BONAFIDE™ SPECIFICATION V1.0 — PART 13

Compliance Profiles & Global Deployment

Open and Regulated profiles, explicit no Surveillance Profile, global market tiers, regulatory framework mapping, data residency enforcement, and compliance evolution

1. Purpose

Bonafide is designed for global deployment, but the global regulatory landscape is not uniform. Some jurisdictions encourage strong encryption. Others mandate lawful access capabilities. Others prohibit encryption that the state cannot penetrate.

This part defines compliance profiles—configurable policy layers that adapt the Bonafide system to different regulatory environments without changing the core cryptographic architecture. It maps the world's jurisdictions to deployment tiers and provides guidance on how Bonafide operates in each regulatory context.

The governing principle: Bonafide cooperates with lawful authority through audited, scoped mechanisms. It does not provide bulk surveillance capability, backdoors, or master keys under any profile. If a jurisdiction requires capabilities that the specification cannot provide without compromising the security model for all users, Bonafide cannot be deployed in that jurisdiction.

2. Compliance Profiles

2.1 Open Profile (Default)

The Open Profile is the canonical Bonafide specification with no modifications. It is the default for all deployments unless a jurisdiction-specific profile is configured.

- **Content neutrality:** Full. The vault encrypts, authorizes, and audits. It does not inspect, filter, or classify content.
- **Backdoors:** None. No master key, no government access key, no vendor recovery key.
- **Lawful access:** Through the institutional key path (Part 12, Section 4). Court orders are served on institutions, scoped to specific data, and recorded in the immutable ledger. The user is notified.
- **Data residency:** No restriction. Vault data may be stored in any jurisdiction, replicated across jurisdictions, or restricted to specific jurisdictions at the user's discretion.
- **Persona support:** Full. Unlinkable personas, duress protection, focus profiles. No restrictions on the number or purpose of personas.
- **Validator network:** Open participation. Any certified validator from any jurisdiction.

The Open Profile is appropriate for jurisdictions with no mandatory decryption requirements, no content filtering mandates, and no data localization laws that conflict with distributed vault storage.

2.2 Regulated Profile

The Regulated Profile adds configurable compliance controls that satisfy lawful access requirements in democratic jurisdictions with judicial oversight. The core cryptographic architecture is unchanged. The profile pre-configures certain override authorities and reporting mechanisms.

- **Content neutrality:** Maintained. The vault does not inspect or filter content. Lawful access to specific content is available through the override mechanism.
- **Backdoors:** None. The Regulated Profile does not add any key, capability, or mechanism that does not exist in the Open Profile. It configures existing mechanisms (quantum-level override, institutional key path) for compliance.
- **Lawful access:** Enhanced documentation. The override mechanism pre-registers authorized legal authorities (courts, regulators) for the jurisdiction. Override requests from registered authorities are processed through a streamlined workflow with jurisdictionally appropriate scope limits. All access remains scoped, audited, and visible to the data owner.
- **Data residency:** Configurable. The profile can enforce that vault data for users in a specific jurisdiction is stored only on infrastructure in that jurisdiction (or in approved jurisdictions). This satisfies GDPR data transfer restrictions, India's data localization requirements, and similar regulations.
- **Reporting:** The profile can enable automated compliance reporting to regulators—aggregate statistics on vault operations, override frequency, and incident response. Reports contain no user-identifiable data.

- **Persona support:** Full. The Regulated Profile does not restrict personas. Lawful access operates through the institutional key path, which accesses only the persona that peered with the target institution. Other personas remain undetectable.
- **Validator network:** Configurable. The profile can restrict validator selection to certified validators within specific jurisdictions or approved jurisdictions.

The Regulated Profile is appropriate for jurisdictions with lawful intercept requirements that can be satisfied through scoped, court-ordered access—including the EU (GDPR + eIDAS), the United Kingdom (Investigatory Powers Act), Australia (Assistance and Access Act), India (IT Rules), and Brazil (Marco Civil).

