

# Veilo Layer LLC – Acceptable Use Policy

---

## Acceptable Use Policy

---

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

---

### 1. Purpose

---

This Acceptable Use Policy (“**AUP**”) sets out the rules for using the Services provided by **Veilo Layer LLC**, a Wyoming limited liability company (Wyoming Secretary of State Entity ID **2026-001871701**, formed January 20, 2026) (“**Company**”, “**Veilo**”, “**we**”, “**us**”, or “**our**”). “**Services**” has the meaning given in the [Terms of Service](#).

This AUP is incorporated into the Terms of Service. Capitalised terms used but not defined herein have the meanings given to them in the Terms of Service.

By accessing or using any Service, you agree to comply with this AUP. **Violation may result in immediate suspension or termination of your access to the Services**, with or without notice, and may be reported to law-enforcement authorities or applicable regulators where required by law.

---

### 2. Restricted Persons

---

You **may not** access or use the Services if you are a Restricted Person. A “**Restricted Person**” includes any individual, entity, or other person that meets one or more of the following criteria.

## 2.1 United States

**The Services are not offered to, and may not be used by or on behalf of, any U.S. person.** A U.S. person includes any person:

- resident in, located in, ordinarily resident in, organized under the laws of, or otherwise present in any state, district, territory, possession, or commonwealth of the United States of America (including without limitation all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and all U.S. military and diplomatic locations);
- who is a citizen or national of the United States, regardless of residence;
- who is a U.S. permanent resident (“green card” holder), regardless of residence;
- who is a U.S. tax resident, regardless of citizenship or residence;
- who is acting on behalf of, for the account of, or for the benefit of, any of the above; or
- who is otherwise a “U.S. person” within the meaning of any applicable U.S. law, including without limitation 31 CFR § 1010.605, 17 CFR § 230.902(k), or the U.S. Internal Revenue Code.

This restriction reflects the Company’s decision to offer the Services on a jurisdictionally limited basis. It is not a representation that U.S. persons are precluded by law from using non-custodial software, but a contractual restriction on access to the Services.

## 2.2 Comprehensively-sanctioned jurisdictions

The Services are not offered to, and may not be used by, any person resident in, located in, ordinarily resident in, organised under the laws of, or accessing the Services from any country or territory subject to comprehensive U.S., U.N., E.U., or U.K. sanctions. As of the Effective Date, this includes:

- Cuba
- Iran
- North Korea (Democratic People’s Republic of Korea)
- Russia
- Belarus
- Syria
- The non-government-controlled areas of Ukraine, including the so-called Donetsk People’s Republic, the so-called Luhansk People’s Republic, and the Kherson and Zaporizhzhia regions
- The Crimea region of Ukraine

The Company may update this list at any time to reflect changes in applicable sanctions.

## 2.3 Other Restricted Jurisdictions

The Services are not offered in any jurisdiction where the Company has determined that the Services are not made available, including without limitation jurisdictions on the Financial Action Task Force (FATF) "high-risk" or "increased monitoring" lists, jurisdictions identified as high-risk for money-laundering or terrorist-financing purposes, and any jurisdiction where local law would require the Company to obtain licenses, registrations, or authorisations that the Company has not obtained. The current additional Restricted Jurisdictions are: Afghanistan, Myanmar, Venezuela, Yemen, Zimbabwe, and any jurisdiction designated by FATF as high-risk or under increased monitoring.

## 2.4 Sanctioned persons

You are a Restricted Person if you are:

- listed on, owned 50% or more (in aggregate) by parties listed on, or otherwise subject to:
  - the OFAC Specially Designated Nationals and Blocked Persons List (SDN);
  - the OFAC Sectoral Sanctions Identifications List (SSI);
  - the OFAC Foreign Sanctions Evaders List (FSE);
  - any other OFAC list;
  - the U.S. Department of Commerce Bureau of Industry and Security Entity List, Denied Persons List, or Unverified List;
  - the U.S. Department of State's lists of arms-traffickers, foreign terrorist organisations, or weapons-proliferators;
  - the Consolidated UN Security Council Sanctions List;
  - the Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions;
  - the UK HM Treasury Consolidated List of Financial Sanctions Targets; or
  - any other applicable list of sanctioned persons;
- acting on behalf of, or for the benefit of, any person described above; or
- owned or controlled by, or owned 50% or more (individually or in aggregate) by, any person described above.

## 2.5 Eligibility representation

By accessing or using the Services, you represent and warrant on a continuing basis that you are not a Restricted Person and that all eligibility representations made in the Terms of Service remain true. You agree to immediately discontinue use of the Services and (if applicable) withdraw any value held within the Privacy Pool if your status changes such that you become a Restricted Person. **Misrepresentation of eligibility is a material breach of the Terms of Service and may give rise to civil and criminal liability under applicable law.**

## 2.6 No circumvention

You may **not** use a virtual private network (VPN), proxy server, anonymising network (such as Tor), false location indicator, false jurisdictional representation, or any other method or technology to:

- circumvent the Company's geo-restriction, sanctions screening, or Restricted-Person filters;
- conceal your true location, residence, citizenship, or status; or
- access the Services from a Restricted Jurisdiction or while being a Restricted Person.

