VAULTO, INC. PRIVACY POLICY

Effective Date: February 28, 2026

Last Updated: February 28, 2026

---

1. Introduction

This Privacy Policy describes how Vaulto, Inc., a Delaware corporation ("**Vaulto**," "**we**," "**us**," or "**our**"), collects, uses, discloses, and protects personal information in connection with our suite of web applications and application programming interface (collectively, the "**Services**"). The Services include Vaulto Search, Vaulto Swap, Vaulto Stake, Vaulto Ramp, and the Vaulto API platform.

We are committed to protecting your privacy and handling your personal information with transparency and care. This Privacy Policy applies to all users of the Services and should be read in conjunction with our Terms of Service.

Controller Information:

Vaulto, Inc.
10915 Strathmore Dr
Los Angeles, CA 90024
United States of America
Email: support@vaulto.ai

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy and consent to the collection, use, and disclosure of your personal information as described herein.

---

2. Scope and Applicability

This Privacy Policy applies to personal information collected through:

- Vaulto's websites and web applications, including Vaulto Search, Vaulto Swap, Vaulto Stake, and Vaulto Ramp.
- The Vaulto API platform and associated developer tools.
- Communications with Vaulto, including email correspondence and support requests.

This Privacy Policy does not apply to third-party websites, services, or applications that may be linked to or integrated with the Services, even if accessible through our platform. Users are encouraged to review the privacy policies of such third parties.

---

3. Information We Collect

We collect personal information to provide, secure, and improve the Services. The categories of information we collect depend on how you interact with the Services.

3.1 Information Collected from Web Application Users

For users accessing Vaulto Search, Vaulto Swap, Vaulto Stake, and Vaulto Ramp through wallet connection:

- **Wallet Addresses:** Cryptocurrency wallet addresses you connect to access the Services.
- **On-Chain Activity:** Publicly available blockchain transactions and interactions associated with your wallet address that are surfaced or processed through the Services.
- **Device and Usage Data:** IP addresses, browser type and version, operating system, device identifiers, pages visited, features accessed, timestamps, referral sources, and interaction events.
- **Cookies and Tracking Technologies:** Data collected through cookies, pixels, and similar technologies, including Google Analytics and Meta advertising pixels (see Section 4).

3.2 Information Collected from API Platform Users

For users accessing the Vaulto API platform:

- **Account Information:** Names and email addresses provided during registration or authentication via Google OAuth or other supported identity providers.
- **Linked Wallet Addresses:** Cryptocurrency wallet addresses voluntarily linked to your authenticated account to facilitate streamlined access and signing-based authentication.
- **API Usage Data:** Endpoint requests, request timestamps, response codes, error logs, rate limit status, and usage patterns.
- **Payment and Billing Information:** Transaction records related to API usage fees paid in USDC or other supported payment methods, and billing metadata for subscription services processed through PayPal (we do not store full payment card numbers).

3.3 Information We Do Not Collect

Vaulto does **not** collect:

- Know-your-customer (KYC) or identity verification data such as government-issued identification documents, dates of birth, social security numbers, or biometric information.
- Private keys, seed phrases, or wallet passwords.
- Sensitive personal information such as health data, precise geolocation data, or financial account numbers (other than wallet addresses and blockchain transaction data).

For users interacting with Vaulto Ramp, any KYC, identity verification, or fiat transaction processing is conducted exclusively by third-party payment providers such as Venmo. Vaulto does not receive, store, or process such information.

---

4. Cookies and Tracking Technologies

We use cookies, web beacons, pixels, and similar tracking technologies to enhance your experience, analyze usage patterns, and deliver relevant advertising.

4.1 Types of Cookies and Tracking Technologies

- **Essential Cookies:** Required for basic site functionality, including session management, wallet connection authentication, and security features.
- **Analytics Cookies:** Used to collect aggregated data on site usage, user behavior, page views, and feature interactions. We use Google Analytics to understand how users interact with the Services and to improve user experience.
- **Advertising Cookies and Pixels:** Used to deliver targeted advertising and measure advertising effectiveness. We use Meta (Facebook) advertising pixels to support retargeting campaigns and measure ad performance.

