Veilo Layer LLC — Privacy Policy

Privacy Policy

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

1. Introduction and Scope

This Privacy Policy ("**Policy**") describes how **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**"), collects, uses, stores, discloses, and otherwise processes information in connection with access to and use of the Veilo financial privacy protocol (the "**Veilo Protocol**" or "**Protocol**"), the reference implementations and interfaces operated by the Company (collectively, the "**Services**"), and related off-chain infrastructure.

This Policy is derived from, and implements, the Company's internal privacy and data-handling standards, which are designed to reflect privacy-by-design, data-minimisation, and security-by-default principles appropriate to a decentralised, non-custodial Smart-Contract system. This Policy is intended to provide transparency into how those standards apply in practice and to accurately reflect the technical architecture and operational boundaries of the Protocol. **It does not create any fiduciary, custodial, advisory, or monitoring obligations, nor does it imply that the Company possesses technical capabilities or access beyond what is expressly described herein.**

For purposes of the EU General Data Protection Regulation (Regulation (EU) 2016/679; "**GDPR**"), the UK Data Protection Act 2018 / UK GDPR, the Brazilian Lei Geral de Proteção de Dados (Law 13.709/2018; "**LGPD**"), and analogous frameworks, the data controller (in respect of the limited categories of

information actually processed by the Company) is Veilo Layer LLC, with its registered office in the State of Wyoming, United States. The data controller's representative for European Union data subjects is `[name and address — confirm pending Art. 27 GDPR appointment]`.

This Policy is incorporated into the Veilo Terms of Service and must be read together with the Acceptable Use Policy, Risk Disclosure, Disclaimers, and Compliance Statement. Capitalised terms not otherwise defined in this Policy have the meanings given to them in the Terms of Service. In the event of any inconsistency between this Policy and the Terms of Service, the Terms of Service shall prevail to the extent of such inconsistency.

For privacy questions, requests, or complaints, contact us at `manager@veilo.network`.

---

2. Core Privacy Position and Regulatory Baseline

2.1. **Data minimisation and architectural constraints.** The Veilo Protocol is architected to minimise the collection, processing, and retention of information and to avoid processing information that could reasonably be used to identify Users wherever technically feasible. The majority of User interactions occur on-chain or locally within the User's environment, without reliance on Company-operated accounts, centralized databases, or identity-linked records. The Company intentionally limits its information-handling activities to what is strictly necessary to operate, secure, and maintain the off-chain interfaces and infrastructure that surround the autonomous on-chain Protocol.

2.2. **Absence of identity verification.** The Company does **not**:

- request or collect government-issued identifiers;
- request or collect biometric information;
- require identity verification, KYC onboarding, or compliance screening keyed to natural persons;
- maintain records linking wallet addresses to real-world identities;
- perform User identification, profiling, behavioural classification, or risk scoring;
- monitor User transactions for marketing, advertising, or commercial-data purposes;
- perform wallet clustering, transaction-graph analysis, address-linkage analysis, deanonymisation, behavioural analytics, or any similar surveillance.

Any association between a User and a Blockchain address is established solely by the User through their chosen wallet software and exists independently of the Company's systems, records, or infrastructure.

2.3. **No custody, no surveillance, no profiling.** Privacy properties associated with the Protocol arise from cryptographic design and User-controlled key management, not from trust placed in the Company. The Company does not:

- have the technical ability to access, decrypt, modify, reverse, or associate on-chain transaction contents, Encrypted Notes, viewing keys, master viewing keys, decryption keys, or other cryptographic material with identified or identifiable individuals;
- perform wallet clustering, transaction-graph analysis, address linkage, behavioural analysis, or attempt to deanonymise Users;
- sell, rent, license, or otherwise monetise User information; or
- enrich Blockchain data with off-chain identifiers.

Any execution coordination, routing logic, abuse prevention, or interface-level control introduced by the Company does not grant the Company access to User assets, private keys, viewing keys, decrypted balances, transaction contents, or protocol state, and does not alter the non-custodial nature of the Protocol.

2.4. **Controller / processor positioning.** To the extent that privacy or data-protection principles may be deemed applicable, the Company determines the limited purposes and means of processing **solely in relation to** technical, operational, and administrative information processed in connection with the Site, the Web App, the Extension, the Mobile App, the Docs, the Reference Relayer infrastructure, the SDK, and User-initiated communications. The Company **does not** act as a controller, processor, joint controller, fiduciary, custodian, or trusted intermediary in respect of:

- on-chain transaction data (commitments, nullifiers, Merkle tree leaves, transaction hashes, signatures, timestamps);
- Encrypted Notes, cryptographic commitments, or ciphertexts in their authoritative or Protocol-governing form;
- private keys, plaintext viewing keys, master viewing keys, decryption keys, or cryptographic secrets in any form accessible or controllable by the Company;
- Solana validator activity, MPC node activity (if and when adopted), Relayer-internal activity outside the Reference Relayer, or RPC-provider activity; or
- any data processed exclusively within User-controlled wallets, devices, or decentralised infrastructure.

