PRIVACY POLICY

Last Updated: March 9, 2026

This Privacy Policy (the "Policy") describes how Aetheryn LTD, a company incorporated under the laws of the British Virgin Islands (the "Company", "we", "us", or "our"), collects, uses, processes, discloses, and protects Personal Data in connection with your access to and use of the website located at the https://voice.fun and any associated applications, interfaces, campaign pages, SocialFi features, and related services (collectively, the "Services").

This Policy forms an integral part of the Terms and Conditions governing the Services.

By accessing or using the Services, you acknowledge that you have read and understood this Policy.

1. ROLE OF THE COMPANY

The Company acts as a data controller in respect of Personal Data collected and processed in connection with the Services, except where otherwise expressly stated.

The Company operates the Services as a technology platform facilitating user engagement, campaign participation, and blockchain-enabled interactions. The Company does not act as a custodian of private cryptographic keys and does not control blockchain wallets or Digital Assets belonging to users.

2. CATEGORIES OF PERSONAL DATA

We may collect and process the following categories of Personal Data.

2.1 Account and Identity Information

This may include:

- email address;
- username, alias, or nickname;
- authentication credentials and identifiers;
- referral identifiers;
- campaign participation status;
- whitelist or eligibility status.

Such information is collected when you register, authenticate, or interact with the Services.

We may collect your email address where you voluntarily provide it, including when you register, join a waitlist, participate in campaigns, subscribe to communications, or otherwise interact with the Services.

Users may withdraw consent to receive communications or processing of email addresses for promotional purposes at any time by using the unsubscribe functionality in communications or by contacting the Company. Withdrawal of such consent will not affect access to the core functionality of the Services, except where the email address is required for account authentication or security purposes.

We may also collect identifiers generated by authentication providers, including internal user identifiers assigned to the account, in order to associate that account with wallet addresses, campaign participation, referrals, and points balances.

2.2 Wallet and Blockchain Information

This may include:

- blockchain wallet addresses;
- wallet connection metadata;
- wallet-account association data;
- public blockchain transaction data;
- participation in token-enabled features, where applicable.

Blockchain wallet addresses and transactions are publicly accessible and may be permanently recorded on public blockchain networks.

The Company does not collect, access, or store private keys, seed phrases, or cryptographic signing credentials.

The Company does not collect, store, or have access to users' private keys, seed phrases, or full wallet credentials. Wallet infrastructure may be provided by third-party embedded wallet providers, but neither the Company nor its employees have the ability to access or control users' private keys or seed phrases.

Users remain solely responsible for the security of their wallet credentials.

2.3 Campaign, Engagement, and Points Data

This may include:

- participation in campaigns, quests, or promotional programs;
- referral activity, including relationship mapping, link generation, and attribution data;
- leaderboard rankings;
- engagement metrics;
- points balances;
- reward allocation data, where applicable.
- quest completion verification data;
- whitelist eligibility status;
- internal engagement scoring metrics;
- public social media metadata provided by authentication providers for verification purposes.

The Company does not obtain access to private messages or restricted account content.

Such information is necessary for the operation of engagement features and promotional programs.

Such information is processed solely for the purpose of operating engagement systems, preventing fraud or Sybil activity, ensuring campaign integrity, and administering referral and rewards mechanisms. The Company does not use this information for automated profiling intended to produce legal or similarly significant effects on users.

2.4 Technical and Device Information

This may include:

- IP address;
- browser type and version;
- device identifiers;
- operating system;
- session identifiers;
- interaction and usage data.

Such information is collected automatically through use of the Services.

IP addresses may be processed for security monitoring, fraud prevention, and service analytics. Where applicable, IP addresses may be truncated or anonymized after initial processing.

Certain technical data may be collected through cookies or similar technologies. Where required by applicable law, the Services will request user consent for the use of non-essential cookies through a cookie consent mechanism.

Additional information regarding cookies and tracking technologies may be provided in a separate Cookie Policy or within this Policy.

2.5 Communications

Where you communicate with the Company, we may collect:

- email address;
- communication content;
- communication metadata.

