Privacy Policy

Vaulto LP Platform
Effective Date: February 5, 2026
Last Updated: February 5, 2026

1. Introduction

1.1 Overview

Vaulto Inc. ("Vaulto," "we," "us," or "our") is committed to protecting the privacy and security of your personal information. This Privacy Policy describes how we collect, use, disclose, and safeguard information when you access or use our digital asset liquidity provision platform, website, services, and applications (collectively, the "Platform").

1.2 Scope

This Privacy Policy applies to all users of the Vaulto Platform, including visitors, registered users, and institutional clients. By accessing or using the Platform, you acknowledge that you have read, understood, and agree to the collection, use, and disclosure of your information as described in this Privacy Policy.

1.3 Acceptance

If you do not agree with the terms of this Privacy Policy, you must immediately discontinue use of the Platform. Continued use after changes to this Privacy Policy constitutes acceptance of those changes.

1.4 Regulatory Context

Vaulto operates in a highly regulated environment involving digital assets, securities tokenization, and financial services. We collect and process information necessary to comply with:

- Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations
- Know Your Customer (KYC) and Know Your Business (KYB) requirements
- Securities laws and regulations applicable to tokenized assets
- Data protection regulations including GDPR, CCPA, and other applicable privacy laws
- Financial services regulatory requirements in jurisdictions where we operate

2. Information We Collect

2.1 Information You Provide Directly

Account Registration Information:
When you create an account using Google OAuth authentication, we collect:

- Full legal name
- Email address
- Google account identifier
- Profile information from your Google account (if provided)

Identity Verification Information (KYC/KYB):
To comply with regulatory requirements, we collect comprehensive identification and verification information:

For Individual Users:

- Full legal name and any aliases
- Date of birth and place of birth
- Residential address and address history
- Government-issued identification documents (passport, driver's license, national ID card)
- Photographs or scans of identification documents
- Proof of address documentation (utility bills, bank statements, government correspondence dated within 90 days)
- Tax identification number (TIN), Social Security Number (SSN), or equivalent
- Nationality and citizenship status
- Occupation and employment information
- Source of funds and wealth information
- Expected transaction volumes and investment purposes
- Politically Exposed Person (PEP) status and associations
- Sanctions screening information

For Entity Users:

- Legal entity name and any "doing business as" (DBA) names
- Entity type (corporation, LLC, trust, partnership, etc.)
- Jurisdiction and date of incorporation or formation
- Registration numbers and tax identification numbers
- Principal place of business address
- Registered office address and mailing address
- Nature and industry of business operations
- Memorandum and Articles of Association or equivalent organizational documents
- Certificate of Incorporation, Formation, or Registration
- Entity proof of address documentation
- Ownership structure and Ultimate Beneficial Owners (UBOs) with 10% or greater ownership
- Information about control persons, directors, and officers
- Authorized signatories and representatives
- Entity financial information and source of funds
- Expected transaction volumes and business purposes
- Professional investor or accredited investor status documentation
- Tax self-certification forms (W-8, W-9, or equivalent)

- Sanctions screening and PEP declarations for entity and associated individuals

Financial Information:

- Bank account details for fiat funding (processed through third-party providers)
- Payment method information (processed through Ramp Network)
- Transaction history and payment records
- Wallet addresses for digital asset deposits and withdrawals
- Investment amounts and allocation preferences

Communication Information:

- Messages, inquiries, and correspondence with Vaulto support team
- Feedback, suggestions, and survey responses
- Recorded communications (phone, video, or chat) when you interact with our support services

2.2 Information Collected Automatically

Wallet and Transaction Information:

- Ethereum wallet addresses generated and assigned to your account
- Encrypted private keys stored securely on our servers
- Transaction hashes and blockchain records
- Wallet balances and asset holdings
- Liquidity position details (pool allocations, LP token balances, fee earnings)
- Hedging position information (options contracts, strikes, premiums, expirations)
- Deposit and withdrawal activity
- Smart contract interactions on blockchain networks

Platform Usage Information:

- IP addresses and geolocation data
- Device information (type, operating system, browser type and version, unique device identifiers)
- Access times, dates, and session duration
- Pages viewed, features accessed, and navigation patterns
- Referral sources and exit pages
- Performance metrics and error logs
- Click-stream data and interaction patterns