The Company may operate non-authoritative off-chain infrastructure that mirrors or derives cryptographic commitments, Merkle tree state, or UTXO-related data from publicly verifiable on-chain state solely to support Service usability. Such infrastructure introduces no trust assumptions, does not alter Protocol state, and can be independently replicated or verified by anyone using public Blockchain data. The Protocol may also involve handling of encrypted key material (including encrypted master viewing keys) which cannot be decrypted by the Company and may only be re-encrypted pursuant to explicit, User-authorised on-chain permissions. The Company has no unilateral ability to access, derive, or disclose private keys, viewing keys, balances, or other sensitive information.

2.5. **Public Blockchain data disclaimer.** Public Blockchain networks, including Solana, are transparent, immutable, and globally accessible by design. The Company does not control, curate, modify, delete, or restrict access to Blockchain data. For the avoidance of doubt:

- Blockchain addresses, transaction hashes, timestamps, commitments, nullifiers, Merkle roots, and related metadata are **not collected or processed by the Company as personal data**; they are public-ledger records produced by the Solana network and are not, of themselves, intended to identify natural persons;
- the Company does not determine the purposes or means of processing such data; and
- such data falls **outside** the Company's technical and operational control for purposes of this Policy.

To the extent that information recorded on public Blockchains could be interpreted as personal data under certain frameworks when combined with off-chain information, such information is generated, propagated, and made publicly available by decentralised Blockchain infrastructure operating independently of the Company. The Company does not have the technical ability to modify, delete, or restrict access to on-chain data and cannot honour erasure or rectification requests directed at on-chain state.

2.6. **No automated decision-making or profiling.** The Company does not engage in automated decision-making, profiling, scoring, or classification of Users that produces legal or similarly significant effects within the meaning of GDPR Art. 22. Any automated processes associated with the Veilo Protocol — including cryptographic verification, transaction validation, ZK-proof verification, and Smart Contract execution — are performed autonomously by decentralised systems and do not constitute decisions made by the Company.

2.7. **No expansion of obligations.** Nothing in this Policy shall be construed as:

- an admission that the Company processes information beyond what is expressly described herein;
- an agreement to assume obligations, roles, or technical capabilities beyond those expressly set out in this Policy;
- an undertaking to eliminate all privacy risks;
- a commitment to maintain specific cryptographic standards indefinitely; or
- an assumption of fiduciary, custodial, monitoring, surveillance, or recordkeeping obligations beyond those imposed by applicable law.

The Company may modify technical implementations over time to further reduce information processing where feasible, without expanding the scope of data processed or altering the non-custodial nature of the Protocol.

---

3. Privacy Principles

The Services are designed around three principles:

1. **Local first.** Recovery phrases, private keys, passwords, plaintext Note contents, viewing keys, and decryption keys are stored on your device. The Company has no technical means to access them.
2. **Minimum necessary.** The Company collects the minimum data necessary to operate the off-chain components of the Services. The Company does not sell, rent, trade, monetise, or otherwise commercially exploit User data.
3. **Transparent.** The Company tells you what it collects, why, with whom it is shared, and how long it is retained. Information is processed only for defined, proportionate, and legitimate purposes set out in this Policy.

---

4. Categories of Data We Process

The data the Company processes depends on which Service you use. The Company adheres to a principle of strict data minimisation; information is processed only to the limited extent necessary to operate and maintain the off-chain components of the Services, ensure technical security and integrity, and respond to User-initiated communications. **The Company does not process personal data as part of the core functioning of the Veilo Protocol itself.** The Protocol operates autonomously on the Solana blockchain through decentralised Smart Contracts, without reliance on Company-controlled databases, identity systems, or custodial infrastructure.

4.1 Stored on your device only — the Company never sees this

Data	Where	How protected
12-word BIP-39 recovery phrase	Device storage (encrypted)	AES-256-GCM with PBKDF2-derived key from your password
Private keys (Solana primary, auxiliary Veilo keys)	Device storage (encrypted)	Same as above
Wallet password	Memory only during active session	Never written to disk; never transmitted
Plaintext Note contents	Device storage	AES-256-GCM at rest; decrypted only in volatile memory when needed
Auxiliary viewing keys, master viewing keys, decryption keys	Device storage (encrypted)	AES-256-GCM at rest

The Company has **no technical ability** to access this data. It cannot be retrieved by the Company, by law enforcement, or by any party with access to the Company's servers.