Circumvention of the Company's Interface-Level Controls is a material breach of the Terms of Service and may give rise to civil and criminal liability.

---

## 3. Prohibited Activities

---

You **may not** use the Services to:

### 3.1 Engage in unlawful activity

- engage in money laundering, terrorist financing, sanctions evasion, fraud, tax evasion, market manipulation, insider dealing, ransom payment, bribery, theft, or any other criminal activity;
- process, transmit, hold, conceal, layer, or integrate proceeds of crime or property derived from crime;
- facilitate any transaction that violates applicable law in your jurisdiction or any jurisdiction in which the transaction has effect;
- engage in any activity that finances or facilitates the proliferation of weapons of mass destruction;
- engage in any activity that constitutes child sexual abuse material (CSAM), human trafficking, modern slavery, or any other crime against persons; or
- engage in any activity related to dark-net market operations, ransomware deployment, ransomware payments, or other malicious-software-related financial flows.

### 3.2 Transact with sanctioned counterparties

- send to, receive from, or otherwise transact with any address known or reasonably suspected to be associated with a sanctioned person, a sanctioned jurisdiction, or a sanctioned activity;
- use the Privacy Pool to obscure the origin or destination of funds in a transaction involving a sanctioned counterparty;
- help any other person evade sanctions; or
- structure transactions to avoid sanctions screening or reporting.

### 3.3 Misuse the Privacy Pool

- use the Privacy Pool with the primary purpose of concealing the proceeds of crime or evading legal obligations (taxes, court orders, sanctions, judgments, subpoenas);
- conduct transactions that, but for the use of Veilo, would be illegal or non-compliant with applicable law;
- structure transactions to evade reporting thresholds or trigger detection thresholds; or
- attempt to evade selective-disclosure or compliance-attestation obligations applicable to you.

### 3.4 Attack the Services or the underlying infrastructure

- probe, scan, or test the security of the Services without prior written authorisation, except as expressly permitted by the Company's responsible-disclosure policy at `manager@veilo.network` (or, once operational, `security@veilo.network`);
- exploit any vulnerability in the Services for any purpose other than reporting it to the Company in good faith;
- attempt to gain unauthorised access to the Services, the Smart Contracts, related systems, other Users' accounts, or other Users' devices;
- submit malicious payloads, malformed proofs, or otherwise attempt to manipulate the on-chain Privacy Pool, the Reference Relayer, the SDK, any independent Relayer, or any wallet in unintended ways;
- conduct denial-of-service attacks, including by submitting unreasonable volumes of requests, exploiting rate limits, or attempting to drain Reference Relayer resources;
- reverse engineer, decompile, or disassemble any non-open-source component of the Services, except where this restriction is unenforceable under applicable mandatory law; or
- attempt to extract trusted-setup secrets, prover keys, or other cryptographic material from any Company-operated infrastructure.

### 3.5 Misuse Relayers

- operate or attempt to operate an unauthorised competing Relayer using the Company's infrastructure, proprietary code, or service (the Veilo Protocol is permissionless and you may operate your own Relayer independently, but you may not parasitise the Reference Relayer's infrastructure);
- resell, sublicense, or otherwise commercially provide Reference Relayer access without our prior written consent;
- submit transaction requests on behalf of third parties for whom you do not have proper authorisation;

- submit batch or automated requests at a rate that disrupts service for other Users (consumer or developer use of normal request rates is acceptable; abusive automation is not);
- use the Reference Relayer to inflate transaction volume artificially (e.g., wash trading, sybil volume gaming, fee-harvest farming); or
- attempt to compel the Reference Relayer to broadcast a transaction in violation of applicable Interface-Level Controls.

### **3.6 Misuse the SDK**

- use the SDK in any product that violates this AUP or any applicable law in any jurisdiction where your product is available;
- distribute or operate a product based on the SDK without binding your end users to terms substantively equivalent to (or stricter than) the Veilo [Terms of Service](#), including this AUP, the [Risk Disclosure](#), and the U.S.-person restriction;
- misrepresent your product as official, endorsed, partnered, or affiliated with the Company without our prior written consent;
- offer your SDK-based product to Restricted Persons (including U.S. persons); or
- use the SDK to build a product that circumvents the Restricted-Person restrictions in the Veilo Terms of Service.

### **3.7 Misuse usernames, branding, or content**

- choose a username that impersonates another person, entity, brand, or that is unlawful, defamatory, obscene, threatening, harassing, or infringing;
- display, distribute, or transmit User Content that is unlawful, defamatory, obscene, threatening, harassing, infringing, or otherwise objectionable;
- use the Company's name, logos, trademarks, or domain names without our prior written consent (subject to permitted uses under applicable open-source licenses);
- engage in phishing, impersonation of the Company, or other deceptive conduct; or
- claim or imply that any third-party product, service, or relationship is endorsed by, partnered with, or affiliated with the Company without our prior written consent.

