**2) Tenant Data Retention Matrix — “Hot/Warm/Archive + Legal Holds”**

**Intent**  
Keep costs low while preserving auditability: tier every artifact with explicit lifetimes and legal-hold overrides.

**Actors**  
Retention Engine • Tiered Storage • Legal Hold Service • Ops Pilot • Tenants

**Preconditions**

* Artifacts cataloged: Partners, Materials, Decisions, Snapshots, Tokens (CBT/LRT), Logs, Evidence Packs.
* Default policy per tier.

**Flow**

1. **Matrix Setup**: define per-artifact policy (Hot/Warm/Archive durations, delete actions).
2. **Lifecycle Labels**: write every object with retention\_class, tenant\_id, delete\_at.
3. **Auto-Tiering**: move objects at boundaries (e.g., Hot→Warm at 90d) with **tier-switch receipts**.
4. **Legal Hold Token**: apply hold that **freezes** delete/tier moves; every hold has scope, reason, owner, expiry.
5. **Right-to-Erase (where lawful)**: create redacted shadow + store a **Tombstone Receipt** (hash of removed PII, requestor, time).
6. **Recall ETA Predictor**: for restores from archive, show ETA (hours) to Ops & tenant.
7. **Policy Drift Guard**: policy change triggers preview of impacted objects before commit.

**Acceptance**

* No object deleted while active **Legal Hold** exists.
* Tier moves verifiable by receipts; recalls succeed within displayed ETA.
* PII erasures logged with Tombstone Receipt; decisions remain reproducible (inputs redacted but hashed).

**Innovations**

* **Tombstone Receipts** for regulated erasure.
* **Recall ETA Predictor** (reduces support ping-pong).