4.2 Processed by Company-operated off-chain systems

Data	Source	Why we process it	Retention
Solana wallet address (public)	You, when you create or connect a wallet	Account identification; balance queries; service routing	Until account deletion
Username (public; self-selected)	You, when you create an account	So other Veilo Users may send you private transfers by name	Until account deletion
Encrypted Veilo keys (ciphertext only)	Generated locally; transmitted encrypted	Multi-device restoration of encryption material; we cannot decrypt	Until account deletion
Encrypted Notes (ciphertext only)	Generated and encrypted on your device	Backup so you may restore Privacy Pool balances on a new device; we cannot decrypt	Until account deletion or 365 days after last access (whichever is sooner)
Authentication challenges and signatures	You, during sign-in	Prove control of wallet without passwords	7 days (rolling)
Authentication tokens (JWTs)	Issued by us	Maintain session	7-day expiry
Push-notification tokens (Mobile App only)	Apple/Google, with your consent	Send transaction notifications	Until you revoke notification permission or delete account
Encrypted transaction request payloads	You, at the time of a private withdrawal/transfer/swap submitted through the Reference Relayer	Process the transaction; decrypted only in volatile memory; not retained	Discarded immediately after processing
Pseudonymous transaction stats (count, success rate, latency, fee paid — never amount or identity)	Generated by the Reference Relayer	Operations and performance monitoring	24 months (aggregated/anonymized thereafter)

Data	Source	Why we process it	Retention
Public on-chain events (commitments, nullifiers, Merkle leaves) indexed by us for usability	Solana network (public)	Off-chain mirror to speed up Merkle-tree synchronisation; publicly readable on the blockchain	Indefinitely (mirrors public chain)

4.3 Network-level technical data

Data	Why	Retention
IP address (server logs; truncated where feasible)	Security, abuse prevention, geo-restriction enforcement (including United States restriction)	30 days
User-agent / device-type	Compatibility, debugging	30 days
Timestamp of API requests	Operations, abuse prevention	30 days
Crash reports (Mobile App only, via Sentry; opt-out available)	Debugging	90 days

Network-level data is processed at the interface or infrastructure level only and is not used to identify Users, build profiles, or associate technical data with wallet addresses, transactions, or Protocol activity. Where feasible, network-level data is processed in an aggregated, transient, or anonymised form.

4.4 What we do not collect

The Company does **not** collect, request, or receive:

- your name, email address, postal address, phone number, or other personally identifying information;
- government-issued identifiers;
- tax identifiers, social-security numbers, or financial-institution information;
- biometric data (Face ID / Touch ID / fingerprint authentication is performed locally by your operating system; the Company never sees biometric data);
- location data (the Services do not use GPS, geolocation services, or location APIs; IP-based geo-restriction is performed at the network edge and produces only coarse jurisdiction signals);
- contacts, calendar, microphone, camera, or photo-library data;
- browsing history outside the Services, websites visited, or content of pages you view;

- health data, racial, religious, political, sexual-orientation, trade-union, or any other special-category data within the meaning of GDPR Art. 9;
- advertising identifiers, advertising cookies, behavioural-tracking pixels, cross-site tracking technologies, or fingerprinting technologies;
- credit-card, debit-card, or other payment-instrument data (the Services do not accept fiat or off-chain payments).

The Company does not intentionally collect data from children (see Section 11).

4.5 Data accuracy and User responsibility

To the extent you voluntarily provide information to the Company, you are responsible for ensuring that such information is accurate and appropriate. The Company does not independently verify User-provided information and does not rely on User-provided information for automated decision-making, scoring, or profiling.

---

5. Purposes and Legal Bases for Processing

The Company processes limited categories of information only where such processing is necessary, proportionate, and directly related to the operation, security, and integrity of the off-chain components of the Services, or to respond to User-initiated communications. The Company does not process information for purposes unrelated to the functioning of the Services, does not engage in surveillance or commercial data exploitation, and does not process information in a manner inconsistent with the non-custodial, decentralised design of the Veilo Protocol.

5.1 Permitted purposes and lawful bases

Processing	Lawful basis (GDPR Art. 6)
Operating the off-chain Services: account creation, authentication, multi-device sync, balance display, Reference Relayer transaction submission, push notifications you have opted into	**Contract** (Art. 6(1)(b)) — necessary to perform the agreement with you
Operation, maintenance, performance, and security of the Site, Web App, Extension, Mobile App, Reference Relayer, SDK, and Docs	**Legitimate interests** (Art. 6(1)(f)) — necessary for our security and the integrity of the Services
Security, abuse prevention, sanctions screening, geo-restriction enforcement, refusal of service to Restricted Persons, integrity protections	**Legitimate interests** (Art. 6(1)(f)) and **legal obligation** (Art. 6(1)(c))
Compliance with sanctions, AML, court orders, lawful regulatory requests	**Legal obligation** (Art. 6(1)(c))
Push notifications	**Consent** (Art. 6(1)(a)) — you control via OS permission
Crash reporting (Sentry)	**Legitimate interests** (Art. 6(1)(f)) with opt-out — debugging the application; you may disable in settings

5.2 No secondary or incompatible use

Information processed by the Company is **not** used for secondary purposes that are incompatible with the purposes described above. In particular, the Company does not process information for:

- marketing, advertising, or promotional activities;
- behavioural analysis or User profiling;
- targeted communications or segmentation;
- automated decision-making producing legal or similarly significant effects;
- training machine-learning models incorporating personal data; or
- sale, rental, licensing, or monetisation of information.