Technical and Security Information:

- Authentication logs and login history
- Security events and anomaly detection data
- Browser settings and preferences
- Cookies and similar tracking technologies data
- API usage and integration activity

2.3 Information from Third-Party Sources

Identity Verification Services:
We partner with third-party identity verification and compliance providers who may provide:

- Enhanced identity verification results
- Document authentication and validation
- Biometric verification data
- Fraud detection and risk assessment scores
- Sanctions screening and PEP database results
- Adverse media and watchlist screening results

Blockchain Data:
We collect publicly available information from blockchain networks including:

- Transaction history associated with your wallet addresses
- Token holdings and transfer records
- Smart contract interaction history
- Gas fees and network usage patterns
- DeFi protocol interaction data (Uniswap, Ondo Finance, etc.)

Third-Party Service Providers:
We receive information from integrated service providers:

Ramp Network (Fiat-to-Crypto On-Ramp):

- Transaction completion confirmations
- Funding amounts and payment method types
- KYC verification status from Ramp's independent verification process
- Transaction dispute or compliance flag information

Ondo Finance (Tokenized Securities):

- Account approval status and compliance review results
- Eligibility determinations and accreditation verification
- Transaction activity involving Ondo tokenized assets
- Regulatory compliance information

Alpaca Markets (Options Hedging):

- Options position data and execution confirmations
- Account status and trading permissions
- Risk metrics and margin requirements

Google OAuth:

- Authentication status and session information
- Email address and basic profile information
- Account security events

Analytics and Monitoring Services:

- Aggregated usage statistics and performance metrics

- Security incident reports and threat intelligence
- Customer support interaction summaries

2.4 Sensitive Information

We collect and process sensitive personal information including:

- Government identification numbers (SSN, TIN, passport numbers)
- Financial account information and transaction records
- Biometric data (if applicable for identity verification)
- Information revealing political opinions or affiliations (for PEP screening)
- Criminal records or legal proceedings (if required by compliance screening)

We collect sensitive information only when legally required or necessary for service provision and handle it with enhanced security measures.

3. How We Use Your Information

3.1 Service Provision and Account Management

We use your information to:

- Create, maintain, and secure your account
- Generate and manage custodial wallets on your behalf
- Authenticate your identity and prevent unauthorized access
- Process deposits, withdrawals, and transactions
- Execute liquidity provision strategies and manage LP positions
- Implement hedging strategies through options contracts
- Provide portfolio analytics, performance metrics, and reporting
- Facilitate access to third-party services (Ramp Network, Ondo Finance, Alpaca Markets)
- Communicate service updates, transaction confirmations, and account status
- Respond to your inquiries and provide customer support

3.2 Compliance and Legal Obligations

We use your information to:

- Verify your identity and conduct KYC/KYB due diligence
- Screen against sanctions lists and PEP databases
- Detect and prevent money laundering, terrorist financing, and fraud
- Comply with AML/CTF regulations and reporting requirements
- Fulfill securities law compliance obligations for tokenized assets
- Respond to lawful requests from regulatory authorities and law enforcement
- Maintain records required by financial services regulations
- Conduct ongoing compliance monitoring and periodic reviews
- Investigate suspicious activity and file Suspicious Activity Reports (SARs) when required
- Enforce our Terms of Service and policies

3.3 Risk Management and Security

We use your information to:

- Assess creditworthiness and investment suitability
- Monitor transactions for fraud, abuse, and prohibited activities
- Detect and prevent unauthorized access and cyber threats
- Analyze risk exposures and portfolio concentrations
- Implement security controls and access restrictions
- Conduct security audits and vulnerability assessments
- Investigate security incidents and data breaches
- Protect Platform integrity and user safety

3.4 Platform Improvement and Analytics

We use your information to:

- Analyze usage patterns and user behavior
- Optimize Platform performance and functionality
- Develop new features and services
- Conduct market research and user experience studies
- Test and evaluate service improvements
- Generate aggregated and anonymized analytics
- Benchmark performance against industry standards

3.5 Marketing and Communications (With Consent)

With your explicit consent where required by law, we may use your information to:

- Send promotional materials and service announcements
- Provide educational content about liquidity provision and DeFi strategies
- Notify you of new features and investment opportunities
- Conduct surveys and request feedback
- Personalize user experience and recommendations

You may opt out of marketing communications at any time by following unsubscribe instructions or contacting us directly.