2.6 Social Media Account Information

Where you voluntarily connect a social media account (including X/Twitter), we may collect information associated with that account, including your user ID, username, profile identifier, and related metadata provided by the authentication provider.

This information is used to enable authentication, campaign participation, referral tracking, quest verification, and engagement features.

We do not collect passwords associated with your social media accounts.

The Company does not obtain access to private messages, password credentials, or restricted account content.

3. DATA COLLECTED THROUGH THIRD-PARTY PROVIDERS

The Services may integrate third-party account abstraction and wallet providers, including embedded wallet providers.

Such providers may independently collect and process Personal Data in accordance with their own privacy policies.

Wallet addresses generated or connected through such providers may be associated with your account for purposes of operating the Services.

The Company does not control and is not responsible for third-party processing practices.

Third-party authentication providers may generate and provide us with unique identifiers associated with your account, which we use to operate and secure the Services.

4. PURPOSES OF PROCESSING

The Company processes Personal Data for the following purposes:

- to provide, operate, and maintain the Services;
- to authenticate users and maintain account integrity;
- to associate blockchain wallets with user accounts;
- to operate campaigns, promotional programs, and points systems;
- to operate referral systems, leaderboard functionality, and engagement features;
- to allocate rewards and determine eligibility for campaigns or promotional programs;
- to ensure security, prevent fraud, abuse, manipulation, or unauthorized access;
- to comply with applicable legal and regulatory obligations;
- to respond to lawful requests from competent authorities;
- to improve and enhance the Services.
- to verify completion of quests and campaign tasks using automated systems and third-party integrations;
- to operate the whitelist eligibility and campaign access controls;
- to associate referral links and referral activity with user accounts;
- to detect and prevent Sybil activity, fraud, or manipulation of engagement systems;

Note: Where automated systems are used to detect potential fraud, Sybil activity, or manipulation of engagement systems, users may contact the Company to request review of the relevant decision. Requests may be submitted to the contact email specified in this Policy.

5. LEGAL BASIS FOR PROCESSING

Where applicable under data protection law, the Company processes Personal Data based on one or more of the following legal bases:

- performance of a contract;
- legitimate interests in operating, securing, and improving the Services;
- compliance with legal obligations;
- user consent, where required.

6. PUBLIC BLOCKCHAIN DATA

Blockchain networks operate as decentralized public ledgers.

Wallet addresses, transactions, and related blockchain data are publicly accessible and may be permanently recorded. Blockchain data may be associated with user accounts and campaign participation within the Services.

The Company does not control and cannot modify or delete blockchain records.

Wallet addresses may be associated with user accounts within the Services for operational purposes.

Users acknowledge that blockchain transactions and wallet addresses may be analyzed by third parties using blockchain analytics tools, which may result in the association of blockchain activity with identifiable individuals or entities. The Company does not control such third-party analysis and is not responsible for any deanonymization resulting from public blockchain data.

7. PUBLIC DISPLAY OF INFORMATION

Certain information may be publicly displayed within the Services, including usernames, aliases, leaderboard rankings, campaign participation status, and truncated wallet identifiers.

Such information may be visible to other users and visitors of the Services.

8. DISCLOSURE OF PERSONAL DATA

The Company may disclose Personal Data to:

- authentication and wallet providers;
- infrastructure, hosting, and cloud providers;
- analytics and security providers;
- fraud detection providers;
- social media authentication providers;
- legal or regulatory authorities, where required by law.

The Company does not sell Personal Data.

9. INTERNATIONAL DATA TRANSFERS

Personal Data may be transferred to and processed in jurisdictions outside your country of residence, including jurisdictions that may not provide equivalent levels of data protection.

By using the Services, you acknowledge and expressly consent to such transfers where permitted by applicable law.

We may preserve and disclose Personal Data to comply with legal obligations, enforce our Terms, or protect the integrity of the Services.

Where required under applicable data protection laws, the Company implements appropriate safeguards for international data transfers, which may include Standard Contractual Clauses (SCCs) or other lawful transfer mechanisms.

10. DATA RETENTION

Personal Data will be retained only for as long as necessary to:

- provide and operate the Services;
- maintain platform integrity and security;
- comply with legal obligations;
- resolve disputes and enforce agreements.