5.3 Purpose limitation and proportionality

The Company applies strict purpose-limitation and proportionality principles and ensures that only the minimum amount of information necessary is processed for each permitted purpose. Information is not retained or repurposed beyond what is reasonably required to achieve the specific purpose for which it was processed, and processing activities are periodically reviewed to ensure continued alignment with the non-custodial, privacy-preserving design of the Services.

---

6. How We Use Your Data

The Company uses data only to:

- provide the Services (account creation, authentication, multi-device sync, transaction processing through the Reference Relayer, balance display, notifications);
- maintain the security, integrity, availability, and performance of the off-chain components of the Services;
- diagnose problems, improve reliability, and develop new features;
- enforce these Terms, the Acceptable Use Policy, and applicable law (including Restricted-Person screening, sanctions screening, and refusal of service to U.S. persons);
- comply with legal and regulatory obligations applicable to the Company; and
- communicate operational updates such as critical security advisories.

The Company does **not** use your data to:

- sell, rent, or share with data brokers;
- serve advertising or perform marketing profiling;
- train machine-learning models that include your personal data;
- build behavioural profiles for any purpose other than legitimate fraud, abuse, or sanctions screening; or
- monitor User behaviour for compliance surveillance, behavioural analysis, or commercial exploitation.

---

7. Disclosure to Third Parties

7.1 No sale or commercial disclosure

The Company does **not** sell, rent, license, trade, monetise, or otherwise commercially disclose information processed in connection with the Services. Information is disclosed to third parties only where such disclosure is strictly necessary to operate and secure the off-chain components of the Services, respond to User-initiated requests, or protect the integrity and legitimate interests of the Company, and only to the minimum extent required for the relevant purpose.

7.2 Sub-processors (data processors acting on our behalf)

The Company engages carefully selected service providers that support operation of the off-chain components. All sub-processors are engaged under contractual arrangements that require them to:

- process information solely on the Company's instructions and only for the specified purpose;
- maintain appropriate confidentiality and security safeguards;
- refrain from using information for independent or commercial purposes; and
- delete or return information once the relevant services are complete, where feasible.

Disclosure to sub-processors does **not** include access to private keys, recovery phrases, plaintext Notes, viewing keys, master viewing keys, decryption keys, cryptographic secrets, decrypted balances, transaction contents in plaintext, or Protocol-level state.

Sub-processor	Role	Data shared	Region
MongoDB Atlas (`mongodb.com`)	Database hosting for the Reference Relayer	All Section 4.2 data (encrypted material remains encrypted)	`[us-east-1 / EU region — confirm]`
Helius Labs Inc.	Solana RPC provider	Wallet address (when querying balances), publicly broadcast transaction data	United States
Functional Software, Inc. d/b/a **Sentry**	Mobile App crash reporting	Stack traces, device model, OS version, app version (no wallet address or PII)	United States
Expo, Inc.	Mobile App push notifications	Push token (opaque), wallet address (for routing)	United States
Apple Inc.	iOS distribution and push notifications (APNs)	Device push token, basic device telemetry per Apple policy	United States
Google LLC	Android distribution and push notifications (FCM); Chrome Web Store distribution	Device push token, basic device telemetry per Google policy	United States
Vercel, Inc.	Hosting for `veilo.network`, `docs.veilo.network`, dApp	IP, user-agent, request logs (HTTP-server level)	Global edge
Cloudflare, Inc.	DNS, CDN, DDoS protection, geo-restriction enforcement	IP, user-agent, request logs	Global edge

7.3 Public Blockchain data

When a transaction is submitted to the Solana network (whether self-signed and self-broadcast, signed and broadcast through the Reference Relayer, or signed and broadcast through any independent Relayer), the transaction is broadcast to a globally public, immutable ledger. **Once broadcast, on-chain data is permanently visible to anyone.** This is a fundamental property of public Blockchains, not

something the Company controls. The Privacy Pool is designed to minimise the on-chain link between sender and recipient, but does not eliminate all metadata, and the Company has no technical ability to modify, delete, or restrict access to on-chain data.

7.4 Independent third parties (Relayers, RPC providers, validators, wallets, etc.)

The Veilo Protocol relies on independent third parties, including Blockchain validators, independent Relayer operators (beyond the Reference Relayer), RPC providers, MPC node operators (if and when adopted), wallet providers, indexers, decentralized exchanges, and other network participants. **These parties operate autonomously, are not controlled or directed by the Company, and independently determine the purposes and means of any information processing they perform.** The Company does not act as a joint controller, processor, agent, or intermediary with respect to such parties and does not assume responsibility for their data-handling practices. Users interact with such third parties at their own discretion and are responsible for reviewing the privacy practices of each such third party.

