

UNVAULTED

Privacy Policy

Effective Date: February 3, 2026

Unvaulted Inc.
A Delaware Corporation

Table of Contents

1. Introduction
2. Data Controller
3. Information We Collect
4. Lawful Bases for Processing (EEA/UK Users)
5. How We Use Your Information
6. How We Share Your Information
7. Record Permanence and Data Retention
8. Your Rights and Choices
9. Rights for EEA and UK Residents (GDPR)
10. Rights for California Residents (CCPA/CPRA)
11. Rights Under Other State and National Laws
12. International Data Transfers
13. Cookies and Tracking Technologies
14. Data Security
15. Children's Privacy
16. Third-Party Links and Services
17. Changes to This Privacy Policy
18. Contact Information

1. Introduction

Unvaulted Inc. (“**Unvaulted**,” “**we**,” “**us**,” or “**our**”) is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use the Unvaulted platform, including the website at unvaulted.com, associated applications, tools, APIs, and all related services (the “**Service**”).

Unvaulted is a credibility infrastructure platform that enables cryptocurrency and blockchain project founders to build permanent, verifiable execution records. Because of the Platform’s core design around record permanence and public credibility signals, certain information you submit is intentionally made publicly available and is designed to be immutable. This Privacy Policy describes what information is public, what is private, what is permanent, and what choices you have.

By accessing or using the Service, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our practices described herein, please do not use the Service.

2. Data Controller

For the purposes of applicable data protection laws, including the EU General Data Protection Regulation (GDPR) and the UK GDPR, the data controller for your personal data is:

Unvaulted Inc.

A Delaware Corporation, United States

Email: privacy@unvaulted.com

If you are located in the European Economic Area (EEA) or the United Kingdom (UK), you may contact us regarding any data protection matters at privacy@unvaulted.com. We have not appointed a representative in the EEA or UK at this time. If required by law to do so, we will appoint one and update this Privacy Policy accordingly.

3. Information We Collect

We collect information in several categories, as described below.

3.1 Account and Identity Information

When you create an account, we collect: (a) your email address, used for authentication (magic link), account recovery, and communications; (b) the display name, username, and optional one-liner description you create on Unvaulted; and (c) your profile photo, if provided. In the future, we may offer additional identity verification methods, such as social media account linking or blockchain wallet verification. If and when such methods are introduced, we will update this Privacy Policy to describe the specific data collected through those methods before collecting any such data.

3.2 Profile and Project Information

When you create your profile and list projects, we collect: (a) your founder profile information; (b) project details, including project name, description, category, links, team members, partnership information, and lifecycle status; (c) token information you provide, including ticker symbols, contract addresses, and chain identifiers; and (d) your intent selection (builder, researcher, or other roles).

3.3 Execution Record Data

As you use the Platform, we collect all content you create as part of your execution record, including: (a) updates across all update types (Ship, Traction, Learning, Commitment, Setback, Decision, Team, and Partnership), including content, timestamps, and associated projects; (b) commitment declarations, including deliverable descriptions, target completion dates, proof methods, and additional context; (c) commitment lifecycle events, including creation, progress, timeline disclosures (including timing relative to target dates), completion evidence, and withdrawal documentation; (d) articles and insights you publish; (e) project lifecycle transitions and required documentation; (f) team composition changes and partnership records; and (g) outcome documentation for projects that are paused, pivoted, failed, or otherwise cease active development.

3.4 Verification and Credibility Data

We collect and generate data related to your verification and credibility, including: (a) your verification tier status and the data used to determine tier eligibility; (b) credibility scores calculated from your execution behavior; (c) recognition facet assignments; (d) commitment delivery statistics and outcome classifications; and (e) content quality and clarity assessments.

3.5 Usage and Analytics Data

We automatically collect information about your use of the Service, including: (a) pages viewed, features used, and actions taken; (b) session duration, visit frequency, and navigation patterns; (c) referral sources and exit pages; (d) content interactions, including bookmarks, follows, and return visits; (e) search queries; and (f) feature engagement patterns.

