LEGAL & COMPLIANCE FRAMEWORK

DNA-Messenger

Cryptographic Infrastructure
Legal Classification & Compliance Posture

cpunk.io | March 2026 | Enterprise, Government & Defense

Table of Contents

DNA-Messenger is cryptographic infrastructure, not a cloud messaging service. It operates with zero centralized custody, no data harvesting and post-quantum security, reducing regulatory exposure for enterprises, governments and defense contractors.

1. Legal Classification

DNA-Messenger is a communications protocol and cryptographic software system. It is not a telecommunications provider, cloud messaging platform or managed data service.

The protocol operates as:

- Peer-to-peer software layer
- Cryptographic identity infrastructure
- Post-quantum secure messaging protocol
- Decentralized routing architecture

No centralized message processing, content inspection or metadata indexing is performed.

2. Decentralized User-Controlled Custody

DNA-Messenger is designed around a decentralized user-controlled encrypted custody model:

- No centralized message storage
- No server-side archives or logs

- Decentralized public key directory — all user data (contacts, settings) encrypted with AES-AEAD (keys derived via KEM)
- No metadata aggregation or analytics pipeline

Data Storage Model

- All data encrypted with AES-AEAD (keys derived via KEM) before storage
- Stored on decentralized DHT for multi-device sync
- Only the user can decrypt their own data
- No protocol-level visibility of content or identity

3. Privacy by Design

DNA-Messenger enforces privacy through cryptography instead of policy documents. There are no hidden analytics or tracking systems inside the protocol.

- No phone numbers or emails required for identity
- No advertising IDs, fingerprinting or profiling
- No telemetry or background analytics
- No passive collection of behavioral data

4. Regulatory Exposure Reduction

By removing centralized custody, DNA-Messenger reduces the regulatory burden under:

- **GDPR** — EU data protection and privacy
- **ISO/IEC 27001** — Information security management
- **SOC 2** — Security and confidentiality
- **HIPAA** — Healthcare data security
- **PCI-DSS** — Payment card industry data security
- **Financial obligations** — Communication and record-keeping

> There is no central breach domain, no cloud audit scope and no third-party data processing exposure at the protocol level.

5. Jurisdictional Independence

DNA-Messenger does not operate data centers, managed servers or cloud-hosted infrastructure. There is no fixed geographical location for message handling.

- No protocol-owned servers to subpoena, seize or compromise
- No cross-border data transfers performed by the protocol itself

- Routing is dynamic, peer-selected and operator-controlled

6. Encryption & Lawful Access

All DNA-Messenger traffic is end-to-end encrypted using post-quantum resistant cryptography.

- No master decryption keys
- No key escrow or recovery backdoors
- No administrator access to message content
- No protocol-level lawful intercept interface

> Lawful access, where required by domestic law, can only occur at the endpoint level under the control of the deploying organization or user.

7. Export Control Notice

DNA-Messenger includes cryptographic functionality that may fall under national export control regimes. The protocol itself does not ship as a cloud service or managed product.

Organizations deploying enterprise or white-label editions are responsible for:

- Export classification and licensing
- National cryptography registrations (where applicable)
- Compliance with regional regulations on strong encryption

8. Liability Model

DNA-Messenger is provided as protocol software and reference implementation. The protocol authors:

- Do not operate live networks or messaging services
- Do not host, store or process user data
- Do not act as identity authorities for end-users

Deploying organizations retain full responsibility for operational security, governance, compliance configuration and lawful use.

9. Intellectual Property

DNA-Messenger consists of a protocol specification, software implementation and cryptographic integration framework.

White-label and enterprise partners receive contractual rights to:

- Deploy and operate their own networks and bootstrap nodes

- Integrate the protocol into products and platforms
- Apply custom branding and identity namespaces

10. Neutrality Position

DNA-Messenger is politically neutral and jurisdiction-agnostic. It does not embed policy, censorship or moderation logic into the protocol layer.

- No hard-coded content filters
- No geopolitical routing controls
- No opinionated governance decisions embedded in the stack

Usage governance is handled by the organizations that deploy and operate DNA-Messenger-based networks.

11. Disclaimer & Executive Summary

DNA-Messenger is not a service provider — it is cryptographic infrastructure.

There is no central authority that controls, stores or processes user messages. Enterprises and sovereign operators retain full custody of identities, keys and network topology.

This legal and technical posture is designed to minimize regulatory exposure while maximizing control, sovereignty and post-quantum security for operators and their customers.

Compliance Snapshot

Designed to reduce audit scope

- No cloud message stores to audit
- No vendor access to confidential communications
- No third-party analytics or telemetry feeds
- Cryptographic guarantees instead of policy-only promises

Who Is This For?

Enterprise, Government & Defense

This framework is intended for compliance teams, regulators, procurement officers and legal counsel evaluating DNA-Messenger for:

- Financial institutions and critical infrastructure
- Healthcare and regulated industries
- Government agencies and defense contractors
- Sovereign and white-label deployments

— Quantum-safe, Decentralized, Community-driven. This document is provided for informational purposes only. It does not constitute legal advice. Organizations should consult their own legal and compliance teams before deployment. All information reflects the current state of the protocol and may be updated as the project evolves.