DECISIONFLOW

# Data, Privacy and AI Decommissioning Plan

*Exporting, retaining, deleting, and verifying customer and AI-related data through a governed closure process*

RETIRE PHASE | Version 1.0 | Illustrative controlled retirement and knowledge-preservation program

**EVIDENCE & PUBLISHING INTEGRITY**

This public portfolio edition distinguishes actual evidence, assumed continuity steps, simulated case-study outcomes, targets, and recommendations. Simulated customers, commercial results, benchmarks, incidents, quotations, and later-lifecycle outcomes are illustrative and must not be interpreted as results from a live commercial product. Evidence labels are retained throughout the package to support transparent and responsible interpretation.

## Document Control

| Control | Definition |
|---|---|
| Document code | RET-03 |
| Version / status | 2.0 — Final Public Portfolio Edition — Simulated Retirement Scenario |
| Baseline / author | 14 July 2026 - Min Thu Kyaw |
| Scenario horizon | Illustrative 24-month post-scale operating period followed by a 180-day retirement program. |
| Lifecycle continuity | Actual MVP -> assumed productionization -> simulated Launch -> Qualify -> Deliver -> Controlled Scale -> Retire. |
| Retirement decision | Retire the standalone service through a controlled transition while preserving reusable product, AI, and technical assets. |
| Scope boundary | No new collaboration, integration, richer-ingestion, multilingual, SSO, or enterprise-platform build is assumed. |
| Evidence rule | Actual, assumed, simulated, target, recommendation, and verified-shutdown statements are separated. |

### Actual Project Artifacts

| Artifact | Reference |
|---|---|
| Low-Fidelity Prototype | View prototype |
| High-Fidelity Prototype | View prototype |
| MVP Frontend Repository | Open repository |
| MVP Backend Repository | Open repository |

# Contents

# Objectives and Governing Principles

- Customer records remain owned and accessible only according to the existing authorization model during transition.
- Retention is minimized and tied to customer choice, contract, law, legal hold, security, or verified operational need.
- Deletion includes primary stores, temporary exports, caches, logs where applicable, backups after their retention window, and third-party processors according to contract.
- Customer content is excluded from preserved prompt, evaluation, demonstration, and research assets unless separately authorized and anonymized.
- Every destructive action requires evidence, ownership, exception handling, and independent review.

# Data Inventory and Classification

| Data class | Examples | Retirement disposition | Owner |
|---|---|---|---|
| Account identity | Email, name, password hash, account status. | Retain only through transition, billing, dispute, or legal requirements; then delete. | Identity / Privacy |
| Decision content | Transcripts, notes, options, criteria, recommendations, risks, actions. | Export or delete by account disposition; never reuse by default. | Product Data |
| AI metadata | Model, prompt version, latency, usage, fallback, confidence. | Export with record where useful; retain aggregated non-content metrics only if approved. | AI Operations |
| Audit and security | Access logs, history, incident evidence. | Retain for approved security/legal period; minimize identifiers. | Security |
| Billing and contracts | Invoices, credits, payment identifiers, agreements. | Retain under finance and legal schedule. | Finance / Legal |
| Analytics | Event data and cohort metrics. | Delete direct identifiers; retain only approved aggregated evidence. | Product Operations |
| Backups | Encrypted database and object-store snapshots. | Expire according to documented schedule; prevent restoration into active service. | Platform |

# Export, Retention and Legal Holds

| Condition | Action | Control evidence |
|---|---|---|
| Customer export selected | Generate complete archive and retain temporary file only for the approved download period. | Checksum, record count, delivery log, expiry record. |
| Customer deletion selected | Queue eligible content for deletion after identity verification and cooling-off period. | Request, verification, deletion job, completion notice. |
| No customer response | Apply published contract/privacy default after repeated notice and escalation. | Communication log and policy reference. |
| Legal hold | Segregate affected data; suspend deletion only for defined scope and period. | Counsel approval, hold ID, owner, review and release date. |
| Security investigation | Retain minimum necessary evidence under security policy. | Incident ID, scope, access restriction, disposition date. |

## Legal-hold register controls

- Legal holds are never inferred from customer tier or internal preference.
- Each hold identifies authority, data scope, accountable counsel, access list, review date, and release condition.
- Held data is encrypted, isolated from active application paths, and excluded from model evaluation.
- At release, the normal deletion workflow resumes and evidence is appended to the hold record.

# Deletion and Backup Expiration

1. Freeze data-model changes and complete the authoritative inventory.
2. Delete temporary export files after delivery or expiry.
3. Delete eligible active-database records and associated object storage.
4. Invalidate caches, indexes, search replicas, queues, and derived stores.
5. Mark backups containing deleted data as non-restorable to production and allow them to expire under the approved schedule.
6. Verify deletion jobs, exception queues, and legal-hold exclusions.