Blockchain-related data may be permanently recorded on public blockchain networks.

We may retain campaign participation, referral, whitelist, and points-related data for as long as necessary to ensure platform integrity, prevent abuse, and maintain accurate campaign records.

Where possible, the Company applies the following general retention periods:

- account and authentication data — retained while the account remains active and for up to 24 months after account inactivity;
- campaign and engagement data — retained for up to 24 months following the conclusion of the relevant campaign;
- security and fraud detection data — retained as necessary to investigate and prevent abuse.

Retention periods may be extended where required for legal obligations, dispute resolution, or security purposes.

11. SECURITY

The Company implements appropriate technical and organizational safeguards designed to protect Personal Data against unauthorized access, loss, misuse, or alteration.

However, no security system can guarantee absolute security.

Users remain responsible for securing their devices, credentials, and wallet access.

Security of blockchain wallets and embedded wallets is the responsibility of users and wallet providers. The Company does not control private keys.

Embedded wallet providers are responsible for their own security infrastructure.

If the Company becomes aware of a personal data breach that is likely to result in a risk to the rights and freedoms of users, the Company will notify affected users and, where required, the competent supervisory authority without undue delay in accordance with applicable data protection laws.

Notifications may be provided via email, platform notice, or other reasonable communication channels.

12. THIRD-PARTY SERVICES

The Services may integrate or link to third-party services, including blockchain networks, authentication providers, wallet providers, and external platforms.

The Company does not control and is not responsible for third-party privacy practices.

We are not responsible for the privacy practices of third-party platforms used in connection with quests, campaigns, or authentication.

Where you authenticate or connect third-party accounts (such as X/Twitter), the relevant third-party provider may share certain account identifiers with us in accordance with your authorization and their privacy policies.

When users interact with blockchain networks through the Services, certain infrastructure providers such as RPC nodes, blockchain indexers, or analytics providers may independently collect information including IP addresses and public wallet addresses in accordance with their own privacy policies.

Interactions with smart contracts may result in blockchain transactions that publicly record wallet addresses and transaction data on decentralized networks.

13. CHILDREN

The Services are not intended for individuals under eighteen (18) years of age.

The Company does not knowingly collect Personal Data from minors.

As the Company does not conduct mandatory identity verification, it relies on users to comply with age requirements in good faith. If the Company becomes aware that a user is under the required age, it reserves the right to suspend the account and delete associated off-chain Personal Data where feasible.

14. USER RIGHTS

Subject to applicable law, you may have the right to:

- request access to Personal Data;

- request correction of inaccurate Personal Data;
- request deletion of Personal Data, where feasible;
- request restriction of processing;
- object to processing;
- request data portability.

The Company may retain Personal Data where required for legal, regulatory, or security purposes.

Requests may be submitted to privacy@voice.fun. We will respond to valid requests within thirty (30) days as required by applicable law.

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, unless necessary for entering into or performing a contract between you and the Company. You have the right to obtain human intervention, express your point of view, and contest the decision regarding fraud prevention or account restriction.

The right to deletion does not apply to data permanently recorded on public blockchain networks, including wallet addresses, smart contract interactions, or transaction records. While the Company may delete or anonymize off-chain data stored within its systems, it cannot modify or remove data recorded on decentralized blockchain networks.

Where applicable under data protection law, users may also have the right to lodge a complaint with a competent data protection supervisory authority.

15. PRE-LAUNCH AND PROMOTIONAL CAMPAIGNS

The Services may include pre-launch campaigns, engagement programs, and promotional initiatives, including points programs.

The Company may process Personal Data in connection with such programs to administer participation, determine eligibility, allocate rewards, and maintain platform integrity.

Such campaigns may involve collection and processing of email addresses, wallet addresses, and social media identifiers voluntarily provided by users.

Such programs may be modified, suspended, or terminated at any time.

16. CHANGES TO THIS POLICY

The Company reserves the right to amend this Policy from time to time.

The most current version will be published on the website.

Continued use of the Services after the effective date of the updated Policy constitutes acceptance of the changes.

17. CONTACT

All privacy-related inquiries should be directed to: privacy@voice.fun.