KeyShare

Visitor Management Compliance Guide

Biometric privacy, consent frameworks, data retention, NDA compliance, and audit trail specifications — across BIPA, GDPR, CCPA, and Texas CUBI.

For Data Protection Officers, Compliance Officers, and Legal Counsel evaluating identity-verified visitor management.

1. Biometric Privacy Framework

KeyShare uses a fundamentally different biometric architecture than traditional visitor management systems. Rather than storing biometric templates in a database for future comparison (1:N matching), KeyShare performs ephemeral 1:1 face matching — comparing the live image to the photo on the visitor's government-issued ID in real-time, in RAM only.

How Ephemeral 1:1 Matching Works

- The visitor presents their government-issued ID to the Puck NFC reader.
- The Puck reads the photo from the ID's secure chip (ISO 18013-5 or ICAO 9303).
- The Visitor Experience Platform (VEP) captures a live image from the camera.
- A 1:1 comparison runs in volatile memory (RAM). Match/no-match result is logged.
- Both images are discarded immediately. No biometric template is created. No facial data is written to disk, database, or cloud storage.

This architecture means there is no biometric database to breach, no templates to steal, and no facial recognition database to subpoena. The only record of the biometric event is the match/no-match result in the audit log — with no biometric data attached.

Why This Matters for Compliance

Template-based systems (1:N) create a persistent biometric database that falls under the strictest tier of every biometric privacy law. Ephemeral 1:1 processing significantly reduces regulatory exposure — though it does not eliminate the need for consent in jurisdictions that regulate biometric collection (not just storage).

> *KeyShare's position: consent before capture, plus zero retention. This provides the strongest defensible posture under all major biometric privacy frameworks.*

2. Jurisdiction-by-Jurisdiction Consent Requirements

Each jurisdiction has distinct requirements for biometric data processing. The table below maps the key requirements and KeyShare's implementation for each.

Jurisdiction	Key Requirement	KeyShare Implementation
BIPA (Illinois)	Written consent before collection. Retention schedule required. Private right of action.	Explicit digital consent captured before any biometric processing. Zero retention policy eliminates retention schedule risk.
GDPR (EU)	Explicit consent for biometric processing (Art. 9(2)(a)). DPIA required (Art. 35).	Two-tier legal basis: legitimate interest for non-biometric ID verification; explicit consent for face matching. Pre-filled DPIA template included (Sec. 8).
CCPA/CPRA (CA)	Right to know, delete, opt-out. Biometric data is sensitive PI.	Nothing to delete — no biometric data retained. Audit logs available for "right to know" requests.
Texas CUBI	Informed consent before capture. No sale of biometric data.	Consent captured before processing. No biometric data exists to sell.
Washington HB 1493	Notice required for commercial biometric use. Consent for enrollment in database.	Notice provided at check-in. No enrollment in any database — ephemeral processing only.

3. Two-Tier GDPR Legal Basis

A common mistake in GDPR compliance for visitor management is relying on consent as the legal basis for all processing. KeyShare recommends a two-tier approach that provides a stronger legal foundation:

Tier 1: Non-Biometric ID Verification

Legal basis: Legitimate interest (Art. 6(1)(f)). Verifying a visitor's identity from their government-issued ID is a legitimate security interest for any organization controlling physical access. A Legitimate Interest Assessment (LIA) documents the balancing test.

Tier 2: Biometric Face Matching

Legal basis: Explicit consent (Art. 9(2)(a)). Biometric processing requires explicit, freely given, informed consent. The visitor must be able to decline biometric matching and still proceed with non-biometric ID verification.

> *Why "consent for everything" is a weaker position: If consent is withdrawn, you lose the legal basis for ALL processing — including basic ID verification. The two-tier approach ensures that withdrawing consent for biometric matching doesn't disable visitor check-in entirely.*

DPIA Requirement

GDPR Article 35 requires a Data Protection Impact Assessment for any processing that uses biometric data for identification purposes. Section 8 of this guide includes a pre-filled DPIA template covering both processing tiers.

4. Data Retention Policies

KeyShare's data retention follows a clear principle: retain only what is needed for audit and compliance, and retain nothing biometric.

