

# Product Policy Document: Legora (platform): Contract-Verified

---

**Product and vendor:** Legora (Legora AB). Collaborative legal AI platform: the aOS workspace, Tabular Review, workflows, legal research, plus Word and Outlook add-ins and an Agent surface.

**Way of working:** Platform, with add-in surfaces. The core posture is upload-first into Legora's Azure-hosted cloud; the Word and Outlook add-ins are extensions of the same account, and they inherit this row's posture (see Section 3, step 5).

**Status: Ready to adopt (contract-verified), subject to the order-form confirmations in Section 3.** Legora publishes region-specific contract stacks, and the US stack was read in full on 2026-08-05. The earlier report in this workstream ("no published provider-level ZDR; ask") was wrong and has been corrected: the US General Terms contain protections near-verbatim to Harvey's, same drafting lineage, same liability numbers (Exhibit 19).

**Implements:** Model Firm AI Use Policy (42/02). Exhibits: 18 (Legora US General Terms and Conditions, updated May 2026, retrieved 2026-08-05); 19 (Legora contract stack verification memo, 2026-08-05; the legal index page re-checked 2026-08-08, same document set published); 11 (Wave 1 exhibits pass memo).

**Document date:** 2026-08-08.

## 1. What this is

Legora is a vendor-hosted legal AI platform sold by negotiated subscription: the firm's documents upload into Legora's cloud (hosted on Azure), and review, research, and drafting workflows run over them with models Legora chooses. The US-region AI chain is OpenAI (direct, US residency), Microsoft, AWS, and Google; **Anthropic appears nowhere on the pre-approved sub-processor list** (Exhibit 19).

The contract posture matches Harvey's almost clause for clause. **No training:** Legora will not use the firm's Confidential Information to train or fine-tune AI models, nor allow its subcontractors to (US GTC clause 8.3.3). **No provider retention:** no subprocessor, "except for cloud storage providers," retains or logs Subscriber Content for human review (clause 9); Subscriber Content is defined to reach prompts, documents, and outputs. **Stability:** Legora may not alter the terms in a way that detracts from its confidentiality, content, or security obligations without the Subscriber's express written consent (clause 10.10.2). **Exit:** retrieval assistance in machine-readable format, deletion of remaining Subscriber Content 30 days after termination, written certification on request (clause 4.3.2); confidentiality of Subscriber Content survives for at least 100 years (clause 4.3.3).

Two differences from Harvey matter operationally. First, **there is no covered-model mechanism in the published stack:** no Extended-AI-Features-style carve-out, no Anthropic subprocessor, so as published there is no 30-day-safety-window model in the chain, and no opt-in decision to make. Even the Beta Features clause (2.4) expressly preserves the confidentiality and content protections, so the beta path cannot quietly relax retention. That is one less decision and one less risk surface. Second, **the enterprise packages hand the firm more residence controls than Harvey publishes:** the firm sets the storage location, sets the retention period, and can manage its own encryption keys (Security Measures section 17, via Exhibit 19). The same upload-first architecture caveat applies: the cloud-storage exception in clause 9 is where the firm's documents live for the term, so the Section 6 record habit carries the same weight here.

## 2. The Approved Tool List row (implements Section 3)

**Legora (platform, including Word and Outlook add-ins). Tier / account type:** Enterprise subscription; order form [reference] | **Training disabled:** Yes; contract (US GTC 8.3.3) | **Memory off / scoped:** No vendor personalization

feature published [confirm at order-form review] | **Retention terms:** Provider retention barred by contract, cloud storage excepted (GTC 9); firm sets storage location, retention period, and keys (enterprise package); deletion 30 days after termination, certification on request (GTC 4.3.2) | **Permitted input tier:** Tier 2 upon signature | **Agentic capabilities:** Legora Agent and workflows: platform-hosted; policy Section 5 human-review rules apply; enumerate enabled surfaces here | **Approved date:** [date of adoption] | **Notes:** No covered model in the published stack; no opt-in decision pending. Terms-stability clause GTC 10.10.2. ISO 27001 warranted through the term (7.3.2)

### 3. Required setup (implements Sections 3 and 4): the order-form checklist

Steps 1 through 7 are the Administrator's; step 8 is every user's.

1. **Confirm the US stack applies unmodified.** Legora's legal page is region-selectable (EU, UK, US, AU); confirm the order form incorporates the US General Terms and the US Data Processing Agreement, and that nothing in it detracts from clauses 8.3.3, 9, or 4.3.2. File the executed set with this document.
2. **Set the residence controls.** The enterprise package lets the firm set storage location, retention period, and key management (Exhibit 19). Set US storage, set the retention period as a deliberate choice against the Section 6 record needs, and record all three settings on the row. This is the one place Legora gives the firm more control than Harvey publishes; use it.
3. **Verify the ethical walls.** Cross-matter isolation and ethical walls are advertised product features; the policy requires walls verified at vetting, not taken on the brochure. Test with two dummy matters before first client use, and map workspaces to matters one-to-one, mirroring the folder-scoping rule.
4. **Enumerate and gate the agent surfaces.** Workflows, Tabular Review runs, and the Legora Agent execute multi-step work on the platform; each enabled surface goes on the row, and the autonomous-action prohibition applies unchanged (nothing files, sends, or communicates externally without attorney review). The Outlook add-in touches client communications; decide deliberately whether it is enabled at all in wave one of the rollout.
5. **Record the add-in binding.** The Word and Outlook add-ins are this account's surfaces, and they inherit this row (the policy's add-in rule: the add-in's posture is the posture of the account behind it). The document-wide-disclosure warning applies: an add-in reads the whole open document, so the Tier check is on the document, not the highlighted passage.
6. **Subscribe to sub-processor change notices** (30-day advance posting and objection right, with fee adjustment or termination as outcomes, DPA clause 4.2). The Administrator receives these. Watch for one change in particular: Anthropic appearing on the list would put a covered model in the chain and re-open the safety-window analysis this row currently does not need.
7. **Ask the pricing-model questions** (policy Section 3, vetting item 6): seat definitions, staff seats, usage components, cap behavior before deadlines.
8. **Users: complete training** before first client use: the upload-first fact (Section 4), the export habit (Section 6), the add-in document-wide-disclosure rule, and the tracked-changes rule for documents Legora edits.

