Privacy Policy

Last updated: 1 June 2026

This Privacy Policy explains how **VENT AI LIMITED**, a company incorporated in Cyprus with registration number **HE 447148** and registered office at **Riga Feraiou, 4 OMEGA COURT, GROUND FLOOR, Office 07, 3095, Limassol, Cyprus** ("**UFarm**", "**we**", "**us**" or "**our**"), collects and uses personal data in connection with the UFarm website, interfaces, applications, dashboards, wallet connection features, transaction relay features, gas sponsorship features, strategy access features and related services.

For questions about this Privacy Policy or personal data, contact us at **legal@ufarm.digital**. For product support, contact **support@ufarm.digital**.

1. Who is responsible for your personal data

VENT AI LIMITED is the controller of personal data processed for UFarm's own website and software services.

Some third-party services accessible through UFarm are provided by independent third parties, such as Strategy Providers, wallet providers, blockchain infrastructure providers, on-ramp providers and other partners. Those third parties may act as independent controllers under their own privacy policies. UFarm is not responsible for their privacy practices except where required by law.

2. Summary

UFarm operates a non-custodial software and technical interface. We do not control your wallet, private keys, seed phrase, MPC fragments, session keys or other access credentials.

We may process personal data such as account information, wallet addresses, blockchain transaction metadata, device and usage logs, support communications, security logs and service interaction data.

We do **not** use cookies or non-essential similar technologies for analytics, advertising, attribution, retargeting, fingerprinting or cross-site tracking. Strictly necessary browser or device storage may be used for security, session management, wallet connection, abuse prevention or other user-requested features.

We do **not** transfer off-chain personal data outside the European Economic Area.

Public blockchain data may be visible to anyone and may not be controlled, deleted or modified by UFarm.

3. Data we collect

We collect only the data needed to provide, secure, operate, support and improve the Services.

3.1 Account and contact data

This may include:

- Email address
- Account ID
- Username or display name, if provided
- Support requests and messages
- Communication preferences

3.2 Wallet and blockchain data

This may include:

- Wallet address
- Connected network or chain ID
- Transaction hash
- Smart-contract interaction
- Public on-chain balances or positions displayed through the interface
- Token, protocol or strategy interaction metadata
- Wallet addresses and transaction data may be personal data if they can be linked to you.

3.3 Transaction relay and gas sponsorship data

If you use transaction relay, account-abstraction, meta-transaction or gas sponsorship features, we may process:

- Signed transaction payload metadata
- Relay request metadata
- Timestamp
- Network / chain ID
- Transaction status
- Gas sponsorship record
- RPC/node response
- Error logs
- Abuse-prevention or rate-limit data

We do not store your private keys, seed phrase, wallet credentials, MPC fragments or session keys.

3.4 Strategy interaction data

If you view or interact with strategies made available through the Services, we may process:

- Viewed strategies
- Selected strategy pages
- Interaction timestamps
- Related wallet address
- Transaction interaction history
- UI events needed to operate the interface

Strategy Providers may separately collect or process personal data under their own terms and privacy policies.

3.5 Device, log and usage data

When you use the Services, our systems may process technical data such as:

- IP address
- Approximate location derived from IP address
- Browser type and version
- Operating system
- Device type
- Referring URL
- Pages or screens viewed
- Date and time of access
- Session and diagnostic logs
- Strictly necessary browser or device storage data used for session security, wallet connection, user-requested functionality, debugging or abuse prevention
- Error logs
- Security logs

We use this data to operate, secure, debug and improve the Services.

3.6 Security and compliance data

We may process data needed to protect the Services and comply with applicable law, including:

- IP address
- Wallet address
- Device and session data
- Risk flags
- Sanctions or abuse-prevention screening results
- Geolocation approximation
- Fraud, spam or attack indicators
- Access-control logs

3.7 On-ramp and partner handoff data

If you access an on-ramp, payment, KYC or similar third-party service through UFarm, the relevant third-party provider is responsible for its own service and privacy practices.

