TESSURE · LEGAL + OPS BRIEF

# Privacy Posture

How Tessure treats identity, evidence, and data exposure — and why privacy-by-design is a structural product choice, not a compliance tax.

VERSION 0.1 TESSURE SYSTEMS, INC. APRIL 2026

# 1. Position

Physical-security systems collect deeply personal data: images of people, movement patterns, biometric inferences, locations, associations. Poorly designed, they become surveillance infrastructure. Well designed, they reduce physical risk while minimizing what is observed, stored, shared, and retained.

Tessure is designed to the second case. Three explicit commitments govern every architectural decision:

1. **Minimize observation.** Do not collect what we do not need.
2. **Process on-site.** Raw sensor data stays at the facility where it was captured.
3. **Keep a clean audit trail.** Every access to data produces a log entry that the customer can inspect.

## 1.1 What this document is

A six-page reference for security officers, legal counsel, data-protection officers, and procurement reviewers. It states what the platform does and does not do with personal data, and maps posture to the named regulations most likely to appear in a procurement questionnaire.

# 2. What Tessure collects, where it lives

## 2.1 Sensor data classes

| CLASS | LIVES WHERE | DEFAULT RETENTION |
|---|---|---|
| Raw video / thermal / radar / acoustic | On-site (Fusion Node local storage) | Customer-configured; default 14 days for unverified, 90 days for verified events |
| Fused event metadata | On-site + optional Cloud Assist | As customer configures |
| Evidence packages (redacted) | On-site + customer-chosen cloud | Customer policy; often insurance- or regulator-driven |
| Unredacted originals | On-site only; access-gated + audit-logged | Customer policy |
| Biometric features (face, plate) | Not generated by default | Opt-in, per-site, per-feature |

## 2.2 What never leaves the site (by default)

- Raw video streams.
- Raw thermal imagery.
- Raw audio recordings.
- Face embeddings, license-plate text, or any other biometric inference (unless a site operator has affirmatively enabled that capability with documented legal sign-off).

> CONTRAST
>
> Most camera-first and cloud-first products stream raw content to a vendor-operated cloud by default. That means the vendor has copies of your site’s imagery, and your data-protection exposure extends to the vendor’s subprocessors. Tessure’s edge-first architecture keeps raw data on customer-owned hardware.

# 3. Redaction by default

Every frame processed by the Fusion Node passes through a redaction pipeline before any storage:

1. Face detection (RetinaFace).
2. License-plate detection.
3. Gaussian blur applied to both classes.
4. Redacted frame is the one that hits disk.

Unredacted originals can be generated on demand, but only:

- By an authorized operator with role permission.
- After providing a reason string that is stored with the access log entry.
- Delivered once, non-retained at the requester’s endpoint unless the customer explicitly allows download.

# 4. Identity recognition — opt-in only

Face recognition and license-plate recognition are **disabled by default**. Enabling either requires:

- A per-site configuration change by a role with the `enable_biometrics` permission.
- Acknowledgement of the jurisdiction-specific legal obligations (BIPA for Illinois, CCPA / CPRA for California, EU AI Act for EU sites, and any applicable state or municipal laws).
- A documented justification stored with the site configuration.

When enabled:

- The Fusion Node logs every identification event.
- The customer can produce a report of identification events for any window of time.
- Data subjects' access and deletion requests can be honored at the site level without contacting Tessure.

# 5. Evidence as a privacy feature, not a leak

Evidence packages are the single most consequential privacy artifact Tessure produces. They leave the site and can reach insurance adjusters, regulators, or law enforcement. Designed wrong, they would become mass exposure vectors.

## 5.1 Evidence-package contents

- Redacted video and thermal clips.
- Sensor telemetry (radar, acoustic).
- Fusion decision log.
- Operator actions (who approved what, when).
- Cryptographic hash tree (SHA-256 → Merkle root → site-key signature).

## 5.2 What evidence packages do NOT include

- Unredacted faces or plates (unless the customer explicitly enabled biometrics and then re-authorized unredaction).
- Biometric feature vectors.
- Any data from a different site.
- Any personal data about staff, delivery drivers, guests, or other recurring parties unless they are directly involved in the verified event.

## 5.3 Signed, auditable, revocable

Evidence packages can be verified against the site’s public signing key, and revoked (marked superseded) if an error in the processing pipeline is later discovered. Revocation is logged and the audit trail is preserved.

# 6. Regulatory posture

Tessure is engineered to satisfy the regulations most relevant to the buyer segments it serves.

| REGULATION | RELEVANCE | TESSURE POSTURE |
|---|---|---|
| Illinois BIPA (740 ILCS 14/) | Biometric Information Privacy Act — consent + notice for face/fingerprint/voiceprint collection | Biometrics off by default; per-site opt-in requires documented policy; per-individual consent flow available for employee-monitoring use cases. |
| California CCPA / CPRA | Commercial surveillance disclosure + access/deletion rights | Per-site data inventory, automated access/deletion response tooling, vendor-agreement template ready. |
| EU AI Act (high-risk AI obligations live Aug 2 2026) | Physical-security AI may fall into high-risk category | Risk-management documentation, human-in-the-loop above risk thresholds, model cards, post-market monitoring, incident reporting pipeline aligned to the Act's obligations. |
| GDPR (EU) | Personal data processing | On-site processing reduces controller/processor scope; DPA templates per tier; data subject rights tooling. |
| NERC CIP-014-4 | Physical security of high-risk transmission substations | Tessure evidence packages satisfy the "event-response and documentation" clauses; integrates with the customer's broader CIP-014 plan, not a substitute for it. |
| TSA Pipeline Security Directive SD02F (effective May 3 2025) | Pipeline cybersecurity and physical security | Verified-event + evidence architecture fits the directive's detection-and-response requirements. |

> **NOTE**
>
> Nothing in this document is legal advice. Engage your own counsel for jurisdiction-specific compliance. Tessure provides the tooling, documentation, and configuration surface; the customer remains the controller of personal data processed at their sites.

# 7. Access control & audit

- **Role-based access control.** Roles are site-scoped by default; cross-site access requires explicit grant.
- **Every access logged.** Viewing unredacted content, exporting evidence, and changing configurations all produce audit-log entries that the customer can query or stream to a SIEM.
- **Session reason codes.** Sensitive actions require the operator to attach a reason that is preserved in the audit log.
- **Retention and hold controls.** Customer configures retention windows per data class; legal-hold overrides retention and produces its own audit record.

# 8. What Tessure sees from a customer site

When Cloud Assist is enabled (optional), Tessure receives:

- Signed event metadata (timestamps, classifications, confidence scores, geo-cell references).
- Aggregate health telemetry (node status, sensor availability, model version).
- Optional: redacted evidence artifacts if the customer has elected cross-site correlation.

Tessure does not receive:

- Raw sensor streams.
- Unredacted imagery.
- Biometric feature vectors.
- Identifying details about individuals at the site, unless the site has explicitly enabled biometrics and explicitly shared such data with Tessure — a separate, auditable decision.

---

Companion to the *Architecture Whitepaper*. If a procurement team asks a question about privacy that this brief does not answer, email sean.florez@colorado.edu. The thesis is archived; the document set is public.