When you swap tokens, the swap request and parameters are sent to **Jupiter**, **Raydium**, or another DEX program for routing and execution. When the Service displays prices or charts, requests are made to **CoinGecko**, **DexScreener**, and **GeckoTerminal**. Those price/data requests include only the token identifier whose price is being displayed and do not include your wallet address.

7.5 Disclosure for security, abuse prevention, and platform integrity

The Company may disclose limited information where reasonably necessary to investigate, prevent, or respond to security incidents, abuse, misuse of the Services, sanctions exposure, or violations of these Terms or the AUP. Such disclosures are limited to off-chain information within the Company's possession or control and do not involve monitoring or disclosure of on-chain activity, transaction contents, or cryptographic material that the Company does not have.

7.6 Disclosure required by law

The Company may disclose data in response to:

- a binding subpoena, court order, search warrant, or other legally enforceable request from a competent authority with jurisdiction over the Company;
- a Mutual Legal Assistance Treaty (MLAT) request routed through proper channels;
- a sanctions or regulatory order from an authority with jurisdiction; or
- an emergency disclosure request where there is an imminent risk of death or serious bodily harm.

Where lawful, the Company will:

- notify the affected User before responding so they may seek to challenge the request;
- limit disclosure to the minimum required by the request; and

- publish an aggregate transparency report `[ANNUALLY — to be confirmed]`.

The Company does **not** voluntarily share User data with law enforcement or governments absent a legally valid request, except where there is an imminent threat to life or safety.

7.7 Limitations on what the Company can disclose

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

- recovery phrases, private keys, passwords;
- plaintext Note contents, viewing keys, master viewing keys, or decryption keys;
- data that exists only on your device; or
- on-chain assets in the Privacy Pool — the deployed Smart Contract has no admin function for the Company or anyone else to freeze, blacklist, or seize.

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); and
- information from sub-processors listed in Section 7.2 to the extent the Company controls it.

7.8 Corporate transactions

In the event of a merger, acquisition, restructuring, financing, insolvency, or similar corporate transaction, limited information may be disclosed to professional advisers, counterparties, or potential acquirers solely to the extent reasonably necessary to evaluate or complete the transaction. Any such disclosure is subject to appropriate confidentiality obligations and does not expand the purposes for which information is processed.

7.9 No public disclosure by the Company

The Company does not publicly disclose information processed in connection with the Services, including through public reports, transparency dashboards, or analytics outputs. Any information visible on public Blockchains exists independently of the Company's actions and is not disclosed, published, or controlled by the Company.

---

8. International Data Transfers

The Company is established in the United States. If you use the Services from outside the United States, your information may be transferred to and processed in the United States and other jurisdictions where the Company's sub-processors operate.

For Users in the United Kingdom, Switzerland, or another jurisdiction with cross-border-transfer restrictions, where data is transferred to a country not deemed adequate by the relevant authority, the Company relies on:

- the **Standard Contractual Clauses** (2021/914) approved by the European Commission, with relevant supplementary measures (for EEA transfers, where applicable);
- the **UK Addendum to the SCCs** for UK transfers;
- `[Data Privacy Framework / Swiss–U.S. Data Privacy Framework – confirm if certified]`.

Decentralised infrastructure participants (validators, independent Relayer operators, MPC node operators, RPC providers, wallet providers) operate independently and may process information in jurisdictions of their choosing. The Company does not control the location, governance, or data-handling practices of such participants and does not act as an intermediary or joint operator in respect of their activities.

> **Note:** As stated in the Acceptable Use Policy, the Services are **not offered to U.S. persons**. Accordingly, data transfers to or processing of U.S. persons should not occur in the ordinary course; the United States location of certain sub-processors reflects the location of infrastructure rather than the location of Users.

---

9. Data Retention and Storage Limitation

9.1 Principles

The Company adheres to strict data-minimisation and storage-limitation principles. Information is retained only for as long as is reasonably necessary to fulfil the specific, explicit, and legitimate purposes for which it is processed, as described in this Policy. The Company does not retain information on a continuous, indefinite, or speculative basis, and does not retain information for profiling, behavioural analysis, surveillance, or any purpose inconsistent with the non-custodial, decentralised, permissionless nature of the Protocol.

9.2 Retention periods

Retention periods are determined on a category-specific basis and are proportionate to the purpose for which the information is processed. See the retention column in Section 4 for specific periods. Where feasible, information is anonymised or aggregated prior to extended retention.

For the avoidance of doubt, the Company does **not** retain: private keys, recovery phrases, plaintext Note contents, viewing keys, master viewing keys, decryption keys, cryptographic secrets, decrypted balances, plaintext transaction contents, Protocol-level state, or persistent identifiers intended to track or correlate User activity over time.