3.6 Device and Technical Data

We automatically collect: (a) IP address; (b) device type, operating system, and browser type and version; (c) screen resolution and device identifiers; (d) time zone and language preferences; and (e) network information.

3.7 Communication Data

We collect information from your communications with us, including support requests, feedback, survey responses, beta testing communications, and email correspondence.

4. Lawful Bases for Processing (EEA/UK Users)

If you are located in the European Economic Area or the United Kingdom, we process your personal data only when we have a valid lawful basis. The table below sets out the lawful bases we rely on for each category of processing.

Processing Activity	Lawful Basis	Details
Account creation and authentication	Contract	Necessary to perform our contract with you (the Terms of Service)
Displaying your public profile and Execution Records	Contract / Legitimate Interest	Necessary to perform our contract; also our legitimate interest in operating the Platform's core function
Calculating verification tiers and credibility scores	Contract / Legitimate Interest	Necessary to provide the Service as described in the Terms; legitimate interest in maintaining Platform integrity
Content moderation and anti-gaming enforcement	Legitimate Interest	Our legitimate interest in maintaining signal quality and preventing abuse
Analytics and Platform improvement	Legitimate Interest	Our legitimate interest in understanding usage and improving the Service
Email communications (service-related)	Contract	Necessary to perform our contract and deliver essential service notifications
Aggregated data analysis and licensing	Legitimate Interest	Our legitimate interest in developing products and services; data is anonymized
Retention of anonymized Execution Records after account deletion	Legitimate Interest	Our legitimate interest in maintaining Platform integrity and the reliance interests of third parties (see Section 7)
Compliance with legal obligations	Legal Obligation	Necessary to comply with applicable law

Where we rely on legitimate interest as a lawful basis, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms. You may request information about these balancing tests by contacting us at privacy@unvaulted.com.

Where we rely on consent, you may withdraw consent at any time by contacting us. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

5. How We Use Your Information

5.1 Providing and Operating the Service

We use your information to: (a) create and maintain your account; (b) authenticate your identity; (c) display your founder profile, project pages, and execution records; (d) calculate and display your verification tier, credibility scores, and recognition facets; (e) generate commitment delivery statistics; (f) power the Builders Hub, including the Execution Stream, Index, and Insights Library; (g) generate embeddable badges and credentials; (h) enable content browsing, discovery, and filtering; and (i) provide notifications about activity relevant to your account.

5.2 Platform Integrity and Quality

We use your information to: (a) enforce our Terms of Service and anti-gaming provisions; (b) detect, investigate, and prevent fraudulent, unauthorized, or illegal activity; (c) assess content quality and determine eligibility for display and curation; (d) conduct anomaly detection and gaming pattern analysis; (e) maintain signal quality; and (f) perform editorial review and curation.

5.3 Analytics and Improvement

We use your information to: (a) understand how users interact with the Service; (b) identify trends and areas for improvement; (c) conduct research and analysis; (d) validate Platform assumptions; (e) develop new features; and (f) generate aggregated and anonymized insights.

5.4 Communications

We use your information to: (a) respond to support requests; (b) send service-related notices (account verification, security alerts, technical notices); (c) communicate about Platform updates and policy changes; and (d) facilitate beta testing communications.

5.5 Legal and Compliance

We use your information to: (a) comply with applicable laws, regulations, and legal processes; (b) respond to lawful government requests; (c) enforce our legal rights and resolve disputes; and (d) protect the rights, property, and safety of Unvaulted, our users, and the public.

6. How We Share Your Information

6.1 Publicly Available Information

The following information is publicly available by design and accessible to all Platform users and visitors: (a) your founder profile (display name, username, one-liner, profile photo); (b) your verification tier and recognition facets; (c) your project pages, including execution histories and team information; (d) your updates, commitments, commitment outcomes, and all other Execution Records; (e) your credibility score and commitment delivery statistics; (f) your articles and insights; (g) project lifecycle status and outcome documentation; and (h) embeddable badges and credentials. You acknowledge and consent to this information being publicly available as a core feature of the Platform.