3.6 Legal Proceedings and Protection of Rights

We may use your information to:

- Establish, exercise, or defend legal claims
- Protect Vaulto's rights, property, and safety
- Protect the rights, property, and safety of our users and the public
- Enforce our agreements and policies
- Cooperate with legal processes and investigations

4. How We Share Your Information

4.1 Third-Party Service Providers

We share your information with trusted third-party service providers who assist in Platform operations:

Ramp Network (Fiat-to-Crypto On-Ramp):

- Identity and contact information for KYC verification
- Wallet address for deposit destination
- Transaction amounts and funding requests
- Compliance and risk screening information

Purpose: To facilitate fiat-to-cryptocurrency conversions for wallet funding. Ramp Network is an independent service provider licensed to conduct money transmission and operates under their own Privacy Policy and Terms of Service.

Ondo Finance (Tokenized Securities Platform):

- Complete KYB/KYC documentation and verification information
- Entity structure and beneficial ownership information
- Accreditation and professional investor status documentation
- Wallet addresses for tokenized asset transactions
- Transaction activity and compliance information

Purpose: To facilitate access to tokenized securities products and comply with regulatory requirements for securities offerings.

Alpaca Markets (Options Trading):

- Account identification and verification information
- Trading instructions and position management data
- Risk metrics and portfolio information
- Financial suitability information

Purpose: To execute options hedging strategies for impermanent loss mitigation.

Identity Verification and Compliance Providers:

- Identification documents and personal information
- Biometric data (if applicable)
- Address and entity documentation
- Beneficial ownership information

Purpose: To conduct enhanced due diligence, sanctions screening, PEP checks, and fraud prevention.

Cloud Infrastructure and Hosting Providers:

- Account data stored on secure cloud servers
- Encrypted private keys and wallet information
- Transaction and usage logs

Purpose: To provide secure, scalable infrastructure for Platform operations.

Analytics and Monitoring Services:

- Aggregated and anonymized usage data
- Performance metrics and error logs
- Security event information

Purpose: To monitor Platform performance, identify issues, and improve user experience.

Customer Support and Communication Tools:

- Contact information and communication history
- Support tickets and inquiries
- User feedback and survey responses

Purpose: To provide efficient customer service and resolve user issues.

Payment Processors:

- Payment method information (where applicable)
- Transaction amounts and billing information

Purpose: To process fee payments and subscription charges (not for fiat-to-crypto conversion, which is handled by Ramp Network).

4.2 Blockchain Networks and Public Ledgers

Certain information is inherently public when recorded on blockchain networks:

- Wallet addresses assigned to your account
- Transaction hashes and amounts
- Smart contract interactions
- Token holdings and transfers
- Liquidity pool participation

Note: While wallet addresses are pseudonymous, they may be linked to your identity through on-chain analysis or third-party services. We do not control information recorded on public blockchains.

4.3 Regulatory Authorities and Law Enforcement

We may disclose your information to:

- Financial regulators (SEC, CFTC, FinCEN, state regulators)
- Law enforcement agencies
- Tax authorities
- Courts and legal proceedings
- Government agencies conducting investigations

Disclosure occurs when:

- Legally required by subpoena, court order, or regulation
- Necessary to comply with AML/CTF reporting requirements (e.g., SARs)
- Required to respond to lawful government requests

- Necessary to protect legal rights or comply with legal obligations

4.4 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of assets, your information may be transferred to successor entities or acquirers. We will notify you of any such change in ownership or control of your information and provide choices regarding your information where legally required.

4.5 With Your Consent

We may share your information with other third parties when you provide explicit consent or direction to do so.

