Definica Privacy Policy

Privacy terms for definica.com, the future Definica dApp, wallet connection flows, governance interfaces, security processes, and related protocol services.

Effective Date	May 22, 2026
Last Updated	May 22, 2026
Website	https://definica.com
Protocol	Definica - Ethereum-native liquid staking and liquidity protocol
Governance	DAO-governed protocol structure
Contact	privacy@definica.com

1. Introduction

This Privacy Policy explains how Definica collects, uses, discloses, retains, and protects personal data, technical information, wallet-related information, and other information in connection with the Definica website, future dApp, governance interfaces, documentation, communications, security processes, and related services.

Definica has operated in a private capacity since 2024 and is currently undergoing a rebranding process to operate publicly as a DAO-governed DeFi protocol focused on liquid staking, ETH staking, osETH utility, aEthosETH liquidity, and future collateralized borrowing infrastructure.

This Privacy Policy applies to the Website at definica.com, official Definica subdomains, any future Definica dApp, official forms, email communications, security reports, governance interfaces, analytics, cookies, and other services operated by or on behalf of Definica.

This Privacy Policy does not change the public, transparent, and persistent nature of information recorded on public blockchains such as Ethereum.

2. Controller and DAO Structure

For purposes of data protection laws, the controller of personal data processed through the Website and official Definica interfaces is Definica DAO and/or any legal wrapper, foundation, company, or operator designated by Definica DAO governance or by an official Definica legal notice.

If Definica DAO designates a legal wrapper, foundation, company, or website operator, the relevant legal name, registered address, and jurisdiction may be published in an official Definica legal notice. Until such information is published, privacy inquiries may be sent to privacy@definica.com.

Some decentralized components of Definica may operate on public blockchain infrastructure that is not controlled exclusively by Definica. Public blockchain records may be processed by independent nodes, validators, indexers, block explorers, analytics providers, and other third parties worldwide.

3. Scope of This Privacy Policy

This Privacy Policy applies to information processed in connection with:

- the Website and any official Definica subdomains;
- the future Definica dApp and wallet connection flows;
- staking, osETH exposure, aEthosETH balances, lock-up dashboards, reward dashboards, and liquidity module dashboards;
- governance interfaces, proposals, voting, and delegation activity;
- contact forms, email communications, partnership inquiries, legal inquiries, media inquiries, and support requests;
- security reports, responsible disclosures, bug bounty communications, and incident response;
- analytics, cookies, security logs, and technical monitoring.

This Privacy Policy does not apply to independent third-party websites, wallets, block explorers, RPC providers, social media platforms, partner protocols, StakeWise, Aave, Ethereum clients, or other third-party services. Those services are governed by their own privacy policies and terms.

4. Information We May Collect

4.1 Website and technical information

When you visit the Website or use an official interface, Definica may collect technical information, including:

- IP address;
- browser type and version;

- device type and operating system;
- cookie identifiers or similar identifiers;
- language settings and time zone;
- referrer URL and pages visited;
- date and time of visit;
- events, performance logs, error logs, security logs, and diagnostic data.

4.2 Wallet and on-chain information

If you connect a wallet, interact with the dApp, or use protocol interfaces, Definica may process information associated with your public wallet address and on-chain activity, including:

- public wallet address;
- transaction hashes and smart contract interactions;
- public token balances and position data;
- ETH staking positions and osETH-related exposure;
- aEthosETH balances, lock-up periods, lock-up status, and unlock timing;
- reward eligibility, validator-backed reward data, incentive campaign participation, and liquidity contribution data;
- governance votes, proposals, delegation activity, and public governance participation;
- other information visible on Ethereum or another public blockchain.

Definica does not collect or store your private keys, seed phrase, wallet recovery data, or information that allows Definica to control your wallet.

4.3 Contact and communication information

If you contact Definica, subscribe to communications, submit a security report, or participate in community or governance processes, Definica may collect:

- email address, name, pseudonym, organization name, or role;
- message content, attachments, and correspondence history;
- bug reports, vulnerability details, proof-of-concept materials, and security communications;
- partnership, legal, media, investor, or governance inquiry details;
- newsletter preferences or consent records, if a newsletter is offered.

4.4 Compliance, fraud prevention, and security information

To protect the Protocol, users, and infrastructure, Definica may process compliance, fraud prevention, and security-related information, including:

- wallet addresses associated with sanctions, illicit finance, exploit activity, high-risk activity, or fraud signals;
- blockchain analytics results and risk scores;
- IP-based or region-based access signals;
- information needed to enforce the Terms of Service;
- incident response information, exploit reports, vulnerability information, and threat intelligence.

5. Public Blockchain Data

Ethereum transactions, wallet addresses, token transfers, contract calls, staking interactions, governance votes, delegations, and other blockchain records are public. Anyone may view, copy, index, analyze, or retain public blockchain data.

