
Required edits / open follow-ups	

Suggested approval wording: I reviewed the Ovieda legal/privacy/security packet for customer-evaluation accuracy. The privacy, terms, DPA, subprocessor/data-flow, retention/deletion, trust/security, and AI disclosure language matches the live product to the best of my knowledge, the contractual-use boundary is documented, and I know of no unsupported overclaims.