4.6 Aggregated and Anonymized Data

We may share aggregated, anonymized, or de-identified information that cannot reasonably be used to identify you with:

- Business partners for analytics and research
- Industry organizations for benchmarking
- Academic institutions for research purposes
- The public for transparency reporting

5. Data Security and Protection

5.1 Security Measures

We implement industry-standard technical and organizational security measures to protect your information:

Encryption:

- Private keys encrypted at rest using AES-256-GCM encryption
- TLS/SSL encryption for data in transit
- End-to-end encryption for sensitive communications
- Database encryption and encrypted backups

Access Controls:

- Role-based access control (RBAC) limiting employee access
- Multi-factor authentication (MFA) for administrative access
- Principle of least privilege for system access
- Regular access reviews and permission audits

Infrastructure Security:

- Secure cloud hosting with reputable providers
- Network segmentation and firewalls
- Intrusion detection and prevention systems
- Regular security assessments and penetration testing
- DDoS protection and rate limiting
- Hardware Security Modules (HSMs) for key management

Operational Security:

- Comprehensive logging and monitoring
- Security incident response procedures
- Regular security training for employees
- Background checks for personnel with data access
- Vendor security assessments
- Business continuity and disaster recovery planning

Application Security:

- Secure coding practices and code reviews
- Regular vulnerability scanning and patching
- Web application firewalls
- Input validation and sanitization
- Protection against common attacks (SQL injection, XSS, CSRF)

5.2 Data Retention

We retain your information for as long as necessary to:

- Provide Platform services and maintain your account
- Comply with legal and regulatory obligations (typically 7+ years for financial records)
- Resolve disputes and enforce agreements
- Prevent fraud and abuse

Retention Periods:

- Account information: Duration of account relationship plus 7 years
- Transaction records: 7 years minimum (may be longer based on jurisdiction)
- KYC/KYB documentation: 7 years after account closure
- Communication records: 7 years
- Technical logs: 1-2 years unless required for investigations

When information is no longer necessary, we securely delete or anonymize it. You may request deletion of certain information subject to our legal retention obligations.

5.3 Data Security Limitations

While we implement robust security measures, no system is completely secure. You acknowledge that:

- Internet transmission and electronic storage carry inherent security risks
- Unauthorized access, data breaches, or cyber-attacks may occur despite our efforts
- You are responsible for maintaining the security of your Google account credentials
- You should promptly notify us of any suspected security incidents

We will notify you of data breaches affecting your information as required by applicable law.

6. Your Privacy Rights and Choices

6.1 Access and Portability

You have the right to:

- Request access to the personal information we hold about you
- Receive a copy of your information in a structured, machine-readable format
- Request transmission of your information to another service provider (data portability)

To exercise these rights, contact us at privacy@vaulto.ai with your request.

6.2 Correction and Update

You have the right to:

- Correct inaccurate or incomplete personal information
- Update your account information and preferences

You can update certain information directly through your Platform account settings. For other corrections, contact support@vaulto.ai.

6.3 Deletion and Erasure

You have the right to request deletion of your personal information, subject to:

- Our legal and regulatory obligations to retain records
- Legitimate business needs (e.g., fraud prevention, dispute resolution)
- Pending transactions or legal claims

To request deletion, contact privacy@vaulto.ai. Note that some information may remain in backups or archives for compliance purposes.

6.4 Objection and Restriction

You have the right to:

- Object to processing of your information for direct marketing purposes
- Restrict processing of your information in certain circumstances
- Withdraw consent where processing is based on consent

Contact privacy@vaulto.ai to exercise these rights.

6.5 Marketing Communications Opt-Out

You may opt out of marketing communications by:

- Clicking "unsubscribe" links in emails
- Adjusting communication preferences in your account settings
- Contacting support@vaulto.ai

Note that you cannot opt out of transactional or service-related communications necessary for account operation.

6.6 Cookie Management

You can control cookies through your browser settings. Note that disabling cookies may affect Platform functionality. See Section 8 for details on our cookie usage.

6.7 California Privacy Rights (CCPA/CPRA)

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

Right to Know: Request disclosure of categories and specific pieces of information collected, sources, purposes, and third parties with whom information is shared.

Right to Delete: Request deletion of personal information, subject to exceptions.

Right to Opt-Out: Opt out of "sale" or "sharing" of personal information (Note: We do not sell personal information).

Right to Correct: Request correction of inaccurate personal information.