Definica does not control Ethereum, validators, nodes, block explorers, indexers, analytics providers, archival services, or third-party copies of blockchain records. Due to the nature of public blockchains, Definica may be unable to delete, modify, hide, restrict, or anonymize information recorded on-chain.

You should avoid linking personal information to wallet addresses where you do not want that connection to become public or persistent. You may consider using separate wallets for different activities and carefully managing any information that connects your identity to on-chain activity.

6. How We Collect Information

Definica may collect information from the following sources:

- directly from you when you submit information, contact Definica, or subscribe to communications;
- automatically when you visit the Website, use the dApp, connect a wallet, or interact with an official interface;
- from public blockchains and blockchain indexers;
- from wallet connection tools, RPC providers, analytics providers, security providers, and infrastructure providers;
- from community, governance, and security channels where you voluntarily participate;
- from compliance, sanctions screening, fraud prevention, and blockchain analytics providers.

7. Purposes and Legal Bases for Processing

Definica may process information for the following purposes:

- operating, maintaining, and securing the Website, dApp, and protocol interfaces;
- enabling wallet connection and display of protocol positions;
- displaying ETH staking positions, osETH exposure, aEthosETH balances, lock-up status, and reward eligibility;
- supporting liquidity module dashboards and future borrowing-related dashboards;
- processing governance activity, proposals, votes, delegations, and community participation;
- responding to communications, legal inquiries, support requests, partnership requests, and security reports;
- detecting, preventing, and investigating fraud, misuse, exploits, sanctions risk, and violations of the Terms of Service;
- debugging, monitoring, analytics, performance measurement, and product improvement;
- complying with legal obligations and responding to lawful requests;
- establishing, exercising, or defending legal claims.

Where GDPR, UK GDPR, Swiss data protection law, or similar laws apply, Definica may rely on the following legal bases:

Legal basis	Examples
Contract	Providing the Website, dApp, user-requested interfaces, wallet-related displays, communications, and requested services.
Legitimate interests	Security, fraud prevention, analytics, product improvement, protocol protection, governance operations, and enforcement of Terms.

Legal basis	Examples
Consent	Optional cookies, newsletter subscriptions, marketing communications, and other consent-based features.
Legal obligation	Compliance with applicable law, sanctions, regulatory requirements, or lawful requests.
Claims	Establishing, exercising, or defending legal claims and protecting Definica, users, contributors, and infrastructure.

8. Cookies and Similar Technologies

Definica may use cookies, local storage, session storage, pixels, software development kits, analytics scripts, and similar technologies to operate the Website, remember preferences, secure services, analyze usage, improve performance, and support optional communications or marketing features.

Categories of cookies and similar technologies may include:

Category	Purpose	Consent
Strictly necessary	Website operation, security, session management, wallet interface functionality, and cookie consent management.	Usually not required where strictly necessary.
Preferences	Remembering language, interface preferences, display preferences, and similar settings.	May depend on jurisdiction.
Analytics	Understanding Website usage, performance, errors, and user experience.	Often required unless configured as strictly necessary or exempt.
Marketing	Campaign measurement, remarketing, cross-site tracking, or promotional analytics.	Required where used.
Third-party	Embedded tools, analytics, security, support, wallet connection, or infrastructure integrations.	Depends on function and jurisdiction.

You may manage cookies through your browser settings or, where available, the Definica cookie consent tool. Disabling certain cookies may affect Website or dApp functionality.

Definica may publish a current cookie list identifying actual cookies, providers, purposes, duration, and consent categories used on definica.com.

9. Wallet Connections

Connecting a wallet may reveal your public wallet address, selected token balances, protocol positions, transaction history, and other public blockchain data to Definica, wallet connection providers, RPC providers, or other infrastructure providers used by the interface.

Connecting a wallet does not give Definica access to your private keys and does not allow Definica to execute transactions without your wallet signature. You should carefully review every signature request and transaction before approving it.

Definica is not responsible for transactions signed through phishing sites, fake front-ends, malicious browser extensions, compromised devices, malware, unauthorized wallet access, or third-party wallet provider failures.

10. How We Share Information

Definica may share information with the following categories of recipients where appropriate:

- hosting providers, CDN providers, and infrastructure providers;
- analytics, diagnostics, monitoring, and performance providers;
- security, fraud prevention, blockchain analytics, and compliance providers;

- wallet connection providers, RPC providers, indexers, and block explorers;
- email, newsletter, helpdesk, and communication providers;
- legal, tax, accounting, audit, and professional advisers;
- authorized DAO contributors, operators, moderators, or service providers who need access for defined tasks;
- government authorities, courts, regulators, law enforcement, or other third parties where required by law or necessary to protect rights;
- entities involved in reorganization, rebranding, DAO wrapper formation, merger, acquisition, treasury restructuring, or similar organizational changes.