9.3 On-chain and decentralised data

Blockchain data (transaction records, commitments, nullifiers, Merkle tree updates, encrypted balances, and other Protocol-level state) is recorded on the public Solana Blockchain System outside the Company's control. Such data is not stored by the Company in off-chain databases as authoritative state, cannot be modified, deleted, or selectively retained by the Company, and is governed exclusively by the rules of the underlying Blockchain network. Accordingly, on-chain data does not constitute Company-retained information for the purposes of this Policy.

9.4 Account deletion

When you delete your account:

- Your username, encrypted Veilo keys, encrypted Note backups, and authentication records are deleted from active systems within **30 days**;
- Backups containing your data are overwritten or anonymised within **180 days** of deletion (this is a function of the Company's backup retention cycle);
- Pseudonymous transaction statistics that contain no identifier linkable to you are not deleted because they are not personal data after the linking identifiers are removed;
- On-chain data **cannot be deleted** because it resides on a public Blockchain the Company does not control.

9.5 Deletion and anonymisation

The Company implements procedures designed to ensure that information is deleted without undue delay once it is no longer necessary for the purposes for which it was processed, or irreversibly anonymised so that it can no longer be associated with an identifiable individual. Deletion may occur automatically through system processes or manually following periodic review.

9.6 No custodial, monitoring, or recordkeeping obligations

Nothing in this Section shall be interpreted as creating any obligation on the Company to monitor User activity, retain transaction-level data, act as a recordkeeper, or assume custodial, fiduciary, or surveillance responsibilities in respect of User assets or Protocol interactions.

---

10. Data Security and Safeguards

10.1 Security-by-design and proportionality

The Company implements security measures designed to protect information processed in connection with the off-chain components of the Services against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. Such measures are implemented on a proportionate basis, taking into account the limited nature of the information processed by the Company, the decentralised and non-custodial architecture of the Veilo Protocol, the role of the Company as an interface and tooling provider, and the technical feasibility of safeguards. The Company does not maintain centralized repositories of Protocol transaction data, decrypted cryptographic material, or User identity records.

10.2 Technical and organisational measures

Technical safeguards include, where appropriate: industry-standard encryption (AES-256-GCM, NaCl box, TLS 1.3) for data in transit and at rest; PBKDF2 with high iteration counts for password-derived keys; secure hosting and infrastructure environments; access controls, authentication mechanisms, and role-based permissions; system hardening, patch management, and environment segregation; logging and monitoring for security and integrity purposes; and reasonable measures to prevent unauthorised access or misuse of systems.

Organisational safeguards include internal access restrictions, confidentiality obligations for personnel and contractors, and internal procedures governing handling of information. Access to information is limited to authorised individuals on a need-to-know basis.

The Company has commissioned independent security audits of critical components: `relayer-server` (January 2026, 12 findings addressed); `privacy-program` on-chain (March 2026, 1 medium-severity finding); `zk-circuits` `[audit status — confirm]`.

10.3 Cryptographic security boundary

The Company does not have access to private keys, recovery phrases, viewing keys, encryption keys, or decrypted Protocol data and **therefore cannot secure, recover, or restore such information**.

The security of on-chain transactions, encrypted balances, and Protocol-level state depends in part on factors outside the Company's control, including the security of User-managed wallets, private keys, devices, and third-party infrastructure (Solana validators, independent Relayer operators, RPC providers, wallet providers). The Company does not control and cannot guarantee the security, availability, or correctness of decentralised networks or third-party systems.

10.4 No absolute security guarantee

No system is completely secure. The Company does not warrant or guarantee that information, cryptographic mechanisms, decentralised infrastructure, or third-party services will be immune from unauthorised access, compromise, failure, or attack. Users acknowledge and accept that residual risks are inherent in the use of decentralised and cryptographic systems.

10.5 User security responsibilities

Users are solely responsible for safeguarding their private keys, recovery phrases, viewing keys, master viewing keys, decryption keys, credentials, devices, wallet software, and any other tools used to access the Services. The Company cannot recover lost credentials, restore access, or reverse transactions resulting from User error, compromise, loss of keys, or misuse of third-party services.

10.6 Incident response

The Company maintains internal procedures designed to identify, assess, and respond to security incidents affecting information processed in connection with the off-chain components of the Services. Where a personal-data breach affects the rights and freedoms of data subjects, the Company will notify affected Users and the relevant supervisory authority within the timeframes required by applicable law (e.g., GDPR Art. 33 — 72 hours where applicable).

10.7 No monitoring or surveillance obligation

Nothing in this Section shall be construed as imposing any obligation on the Company to monitor User activity, conduct proactive surveillance, analyse Protocol transactions, or assume custodial, fiduciary, compliance, or enforcement responsibilities.

---

11. Your Privacy Rights

11.1 Scope of rights

To the extent the Company processes limited categories of information in connection with the off-chain components of the Services, Users may exercise reasonable rights of access, correction, deletion, restriction, objection, and portability, subject to the technical and operational constraints described in this Policy and to applicable law. For the avoidance of doubt, this Section applies only to information processed by the Company in its capacity as an operator of off-chain interfaces and resources. It does **not** apply to:

- data recorded on public or permissionless Blockchain networks;
- cryptographic commitments, encrypted balances, nullifiers, Merkle tree data, or Protocol-level state;
- information processed exclusively within User-controlled wallets or devices; or
- information processed independently by third parties outside the Company's control (independent Relayers, RPC providers, validators, MPC node operators, wallet providers, indexers, etc.).