UFarm may process limited integration data, such as:

- Redirect or session metadata
- Partner reference ID
- Status callback, if technically required
- Support metadata related to the handoff

We do not receive or store your full card details, bank credentials or fiat payment account credentials.

3.8 Content data

If the Services allow users, Strategy Providers or other third parties to submit, publish or display content, we may process that content and related metadata.

This may include:

- Strategy descriptions
- Provider profiles
- Documents
- Names
- Images
- Comments
- Reports
- Moderation records

Do not submit personal data, confidential information or unlawful content unless necessary.

4. Data we do not collect

UFarm does not collect or store:

- Private keys
- Seed phrases
- Wallet passwords
- MPC fragments
- Session keys controlled by the user
- Full card details
- Bank login credentials
- Government ID documents, unless a specific UFarm feature later requires them and this Privacy Policy is updated
- Non-essential cookies or similar technologies for analytics, advertising, attribution, retargeting, fingerprinting or cross-site tracking

This does not prevent UFarm from using strictly necessary cookies or similar technologies where required to provide a user-requested feature, maintain security, connect a wallet, prevent abuse or operate the Services. Third-party providers may collect some of this data if you use their services. Their own privacy policies apply.

5. Cookies and similar technologies

UFarm does not use cookies or non-essential similar technologies for analytics, marketing, advertising, attribution, retargeting, fingerprinting or cross-site tracking.

The Services may use strictly necessary browser or device storage or access, such as localStorage, sessionStorage, IndexedDB, wallet SDK or wallet-connection storage, or similar technical mechanisms, only where required to provide a feature explicitly requested by you, maintain a secure session, connect or reconnect your wallet, prevent fraud or abuse, remember non-tracking interface preferences, debug errors or operate the Services.

We do not use pixels, tags, fingerprinting scripts, third-party advertising technologies or embedded tracking iframes for profiling or cross-site tracking.

Embedded third-party services, such as wallet, on-ramp, support, security, blockchain infrastructure or compliance providers, may use their own technologies when you choose to interact with them. Where those third parties act as independent controllers, their own privacy notices apply.

We will not load non-essential third-party tracking technologies before obtaining consent where consent is required by applicable law.

If we later introduce non-essential cookies or similar technologies, we will update this Privacy Policy and implement a consent management mechanism that allows you to accept or reject categories of non-essential technologies and access relevant vendor information.

Technical data may still be processed through ordinary server logs when you access the Services, such as IP address, request timestamp, browser type, security logs and error logs. This is not cookie-based tracking.

6. Public blockchain data

Blockchain networks are public or shared ledgers. Wallet addresses, transaction hashes, smart-contract interactions, token balances and related metadata may be publicly visible.

UFarm does not control public blockchain networks and cannot delete, modify, hide, reverse or correct data recorded on a blockchain.

Even if a wallet address does not directly identify you, it may become personal data if combined with other information.

Your GDPR rights apply to personal data controlled by UFarm. They may not allow UFarm to alter or erase public blockchain records that UFarm does not control.

7. How we use personal data and legal bases

We process personal data only where we have a legal basis under applicable data protection law.

Purpose	Data used	Legal basis
Provide account access and user support	Account, contact, support, wallet and usage data	Performance of contract; legitimate interests
Operate wallet connection features	Wallet address, chain ID, device/session data, strictly necessary wallet-connection and session storage	Performance of contract
Provide transaction relay	Wallet address, transaction metadata, relay logs, status data	Performance of contract
Provide gas sponsorship	Wallet address, transaction metadata, gas sponsorship logs	Performance of contract; legitimate interests
Display strategies and related information	Wallet, strategy interaction, public blockchain and usage data	Performance of contract; legitimate interests
Integrate with third-party on-ramp or partner services	Handoff metadata, partner reference ID, support metadata	Performance of contract; legitimate interests

