Veilo Layer LLC — Compliance Statement

Compliance Statement

Effective Date: April 30, 2026 **Last Updated:** May 12, 2026

1. Purpose

Veilo Layer LLC (“**Company**”, “**Veilo**”), a Wyoming limited liability company (Wyoming Secretary of State Entity ID **2026-001871701**, formed January 20, 2026, in good standing), develops and operates reference implementations and off-chain interfaces for the Veilo Protocol, a non-custodial cryptographic privacy protocol deployed on the Solana blockchain. Privacy is a legitimate use case for honest users and a fundamental property of cash-like financial systems. The Company is also committed to operating within applicable law and to denying the use of its Services to Restricted Persons and to bad actors.

This Compliance Statement describes the framework and controls the Company applies. It is published in the interest of transparency, to inform Users, regulators, partners, and investors of the Company’s posture. Capitalised terms not otherwise defined have the meanings given in the Terms of Service.

2. Compliance Principles

1. **Lawful design.** The Services are designed to provide privacy to lawful users of the Veilo Protocol. The Company does not design features whose primary use is to facilitate sanctions evasion, money laundering, terrorist financing, fraud, or other criminal activity.

2. **Jurisdictional scope.** The Services are offered on a jurisdictionally limited basis. **The Services are not offered to U.S. persons** or to persons in comprehensively-sanctioned jurisdictions or otherwise Restricted Jurisdictions, as set out in the Acceptable Use Policy.
3. **Sanctions compliance.** The Company complies with sanctions administered by the U.S. Office of Foreign Assets Control (OFAC), the United Nations Security Council, the European Union, the United Kingdom, and any other sanctions authority with jurisdiction over the Company.
4. **Cooperation with lawful authorities.** The Company cooperates with valid legal process. The Company does **not** voluntarily share User data without legal compulsion or imminent threat to life or safety. Where permitted, the Company notifies affected Users so they may seek to challenge requests.
5. **Minimum-data principle.** The Company collects only the data needed to operate the off-chain components of the Services. The Company does not require KYC for standard use of the Services. The Company may add tiered controls (transaction monitoring, risk scoring, additional jurisdictional restrictions) as required by law or its risk assessment.
6. **Non-custody.** The Company does not custody, control, or have access to User funds, private keys, recovery phrases, plaintext Notes, viewing keys, master viewing keys, or decryption keys. The on-chain Privacy Pool has no admin function permitting the Company (or any other party) to freeze, seize, blacklist, redirect, or unilaterally move User value.
7. **Transparency.** The Company publishes this Statement and intends to publish a periodic transparency report. The Company does not silently monitor User transactions for marketing or commercial purposes.

---

3. Sanctions Compliance

3.1 Restricted Persons

The Services are not available to Restricted Persons, defined in the Acceptable Use Policy. This includes (without limitation):

- **U.S. persons** (residents, citizens, organizations, permanent residents, tax residents, persons present in the U.S., persons acting on behalf of any of the foregoing, or otherwise within the meaning of 31 CFR § 1010.605 or 17 CFR § 230.902(k));
- persons resident, located, or organised in any country subject to comprehensive sanctions, currently: **Cuba, Iran, North Korea, Russia, Belarus, Syria, the so-called Donetsk and Luhansk People's Republics, the Kherson and Zaporizhzhia regions, and the Crimea region of Ukraine**;

- persons listed on:
  - the OFAC Specially Designated Nationals (SDN) List, the Sectoral Sanctions Identifications (SSI) List, the Foreign Sanctions Evaders (FSE) List, and any other OFAC list;
  - the UN Consolidated Sanctions List;
  - the EU Consolidated Financial Sanctions List;
  - the UK HM Treasury Consolidated List;
  - any other list of sanctioned persons applicable to the Company;
- persons acting on behalf of, or for the benefit of, any of the above; and
- persons in any other Restricted Jurisdiction enumerated by the Company from time to time.