Right to Limit Sensitive Information Use: Limit use of sensitive personal information (we use sensitive information only as necessary for services).

Right to Non-Discrimination: Exercise privacy rights without discriminatory treatment.

Authorized Agent: Designate an authorized agent to make requests on your behalf.

To exercise CCPA/CPRA rights, contact privacy@vaulto.ai or call our toll-free number (to be established). We will verify your identity before processing requests.

6.8 European Union and UK Rights (GDPR/UK GDPR)

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

Legal Basis for Processing:

- Contractual necessity: To provide Platform services
- Legal obligation: To comply with AML/KYC and financial regulations
- Legitimate interests: For security, fraud prevention, and service improvement
- Consent: For marketing communications (where required)

Additional Rights:

- Right of access and data portability
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to object to processing
- Right to withdraw consent
- Right to lodge a complaint with supervisory authority

International Data Transfers:
Vaulto is based in the United States. We transfer data from the EEA/UK to the US using appropriate safeguards including:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions where applicable
- Appropriate technical and organizational security measures

To exercise GDPR rights or for questions about international transfers, contact privacy@vaulto.ai.

6.9 Response Timeline

We will respond to privacy rights requests within:

- 30 days for GDPR requests (may extend to 60 days for complex requests)
- 45 days for CCPA requests (may extend to 90 days for complex requests)
- Reasonable timeframes for other jurisdictions

7. International Data Transfers

7.1 Cross-Border Transfers

Vaulto operates from the United States and processes information globally. Your information may be transferred to, stored in, and processed in:

- United States (primary operations)
- Countries where third-party service providers operate
- Jurisdictions where blockchain infrastructure is located

7.2 Transfer Safeguards

When transferring information internationally, we implement appropriate safeguards:

- Standard Contractual Clauses (EU Commission-approved)
- Adequacy decisions for countries with adequate data protection
- Privacy Shield certification (where applicable and valid)
- Binding Corporate Rules (where applicable)
- Contractual obligations with service providers
- Technical security measures (encryption, access controls)

7.3 Country-Specific Information

European Economic Area and United Kingdom:
Data transfers to the US and other countries are governed by SCCs and additional security measures to meet GDPR adequacy requirements.

Canada:
We comply with PIPEDA requirements for Canadian users and ensure cross-border transfers meet Canadian privacy standards.

Australia:
We comply with Australian Privacy Principles (APPs) for Australian users.

Other Jurisdictions:
We comply with applicable data protection laws in jurisdictions where we operate.

8. Cookies and Tracking Technologies

8.1 Types of Cookies Used

We use cookies and similar technologies to enhance Platform functionality, security, and user experience:

Essential Cookies:

- Authentication and session management
- Security features and fraud prevention
- Load balancing and performance optimization
- **Retention:** Session duration or as needed for security

Functional Cookies:

- User preferences and settings
- Language and region selection
- Interface customization
- **Retention:** Up to 1 year

Analytics Cookies:

- Usage patterns and feature adoption
- Performance metrics and error tracking
- User journey analysis
- **Retention:** Up to 2 years

Marketing Cookies (With Consent):

- Targeted advertising and promotions
- Campaign effectiveness measurement
- Conversion tracking
- **Retention:** Up to 1 year

8.2 Third-Party Cookies

Third-party services may set cookies for:

- Google Analytics (usage analytics)
- Authentication providers (Google OAuth)
- Security and fraud prevention services
- Content delivery networks

8.3 Cookie Management

You can manage cookie preferences through:

- Browser settings (blocking or deleting cookies)
- Platform cookie consent manager (where provided)
- Opt-out mechanisms provided by third-party services

Note: Disabling essential cookies will impact Platform functionality and may prevent access to certain features.

8.4 Do Not Track Signals

Our Platform does not currently respond to Do Not Track (DNT) browser signals due to lack of industry standards. You can manage tracking through browser settings and cookie controls.

9. Children's Privacy

9.1 Age Restrictions

The Platform is not intended for individuals under 18 years of age (or the age of majority in their jurisdiction). We do not knowingly collect personal information from minors.