Data Category	Retained?	Retention Period	Configurable?
Biometric images (face photos)	Never retained	N/A — ephemeral processing only	N/A
Biometric templates	Never created	N/A — no template-based matching	N/A
Audit log entries (match/no-match)	Yes	1 year default	Yes — per jurisdiction
Consent records	Yes	3 years default (or as required by law)	Yes — per jurisdiction
NDA signatures	Yes	Duration of NDA + retention period	Yes — per document
Visitor check-in records	Yes	1 year default	Yes — per jurisdiction

5. NDA Electronic Signature Compliance

KeyShare links NDA electronic signatures to cryptographically verified identities. When a visitor signs an NDA during check-in, the signature is bound to the verified identity from the government-issued ID — not just an email address or typed name.

- **ESIGN Act (US):** Electronic signatures are legally equivalent to handwritten signatures. KeyShare captures: signer identity (verified), timestamp, document hash, consent record.
- **eIDAS (EU):** KeyShare signatures qualify as Advanced Electronic Signatures (AES) when linked to a verified government-issued digital identity. Document versioning and tamper-evident hashing provide integrity.

6. Audit Trail Specifications

Every visitor interaction generates an auditable event record. The audit trail captures:

Event Type	Captured	NOT Captured
Check-in	Timestamp, visitor name, host, verification method, result	Biometric data, face images
Face matching	Timestamp, match/no-match, confidence threshold met	Face images, biometric templates
NDA signature	Timestamp, document hash, signer identity, version	Document content (stored separately)
Consent	Timestamp, consent type, scope, method of capture	N/A
Checkout/badge return	Timestamp, badge ID, return method	N/A

Audit logs are exportable in JSON and CSV formats for compliance review. Retention periods are configurable per jurisdiction.

7. Minor Visitor Handling

Visitors under 18 require additional consent protections. KeyShare implements:

- **COPPA compliance:** No biometric processing of visitors under 13 without verifiable parental consent.
- **Age 13-17:** Biometric face matching requires explicit consent from an accompanying adult (parent, guardian, or authorized school official).
- **Non-biometric fallback:** ID verification without face matching is always available for minor visitors.

8. DPIA Template

The following pre-filled template addresses GDPR Article 35 requirements for biometric visitor management. Customize the highlighted fields for your organization.

DPIA Section	Pre-Filled Content
Processing description	Visitor identity verification using government-issued ID (Tier 1) and optional biometric face matching (Tier 2).
Necessity and proportionality	Physical security requires identity verification. Biometric matching is optional and consent-based.
Risks to data subjects	Biometric data breach (mitigated: no retention). False match/non-match (mitigated: human override).
Safeguards	Ephemeral processing. Zero biometric retention. Explicit consent. Human override capability.
Data controller	[Your organization name]
DPO contact	[Your DPO name and contact]
Review schedule	Annual, or upon material change to processing.

9. ITAR and Export Control Considerations

Facilities subject to ITAR (International Traffic in Arms Regulations) or EAR (Export Administration Regulations) have additional visitor management requirements. KeyShare supports these through:

- **Foreign national detection:** Government-issued digital IDs include nationality information. The VEP can flag foreign national visitors for additional screening or escort requirements based on facility-configured rules.
- **Identity-verified access logging:** Every access event is tied to a cryptographically verified identity — not a badge number. Audit logs meet ITAR record-keeping requirements.
- **Credential lifecycle management:** Visitor credentials are time-bounded and automatically expire. No persistent credentials for visitors to retain after departure.
- **Zone-based access control:** Integration with the existing PACS enables per-zone restrictions. ITAR-controlled areas can require additional verification or restrict access to pre-cleared visitors only.

Note: KeyShare does not provide legal advice on ITAR/EAR compliance. This section describes architectural capabilities that support ITAR compliance documentation. Consult your export control officer or legal counsel for jurisdiction-specific requirements.

Next Steps

- **Request an Architecture Review:** keyshare.id/contact/?type=pacs
- **Explore the Visitor Management Solution:** keyshare.id/physical-access/visitor-management/
- **Review the Security and Trust Center:** keyshare.id/security/