3.2 Operational controls

The Company applies the following Interface-Level Controls to enforce Restricted-Person screening and sanctions compliance:

- **Geographic restriction at the network level.** The Company employs IP-based geo-blocking at the Site, the Web App, the Mobile App, the Extension, and the Reference Relayer to restrict access from the United States and from comprehensively-sanctioned jurisdictions.
- **Address screening.** `[The Reference Relayer screens transaction recipient addresses against sanctions lists obtained from licensed compliance vendors — confirm vendor (Chainalysis, TRM Labs, Elliptic) and implementation timeline]`. Transactions to addresses on a current sanctions list are refused at the Reference Relayer / interface level.
- **Eligibility representation.** Users represent in the Terms of Service that they are not Restricted Persons. Misrepresentation is a violation of the Terms and may give rise to civil and criminal liability under applicable law.
- **No-circumvention restriction.** Users are prohibited from using VPNs, proxies, anonymising networks, or other technologies to circumvent geographic or sanctions controls (see AUP, Section 2.6).
- **Compliance review.** The Company periodically reviews its sanctions controls and updates them in response to new designations, regulatory guidance, and risk assessment.

3.3 Limitations

Address screening is only as effective as the public sanctions data it relies on. New designations, freshly-created addresses, and addresses not yet attributed to sanctioned persons may pass screening. Privacy features mean that, by design, **after** a Privacy Pool deposit, the link between a downstream withdrawal recipient and the original deposit's history is cryptographically obscured — the Company

cannot screen withdrawal recipients against a deposit's history within the Pool. The Company screens the **on-chain participants** (deposit signer, withdrawal recipient) the Company observes at the time of submission.

3.4 Refusal and reporting

If the Company identifies a transaction or attempted transaction involving sanctioned persons or property, the Company will: (i) refuse to process it at the Reference Relayer or interface level; and (ii) report it to OFAC and other relevant authorities to the extent required by law applicable to the Company.

---

4. Anti-Money Laundering and Counter-Terrorist Financing (AML / CFT)

4.1 Policy

The Company prohibits the use of the Services to engage in money laundering, terrorist financing, fraud, or any other financial crime. See the Acceptable Use Policy.

4.2 Risk-based approach

The Company conducts a risk assessment of the Services and operations and applies controls commensurate with the risk identified. The risk assessment considers:

- Customer risk (geography, transaction patterns, counterparty risk);
- Product risk (privacy-preserving transactions present specific obfuscation risks);
- Geographic risk (FATF-listed and high-risk jurisdictions);
- Channel risk (anonymous crypto-native interactions).

4.3 Controls

Current controls include:

- Geographic and sanctions screening (Section 3);
- `[Transaction-monitoring rules at the Reference Relayer to detect patterns indicative of structuring, laundering through high-risk counterparties, or other red flags — confirm implementation]`;
- Refusal of Reference Relayer service to Users whose conduct violates the AUP or applicable law;
- `[Suspicious Activity Report (SAR) filing process if and when the Company is required to register as an MSB or equivalent — confirm with counsel]`;
- Cooperation with lawful authority requests (Section 6).

4.4 Regulatory characterization

The Company's regulatory characterization is the following:

