Sieve Compliance Pack

For government and sovereign procurement teams · gov@mysieve.com

This pack summarizes Sieve's compliance posture, frequently asked questions and a working glossary drawn from the Sieve whitepaper and executive summaries. Sieve is engineered under privacy-by-design and security-by-design: data minimization, AES-256 end-to-end encryption, Zero-Knowledge Proofs, tri-partite sharding and revocable consent. The partner agency is the Data Controller; Sieve operates strictly as Data Processor / Operador under a binding DPA.

Key compliance pillars

• **Non-custodial.** No reconstructable biometric template exists at rest — nothing to breach.

• **Data minimization.** The platform returns an approval token (yes/no) — not PII.

• **Lawful processing.** Partner = Controller; Sieve = Processor / Operador under binding DPA.

• **Transparency.** Every artifact anchored to an append-only Merkle log, verifiable by hash.

• **Revocable consent.** The holder can revoke a grant at any time via the Data Faucet.

Jurisdictional coverage

• **United States.** ESIGN / UETA, HIPAA (BAA), CCPA/CPRA, BIPA, OFAC, NIST 800-63-3 IAL2/AAL2, SOC 2 Type II.

• **European Union.** GDPR, eIDAS 2, AI Act, NIS2, ePrivacy.

• **United Kingdom.** UK GDPR + DPA 2018, Electronic Communications Act 2000, DSIT DIATF.

• **Brazil.** LGPD, Marco Civil, MP 2.200-2/2001 + Lei 14.063/2020, Lei das Estatais (Art. 28 §3º II), BCB / Open Finance, BNMP/CNJ, Sinesp, Interpol.

• **International.** FATF Recommendations and Digital ID Guidance, ICAO 9303, ISO/IEC 27001, 27701, 29115, 30107-3.

• **APAC.** PDPA (SG), APPI (JP), Privacy Act 1988 + APPs (AU), DPDPA 2023 (IN).

• **MEA.** UAE PDPL + DIFC/ADGM, KSA PDPL, POPIA (ZA), Malabo Convention.

Frequently asked compliance questions

How does Sieve store biometric data without creating a honeypot?

Sieve is non-custodial by design. Enrollment produces three encrypted shards using Shamir Secret Sharing over GF(256), each held by a different custodian: the user device, a protocol shard, and a partner/guardian shard. Reconstruction is mathematically impossible without the Biovital Token generated during a fresh, live capture. No single party — Sieve included — ever holds a reconstructable biometric template, so there is no central honeypot of face data or PII to breach.

What personal data leaves the device during a verification?

As little as possible. The capture pipeline runs client-side and returns only an approval token (match: yes/no) plus optional zero-knowledge claims such as “age ≥ 18”. Raw images, templates, and PII are never written to Sieve databases at rest. When identity attributes must be shared, the Data Faucet enforces granular, revocable consent scoped to the exact relying party.

How does Sieve comply with GDPR and LGPD?

The partner agency is the Data Controller (Controlador); Sieve acts strictly as Data Processor (Operador) under a binding Data Processing Agreement. Both frameworks are addressed through privacy-by-design, data minimization, SCC/UK IDTA transfer safeguards, audit-trail access, breach-notification SLAs, and built-in support for data-subject rights including access, rectification, deletion and revocable consent.

Is a Sieve biovital signature legally enforceable?

Yes. The signature envelope binds the act of signing to a live, uncoerced human presence (face + GPS + timestamp + immutable artifact log). This meets the requirements of the U.S. ESIGN Act and UETA, the EU eIDAS framework, and Brazil’s MP 2.200-2/2001 combined with Law 14.063/2020 for advanced and qualified electronic signatures.

How does Sieve address U.S. state biometric laws such as BIPA?

Illinois BIPA and analogous state statutes regulate the collection, storage and disclosure of biometric identifiers. Sieve’s non-custodial architecture means no biometric identifier is stored in reconstructable form by Sieve or the partner. The platform returns a token, not a template, materially limiting the biometric-data footprint that these laws govern.

How are sanctions, PEP and AML/CFT checks handled?

The Sieve Intelligence Core runs real-time screening against OFAC SDN and consolidated sanctions lists, FATF-aligned PEP, UBO and KYB/KYC sources, and — where legally authorized — national public-safety databases such as BNMP/CNJ, Sinesp and Interpol diffusion lists. All hits are logged as auditable artifacts without exposing PII.