### **3.8 Interfere with other Users**

- spam, harass, defraud, or otherwise harm other Users;
- send unsolicited tokens or NFTs (including airdrops, "dust" attacks, or scam tokens) for the purpose of defrauding, deceiving, or de-anonymising recipients;
- solicit recovery phrases, passwords, viewing keys, or other sensitive information from any User;
- falsely represent yourself as Veilo support staff or as another User; or

- attempt to deanonymise, dox, or otherwise compromise the privacy of other Users.
- 

## 4. Geographic and Jurisdictional Restrictions

---

### 4.1 Enforcement

The Company enforces geographic restrictions through Interface-Level Controls, which may include IP-based geo-blocking at the Site, the Web App, the Mobile App, the Extension, and the Reference Relay; sanctions-list screening; and additional measures the Company considers appropriate. Operation of such Interface-Level Controls does not affect, and is not intended to affect, the autonomous operation of the Smart Contracts or transaction-validity at the on-chain Protocol level.

### 4.2 Your responsibility

The Company's geographic restrictions are based on its operational assessment and **are not legal advice to you**. Even if you are not in a Restricted Jurisdiction or otherwise a Restricted Person, you remain responsible for confirming that your access to and use of the Services complies with all laws applicable to you, including the laws of any jurisdiction in which you are a resident, citizen, or located.

You may not use VPNs, proxies, anonymising networks, false location indicators, false jurisdictional representations, or other technologies to circumvent the Company's geographic restrictions or Restricted-Person filters.

### 4.3 Changes

The Company may add or remove jurisdictions from the Restricted Jurisdictions list at any time, including in response to changes in sanctions, regulatory action, court order, FATF designations, or its own risk assessment. Any change is effective when posted unless otherwise stated. The Company may apply additional Interface-Level Controls (rate limiting, refusal of Reference Relay service, etc.) to additional jurisdictions on a per-jurisdiction basis.

---

## 5. Consequences of Violation

---

If the Company determines, in its reasonable discretion, that you have violated this AUP, the Company may take any of the following actions, with or without notice:

- refuse Reference Relay service for one or more transactions;
- suspend or terminate your account and access to the Services;

- cancel pending transactions that would constitute a violation;
- block your wallet address(es) or username(s) from accessing the Reference Relay or other Company-operated Services;
- block the IP address(es), device fingerprint(s), or geographic regions used to access the Services;
- withhold or refund any fees, in the Company's discretion;
- notify law-enforcement authorities, regulators, or third parties where required by law or where there is an imminent threat;
- report suspicious or potentially unlawful activity to applicable financial-intelligence units, regulators, or law-enforcement authorities; or
- take any other action the Company considers necessary to comply with law, protect Users, or protect the Services.

The Company may also pursue legal remedies, including civil claims for damages, injunctive relief, accounting of profits, disgorgement, and recovery of costs and attorneys' fees.

These actions are taken at the off-chain interface and Reference Relay level and do **not** affect the on-chain Privacy Pool, which the Company does not control. Value you have already deposited in the Pool remains yours and continues to be governed by the on-chain Smart Contracts — but if your access to the Reference Relay is terminated and no alternative Relay is available to you, you may be unable to withdraw your value until you obtain access to a compatible Relay (including a Relay you operate yourself).

---

## 6. Reporting Violations

---

If you become aware of a violation of this AUP, please report it to [legal@veilo.network](mailto:legal@veilo.network) (for sanctions or unlawful activity) or [manager@veilo.network](mailto:manager@veilo.network) (for security concerns or impersonation). Include where possible:

- a description of the activity;
- any wallet addresses, transaction signatures, or usernames involved;
- the date and time;
- the channel or surface where the activity was observed; and
- any other information you can provide.

The Company will review reports promptly and take action where warranted. The Company does not guarantee a response to every report.

---

## 7. Cooperation With Authorities

---

The Company cooperates with lawful authorities as described in the [Compliance Statement](#). This includes:

- refusing to process transactions the Company is legally required to refuse;
- disclosing data in response to valid legal process;
- reporting suspicious activity where required by law applicable to the Company.

The Company does **not** voluntarily disclose User data outside these processes. Where legally permitted, the Company will notify affected Users before responding so they may seek to challenge the request.

---

## 8. Updates to This AUP

---

The Company may update this AUP from time to time. When the Company does, it will:

- update the “Last Updated” date at the top;
- for material changes, post notice in the Services or on the Site at least **30 days** before they take effect (or such shorter period as required by law or compelling operational, security, regulatory, or compliance need);
- for minor changes (clarifications, formatting), changes take effect upon posting.

Your continued use after the effective date of an updated AUP constitutes your acceptance of the updated AUP.

---

## 9. Contact

---

Topic	Contact
Reporting AUP violations, sanctions / OFAC inquiries, law-enforcement requests	<code>legal@veilo.network</code> (for law-enforcement, use subject line: “Law Enforcement Request”)
Security-vulnerability disclosures	<code>manager@veilo.network</code> (or, once operational, <code>security@veilo.network</code> )
General support	<code>support@veilo.network</code>

**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.*