9.2 Parental Consent

If we discover that we have collected information from a minor without proper parental consent, we will promptly delete such information. Parents or guardians who believe we may have collected information from a minor should contact privacy@vaulto.ai immediately.

10. Third-Party Links and Services

10.1 External Links

The Platform may contain links to third-party websites, applications, or services (including Ramp Network, Ondo Finance, Alpaca Markets). We are not responsible for the privacy practices of these third parties.

10.2 Third-Party Privacy Policies

We encourage you to review the privacy policies of:

- **Ramp Network:** https://ramp.network/privacy-policy
- **Ondo Finance:** https://ondo.finance/privacy
- **Alpaca Markets:** https://alpaca.markets/privacy
- **Google:** https://policies.google.com/privacy

Your use of third-party services is governed by their respective privacy policies, terms of service, and practices.

10.3 Integration Responsibility

While we conduct due diligence on third-party partners, we do not control their data practices. You provide information to third parties at your own risk.

11. Changes to This Privacy Policy

11.1 Updates and Modifications

We may update this Privacy Policy periodically to reflect:

- Changes in Platform features or operations
- New regulatory requirements or legal obligations
- Evolving privacy practices and technologies
- User feedback and privacy concerns

11.2 Notification of Changes

We will notify you of material changes through:

- Email notification to your registered address
- Prominent notice on the Platform homepage
- In-app notification upon next login
- Updated "Last Updated" date at the top of this policy

11.3 Review Responsibility

You are responsible for periodically reviewing this Privacy Policy. Continued use of the Platform after changes take effect constitutes acceptance of the updated policy.

11.4 Objection to Changes

If you do not agree to Privacy Policy changes, you must discontinue Platform use and may request deletion of your information subject to our retention obligations.

12. Contact Information and Complaints

12.1 Privacy Inquiries

For questions, concerns, or requests regarding this Privacy Policy or our data practices, contact:

Vaulto Inc.
Privacy Officer
Email: privacy@vaulto.ai
Support: support@vaulto.ai
Mailing Address: [To be added - Los Angeles, CA office address]

12.2 Data Protection Officer

For GDPR-related inquiries, contact our Data Protection Officer:
Email: dpo@vaulto.ai

12.3 Response Timeline

We will respond to privacy inquiries within:

- 5 business days for initial acknowledgment
- 30 days for substantive response (may extend for complex matters)

12.4 Complaints and Dispute Resolution

If you believe we have not adequately addressed your privacy concerns, you may:

File a complaint with supervisory authorities:

- **European Union:** Your national Data Protection Authority
- **United Kingdom:** Information Commissioner's Office (ICO) - https://ico.org.uk
- **California:** California Attorney General - https://oag.ca.gov/privacy
- **Canada:** Office of the Privacy Commissioner - https://priv.gc.ca

Seek dispute resolution:

- Informal resolution through privacy@vaulto.ai
- Mediation or arbitration as specified in our Terms of Service
- Legal action in accordance with applicable law

12.5 Third-Party Service Contacts

For privacy issues related to integrated services:

- **Ramp Network:** privacy@ramp.network
- **Ondo Finance:** privacy@ondo.finance
- **Alpaca Markets:** privacy@alpaca.markets

13. Specific Use Case: Ramp Network Integration

13.1 Purpose of Data Sharing with Ramp Network

Vaulto integrates Ramp Network's SDK and widget to provide fiat-to-crypto on-ramp services. This integration is necessary because Vaulto does not hold a Money Transmitter License (MTL) and cannot directly process fiat currency transactions.

13.2 Information Shared with Ramp Network

When you use the Ramp Network widget to fund your wallet, we share:

- Your name and email address
- Your Vaulto wallet address (as deposit destination)
- Transaction amount requests
- Basic account verification status

13.3 Information Ramp Network Collects Directly

Ramp Network independently collects from you:

- Payment method information (credit card, bank account details)
- Additional KYC information required by Ramp's compliance procedures
- Transaction history and purchase patterns
- Geolocation and device information
- Any information required by their banking and payment partners

13.4 Ramp Network's Independent Obligations

Ramp Network operates as an independent licensed money transmitter and is subject to:

- Their own Privacy Policy and Terms of Service
- European and international payment services regulations
- AML/KYC compliance requirements
- Banking partner requirements
- Payment card industry (PCI) compliance standards

13.5 Our Limited Role

Vaulto's role in Ramp Network transactions is strictly limited to:

- Providing technical integration of the Ramp widget in our Platform
- Transmitting your wallet address for deposit destination
- Receiving transaction confirmation webhooks
- Updating your wallet balance display after successful deposits

We do not:

- Process or transmit fiat currency
- Store your payment method information
- Control Ramp Network's fee structure or exchange rates
- Have access to Ramp Network's compliance decisions or customer data beyond basic transaction confirmations

13.6 Data Processing Responsibilities

- **Ramp Network is the data controller** for information collected during the on-ramp process
- **Vaulto is a data processor** only for the limited purpose of facilitating technical integration
- You have separate privacy rights with respect to information held by Ramp Network

13.7 User Consent

By using the Ramp Network on-ramp feature:

- You consent to sharing your name, email, and wallet address with Ramp Network
- You agree to be subject to Ramp Network's Privacy Policy
- You authorize Vaulto to facilitate this integration on your behalf
- You acknowledge that Ramp Network's data practices are governed by their own policies

13.8 Privacy Inquiries for Ramp Transactions

For privacy questions specifically related to Ramp Network transactions, payment methods, or KYC procedures, contact Ramp Network directly:

- **Email:** privacy@ramp.network
- **Support:** support@ramp.network
- **Privacy Policy:** https://ramp.network/privacy-policy

14. Legal Basis for Processing (GDPR)

For users subject to GDPR, we process your information based on the following legal grounds:

14.1 Contractual Necessity

Processing necessary to perform our contract with you (Terms of Service):

- Account creation and management
- Wallet generation and custody services
- Transaction processing
- Liquidity provision services
- Customer support

14.2 Legal Obligation

Processing required to comply with legal and regulatory requirements:

- KYC/KYB verification and due diligence
- AML/CTF compliance and sanctions screening
- Financial services regulatory reporting
- Tax compliance and reporting
- Law enforcement and regulatory requests

14.3 Legitimate Interests

Processing necessary for our legitimate business interests:

- Platform security and fraud prevention
- Service improvement and optimization
- Analytics and usage insights
- Business operations and communications
- Marketing (where consent not required)

We balance our legitimate interests against your privacy rights and do not process information in ways that override your interests.

14.4 Consent

Processing based on your explicit consent:

- Marketing communications (where required)
- Optional data collection beyond service requirements
- Cookie usage for non-essential purposes

You may withdraw consent at any time without affecting the lawfulness of processing based on consent before withdrawal.

14.5 Vital Interests

In rare cases, processing may be necessary to protect vital interests:

- Emergency situations threatening life or safety
- Prevention of serious harm

15. Automated Decision-Making and Profiling

15.1 Use of Automated Processing

We use automated systems and algorithms for:

- Fraud detection and risk assessment
- Sanctions screening and compliance checks
- Transaction monitoring and anomaly detection
- Credit or suitability evaluation
- Portfolio allocation recommendations

15.2 Significant Automated Decisions

Automated decisions that significantly affect you include:

- Account approval or denial based on KYC/KYB verification
- Transaction blocking due to fraud or compliance flags
- Risk-based position size limitations

15.3 Right to Human Review

You have the right to:

- Request human review of automated decisions
- Express your perspective and contest automated decisions
- Receive an explanation of decision-making logic

Contact compliance@vaulto.ai to request human review of automated decisions.

15.4 Profiling

We may create risk and behavioral profiles based on:

- Transaction patterns and history
- Investment preferences and behavior
- Compliance risk indicators
- Platform usage patterns

Profiling is used solely for service provision, security, and regulatory compliance, not for discriminatory purposes.