Provide support and respond to requests	Contact data, messages, account/wallet references	Performance of contract; legitimate interests
Secure the Services and prevent abuse	IP, wallet, device, session, strictly necessary terminal-storage data, risk, security and log data	Legitimate interests; legal obligation where applicable
Enforce Terms and protect legal rights	Relevant account, wallet, usage, security and communication data	Legitimate interests; legal obligation
Comply with applicable law	Data required by law or regulator	Legal obligation
Improve reliability and performance	Technical logs, error data, aggregated usage information	Legitimate interests
Send service communications	Email, account data	Performance of contract; legitimate interests
Send marketing communications, if any	Email, marketing preference	Consent, or legitimate interests where legally permitted

Our legitimate interests include operating and securing the Services, preventing fraud and abuse, debugging errors, improving reliability, enforcing our Terms, protecting users and third-party providers, and defending legal claims.

You may object to processing based on legitimate interests as described in Section 14.

8. Marketing communications

We may send you service-related messages, such as security notices, account messages, support replies and important changes to the Services. These are not marketing messages.

We send marketing emails only where permitted by law. You can opt out of marketing emails at any time by using the unsubscribe link in the email or contacting **legal@ufarm.digital**.

Opting out of marketing does not stop service-related messages.

9. Automated decision-making

UFarm does not use solely automated decision-making that produces legal effects concerning you or similarly significantly affects you.

We may use automated or semi-automated security, sanctions, abuse-prevention, geoblocking, rate-limiting or risk-detection tools. These tools help protect the Services and may result in access being delayed, restricted or blocked. You may contact **legal@ufarm.digital** if you believe a restriction was applied incorrectly.

10. Who we share data with

We may share personal data with the following categories of recipients where necessary:

Recipient category	Purpose
Hosting and infrastructure providers	Operate and host the Services
Blockchain infrastructure providers	Connect to networks, RPC endpoints, nodes or indexers
Security and compliance providers	Fraud prevention, sanctions screening, abuse prevention, security monitoring
Email and support providers	Send service messages and manage support requests
Strategy Providers	Enable strategy-related interactions, where applicable
On-ramp and payment partners	Enable third-party on-ramp or related partner handoff, where requested by you
Professional advisers	Legal, accounting, audit, compliance and corporate administration
Authorities, courts or regulators	Where required by law or necessary to protect legal rights
Corporate transaction parties	In connection with merger, financing, restructuring, acquisition or sale of business assets

We require service providers that act as processors to process personal data only on our instructions and to use appropriate security and confidentiality measures.

Some third parties act as independent controllers. Their own privacy policies apply.

11. Data location and international transfers

UFarm does **not** transfer off-chain personal data outside the European Economic Area.

We use service providers and infrastructure located in the European Economic Area for off-chain personal data controlled by UFarm.

If we later need to transfer personal data outside the European Economic Area, we will update this Privacy Policy and use appropriate safeguards required by applicable data protection law.

Public blockchain networks are decentralized and may be operated by independent nodes worldwide. UFarm does not control where public blockchain data is replicated, validated, stored or accessed.

12. How long we keep data

We keep personal data only for as long as necessary for the purposes described in this Privacy Policy. When the applicable retention period expires, we delete, anonymize or aggregate the relevant data unless a legal hold, investigation, dispute, court or regulatory request, security incident or legal obligation requires longer retention.

Where longer retention is required, we retain only the data categories necessary for that longer purpose, restrict access where practicable and delete, anonymize or aggregate the data when the longer retention reason no longer applies.

Our standard retention periods are:

Data category	Retention period
Account and contact data	While your account is active. After account closure, we delete or anonymize ordinary account profile data within 90 days, unless longer retention is needed for legal, tax, audit, security or dispute purposes. Limited account identifiers, contract records, billing records or legal records may be retained for up to 6 years where necessary.
Wallet connection and session data	For the duration of the active session or wallet connection, then usually up to 90 days after the last connection for security, debugging and abuse-prevention purposes.
Cached wallet display data and public blockchain data displayed through the interface	Cached off-chain display data is refreshed or deleted when no longer needed to provide the interface, usually within 30 days. Public blockchain data is not controlled by UFarm; retention depends on the relevant blockchain network.
Strategy interaction and UI event data	Raw or pseudonymous strategy interaction and UI event data is retained for up to 12 months. Aggregated or anonymized analytics that no longer identify you may be retained for longer.
Support communications	For the duration of the support request, then up to 24 months after the last interaction. Support records relevant to a complaint, dispute, legal claim, regulatory request or financial/accounting matter may be retained for up to 6 years where necessary.
Raw transaction relay and gas sponsorship logs	Raw relay request metadata, RPC responses, error logs and signed-payload metadata are retained for up to 12 months after submission, finality, failure or expiry of the relevant transaction flow.