### 4. What may go in (implements Section 4)

- **Tier 1:** permitted.
- **Tier 2 (client documents and matter facts):** permitted once the order form is executed on the US stack and the Section 3 configuration is done.
- **Tier 3:** prohibited absent informed client consent and Administrator approval, as everywhere. The firm-managed keys and firm-set storage location are relevant facts for any future Tier 3 consent conversation; the call remains case by case.

**This product's specific hazards are the upload reflex and the add-in blur.** The platform hazard is Harvey's: uploading is disclosure, and after a month it stops feeling like it. The add-in hazard is Copilot's: Legora inside Word and Outlook makes the AI ambient in the drafting and correspondence surfaces, and every invocation from an open document is a whole-document input. Matter-scoped workspaces (step 3) and the document-level Tier check (step 5) are the controls.

## 5. Verification (implements Section 5)

Unchanged: the four-step ladder, the statute check, the no-delegation rule. Legora's research and review outputs are aids, not substitutes; court-bound citations get all four steps. Documents edited on the platform or through the Word add-in come back through the reviewable-record rule: keep the before version, compare, review the changes.

## 6. The record (implements Sections 8 and 10)

The platform holds the session log; the firm does not, unless it acts. The habit: for any session that materially assists work product, export the operative content into the matter file the same day. The retention period the firm sets in Section 3, step 2 should be set with this section in mind: long enough to reconstruct billing and revisit sessions, no longer than the confidentiality analysis supports. At termination, use the machine-readable retrieval assistance (GTC 4.3.2) before the 30-day deletion clock, and request the written deletion certification for the file.

Billing: subscription overhead under Section 8; if the order form contains usage components, the pass-through rules (disclosure, actual cost) apply to any client charge.

## 7. Vendor facts and evidence grades

**No training on the firm's Confidential Information, by Legora or subcontractors.** Source: Exhibit 18, US GTC clause 8.3.3 | **Grade:** Contract (standard published form) | **Date:** Updated May 2026, retrieved 2026-08-05

**No subprocessor retention or human-review logging, cloud storage excepted; reaches prompts, documents, outputs.** Source: Exhibit 18, clauses 9 and 12 | **Grade:** Contract | **Date:** Same

**Terms cannot be altered to detract from confidentiality, content, or security obligations without written consent.** Source: Exhibit 18, clause 10.10.2 | **Grade:** Contract | **Date:** Same

**Deletion 30 days after termination, machine-readable retrieval, written certification on request.** Source: Exhibit 18, clause 4.3.2 | **Grade:** Contract | **Date:** Same

**US AI chain: OpenAI (direct, US residency), Microsoft, AWS, Google; no Anthropic.** Source: Exhibit 19 (sub-processor list updated 2026-07-06) | **Grade:** Published list | **Date:** Retrieved 2026-08-05

**Firm-set storage location, retention period, key management (enterprise).** Source: Exhibit 19 (Security Measures section 17) | **Grade:** Published | **Date:** Same

**Beta Features preserve confidentiality, security, and content protections.** Source: Exhibit 18, clause 2.4 | **Grade:** Contract | **Date:** Same

**ISO 27001 maintained through the term.** Source: Exhibit 18, clause 7.3.2 | **Grade:** Contract warranty | **Date:** Same

**Not established:** order-form variation in practice; whether any hyperscaler channel carries an Anthropic covered model in a specific deployment (nothing published suggests so); the US DPA annexes and Specification of Data Processing were skimmed, not read line by line (Exhibit 19, section F). **The ask for the vendor:** written confirmation at signature that no covered frontier model (any model with a retention or human-review carve-out) is in the firm's deployment chain, and the current sub-processor list as of the order-form date.

## 8. Re-vetting triggers (implements Section 12)

1. **Anthropic (or any provider with a safety-window carve-out) appears on the sub-processor list:** this row's no-covered-model posture is its distinguishing feature; that change re-opens the analysis.
2. **US GTC or DPA updates** (the stability clause makes detracting changes require the firm's written consent; the request itself is the trigger).
3. **Sub-processor change notices** (30-day posting; the Administrator objects or accepts deliberately, DPA clause 4.2).
4. **New product surfaces** (the Agent, Monitors, Portal, or a new add-in changing what data leaves the workspace or arrives ambiently).
5. **Changes to the enterprise residence controls** (storage location, retention, key management moving or narrowing).
6. **Pricing model changes.**