16. Data Breach Notification

16.1 Breach Response Procedures

In the event of a data breach involving your personal information, we will:

- Investigate the scope and impact of the breach
- Contain and remediate the security incident
- Assess risks to affected individuals
- Notify affected users and regulatory authorities as required by law

16.2 Notification Timeline

We will notify you of breaches affecting your personal information:

- **GDPR:** Within 72 hours of discovery (where feasible)
- **CCPA:** Without unreasonable delay
- **Other jurisdictions:** As required by applicable law

16.3 Notification Content

Breach notifications will include:

- Description of the incident and affected information
- Potential consequences and risks
- Measures we have taken to address the breach
- Recommended actions you should take
- Contact information for inquiries

16.4 Reporting Security Incidents

If you discover or suspect a security incident or unauthorized access, immediately contact: security@vaulto.ai

17. Additional State-Specific Privacy Rights

17.1 Virginia (VCDPA)

Virginia residents have rights similar to CCPA including access, deletion, correction, data portability, and opt-out of targeted advertising and sale of personal information.

17.2 Colorado (CPA)

Colorado residents have rights to access, correct, delete, and obtain a copy of personal information, and opt out of targeted advertising and sale.

17.3 Connecticut (CTDPA)

Connecticut residents have rights to access, correct, delete, obtain a copy, and opt out of processing for targeted advertising or sale.

17.4 Utah (UCPA)

Utah residents have rights to access, delete, and obtain a copy of personal information, and opt out of targeted advertising and sale.

17.5 Exercising State Rights

To exercise state-specific privacy rights, contact privacy@vaulto.ai with your request and jurisdiction.

18. Recordkeeping and Audit Trail

18.1 Compliance Recordkeeping

We maintain comprehensive records to demonstrate compliance with:

- AML/KYC regulations requiring 7+ year retention
- Securities laws for tokenized asset transactions
- Tax reporting obligations
- Financial services audit requirements
- Data protection regulations

18.2 Audit Trail

We maintain audit logs recording:

- Account creation and modification events
- KYC/KYB verification milestones
- Transaction authorizations and executions
- Access to sensitive information
- Security events and incidents
- Compliance reviews and decisions

18.3 Retention Justification

Information is retained based on:

- Regulatory requirements (longest applicable period prevails)
- Statute of limitations for legal claims
- Business needs and operational requirements
- Consent duration (where applicable)

19. Transparency and Accountability

19.1 Privacy by Design

We incorporate privacy considerations into:

- Platform architecture and development
- New feature design and implementation
- Third-party service selection
- Business process design
- Employee training and policies

19.2 Data Protection Impact Assessments

We conduct Data Protection Impact Assessments (DPIAs) for:

- New processing activities involving sensitive information
- High-risk processing operations
- Implementation of new technologies
- Significant changes to data practices

19.3 Third-Party Audits

We engage independent third parties to:

- Conduct security audits and penetration testing
- Assess compliance with privacy frameworks
- Verify implementation of security controls
- Review data handling practices

19.4 Transparency Reports

We publish transparency reports disclosing (where legally permitted):

- Number and types of law enforcement requests
- Government information requests
- Compliance with data subject requests
- Security incidents and breach notifications

20. Acknowledgment and Consent

20.1 Privacy Policy Acceptance

By creating an account, accessing the Platform, or using our services, you acknowledge that:

- You have read and understood this Privacy Policy
- You agree to the collection, use, and disclosure of your information as described
- You understand the risks associated with digital asset services and blockchain technology
- You have had the opportunity to seek independent advice regarding privacy implications

20.2 Explicit Consents

Where required by law, we will obtain your explicit consent for:

- Processing sensitive personal information beyond regulatory requirements
- Marketing communications
- Optional data collection
- Sharing information with third parties beyond service provision

20.3 Withdrawal of Consent

You may withdraw consent at any time by:

- Adjusting privacy settings in your account
- Contacting privacy@vaulto.ai
- Following opt-out instructions in communications

Withdrawal does not affect the lawfulness of processing based on consent before withdrawal or processing based on other legal grounds.

Document Version: 1.0
Effective Date: February 5, 2026

Contact Information:

- **General Privacy Inquiries:** privacy@vaulto.ai
- **Data Protection Officer:** dpo@vaulto.ai
- **Security Incidents:** security@vaulto.ai
- **Support:** support@vaulto.ai

Regulatory Compliance:

- **EU Representative:** [To be designated if required]
- **UK Representative:** [To be designated if required]

For questions about this Privacy Policy or our data practices, please contact our Privacy Officer at privacy@vaulto.ai.