Nothing in this Section requires the Company to collect additional information, re-identify Users, or compromise the privacy-preserving design of the Veilo Protocol in order to respond to a request.

11.2 Rights

Subject to applicable law and verification of your identity:

Right	What it means	How to exercise
Access	Confirmation of whether the Company processes information relating to you, and receipt of a copy where applicable	Email `manager@veilo.network`
Rectification	Correction of inaccurate or incomplete information held by the Company	Email `manager@veilo.network` or update via Service
Erasure (“right to be forgotten”)	Deletion of information held by the Company	In-app delete-account feature, or email `manager@veilo.network`
Restriction	Limit how the Company processes information	Email `manager@veilo.network`
Objection	Object to processing based on legitimate interests	Email `manager@veilo.network`
Portability	Receive structured, machine-readable copy of information held by the Company	Email `manager@veilo.network`
Withdraw consent	For processing based on consent	Toggle in app settings (notifications, crash reporting)
Lodge a complaint	With your local data-protection authority	See Section 14

The Company will respond to verifiable requests within **30 days** (extendable to 90 days for complex requests, with prior notice).

11.3 LGPD and other regimes

Brazilian residents (LGPD): you have analogous rights and may contact our `[Brazilian representative — confirm]` at the address in Section 14.

> **Note on U.S. state privacy laws.** Under the Acceptable Use Policy, U.S. persons (including residents of California, Colorado, Connecticut, Utah, Virginia, Texas, and other U.S. states with comprehensive privacy laws) are **not eligible** to use the Services. Accordingly, neither the CCPA/CPRA nor analogous state privacy laws should apply to the Services in the ordinary course. If you nevertheless believe you have rights under such laws, contact `manager@veilo.network` and the Company will respond on the merits.

11.4 Verification and limitations

To protect security and integrity, the Company may request reasonable information to verify the request and may decline requests that are manifestly unfounded, excessive, technically infeasible, or incompatible with the decentralised, non-custodial design of the Services. The Company cannot:

- recover data the Company does not have (recovery phrases, private keys, plaintext Note contents, viewing keys, decryption keys);
- delete, modify, or restrict access to data on the Solana Blockchain;
- modify data held by independent third parties under their own controllership.

---

12. Children's Data

The Services are **not intended for children under 18**. The Company does not knowingly collect or process information relating to individuals below the age at which they may lawfully provide information without parental consent.

The Company does not implement age-verification mechanisms or identity checks, as the Services operate on a permissionless, non-custodial, and pseudonymous basis. Compliance with age-related requirements remains the responsibility of Users.

If the Company becomes aware that it has inadvertently processed information relating to a child, it will take reasonable steps to delete such information where technically feasible and appropriate.

---

13. Cookies, Local Storage, and Similar Technologies

13.1 Strictly necessary use

The Site, the Docs, the Web App, and the Extension may use cookies, `localStorage` / `chrome.storage` (Extension and Web App), and `AsyncStorage` / platform-secure storage (Keychain on iOS; Keystore on Android, for the Mobile App) to support core functionality, security, and basic performance of the off-chain components of the Services. The Company limits its use of cookies and similar technologies to:

- **Strictly necessary cookies / storage**, required for operation, security, and core functionality of the Site and interfaces;
- **Performance and error-monitoring technologies**, used solely to detect technical issues, diagnose errors, and maintain operational stability.

13.2 What we do not use

The Company does **not** deploy:

- advertising cookies;
- behavioural-tracking pixels;
- cross-site tracking technologies;
- fingerprinting;
- third-party analytics that profile Users; or
- marketing cookies.

The Company does not permit third-party advertising networks, data brokers, or marketing-analytics providers to place cookies or similar tracking technologies via the Site.

13.3 Information derived from cookies is not linked to Protocol activity

Information derived from cookies or similar technologies is **not** linked, correlated, or associated with:

- wallet addresses or wallet-connection metadata;
- Blockchain transactions or Protocol activity;
- cryptographic commitments, balances, or proofs; or
- any on-chain or Protocol-level state.

Users may configure their browser settings to refuse or limit cookies. Disabling strictly necessary cookies may affect the functionality, security, or availability of certain features.

`[A separate Cookie Policy will be linked here once finalised. Counsel: review whether ePrivacy Directive consent banner is required on EU traffic.]`

---

14. App Store Compliance

14.1 Apple App Store / TestFlight

The Company collects data linked to you only to the extent described in this Policy. The privacy “nutrition label” published in the App Store reflects the same disclosures.

