

Compliance + Audit-Verifier Handbook

Regulatory posture, erasure and encryption, audit-chain architecture, and verifier walkthrough.

§1 Regulatory posture by jurisdiction

Framework	Sparcle's posture	Customer's path
HIPAA (US health)	Architecture deployable. Bolt is self-hosted, so Sparcle operates no system that PHI passes through. The LLM you configure receives the masked prompt. A signed DPA comes with Bolt Certify. BAA available: support keeps PHI out of Sparcle systems, or we sign a BAA where we may see PHI (target November 2026).	Customer's existing HIPAA program covers Bolt as software deployed inside its boundary. The configured LLM provider needs its own BAA.
HITRUST CSF	Not held. On the long-term roadmap, not in flight.	Customer's HITRUST controls map to the deployed architecture (per-tenant CMK, audit chain, ACL pre-filter).
GDPR / UK GDPR	Architecture deployable. Art. 17: per-person erasure with a receipt, with the limits in §1.1. Crypto-shred is per organization, for disposing of a whole tenant. Art. 25 / 32: pseudonymization of detected PII before the model; encryption at rest as in §1.2. Residency via region-pinned deployment.	Customer remains controller. Sparcle deploys inside the customer's processing perimeter. Whether a third-country transfer occurs depends on the LLM endpoint the customer configures.
DPDPA (India)	Architecture designed for DPDPA workflows. Deployed in the region the customer chooses; per-person erasure as under GDPR.	Customer remains the data fiduciary.
CCPA / CPRA (California)	Right to delete is served by the per-person erasure path, with the same limits as GDPR Art. 17 (§1.1). Crypto-shred is not a per-person tool.	Customer's CCPA program covers Bolt as on-premises tooling.
DORA (EU financial)	Architecture deployable. In the self-hosted model Sparcle ships software and operates no ICT service in the customer's data path. Exit-portable via Helm or Docker Compose.	Customer decides whether and how to record Sparcle in its Article 28 register of information.
NIS2 (EU)	The audit chain provides incident evidence for the event set it covers (§2.1).	Customer's NIS2 program covers Bolt as a software dependency.
SEC Reg SCI	The tamper-evident audit chain can support recordkeeping evidence for the events it covers.	Customer's Reg SCI responsibilities supported by the verifier export workflow (§3).
SOX (US public co.)	Architecture deployable. Audit-trail responses, tamper-evident logging and role-based controls support SOX IT general controls.	Customer's ICFR covers Bolt as a deployed system. Scope reviewed during pilot.
GLBA (US financial)	Customer NPI stays in the customer's deployment.	Customer's Safeguards Rule program covers Bolt.
PCI DSS	Not in scope. Bolt is not designed to sit in a cardholder data environment.	Not applicable in normal deployment.
CMMC	Not held. Controls evidence map available for the assessor; the audit chain is an artifact a C3PAO can review.	Customer's CMMC posture covers Bolt as a software dependency in its CUI enclave.
FedRAMP	Not held and not authorized today. Moderate is on the roadmap: a multi-quarter effort with a sponsoring agency.	Customer's existing ATO covers Bolt as deployed software in the boundary.
ITAR / EAR	Architecture deployable. Air-gapped deployment at the Federated Aeira tier. The 8-axis ACL includes a country axis that limits documents to permitted countries.	Customer's export-control program covers Bolt as deployed in its enclave and decides who counts as a US person.
FIPS 140-3	Not held. Bolt performs cryptography in-process. Algorithms other than XChaCha20-Poly1305 are FIPS-eligible; module validation is on the roadmap.	Customer's FIPS-validated KMS or HSM can hold the tenant CMK and the audit signing key.
ISO 27001 / 27017 / 27018	Not held. Independent auditor signed; not certified yet.	Customer's existing ISMS covers Bolt.

This posture is current as of the document version date. Compliance is a relationship, not a state: frameworks evolve and Sparcle's posture evolves with them. Refresh quarterly or on framework-change trigger. Last review: 2026-10.

1.1 Erasure: per person, and per organization

Crypto-shred is per organization. There is one CMK per tenant and no per-person key, so destroying a key cannot erase one data subject while leaving everyone else readable. Crypto-shred disposes of a whole tenant: offboarding, contract end, or a disposal order. Retention duties survive it because the encrypted bytes remain; only their readability is revoked.