4.2 Managing Cookies and Tracking Preferences

You may manage or disable cookies through your browser settings. Most browsers allow you to refuse cookies or alert you when cookies are being sent. Please note that disabling essential cookies may impair certain functionality of the Services.

For more information on managing cookies:

- **Google Analytics Opt-Out:** https://tools.google.com/dlpage/gaoptout
- **Meta Advertising Preferences:** https://www.facebook.com/settings?tab=ads

Users in certain jurisdictions may have additional rights to manage tracking technologies. For information specific to your jurisdiction, see Section 11.

---

5. How We Use Your Information

We use the personal information we collect for the following purposes:

5.1 To Provide and Operate the Services

- Authenticate users through wallet connections and Google OAuth.
- Facilitate user interactions with decentralized protocols, data aggregation, and visualization features.
- Process API requests and deliver data outputs.
- Enable wallet linking to streamline future authentication.
- Monitor system performance and ensure service availability.

5.2 To Secure and Protect the Services

- Detect, prevent, and respond to fraud, abuse, security incidents, and violations of our Terms of Service.
- Enforce rate limits, usage restrictions, and acceptable use policies.
- Maintain logs and audit trails for security monitoring and incident response.

5.3 For Analytics and Product Improvement

- Analyze usage patterns, user behavior, and feature adoption to understand how the Services are used.
- Improve user experience, design, functionality, and performance.
- Conduct research and development to enhance existing features and develop new services.

5.4 For Marketing and Advertising

- Deliver targeted advertisements and retargeting campaigns through Meta advertising platforms.
- Measure the effectiveness of advertising campaigns and optimize marketing strategies.
- Communicate with users regarding new features, product updates, and promotional offers, subject to applicable opt-out rights.

5.5 For Billing and Payment Processing

- Process subscription payments for Vaulto Search premium tiers through PayPal.
- Manage API usage billing and process payments in USDC or other supported methods.
- Maintain billing records, invoices, and transaction histories for accounting and dispute resolution purposes.

5.6 For Legal Compliance and Risk Management

- Comply with applicable laws, regulations, legal processes, and governmental requests.
- Enforce our Terms of Service and other agreements.
- Respond to subpoenas, court orders, or other legal obligations.
- Protect the rights, property, and safety of Vaulto, our users, and the public.
- Maintain records for audit, dispute resolution, and regulatory reporting purposes.

---

6. How We Share Your Information

We do not sell or share personal information for cross-context behavioral advertising or other purposes prohibited by applicable privacy laws. We disclose personal information only in the limited circumstances described below.

6.1 Service Providers and Infrastructure Partners

We share personal information with third-party service providers that perform services on our behalf, including:

- **Hosting and Infrastructure:** Netlify (frontend hosting) and Railway (backend infrastructure) process data to deliver and operate the Services.
- **Analytics:** Google Analytics processes usage data to provide aggregated insights into user behavior and site performance.
- **Advertising:** Meta (Facebook) processes data related to advertising pixels to deliver and measure targeted advertising campaigns.

- **Payment Processing:** PayPal processes payment information for Vaulto Search subscriptions. Payment processors handle billing data in accordance with their own privacy policies and industry-standard security practices.

These service providers are contractually obligated to use personal information only as necessary to provide their services and to protect the information in accordance with industry standards.

6.2 Data Sources and Protocol Integrations

The Services integrate with and retrieve data from third-party sources and decentralized protocols, including:

- Blockchain indexing services and subgraphs (e.g., Uniswap subgraphs, The Graph protocol).
- Financial and market data providers (e.g., Alpha Vantage).
- Decentralized exchange aggregators and liquidity protocols (e.g., Li.Fi, Uniswap).

In most cases, these integrations involve Vaulto retrieving publicly available data or data that does not identify individual users. Where personal information is shared with such providers, it is limited to what is necessary to deliver the requested functionality.

6.3 Third-Party Payment Services (Vaulto Ramp)

Vaulto Ramp provides a guided interface that references third-party payment services such as Venmo for fiat on-ramping and off-ramping. Vaulto does not perform money transmission, custody fiat funds, or conduct KYC verification. All transactions, identity verification, compliance obligations, and data processing related to fiat transfers are handled exclusively by the third-party payment provider. Users must review and comply with the terms and privacy policies of such providers.