2.3 No Surveillance Profile

The Bonafide specification explicitly does not define and will never define a Surveillance Profile. The following capabilities are outside the specification's design space:

- Bulk access to vault data across multiple users
- Real-time interception of vault operations
- Content scanning, filtering, or classification by the vault infrastructure
- Master keys, government access keys, or vendor recovery keys
- Silent access that is not recorded in the ledger or visible to the data owner
- Capability to enumerate users, discover personas, or map vault relationships
- Mandatory client-side scanning of vault contents before encryption

If a jurisdiction requires any of these capabilities as a condition of deployment, Bonafide cannot be deployed in that jurisdiction in a specification-compliant manner. Any implementation that adds these capabilities is non-compliant and cannot carry the Bonafide Certified mark.

This is not a technical limitation. It is a design decision. The capabilities listed above are incompatible with user sovereignty, which is the foundational principle of the specification. Adding them would compromise the security model for all users, not just those in the requiring jurisdiction. The specification protects the global user base by refusing to weaken the protocol for any single jurisdiction.

3. Profile Comparison

Capability	Open Profile	Regulated Profile	Surveillance (DOES NOT EXIST)
Content neutrality	Full	Full	Violated
Backdoors	None	None	Required
Lawful access	Institutional key path + court order	Same + pre-registered authorities	Bulk/silent access
Data residency	User's choice	Configurable per jurisdiction	Mandatory localization
Ledger visibility	User sees all access	User sees all access	Silent access
Persona support	Full / unrestricted	Full / unrestricted	Restricted or enumerable
Validator selection	Open / global	Configurable / jurisdictional	Government-controlled
Content scanning	None	None	Mandatory
Master key	None	None	Required
Specification compliant	Yes	Yes	No — cannot exist

4. Global Market Tiers

Jurisdictions are classified into four tiers based on their regulatory compatibility with the Bonafide specification. Tier classification is based on current law and regulation as of the specification date and is subject to change as legal frameworks evolve.

4.1 Tier 1 — Open Deployment

Jurisdictions where the Open Profile can be deployed without modification. Strong encryption is legal, no mandatory backdoor requirements, and lawful access is available through existing legal process targeting institutions.

Jurisdiction	Key Framework	Notes
United States	No mandatory backdoors, First/Fourth Amendment protections, CLOUD Act for institutional process	Most permissive major market for encryption technology
Canada	PIPEDA, no mandatory decryption	Strong privacy framework, encryption encouraged
Switzerland	Constitutional privacy, Federal Data Protection Act	History of privacy-first products (ProtonMail, Threema)
Japan	APPI (Act on Protection of Personal Information)	Strong privacy law, no anti-encryption provisions
South Korea	PIPA (Personal Information Protection Act)	Comprehensive privacy framework
Taiwan	Personal Data Protection Act	Democratic privacy framework
Israel	Privacy Protection Law, strong tech sector	Active privacy technology market
Brazil	LGPD (Lei Geral de Proteção de Dados)	GDPR-inspired, no anti-encryption mandates
Most of Latin America	Varying national frameworks	Generally permissive for encryption technology

4.2 Tier 2 — Regulated Deployment

Jurisdictions where the Regulated Profile is required. Encryption is legal and encouraged for data protection, but lawful access requirements or data localization mandates require compliance configuration.

Jurisdiction	Key Framework	Bonafide Compliance Approach
European Union	GDPR, eIDAS 2.0, proposed CSAR (Chat Control)	Regulated Profile with EU data residency enforcement. GDPR Article 32 encourages encryption. eIDAS wallet is complementary (identity attestation feeds web of trust). CSAR proposals have stalled repeatedly; Bonafide monitors.

United Kingdom	Investigatory Powers Act, Online Safety Act	Regulated Profile with UK legal authority pre-registration. Override mechanism satisfies scoped access. Apple pulled ADP from UK; Bonafide's scoped lawful access may be distinguishable.
Australia	Assistance and Access Act 2018	Regulated Profile. The Act targets communications providers; Bonafide's vault model (data at rest) may be distinguishable. Override mechanism provides the "technical assistance" the Act requires without backdoors.
India	IT Rules (traceability), Data Protection Act 2023	Regulated Profile with India data residency. Traceability applies to messaging (not data at rest). Data localization satisfied by vault residency configuration.
Germany	GDPR + strong domestic encryption advocacy	Open Profile may be sufficient. Germany has been the strongest EU defender of encryption.
France	GDPR + domestic lawful intercept requirements	Regulated Profile. France has pushed for access capabilities; override mechanism provides scoped path.
Singapore	PDPA (Personal Data Protection Act)	Regulated Profile with Singapore data residency for financial data.