One person's request is a per-person erasure. It is started by the user, with a 30-day grace period they can cancel, or by an administrator or DPO, with a grace period or immediately. It revokes the person's upstream OAuth grants, then deletes their account, sessions, sign-in and connector credentials, pseudonym bindings, devices and notifications. A receipt (signed when a KMS is configured) is stored and a record of the erasure is sealed into the audit chain.

What it does not remove today:

- Sealed audit records, which keep the person's user id so the chain still verifies.
- Chat history on the immediate administrator path. The grace-period path deletes it; otherwise it ages out under the retention window (90 days by default).
- PII-vault pseudonym entries, which neither path reaches yet.
- Recall memory, which the user can delete in the app and which otherwise ages out on its own timer.
- Documents about the person in the Aeira index. Aeira's document delete removes a document's keyword and vector index copies; for someone who is not a Bolt user, that is the path.
- Backups, which are the operator's to handle.

1.2 Encryption at rest

What	How it is protected
Per-tenant envelope encryption (server)	A fresh AES-256-GCM data key per value, wrapped by the tenant's customer master key (CMK) in a local KMS, AWS KMS or HashiCorp Vault. On when a KMS is configured; Bolt warns if it fails. In Bolt's server it covers stored secrets (organization LLM API keys, the Aeira backend client secret); in Aeira, indexed document content and PII-vault entries. Document titles and embedding vectors stay readable so they can be searched.
Sign-in tokens	AES-256-GCM. This is the refresh token that Google and Microsoft mail, calendar and file access run on.
Connector credentials	XChaCha20-Poly1305, for MCP connector credentials.
Conversation content (server)	Message bodies, agent runs and memory are sealed with XChaCha20-Poly1305 under a key from the customer's secret store, not under the CMK. A server deployment configured without that key stores them unencrypted.
Local stores (desktop)	SQLCipher. Clipboard history, notes, and screenshot and file indexes are whole-database encrypted under a key derived on the device.
Memory and conversations (desktop)	Memory content and conversation bodies are encrypted. Titles, short facts, names, dates, file paths and URLs stay readable on the device, because local search needs them. If Bolt cannot save its key, bodies are stored unencrypted with a logged warning. Logs are PII-scrubbed rather than encrypted; full-disk encryption covers those.

Audit records are signed, not encrypted, so destroying a tenant CMK does not make them unreadable and does not stop the chain from verifying (§2.3).

§2 Audit-chain architecture

Covered events are sealed into a Merkle hash chain. Sealed roots are signed with the platform Ed25519 key held in your KMS. The chain is tamper-evident: altering a sealed event breaks the root that covers it.

2.1 The chain

On a server deployment with Postgres and a KMS configured, the chain covers authorization decisions, retrieval access, tool invocations, model calls, agent decisions, admin policy changes, the security-relevant identity transitions (sign-in, sign-out, session delegation and revocation, session attach) and the privileged key and identity operations (KMS rotation and crypto-shred, PII reveal, SCIM token issue and revoke). The audit-seal operation itself is not yet sealed, and OAuth token refresh and the read-only SCIM token list are excluded on purpose.