7. Issue account-level or batch deletion evidence and close residual exceptions.

| Store | Target timing | Verification |
|---|---|---|
| Temporary exports | Within 7 days of download or expiry. | Object inventory and access-log check. |
| Primary application data | By T+60 for eligible records. | Database count reconciliation and deletion job logs. |
| Search/cache/queue derivatives | Within 24 hours of primary deletion. | Service-specific inventory and tombstone verification. |
| Encrypted backups | Expire by T+90 or approved backup schedule. | Backup catalog and restore-control review. |
| Legal-hold archive | At hold release date. | Counsel sign-off and deletion evidence. |

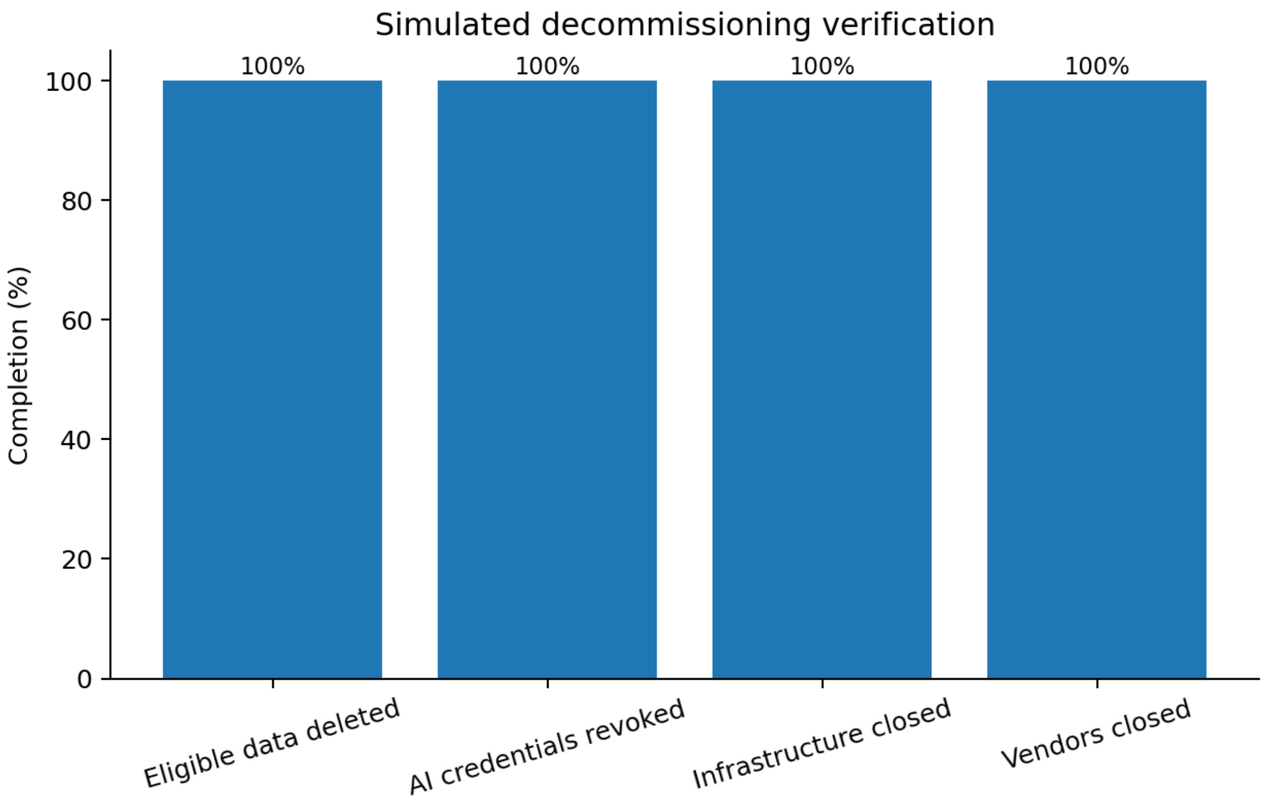
# AI Provider and Credential Closure

| Control | Required action | Evidence |
|---|---|---|
| Generation cutoff | Disable new extraction and recommendation requests before final service shutdown. | Feature flag and API test. |
| Provider credentials | Revoke OpenRouter/model-provider keys and any fallback-provider credentials. | Provider console and secret-manager evidence. |
| Prompt jobs | Stop evaluation, monitoring, scheduled regression, and cost-reporting jobs that invoke models. | Scheduler inventory at zero. |
| Provider data | Exercise contractual deletion/retention rights and record processor response. | Vendor confirmation and DPA reference. |
| Model telemetry | Retain only approved aggregated metrics without customer content. | Dataset review and privacy approval. |
| Fallback logic | Disable production invocation and archive code/config with documentation. | Repository tag and operational sign-off. |

# Prompt, Evaluation and Research Assets

| Asset | Preserve? | Conditions |
|---|---|---|
| System and task prompts | Yes | Remove secrets and customer examples; document purpose, version, and known limitations. |
| Pydantic/JSON schemas | Yes | Preserve as reusable technical IP and traceability evidence. |
| Evaluation methodology | Yes | Retain metrics, rubrics, synthetic fixtures, and scoring code. |
| Customer-derived fixtures | No by default | Delete unless separately authorized, de-identified, and legally approved. |
| Aggregated benchmark results | Yes, if approved | No customer identifiers or reconstructable content. |
| Prompt-injection and safety tests | Yes | Retain synthetic/adversarial cases and remediation history. |
| Product research synthesis | Yes, anonymized | Retain themes, not raw customer transcripts or identifiable quotations. |

# Verification and Evidence




*Simulated decommissioning verification*

| Verification item | Simulated result | Residual control |
|---|---|---|
| Eligible customer data deleted | 100% | 2 legal holds remain separately governed. |
| AI credentials revoked | 100% | Quarterly secret scan of archived repositories. |
| Critical data-loss incidents | 0 | Final export and deletion evidence retained. |
| Processor closure | All AI and hosting processors dispositioned. | Contract archive and vendor confirmation retained. |
| Evidence archive | Complete | Read-only access restricted to approved owners. |

*Evidence discipline: replace all simulated retirement values with observed, reproducible records before presenting them as actual product performance or compliance evidence.*