6.4 Legal and Regulatory Obligations

We may disclose personal information when required or permitted by law, including:

- In response to subpoenas, court orders, legal processes, or governmental requests.
- To comply with applicable laws, regulations, or legal obligations.
- To enforce our Terms of Service or other agreements.
- To protect the rights, property, safety, or security of Vaulto, our users, or the public.
- In connection with investigations of fraud, security incidents, or violations of law.

6.5 Business Transfers

In the event of a merger, acquisition, reorganization, sale of assets, or bankruptcy, personal information may be transferred to a successor entity. Users will be notified via email or prominent notice on our website of any such change in ownership or control of personal information.

6.6 With Your Consent

We may share personal information for other purposes with your explicit consent or at your direction.

---

7. Data Retention

We retain personal information only for as long as reasonably necessary to fulfill the purposes for which it was collected, comply with legal and regulatory obligations, resolve disputes, and enforce our agreements.

7.1 General Retention Periods

- **Usage and Analytics Data:** Retained for up to twenty-four (24) months or as necessary for analytics and product improvement purposes, after which it is aggregated or anonymized.
- **API and System Logs:** Retained for up to twelve (12) months for security monitoring, troubleshooting, and abuse prevention.
- **Billing and Transaction Records:** Retained for up to seven (7) years to comply with accounting, tax, and financial reporting obligations.

- **Account and Authentication Data:** Retained for as long as your account remains active or as necessary to provide the Services, and for a reasonable period thereafter to address support requests, disputes, or legal obligations.

7.2 Deletion and Anonymization

Upon expiration of the applicable retention period, personal information is securely deleted or anonymized such that it can no longer be associated with an identifiable individual. Certain information may be retained in anonymized or aggregated form indefinitely for research, analytics, and product development purposes.

7.3 Legal and Security Retention

Notwithstanding the above, we may retain personal information for longer periods where required or permitted by law, including for litigation, regulatory investigations, fraud prevention, and security purposes.

---

8. Data Security

We implement reasonable technical, administrative, and organizational measures designed to protect personal information from unauthorized access, disclosure, alteration, and destruction.

8.1 Security Measures

Our security practices include:

- **Encryption in Transit:** All data transmitted between users and the Services is encrypted using industry-standard Transport Layer Security (TLS) protocols.
- **Encryption at Rest:** Sensitive data stored in our systems is encrypted using industry-standard encryption algorithms.
- **Access Controls:** Access to personal information is restricted to authorized personnel on a need-to-know basis and subject to authentication and authorization controls.
- **Logging and Monitoring:** We maintain logs of system access and activity and employ monitoring tools to detect and respond

to security incidents.
- **Regular Backups:** Data is backed up regularly to protect against data loss and to support disaster recovery.

8.2 Limitations of Security

No method of transmission over the internet or electronic storage is completely secure. While we strive to protect personal information using industry-standard practices, we cannot guarantee absolute security. Users acknowledge and accept the inherent risks of transmitting information over the internet and interacting with blockchain networks and decentralized protocols.

8.3 User Responsibility

Users are responsible for safeguarding their wallet private keys, seed phrases, authentication credentials, and devices used to access the Services. Vaulto is not liable for unauthorized access resulting from user compromise of credentials or failure to follow security best practices.

8.4 Incident Response

In the event of a data breach or security incident that compromises personal information, we will notify affected users and relevant authorities in accordance with applicable law and will take reasonable steps to mitigate harm.

---

9. International Data Transfers

Vaulto is based in the United States, and the Services are primarily directed at users located in the United States. Personal information collected through the Services may be processed, stored, and transferred to servers and facilities located in the United States and other countries where Vaulto and its service providers operate.

9.1 Cross-Border Transfers

By using the Services, you acknowledge and consent to the transfer of your personal information to jurisdictions that may have data protection laws different from those in your country of residence. We take reasonable measures to ensure that personal information transferred internationally is protected in accordance with this Privacy Policy and applicable law.

9.2 Use from Outside the United States

If you access the Services from outside the United States, you do so at your own risk and are responsible for compliance with local laws and regulations, including data protection and privacy laws. Vaulto does not represent or warrant that the Services comply with the laws of any jurisdiction outside the United States.