6.2 Service Providers

We may share your information with third-party service providers who perform services on our behalf, including hosting and infrastructure providers, analytics providers, email delivery services, and customer support tools. These providers are contractually required to use your information only for providing services to us and to maintain appropriate security measures. Where required by applicable law (including the GDPR), we enter into data processing agreements with these providers.

6.3 Aggregated and Anonymized Data

We may share aggregated and anonymized data that does not identify you personally with third parties for any lawful purpose, including: (a) ecosystem analysis for investors, researchers, and funds; (b) platform and tool integrations through API services; (c) media and industry reporting; and (d) academic research.

6.4 Embeddable Credentials and API

When you use embeddable badges or when third parties access your data through authorized API endpoints, your publicly available Platform data (as described in Section 6.1) is transmitted to the requesting party, always reflecting your current status.

6.5 Legal Requirements

We may disclose your information if required by law or in good faith belief that disclosure is necessary to: (a) comply with a legal obligation or government request; (b) protect Unvaulted's rights or property; (c) prevent or investigate wrongdoing; (d) protect user safety or public safety; or (e) protect against legal liability.

6.6 Business Transfers

In the event of a merger, acquisition, reorganization, or sale of assets, your information may be transferred as part of that transaction. We will provide notice before your information becomes subject to a different privacy policy.

6.7 With Your Consent

We may share your information with third parties when you give us explicit consent.

6.8 No Sale of Personal Data

Unvaulted does not sell your personal data as defined under the CCPA or any other applicable privacy law. We do not share your personal data for cross-context behavioral advertising purposes.

7. Record Permanence and Data Retention

7.1 Execution Record Permanence

As described in our Terms of Service, Execution Records are designed to be permanent and immutable. **By using the Service, you expressly acknowledge and consent to the permanent retention of your Execution Records.** This includes all updates, commitments, commitment outcomes, project lifecycle transitions, team attributions, partnership records, and associated metadata.

7.2 How We Handle Account Deletion and Erasure Requests

When you delete your account or submit an erasure request, we will: (a) delete or anonymize your personally identifiable information (email address, profile photo, and any other directly identifying data) within ninety (90) days, subject to legal retention obligations; (b) replace identifiable information in Execution Records with non-identifiable placeholders (such as "Anonymized

Founder"), so the substance of the execution record remains but no longer identifies you; and (c) retain aggregated and anonymized data derived from your use of the Service indefinitely. After anonymization, the remaining data does not constitute personal data under the GDPR, UK GDPR, CCPA, or other applicable privacy law, and is therefore not subject to further erasure obligations.

7.3 Why Execution Records Are Retained After Anonymization

The retention of anonymized Execution Records serves the following interests: (a) Platform integrity: other users and third parties may have relied upon execution records for evaluation, due diligence, or decision-making, and removing these records would undermine the reliability of the Platform's historical data; (b) third-party reliance: investors, researchers, and ecosystem participants may have referenced or relied upon publicly available execution records, and retroactive removal would cause harm to these third parties; (c) contractual expectation: the permanent nature of Execution Records is a core feature of the Service, clearly communicated before you submitted any content, and forms part of the bargain under the Terms of Service; and (d) the anonymized records do not identify you and therefore do not pose ongoing privacy risks.

7.4 GDPR Right to Erasure: Specific Reconciliation

For users in the EEA and UK: Article 17 of the GDPR provides a right to erasure ("right to be forgotten"). We satisfy this right by deleting or anonymizing all personally identifiable information upon request. The anonymized Execution Records that remain are no longer personal data (as they cannot be used to identify you, directly or indirectly) and are therefore outside the scope of the erasure right. To the extent that any residual data could theoretically be re-identified, we rely on Article 17(3)(b) (compliance with a legal obligation or exercise/defense of legal claims), Article 17(3)(d) (archiving purposes in the public interest), and our legitimate interest in maintaining the integrity of a credibility infrastructure that third parties rely upon, as appropriate. If you disagree with this assessment, you may lodge a complaint with your local data protection authority.