Definica does not sell personal data in the traditional sense. If Definica later uses tools that constitute sale or sharing under applicable privacy laws, Definica will update this Privacy Policy and provide any required opt-out mechanism.

11. International Transfers

Definica operates in a global Web3 environment. Information may be processed in countries other than the country where you are located. Service providers, contributors, infrastructure providers, and blockchain participants may be located worldwide.

Where required by applicable law, Definica will use appropriate transfer safeguards, such as standard contractual clauses, adequacy decisions, data processing agreements, or other lawful transfer mechanisms.

Public blockchain data is globally accessible and may be processed by independent third parties around the world.

12. Data Retention

Definica retains personal data only for as long as necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law, compliance needs, security, audits, dispute resolution, or legal claims.

Data category	Indicative retention period
Contact and support communications	Up to 24 months after the last communication, unless longer retention is needed for legal, security, or operational reasons.
Newsletter data	Until you unsubscribe or withdraw consent, plus a reasonable period for suppression records.
Security logs	Typically 12 to 24 months, unless needed for incident response, fraud prevention, or legal claims.
Cookie consent records	Typically 6 to 12 months or as required by applicable law or consent management settings.
Analytics data	Typically 14 to 26 months, depending on the analytics provider and configuration.
Compliance and risk records	As long as needed for legal, sanctions, fraud prevention, audit, or claims purposes.
On-chain data	Publicly available on the relevant blockchain and potentially retained indefinitely by blockchain participants and third parties.

Definica may be unable to delete, alter, or restrict public blockchain records.

13. Security

Definica uses reasonable technical and organizational measures designed to protect information, the Website, the dApp, and related infrastructure. These measures may include encryption in transit, access controls, logging, monitoring, segmentation, vendor diligence, code review, security reviews, incident response procedures, and responsible disclosure processes.

No system is completely secure. Definica cannot guarantee absolute security of information, smart contracts, interfaces, wallets, third-party systems, or blockchain infrastructure.

14. Your Privacy Rights

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

- request access to personal data;
- request correction of inaccurate personal data;
- request deletion of personal data;
- request restriction of processing;
- object to certain processing;
- request portability of personal data;
- withdraw consent where processing is based on consent;
- object to direct marketing;
- lodge a complaint with a supervisory authority.

To exercise your rights, contact privacy@definica.com. Definica may ask you to provide information needed to verify your identity, your relationship to the relevant wallet address, or your connection to the relevant communication.

Rights requests may be limited where information is public blockchain data, where Definica does not control the data, where deletion is technically impossible, or where retention is required for legal, security, fraud prevention, or claims purposes.

15. Users in the EEA, United Kingdom, and Switzerland

If you are located in the European Economic Area, the United Kingdom, or Switzerland, you may have rights under GDPR, UK GDPR, Swiss data protection law, or similar laws, where applicable.

You may contact Definica at privacy@definica.com regarding privacy questions or rights requests. You may also have the right to lodge a complaint with your local data protection authority. Definica encourages you to contact Definica first so that the matter can be reviewed and addressed where possible.

16. Users in California and Other U.S. States

If California or other U.S. state privacy laws apply, you may have additional rights, such as rights to know, access, delete, correct, opt out of certain sale or sharing activities, limit use of sensitive personal information, or appeal certain privacy decisions.

Definica does not sell personal data in the traditional sense. If Definica later uses technologies or business practices that require a Do Not Sell or Share My Personal Information link or similar mechanism, Definica will provide the required mechanism.

17. Children

Definica is not intended for children or for persons under 18 years of age. Definica does not knowingly collect personal data from children. If you believe that a child has provided personal data to Definica, contact privacy@definica.com.

18. Community Platforms and Social Media

Definica may operate or participate in social media channels, forums, chat platforms, governance forums, or community spaces. Your interactions with third-party platforms are governed by the privacy policies and terms of those platforms.

Information you post publicly in community or governance spaces may be visible to others. Do not publicly share private keys, seed phrases, sensitive personal information, identification documents, or information that you do not want to be public.

19. Third-Party Links and Integrations

The Website or dApp may contain links or integrations to third-party websites, wallets, block explorers, documentation portals, analytics tools, social media platforms, partner protocols, Aave-compatible interfaces, StakeWise-related resources, or other services.

Definica is not responsible for the privacy, security, content, or practices of third-party services. You should review their policies before using them.

20. Changes to This Privacy Policy

Definica may update this Privacy Policy from time to time. Updated versions will be posted on definica.com or another official Definica channel with a new Last Updated date.

If changes are material, Definica may provide additional notice through the Website, dApp, governance forum, newsletter, or official community channels. Continued use of Definica after publication of an updated Privacy Policy means that you have reviewed the updated version.

21. Contact

For privacy questions, rights requests, or data protection inquiries, contact Definica through the following official channels:

Purpose	Contact
Privacy	privacy@definica.com
Legal	legal@definica.com
Security	security@definica.com
Website	https://definica.com