Who is liable for data under the non-custodial model?

Liability is deliberately shifted away from data storage. Because Sieve does not custody recoverable PII, the partner’s data-liability surface is reduced to the approval token and the metadata it chooses to retain. Sieve remains responsible for processor-level security controls, encryption, availability and audit logging, as defined in the DPA and applicable service levels.

Can citizens revoke consent after enrollment?

Yes, at any time. The Data Faucet gives the identity holder a single place to view active grants, limit scopes and revoke access. Once revoked, downstream relying parties receive the revocation event and can no longer depend on the associated approval token or claims.

What security certifications does Sieve maintain?

Sieve’s security and privacy program is mapped to ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 29115 and SOC 2 Type II. NIST 800-63-3 controls support IAL2/AAL2 alignment. Certification status, scope statements and audit reports are shared under NDA.

What is the legal basis for direct public-sector procurement?

In Brazil, the non-competitive route is grounded in Article 28, §3º, II of Lei das Estatais (Lei nº 13.303/2016), which permits direct contracting when the object has particular and exclusive characteristics. The TCU’s Acórdão nº 2488/2020-Plenário recognizes technological uniqueness as a valid basis; Sieve’s proprietary biovital engine and SIDI architecture support that qualification, formalized through a Manifestação de Interesse Privado (MIP) and Contrato de Parceria Estratégica.

Glossary

Biovital. Proprietary liveness signal binding a verification to a real, present, uncoerced human — combining face, micro-motion, rPPG pulse, GPS and timestamp.

Biovital Token. Single-use cryptographic token produced from a fresh live capture; required to reconstruct sharded material.

Tri-partite Sharding. Shamir Secret Sharing (GF(256)) split across device, protocol and partner/guardian. No party holds a reconstructable template.

Sovereign ID (SIDI). Non-custodial sovereign identity architecture in which the citizen, not the platform, controls the identity surface.

Data Faucet. User-facing consent surface for issuing, scoping and revoking grants to relying parties.

Approval Token. Yes/no match artifact returned to the relying party in place of PII.

Zero-Knowledge Claim. Cryptographic assertion (e.g. “age ≥ 18”) that proves a fact without revealing the underlying attribute.

Data Controller / Controlador. Entity that determines purpose and means of processing — under GDPR / LGPD this is the partner agency.

Data Processor / Operador. Entity that processes data on the Controller’s instruction — Sieve’s role under DPA.

DPA. Data Processing Agreement governing the Controller-Processor relationship.

SCC / UK IDTA. EU Standard Contractual Clauses and the UK International Data Transfer Agreement, used to lawfully transfer personal data across borders.

ESIGN / UETA. U.S. federal and state legal framework recognizing electronic records and signatures.

eIDAS. EU Regulation 910/2014 governing electronic identification, authentication and trust services.

BIPA. Illinois Biometric Information Privacy Act — strict regulation of biometric identifier collection and storage.

LGPD. Lei Geral de Proteção de Dados (Lei nº 13.709/2018) — the Brazilian general data-protection law.

Marco Civil da Internet. Lei nº 12.965/2014 — Brazilian internet bill of rights covering privacy and record protection.

MP 2.200-2/2001 + Lei 14.063/2020. Brazilian framework for advanced and qualified electronic signatures.

Lei das Estatais. Lei nº 13.303/2016 — governs Brazilian state-owned enterprises; Art. 28 §3º II grounds direct contracting for technologically unique objects.

MIP. Manifestação de Interesse Privado — formal private-sector proposal mechanism used to initiate a strategic partnership with a public entity.

FATF Recommendations. Global standards on AML/CFT, KYC, PEP, UBO and sanctions screening across 190+ jurisdictions.

OFAC SDN. U.S. Treasury Office of Foreign Assets Control Specially Designated Nationals list — primary U.S. sanctions screening source.

NIST 800-63-3 IAL2/AAL2. U.S. federal digital identity guidelines for identity-proofing and authenticator assurance levels.

ISO/IEC 27001 / 27701 / 29115 / 30107-3. International standards for information security management, privacy management, entity-authentication assurance and biometric presentation-attack detection.

ICAO 9303. International civil aviation standard for machine-readable travel documents (MRZ / NFC e-Passport).

Merkle Anchoring. Append-only cryptographic log used to anchor and verify artifacts by hash without exposing PII.

Contact: gov@mysieve.com · +1 (888) 566-6686 · mysieve.com