4.3 Tier 3 — Institutional Only

Jurisdictions where Bonafide can operate as institutional data protection infrastructure but consumer-facing deployment faces legal barriers. The value proposition shifts from “user sovereignty” to “breach-resistant architecture” and “compliance automation.”

Jurisdiction	Key Constraint	Bonafide Approach
Russia	Encryption licensing by FSB, key escrow for telecom	Institutional deployment using GOST-certified algorithms within Bonafide runtime. Consumer vault sovereignty not feasible under current law.
Turkey	Varying restrictions on encryption, VPN limitations	Enterprise data protection deployment. Consumer privacy features limited by regulatory environment.
UAE / Saudi Arabia / Gulf States	VPN restrictions, content filtering requirements	Enterprise deployment for data breach prevention. Positioned as compliance infrastructure, not consumer privacy.
Thailand	Cybersecurity Act with broad government access	Institutional deployment with regulatory override configuration.

4.4 Tier 4 — Cannot Deploy

Jurisdictions where the legal requirements fundamentally conflict with the Bonafide specification. Any deployment would require architectural changes that compromise the system for all users globally. The specification prohibits deployment in these jurisdictions.

Jurisdiction	Fundamental Conflict	Bonafide Position
China	State-approved algorithms mandatory, government decryption on request, data localization with state access	Cannot deploy. A master key or government access mechanism would violate the specification globally.
Iran	Civilian encryption effectively prohibited	Cannot deploy.
North Korea	No legal framework for private encryption	Cannot deploy.
Myanmar	Military regime, no encryption rights	Cannot deploy.
Vietnam	Cybersecurity Law requires government data access	Cannot deploy under current law.

Tier 4 classification is not permanent. If a jurisdiction’s legal framework evolves to permit user-sovereign encryption, it may be reclassified. The specification does not make political judgments—it assesses technical compatibility between the legal framework and the protocol’s security properties.

5. Regulatory Framework Mapping

The following table maps major regulatory frameworks to Bonafide's architectural features, demonstrating how the specification satisfies or exceeds each framework's requirements.

Framework	Requirement	Bonafide Mechanism
GDPR Article 5(1)(b)	Purpose limitation	Quantum access policies encode permitted use. Override ledger documents any deviation.
GDPR Article 17	Right to erasure	User revocation triggers re-encryption. Tombstone marker replaces Merkle leaf (preserves tree integrity). The data is cryptographically destroyed while proof of deletion is preserved.
GDPR Article 20	Data portability	Vault export: user downloads encrypted branch and re-imports to any compliant provider.
GDPR Article 25	Data protection by design	Per-quantum encryption, privacy scoring, ghost quanta, blind validation. Privacy is architectural.
GDPR Article 32	Appropriate technical measures	AES-256-GCM per quantum, hardware enclave isolation, audit ledger. Exceeds typical measures.
CCPA	Right to know, right to delete, right to opt out	Ledger provides right to know. Revocation provides right to delete. Peering authorization is opt-in.
HIPAA	Protected health information safeguards	Security levels restrict health data to high-classification institutions. Classification A or S recommended.
PCI-DSS	Cardholder data protection	Payment data encrypted per-quantum with dedicated security level.
PSD2 SCA	Strong Customer Authentication (two factors)	Biometric (inherence) + attested device (possession) + optional passphrase (knowledge). Exceeds SCA.
NIST 800-63 AAL2	Two distinct authentication factors	Biometric + device attestation. Two factors, hardware-bound.
NIST 800-63 AAL3	Hardware crypto + verifier impersonation resistance	Tier 1/S enclave + biometric + attestation. Full AAL3 alignment.
FIDO2 / WebAuthn	Authenticator + user verification	Device secure element as authenticator. Biometric as user verification.
eIDAS 2.0	EU digital identity wallet	Complementary: EU wallet provides identity attestation that feeds Bonafide's web of trust as a validator source.