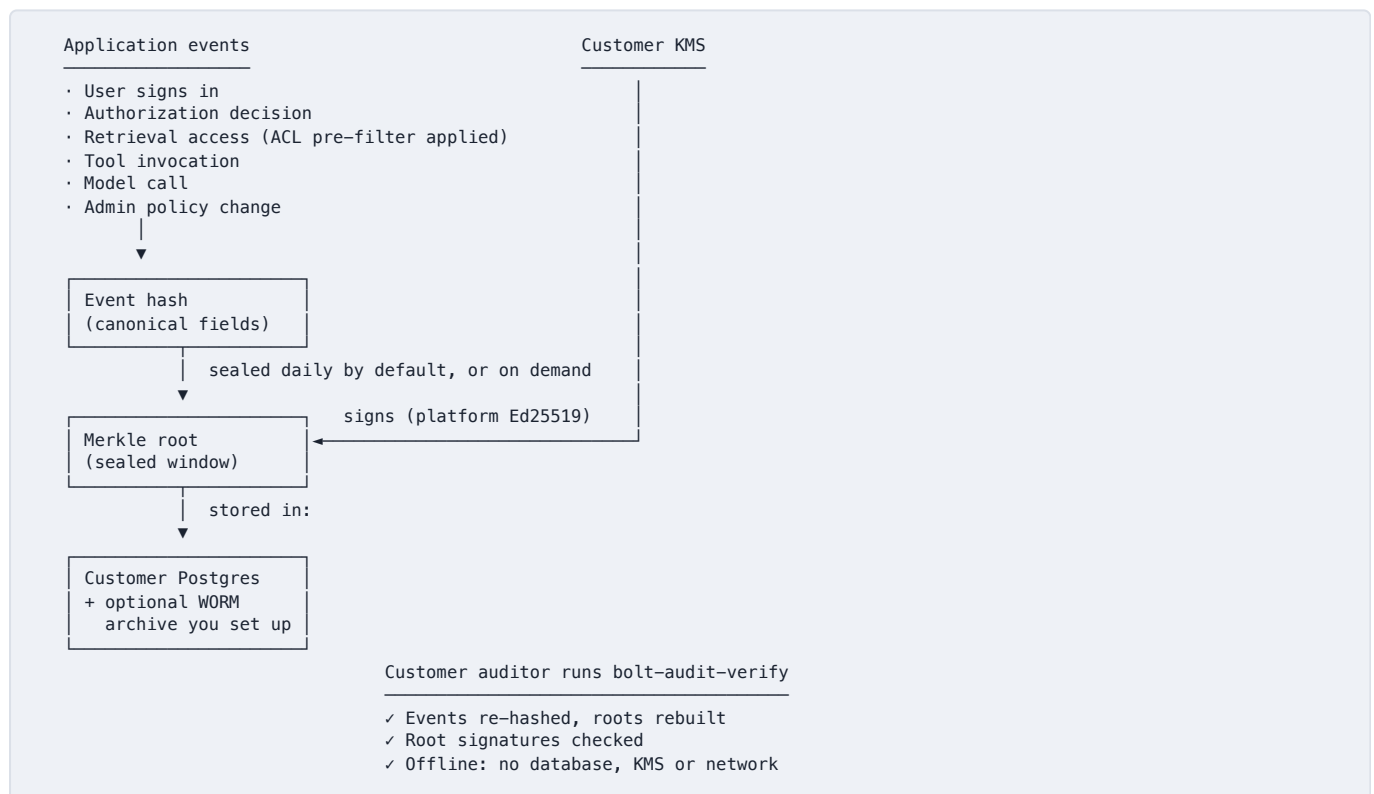
A background sealer rolls each window into a Merkle root once a day by default (configurable, for example hourly for regulated tenants), and an administrator can seal any range on demand. Roots are stored in the customer's Postgres. Pairing them with write-once storage (S3 Object Lock, Azure Immutable Blob, GCS Bucket Lock) is a deployment the customer configures; the storage layer does not enforce it.

2.2 Cross-product byte-compat

The event hash and Merkle root are byte-compatible across Bolt and Aeira, and the canonical encoding is version-tagged so already-sealed roots keep verifying after the encoder moves on. Tests in the shared `aeira-traits-conformance` crate assert the frozen byte shape of each version. They run in that library's CI and are not a release gate on the shipped product. The signature payload is product-specific.

2.3 Keys

Sealed roots are signed with the platform Ed25519 signing key, which is distinct from every tenant CMK. Destroying a tenant CMK therefore does not affect the verifiability of the chain that covers that tenant's events. The auditor receives the public half out of band, never inside the bundle being verified. Tenant CMK rotation runs through an authenticated admin endpoint on the customer's cadence: old data keys continue to decrypt and new writes wrap under the new key id.



§3 Verifier walkthrough

How a customer auditor verifies the audit chain, without Sparcle's cooperation.

3.1 Step by step

1. **Seal the range, then export it.** A bundle only carries a signed root for a window that has been sealed, so seal first with `POST /api/v1/admin/audit/seal`. Then export with `bolt-audit-verify export-bundle`, or the equivalent `POST /api/v1/admin/audit/export` from the running app. Both are read-only and produce byte-identical output. A window is capped at 366 days and 200,000 events per call; `--tenant` scopes it to one tenant.
2. **Obtain the platform verifying key, out of band.** On the file-backed KMS, `bolt-audit-verify export-key` reads the public half and never touches private key material. On AWS KMS it is `GetPublicKey`; on Vault, a read of the transit signing key. Distribute it through your own trusted path and pin it.
3. **Run the verifier offline.** No database, no KMS, no network. It re-hashes every event from its canonical fields, rebuilds each sealed root from the in-window events, compares it to the signed root, and checks each root signature against the key you supplied. Without a key it still checks integrity and reports the signatures as not checked.
4. **Read the exit code, not just the report.** It prints a human report, or JSON with `--json`, and returns a distinct code per finding. Only 0 is a full pass.
5. **Cross-verify.** If the customer archives sealed roots to a separate write-once store, the auditor compares those roots to the export. A match confirms no rewriting occurred since the archive event.