- **United States — FinCEN. The Services are not offered to U.S. persons.** Without prejudice to that fundamental jurisdictional limitation, the Company's position is that the Reference Relayer activity does not constitute money transmission requiring registration as a Money Services Business (MSB) under 31 CFR § 1010.100 because: (i) the Reference Relayer does not custody User funds; (ii) the Reference Relayer acts solely on User-signed cryptographic instructions and cannot modify, redirect, or reject the authorized contents of a transaction; (iii) the Reference Relayer falls within applicable exceptions for anonymizing-software providers and non-custodial transmission facilitators under 31 CFR § 1010.100(ff)(5)(ii); and (iv) U.S. persons are excluded from the Services by contract. **This characterization is subject to change** based on regulatory developments and counsel review.
- **European Union — MiCA.** The Company's position with respect to the Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114) is `[under analysis — counsel review required to determine whether the Reference Relayer's transfer-of-virtual-assets activity falls within the scope of "providing transfer services for crypto-assets" requiring CASP authorisation under Article 60 et seq.]`. The Company's preliminary position is that the Reference Relayer is a non-custodial software facilitator rather than a regulated transfer-service provider.
- **United Kingdom — FCA / MLR.** `[Under analysis — including consideration of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended.]`
- **Other jurisdictions.** The Company applies a risk-based approach and may restrict access from jurisdictions where the regulatory status is unclear or where compliance would be unduly burdensome.

The Company will update this Statement and the Terms of Service as its regulatory position evolves.

4.5 No tax reporting

The Company does not currently issue tax forms (e.g., U.S. Form 1099, EU DAC8 reports). Users are solely responsible for their tax reporting obligations. If the Company becomes legally required to issue tax forms in any jurisdiction, the Company will do so and notify affected Users.

---

5. Customer Identification

The Company does not currently require Users to provide government-issued identification or undergo Know Your Customer (KYC) verification to use the Services. Users provide only:

- a self-selected username;
- a Solana wallet address; and
- cryptographic credentials generated locally on their device.

This approach reflects the Company's view that the Services do not constitute regulated financial intermediation, and is consistent with the exclusion of U.S. persons from the Services. **The Company reserves the right to introduce KYC requirements** for some or all Users in the future if required by law or by the Company's risk assessment, including:

- threshold-based KYC for transactions above specified amounts;
- enhanced due diligence for Users in higher-risk jurisdictions;
- verification of source of funds in response to suspicious activity.

If KYC is introduced, the Company will provide reasonable notice and allow Users to withdraw value before requirements take effect.

---

6. Cooperation With Authorities

6.1 Lawful requests

The Company responds to:

- **Subpoenas, court orders, and search warrants** issued by a court with jurisdiction over the Company;
- **Mutual Legal Assistance Treaty (MLAT) requests** routed through proper channels;
- **Sanctions or regulatory orders** from authorities with jurisdiction over the Company;
- **Emergency disclosure requests** where there is an imminent risk of death or serious bodily harm.

The Company does **not** voluntarily disclose User data outside these processes.

6.2 Notification

Where permitted by the request and applicable law, the Company will notify affected Users before responding so they may seek to challenge the request. The Company will not notify Users where:

- a non-disclosure order or gag order applies;
- notification would interfere with a legitimate ongoing investigation; or
- there is an imminent threat to life or safety.

6.3 Limitations on what the Company can disclose

Because of the architecture of the Services, **the Company cannot disclose what it does not have**. The Company does not have, and therefore cannot disclose:

- recovery phrases, private keys, or passwords;
- plaintext Note contents, viewing keys, master viewing keys, or decryption keys;
- any data that exists only on the User's device;
- the contents of transactions before they are broadcast (they are decrypted only in volatile memory and immediately discarded);
- balances within encrypted token accounts;
- the linkage between a Privacy Pool deposit and a downstream withdrawal (by design — this is the privacy property of the Protocol).

The Company cannot:

- modify, freeze, or seize on-chain assets in the Privacy Pool — the deployed Smart Contract has no admin function for that, and no party (including the Company) has the technical ability to do so;
- reverse, cancel, or modify a confirmed Blockchain transaction;
- decrypt encrypted Notes or encrypted Veilo keys held in backup;
- compel any independent Relayer, validator, MPC node operator, RPC provider, wallet provider, or other Protocol participant to take any action.