6. Quantum-Level Override for Regulated Markets

6.1 How Override Satisfies Lawful Access

The quantum-level override mechanism (Part 3) is the specification's answer to lawful access requirements in Tier 2 jurisdictions. It provides everything a democratic legal system actually needs:

- **Scoped access:** The override targets specific quanta, channels, or branches—never the entire vault. Scope matches the court order's scope.
- **Judicial authorization:** The override requires a registered legal authority (court, regulator). In the Regulated Profile, authorized authorities are pre-registered by jurisdiction.
- **Time-bounded:** Overrides expire. The institution cannot maintain perpetual access through a single override authorization.
- **Auditable:** Every override is recorded in the immutable ledger with the authority, scope, legal basis, timestamp, and accessing entity. The audit trail is permanent and tamper-proof.
- **Visible to the data owner:** The user can see that an override occurred (unless a court order includes a non-disclosure provision, in which case visibility is deferred per the court's order, but the ledger entry still exists for eventual disclosure).

6.2 Override vs. Backdoor

An override is not a backdoor. The distinction is fundamental:

Property	Override (Bonafide)	Backdoor (not Bonafide)
Scope	Specific data, specific time, specific authority	All data, any time, any holder of the key
Authorization	Court order or equivalent legal process	Possession of the master key
Audit trail	Immutable ledger, visible to data owner	None or mutable
Expiration	Time-bounded, automatically expires	Permanent
Discovery	User notified (subject to legal constraints)	Silent, user never knows
Revocation	User can see and challenge after disclosure	Cannot be challenged if undetectable
Impact on other users	None—scoped to target data	Compromises all users if key is leaked

7. Data Residency Enforcement

7.1 Vault Residency Configuration

The Regulated Profile supports data residency enforcement: vault data for users in a specific jurisdiction is stored only on infrastructure in approved jurisdictions. This is configured at the vault level, the branch level, or the quantum level depending on the granularity required.

- **Vault-level:** All data for this user must reside in the EU. All institutional peers must operate infrastructure in the EU.
- **Branch-level:** The health branch must reside in Germany. The banking branch can reside anywhere in the EU. The social branch has no residency restriction.
- **Quantum-level:** Specific quanta (e.g., genetic data) must reside in the originating jurisdiction regardless of branch residency configuration.

7.2 Enforcement Mechanism

Residency constraints are encoded in the vault's configuration and enforced by the Bonafide runtime and the validator network:

- The runtime on the institution's infrastructure reports its geographic location through attestation.
- The validator network verifies that the reported location is consistent with the vault's residency constraints before validating any write operation.
- Replication to personal devices or cloud storage is subject to the same residency constraints—the user cannot replicate EU-restricted data to a US-based cloud provider unless the user explicitly overrides the constraint for their own copy.
- Cross-border transfers require explicit authorization per GDPR Chapter V requirements (adequacy decision, standard contractual clauses, or binding corporate rules).

7.3 Residency and Revocation

Data residency constraints survive revocation. When a user revokes an institution's access and the data is re-encrypted, the re-encrypted data remains in the same jurisdiction. The revocation process does not create cross-border data transfers.

8. Compliance Evolution

8.1 Living Document

This part of the specification is subject to more frequent updates than the cryptographic core. Regulatory frameworks evolve. New laws are enacted. Jurisdictions change tiers. The compliance profiles and market tier mapping will be maintained as a living annex to the specification, updated at least annually and whenever a material regulatory change affects deployment guidance.

8.2 Regulatory Monitoring

The Bonafide Foundation (Phase 2) or Sly Technologies (Phase 1) maintains a regulatory monitoring function that tracks legislative developments in all Tier 1 and Tier 2 jurisdictions and assesses new proposals for compatibility with the specification. When a proposed regulation would require capabilities outside the specification's design space, the monitoring function publishes an assessment and engages with the legislative process where appropriate.

8.3 Community Input

Jurisdiction-specific deployment guidance benefits from local expertise. The specification encourages community contributions for jurisdiction-specific compliance documentation, particularly for Tier 2 markets where the interaction between local law and the Bonafide protocol requires detailed analysis.

8.4 Principled Boundaries

The compliance evolution process has a defined boundary: the specification will add compliance features that work with the existing architecture (override scoping, residency enforcement, authority registration, reporting) but will never add features that compromise the architecture (master keys, bulk access, content scanning, silent access). This boundary is not subject to evolution. It is the specification's identity.

Bonafide™ — Privacy by architecture, not by promise.

An open specification by Sly Technologies Inc. | bonafide.id | bonafideid.org
V1.0 — February 2026