Transaction relay and gas sponsorship audit records	Limited audit records, such as transaction hash, chain ID, timestamp, transaction status, gas sponsorship amount or fee, and related wallet/account reference where required, may be retained for up to 24 months for security, abuse-prevention and operational audit purposes. Records required for tax, accounting, legal claims or disputes may be retained for up to 6 years where necessary.
Security, abuse-prevention and access logs	Usually up to 12 months. High-risk security logs, access-control logs, administrator logs, investigation records or incident records may be retained for up to 24 months, or longer if needed for a specific security incident, legal claim, regulatory request or legal hold.
Sanctions, geoblocking and risk restriction records	For the duration of the review or restriction, then up to 24 months after the decision. Where required to comply with sanctions, court orders, regulatory requests or other legal obligations, limited records may be retained for longer and reviewed periodically.

We may retain anonymized or aggregated data that no longer identifies you.

13. Security

We use technical and organizational measures designed to protect personal data against unauthorized access, loss, misuse, alteration and disclosure.

These measures may include access controls, encryption in transit, logging, monitoring, network security, vendor controls, internal access restrictions and incident response procedures.

No system is completely secure. You are responsible for securing your own wallet, devices, private keys, seed phrase, passwords and other access credentials.

14. Your rights

Depending on your location and applicable law, you may have the right to:

- Access your personal data
- Correct inaccurate personal data
- Delete personal data
- Restrict processing
- Object to processing based on legitimate interests
- Receive a copy of personal data in a portable format
- Withdraw consent where processing is based on consent
- Complain to a data protection authority

To exercise your rights, contact **legal@ufarm.digital**.

We may need to verify your identity before responding. We usually respond within one month, unless the request is complex or numerous, in which case the period may be extended as permitted by law.

These rights apply to personal data controlled by UFarm. They may not allow UFarm to alter, delete or reverse public blockchain records that UFarm does not control.

15. Complaints

You can contact us first at **legal@ufarm.digital**.

You also have the right to lodge a complaint with a supervisory authority. If Cyprus is the relevant authority, you may contact the **Cypriot Data Protection Authority / Office of the Commissioner for Personal Data Protection**. The EDPB lists the Cyprus authority as the Cypriot Data Protection Authority, with email **commissioner@dataprotection.gov.cy**. (European Data Protection Board)

You may also complain to the supervisory authority in your EU/EEA country of habitual residence, place of work or place of the alleged infringement.

16. Children

The Services are not directed to persons **under 18**.

We do not knowingly collect personal data from persons under 18. If you believe a person under 18 has provided personal data to UFarm, contact **legal@ufarm.digital**.

17. Third-party links and services

The Services may include links, widgets, integrations or references to third-party websites, wallets, protocols, blockchain networks, Strategy Providers, on-ramp providers or other services.

Those third parties are responsible for their own privacy practices. You should review their privacy policies before using their services.

UFarm is not responsible for third-party privacy practices except where required by law.

18. 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 posting the updated Privacy Policy, changing the “Last updated” date or using another reasonable method.

Your continued use of the Services after the updated Privacy Policy becomes effective means that you have read the updated version. Where legally required, we will request your consent.

19. Contact

Controller: **VENT AI LIMITED**
Registration number: HE 447148
Riga Feraiou, 4 OMEGA COURT, GROUND FLOOR, Office 07, 3095, Limassol, Cyprus
Privacy/legal contact: **legal@ufarm.digital**
Support contact: **support@ufarm.digital**