3.2 Commands and exit codes

```
# export the sealed range you want to verify
$ bolt-audit-verify export-bundle \
  --from 2026-01-01T00:00:00Z --to 2026-02-01T00:00:00Z \
  --out audit-proof.json

# verify it offline: no database, no KMS, no network
$ bolt-audit-verify verify audit-proof.json \
  --pubkey-file platform.pub.hex --json
```

Exit	Meaning
0	Verified: integrity and signatures pass.
2	Integrity failure: a sealed root does not match its events (tampering).
3	Signature failure against the supplied key.
4	Incomplete export.
5	Integrity ok, but no key supplied, so signatures were not checked.
6	Range not sealed.
1	Usage or IO error.

The verifier ships inside the macOS app bundle on Apple Silicon and beside `bolt-api` in the server container image, and is published as a standalone release artifact for Windows. The Intel macOS bundle does not carry it, and standalone macOS and Linux builds are not published on every release; ask us for the binary if your auditor needs one.

3.3 What the verifier does NOT do

- Does not confirm that the recorded events are complete. Detecting a missing event needs a complementary signal, typically the customer's SIEM or access logs.
- Does not assert that Bolt's behavior was correct, only that the recorded behavior was not altered after sealing.
- Does not judge the content of model responses.
- Does not validate the platform key's chain of custody. That is the trust decision you make when you export and pin the key.
- Does not provide a SOC 2, ISO 27001 or HITRUST attestation.

The verifier provides cryptographic evidence; it does not provide legal compliance. The customer's auditor or regulator interprets the evidence.

§4 Sub-processor list, contractual addenda

4.1 Sub-processors (by deployment mode)

Deployment mode	Sparcle sub-processors in the customer data path
Bolt Authorize, Backbone or Certify · customer self-hosted (Docker Compose or Helm)	None. Bolt runs on customer compute against customer Postgres and Redis. The LLM endpoint, identity provider, KMS, storage, MCP integrations and SIEM are the customer's own relationships; Sparcle does not select them, hold their credentials, or contract with them on the customer's behalf.
Bolt desktop (free local tier or trial)	None. No customer data reaches Sparcle-operated systems. Sparcle is not a data processor.
Hosted Bolt	Does not exist. Sparcle does not host customer data.

Compliance note. In every self-hosted Bolt tier there is no Sparcle-operated system in the data path, so Sparcle adds no sub-processor of its own. The services Sparcle does operate (license issuance, product telemetry made of counts and fingerprints with no customer content, and the website) carry no customer data. Sparcle's own vendors support software delivery and internal operations only; the current list is available on request.

4.2 Customer contractual addenda

- **DPA and BAA (HIPAA):** a signed DPA comes with Bolt Certify. BAA available: support keeps PHI out of Sparcle systems, or we sign a BAA where we may see PHI (target November 2026). Sparcle is not a runtime business associate in the self-hosted model, because no PHI reaches a Sparcle-operated system.
- **Sub-processor changes:** at least 30 calendar days' notice before adding or replacing a sub-processor that handles customer data, with a right to object.
- **SCCs (EU / UK):** self-hosted deployment involves no transfer to Sparcle. Where a sub-processor operates outside the customer's residency jurisdiction, Sparcle relies on the EU / UK Standard Contractual Clauses.
- **Source-code escrow:** not a standard term today. Bolt keeps running without Sparcle: it is self-hosted and its licence is verified offline. If your continuity policy calls for escrow, raise it during contracting.
- **Indemnity, liability caps and breach-notice periods:** set in the executed MSA, DPA or BAA.

4.3 Contact

For security and compliance questions: **security@sparcle.app**
For pilot and contract negotiations: **bolt@sparcle.app**