The Company **can** disclose, in response to lawful process:

- Account metadata (username, wallet address);
- Encrypted Note backups (which the Company cannot decrypt);
- Pseudonymous transaction stats (counts, timestamps, success/failure);
- Server logs (IP, user-agent, request timestamps);
- Information from the sub-processors listed in the Privacy Policy to the extent the Company controls it;
- The fact that a particular wallet address is on the Restricted-Person list and is refused Reference Relayer service.

6.4 Transparency report

`[The Company intends to publish a transparency report at least annually summarising government data requests received and responded to, in aggregate. First report planned for [DATE]. Counsel to confirm whether and how to publish given gag-order constraints.]`

---

7. Compliance With Court Orders Affecting On-Chain Activity

If a court orders the Company to take action that requires modifying on-chain state (e.g., blocking specific addresses from depositing into the Privacy Pool, freezing balances, or seizing value), the Company will assess feasibility:

- The deployed Smart Contracts are **immutable** and do not contain admin functions to freeze, blacklist, or seize. The Company cannot modify on-chain balances or transaction history.
- The Company-operated **Reference Relayer** can be modified to refuse service to specific addresses, transaction patterns, or jurisdictions in response to a binding legal order. The Company will respond to lawful orders by adjusting Reference Relayer behaviour to the extent technically feasible, while complying with applicable due-process, notification, and disclosure requirements.
- The Company has **no control over independent Relayers** that may be operated by third parties or by Users themselves. A court order directed at the Company cannot compel the action of an independent Relayer that the Company does not operate.

Lawful authorities can therefore compel the Company to refuse Reference Relayer service to specific persons or addresses, but **cannot compel the Company to recover or seize value already deposited in the Privacy Pool**, nor compel the Company to compel third parties (validators, independent Relayers, RPC providers, MPC node operators) to take action. Users are advised that **the Company-operated Reference Relayer is a control surface that is subject to legal compulsion**.

In exceptional circumstances involving active exploitation, systemic Protocol risk, or legal compulsion, temporary Interface-Level Controls may be applied to Reference Relayer routing or Service access. Such measures are limited in scope, time-bound, automatically expiring absent renewed justification, and do not affect asset ownership, transaction authorization, or the User's ability to interact with the Protocol via independent means.

---

8. Bug Bounty and Responsible Disclosure

The Company encourages security researchers to report vulnerabilities through the responsible-disclosure process at `manager@veilo.network` (or, once operational, `security@veilo.network`). The Company will:

- acknowledge reports promptly;
- coordinate on remediation timelines;
- credit researchers (with permission); and
- not pursue legal action against good-faith researchers acting in compliance with the Company's `[SECURITY.md — to be created]` policy.

`[Confirm bug-bounty program structure and amounts with counsel; consider Immunefi or HackerOne integration.]`

---

9. Independent Audits

The Company commissions independent security audits of critical components:

- **`privacy-program` (on-chain)** — audited March 2026 (1 medium-severity finding); next audit planned `[DATE]`.
- **`relayer-server`** — audited January 2026 (12 findings, all addressed); next audit planned `[DATE]`.
- **`zk-circuits`** — `[audit status — confirm]`.

Audit reports are `[published / available on request — confirm]`. The existence of an audit is **not** a representation that the audited component is free from defect (see Disclaimers, Section 10).

---

10. Updates and Effective Date

The Company may update this Statement to reflect changes in law, operations, or risk assessment. When the Company does, it will update the "Last Updated" date above and post the updated version at `https://veilo.network/compliance` `[once available]`.

---

11. Contact

Topic	Contact
Compliance / regulatory inquiries, sanctions / OFAC, law-enforcement requests	`legal@veilo.network` (for law-enforcement, use subject line: “Law Enforcement Request”)
Privacy / data-subject requests, security disclosures	`manager@veilo.network`
General support	`support@veilo.network`

Veilo Layer LLC A Wyoming Limited Liability Company (Entity ID 2026-001871701) `[REGISTERED AGENT ADDRESS, WYOMING]` State of Wyoming, United States

---

Built with zero-knowledge proofs on Solana.