7.5 Other Retention Periods

Account and personal information is retained for as long as your account is active. Usage and technical data is retained for the period necessary to fulfill the purposes described in this Privacy Policy, and may be retained in aggregated or anonymized form indefinitely. Communication data is retained for as long as necessary to resolve inquiries and for legitimate record-keeping purposes. We may retain any information as necessary to comply with legal obligations, resolve disputes, and enforce our agreements, even after you request deletion.

8. Your Rights and Choices

8.1 Account Information

You may update, correct, or modify certain account information through your Founder Terminal settings. You may also contact us at privacy@unvaulted.com for changes that cannot be made through the self-service interface.

8.2 Account Deletion

You may request deletion of your account by contacting privacy@unvaulted.com or through your account settings. We will process deletion requests within thirty (30) days. The effects of deletion are described in Section 7.2.

8.3 Data Access and Portability

You may request a copy of the personal information we hold about you by contacting privacy@unvaulted.com. We will provide this in a commonly used, machine-readable format within thirty (30) days. Since Execution Records are publicly available, you may also access your data directly from the Platform.

8.4 Communications Preferences

You may opt out of non-essential communications via unsubscribe links, notification settings, or by contacting us. You cannot opt out of essential service-related communications (security alerts, account verification, legal notices).

8.5 Scope of Deletion Rights

Your right to request deletion is subject to the Execution Record permanence provisions in Section 7. While we will delete or anonymize your personally identifiable information, the substance of Execution Records will be retained in anonymized form as described in Section 7.2.

9. Rights for EEA and UK Residents (GDPR)

If you are located in the European Economic Area or the United Kingdom, you have the following rights under the GDPR and UK GDPR:

Right	Description	How to Exercise
Access	Request a copy of your personal data	Email privacy@unvaulted.com
Rectification	Request correction of inaccurate data	Terminal settings or email privacy@unvaulted.com
Erasure	Request deletion of personal data (subject to Section 7)	Email privacy@unvaulted.com
Restriction	Request restriction of processing in certain circumstances	Email privacy@unvaulted.com
Portability	Receive personal data in machine-readable format	Email privacy@unvaulted.com
Objection	Object to processing based on legitimate interest	Email privacy@unvaulted.com
Withdraw Consent	Withdraw consent where processing is based on consent	Email privacy@unvaulted.com
Complaint	Lodge a complaint with a supervisory authority	Contact your local data protection authority

We will respond to rights requests within one (1) month of receiving a verified request. This period may be extended by two additional months for complex or numerous requests, in which case we will inform you of the extension and the reasons within the first month.

We will not charge a fee for processing your request unless it is manifestly unfounded or excessive. We may request additional information to verify your identity before processing your request.

If we decline a request, we will inform you of the reasons and your right to lodge a complaint with a supervisory authority.

10. Rights for California Residents (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act as amended by the California Privacy Rights Act:

(a) The right to know what personal information we collect, use, and disclose. (b) The right to request deletion of your personal information, subject to certain exceptions, including the Execution Record permanence provisions described in this Privacy Policy. (c) The right to opt out of the “sale” or “sharing” of personal information. We do not sell or share personal information as defined by the CCPA. (d) The right to correct inaccurate personal information. (e) The right to limit the use of sensitive personal information. (f) The right to non-discrimination for exercising your privacy rights.

To exercise your rights, contact us at privacy@unvaulted.com. We will verify your identity before processing your request. You may designate an authorized agent to make a request on your behalf.

Categories of personal information we collect are described in Section 3. We collect information for the business and commercial purposes described in Section 5. We share information with the categories of recipients described in Section 6.

11. Rights Under Other State and National Laws

Residents of Virginia, Colorado, Connecticut, Texas, Oregon, Montana, and other U.S. states with applicable consumer privacy laws, as well as residents of jurisdictions worldwide with applicable data protection legislation (including but not limited to Brazil's LGPD, Canada's PIPEDA, Australia's Privacy Act, Japan's APPI, and South Korea's PIPA), may have similar rights, including rights to access, delete, correct, and port personal information, and to opt out of certain data processing activities.

To exercise your rights under any applicable privacy or data protection law, contact us at privacy@unvaulted.com. We will respond in accordance with the timelines and requirements of the applicable law.