9.3 Additional Protections for International Transfers

Where required by law, we implement appropriate safeguards for international data transfers, such as standard contractual clauses, adequacy decisions, or other legally recognized transfer mechanisms. Users in the European Economic Area (EEA), United Kingdom, or other jurisdictions with specific transfer requirements should contact us at support@vaulto.ai for more information.

---

10. Children's Privacy

The Services are not directed to individuals under the age of eighteen (18), and we do not knowingly collect personal information from children. If we become aware that we have inadvertently collected personal information from a child under the age of 18, we will take reasonable steps to delete such information promptly.

If you are a parent or guardian and believe that your child has provided personal information to Vaulto, please contact us at support@vaulto.ai, and we will work to remove such information.

---

11. Your Privacy Rights and Choices

Depending on your jurisdiction, you may have certain rights regarding your personal information. We are committed to facilitating the exercise of these rights to the extent required and permitted by applicable law.

11.1 General Rights

You may have the right to:

- **Access:** Request confirmation of whether we process your personal information and obtain a copy of such information.
- **Correction:** Request correction of inaccurate or incomplete personal information.
- **Deletion:** Request deletion of your personal information, subject to legal and operational limitations.
- **Restriction:** Request restriction of processing under certain circumstances.
- **Objection:** Object to certain processing activities, including processing for direct marketing purposes.

To exercise these rights, please contact us at support@vaulto.ai with a detailed description of your request. We will respond within a reasonable timeframe in accordance with applicable law.

11.2 Limitations on Rights

Certain rights may be limited or unavailable where:

- Retention is required by law or for legitimate legal, regulatory, security, or business purposes.
- Deletion would impair ongoing investigations, legal proceedings, or the enforcement of agreements.
- Information is necessary for the performance of a contract or the provision of services you have requested.
- Information has been anonymized or aggregated such that it can no longer identify you.

11.3 Rights for California Residents

If you are a California resident, you may have additional rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including:

- The right to know what categories of personal information we collect, use, and disclose.
- The right to request deletion of personal information, subject to exceptions.
- The right to correct inaccurate personal information.
- The right to opt out of the "sale" or "sharing" of personal information. **Note:** Vaulto does not sell or share personal information as those terms are defined under the CCPA/CPRA.
- The right to limit the use and disclosure of sensitive personal information (if applicable).
- The right to non-discrimination for exercising your privacy rights.

To submit a request, contact us at support@vaulto.ai. We may require verification of your identity before processing your request.

11.4 Rights for EEA and UK Residents

If you are located in the European Economic Area (EEA) or United Kingdom (UK), you may have additional rights under the General Data Protection Regulation (GDPR) or UK GDPR, including:

- The right to access, rectify, erase, or restrict processing of your personal information.
- The right to data portability (to receive your personal information in a structured, commonly used, machine-readable format).
- The right to object to processing based on legitimate interests or for direct marketing purposes.
- The right to withdraw consent where processing is based on consent.
- The right to lodge a complaint with your local data protection authority.

To exercise these rights, contact us at support@vaulto.ai. We will respond in accordance with applicable law. You also have the right to lodge a complaint with the relevant supervisory authority in your jurisdiction.

11.5 Marketing Communications

You may opt out of receiving promotional or marketing emails by following the unsubscribe instructions included in such emails or by contacting us at support@vaulto.ai. Please note that even if you opt out of marketing communications, we may still send you transactional or administrative messages related to your use of the Services.

---

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or operational needs. When we make material changes, we will notify users by:

- Posting the updated Privacy Policy on our website with a revised "Last Updated" date.
- Providing notice via email to API users with registered email addresses.
- Displaying a prominent notice on the Services.

Your continued use of the Services after the effective date of the updated Privacy Policy constitutes your acceptance of the changes. We encourage you to review this Privacy Policy periodically to stay informed about how we collect, use, and protect your information.

---

13. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

Vaulto, Inc.
Attention: Privacy
10915 Strathmore Dr

Los Angeles, CA 90024
United States of America

Email: support@vaulto.ai

We will respond to inquiries within a reasonable timeframe and in accordance with applicable law.

END OF PRIVACY POLICY