14.2 Google Play

The Company adheres to the Google Play Data Safety section requirements, which mirror the disclosures in this Policy.

14.3 Chrome Web Store

The use of information received from Google APIs adheres to the Chrome Web Store User Data Policy, including the Limited Use requirements:

- the Company uses data only to provide and improve User-facing features;
- the Company does not transfer data for serving ads;
- the Company does not transfer data for credit-worthiness or lending purposes;
- the Company does not allow humans to read data, except (i) with the User’s affirmative consent, (ii) for security purposes, (iii) to comply with applicable law, or (iv) with data aggregated and used for internal operations.

---

15. SDK, Developer Tools, and Third-Party Implementations

15.1. The Veilo Protocol may be accessed or integrated through SDKs, reference implementations, or tooling made available by the Company. Third-party developers who integrate the Protocol or SDK into their own applications operate independently and are solely responsible for any information processing conducted within their applications or services.

15.2. The SDKs and reference implementations provided by the Company do not transmit personal information, telemetry, analytics, or usage data to the Company by default. The Company does not receive information regarding how third-party applications use the Protocol unless such transmission is explicitly implemented by the third-party developer.

15.3. The Company does not control, audit, or monitor third-party applications built using the Veilo Protocol or the SDK and does not act as an intermediary, controller, or processor with respect to information processed by such applications. Users interact with third-party applications at their own discretion and are responsible for reviewing the privacy practices and terms of such applications.

15.4. The decentralised and open nature of the Veilo Protocol permits independent implementations and integrations beyond the Company's control. The Company does not assume responsibility for the data-handling practices, security measures, or compliance obligations of independent developers or third-party services.

---

16. Wallet Connection Metadata and Abuse Prevention

16.1. **Wallet connection metadata.** When you connect a self-custodied Blockchain wallet to a Company-operated interface, the Company may incidentally process limited connection-related metadata strictly necessary to enable the connection and facilitate interface functionality (wallet software type, network selection, connection status, basic success/failure indicators). The Company does not collect, store, access, or process: private keys, recovery phrases, signing material; wallet addresses as persistent personal identifiers; transaction payloads, message contents, or execution parameters; balances, encrypted balances, commitments, nullifiers, or cryptographic proofs; or Protocol-level state or on-chain activity. Wallet connection metadata is processed on an ephemeral basis, is not retained as a persistent identifier, is not used to track Users across sessions or visits, is not correlated with Protocol activity, and is not used for profiling, behavioural analysis, analytics, or marketing.

16.2. **Abuse prevention and Service integrity.** The Company may implement proportionate technical measures at the Site, the Web App, the Extension, the Mobile App, or the Reference Relayer level to protect the Services from abuse, misuse, denial-of-service attacks, automated scraping, or other activities that could compromise availability, security, or User experience. Such measures are designed solely to protect the availability, stability, and security of the off-chain components and do not involve monitoring, analysing, or restricting Protocol-level transactions or on-chain activity. Abuse-prevention measures rely on limited technical indicators, do not involve persistent tracking of Users or devices, and are not used for profiling, behavioural analysis, surveillance, or compliance monitoring.

Any measures implemented under this Section affect only access to Company-operated interfaces and do not alter, restrict, or interfere with the autonomous operation of decentralised Smart Contracts or on-chain Protocol functionality.

---

17. Changes to This Policy

The Company may amend or update this Policy from time to time to reflect changes in Service functionality, technical architecture, operational practices, or organisational structure. Updates will be effective as of the date indicated at the top of the Policy. For material changes, the Company will notify Users via in-product banner and on the Site at least **30 days** before they take effect (where required by law). Continued use of the Services following an update constitutes acknowledgement of the revised Policy.

---

18. Contact

For privacy questions, requests, or complaints:

- **Email:** `manager@veilo.network`
- **Postal:** Veilo Layer LLC, c/o its registered agent in the State of Wyoming, `[REGISTERED AGENT ADDRESS, WYOMING]`, United States (Wyoming Secretary of State Entity ID 2026-001871701)
- **EU representative (Art. 27 GDPR):** `[name and address — confirm if EU users are served and Veilo has no EU establishment]`
- **UK representative (UK GDPR):** `[name and address — confirm]`
- **Brazilian representative (LGPD):** `[name and address — confirm]`

You may also lodge a complaint with your local data-protection authority. A non-exhaustive list:

- **EU/EEA:** supervisory authorities listing
- **United Kingdom:** Information Commissioner's Office (ICO) — `https://ico.org.uk`
- **Brazil:** Autoridade Nacional de Proteção de Dados (ANPD) — `https://www.gov.br/anpd`

The Company does not maintain User accounts or identity databases beyond what is described in this Policy. Accordingly, responses to requests may be limited by technical feasibility and privacy-preserving constraints. Nothing in this Policy shall be construed as a waiver of any rights or defences available to the Company, or as a representation that the Company processes information beyond what is expressly described herein.

Built with zero-knowledge proofs on Solana.