12. International Data Transfers

Unvaulted is based in the United States. Your information is processed and stored in the United States. If you access the Service from outside the United States, your information will be transferred to, processed in, and stored in the United States, where privacy and data protection laws may differ from your jurisdiction.

12.1 Transfer Mechanisms (EEA and UK Users)

For transfers of personal data from the EEA or UK to the United States, we rely on: (a) Standard Contractual Clauses (SCCs) as approved by the European Commission; (b) the UK International Data Transfer Agreement or UK Addendum to the EU SCCs, as applicable; (c) any adequacy decision issued by the European Commission or UK Secretary of State that covers transfers to the United States; and (d) your explicit consent to the transfer, as a supplementary mechanism where appropriate. We will implement appropriate supplementary measures to ensure an adequate level of protection for your personal data in accordance with applicable law.

12.2 Other International Users

If you are located in any other jurisdiction with data transfer restrictions, by using the Service you consent to the transfer of your information to the United States. We take reasonable steps to ensure your information is treated securely and in accordance with this Privacy Policy.

13. Cookies and Tracking Technologies

13.1 Types of Cookies We Use

Type	Purpose	Duration
Essential	Authentication, security, and basic functionality	Session to 1 year
Analytics	Understanding usage patterns, page views, feature engagement	Up to 2 years
Preference	Storing your display and notification preferences	Up to 1 year

We do not use advertising or targeting cookies. Unvaulted does not serve third-party advertisements and does not track users across external websites for advertising purposes.

13.2 Cookie Management

You can manage cookies through your browser settings. Blocking essential cookies may prevent you from using certain features. For EEA and UK users, we will obtain your consent before placing non-essential cookies, in accordance with applicable law.

13.3 Do Not Track

We currently do not respond to “Do Not Track” browser signals because no universally accepted standard exists. We will update this policy if a standard is adopted.

14. Data Security

We implement and maintain reasonable administrative, technical, and physical security measures to protect your information, including: (a) encryption of data in transit using TLS/SSL; (b) encryption of

sensitive data at rest; (c) access controls on a need-to-know basis; (d) regular security assessments and vulnerability testing; (e) secure authentication mechanisms; and (f) incident response procedures.

No method of transmission over the Internet or electronic storage is completely secure. We cannot guarantee absolute security. You are responsible for maintaining the security of your account credentials and any devices used to access the Service. In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the relevant supervisory authority and, where required, affected individuals in accordance with applicable law (including within 72 hours for GDPR-covered breaches).

15. Children's Privacy

The Service is not directed to children under 18. We do not knowingly collect personal information from children under 18 (or under 16 for EEA/UK users, where applicable). If we become aware that we have collected personal information from a child under the applicable age, we will delete such information promptly. If you believe we have collected information from a child, please contact privacy@unvaulted.com.

16. Third-Party Links and Services

The Service may contain links to third-party websites and services. We have no control over and are not responsible for the privacy policies or practices of third parties. This Privacy Policy applies only to the Service. We encourage you to review the privacy policies of any third-party services you visit.

The Service currently uses third-party services for: (a) hosting and infrastructure; (b) email delivery; and (c) analytics. In the future, we may introduce additional third-party integrations, such as social media OAuth or blockchain wallet verification. We will update this Privacy Policy before any new third-party integration collects your personal data.

17. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will provide notice by: (a) posting the updated Policy with a revised effective date; (b) sending notification through the Service or to your email address; or (c) other reasonable means. Material changes become effective thirty (30) days after notice. Your continued use of the Service after the effective date constitutes acceptance. Where consent is the lawful basis for processing, we will obtain fresh consent for material changes affecting that processing.

We encourage you to review this Privacy Policy periodically.

18. Contact Information

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

Unvaulted Inc.

Privacy Inquiries: privacy@unvaulted.com

General Support: support@unvaulted.com

Legal Inquiries: legal@unvaulted.com

Website: unvaulted.com

For EEA and UK residents, you also have the right to lodge a complaint with your local data protection supervisory authority.

For California residents, you may exercise your rights under the CCPA/CPRA by contacting privacy@unvaulted.com.

© 2026 Unvaulted Inc. All rights reserved.