YetiTrade Privacy and Cookie Policy

Effective date: October 22, 2026

This Privacy Policy (hereinafter referred to as the "**Policy**") is published by NEXODE SOLUTIONS DAO LLC (hereinafter referred to as the **"Operator"**). The Policy governs our privacy practices, data minimization and other instances of data processing pertaining to exclusively web-hosted user interface located at testnet.yetitrade.fi, including any associated subdomains, web applications, mobile software, application programming interfaces (hereinafter referred to as the **"Interface"**).

1. SCOPE AND APPLICABILITY

1.1. This Policy is incorporated by reference into our Terms of Service. By accessing or using the Interface, you agree to our Terms of Use.

1.2. This Policy applies exclusively to the Interface. It does not apply to, nor does it govern, the underlying decentralized exchange protocol (hereinafter referred to as the **"Protocol"**). The Protocol operates as a self-executing, permissionless, and immutable system of core smart contracts deployed on public blockchain networks (including, but not limited to, the Whitechain L2 rollup). The Interface functions solely as a graphical utility and routing mechanism that visualizes public blockchain data and assists individuals (hereinafter referred to as the **"User"**) in preparing cryptographic messages.

1.3. This Policy does not apply to third-party interfaces, aggregators, node providers, or non-custodial wallet applications that integrate or route traffic to the Protocol independently.

1.4. The Infrastructure architecture is entirely non-custodial. The operator does not collect, process, retain or intercept any private keys, seed phrases, mnemonic passwords, or raw cryptographic signatures. The User at all times retains full control over their data and digital assets.

1.5. The Interface does not require creation of personal accounts. To utilize the Interface for its primary decentralized trading functionalities, the User is not required to provide, and the Operator does not intentionally collect, process, solicit, or retain traditional Personally Identifiable Information (hereinafter referred to as the **"PII"**) such as real names, postal addresses, email addresses, phone numbers, or government-issued identification. However, Users who voluntarily engage with secondary off-chain services, such as feedbacks, developer portals, token listing applications, or support channels, may be required to provide contact information (e.g., email addresses or user handles). For API key requesters, personal data including email address, project name, and project type are collected and stored in connection with the generated key.

2. CATEGORIES OF INFORMATION PROCESSED

Data collected	**Purpose for collecting**	**Legal basis**	**Retention Period**
Publicly available blockchain data: *Public cryptographic*	To interact with public blockchain networks to read and display token balances, positions, and historical	**Performance of a Contract. (Article 6(1)(b) GDPR)**	**Indefinitely** On-chain transaction records remain permanently recorded

*wallet address (hereinafter referred to as the **"Public Address"**), token balances, positions, and historical transaction data.*	transaction data associated with your Public Address on the Interface.	*Necessary to deliver the core requested functionality of the Interface.*	on public blockchains outside the Operator's control.
Infrastructure data *Technical network data, including IP addresses, derived coarse geographic location, browser type, device metadata, and operating system.*	To secure the Interface against malicious activity (e.g., DDoS attacks) and enable web routing via infrastructure providers. (Note: The Operator does not correlate IP addresses with Public Addresses).	**Legitimate Interest. (Article 6(1)(f) GDPR)** N*ecessary to ensure network security, technical stability, API rate-limiting, and platform integrity.*	**Indefinitely**
Local storage data *Client-side 'localStorage' (connected wallet state, custom token imports, interface theme, and slippage tolerance settings).*	To ensure basic functionality and preserve user preferences across sessions. (Data remains on your local device and is not transmitted to our servers).	**Performance of a Contract (Article 6(1)(b) GDPR)** *Necessary to provide a seamless UI and remembering user-defined technical parameters.*	**User-Controlled**
Product analytics *Aggregated, pseudonymous usage analytics and technical error logs (interface interactions and performance metrics).*	To diagnose technical bugs and optimize the user experience. (Technical metadata, including IP addresses, may be collected by third-party analytics providers via cookie IDs. The data is segregated and never	**Legitimate Interest (Article 6(1)(f) GDPR)** *Necessary for service optimization and technical diagnostics.*	**Up to 14 Months**

	linked to Public Addresses or on-chain transactions data).		
Voluntarily Provided Data *Contact information (e.g., email addresses)* *Project name, project type*	To issue and manage API keys, to provide feedback, user support.	**Consent (Art. 6(1)(a) GDPR) & Performance of a Contract (Article 6(1)(b) GDPR).**	**Variable** For API key management: data is retained for the duration of the active API key, and for up to 12 months after the key is revoked (for security auditing and abuse prevention). For other cases, retained until the User withdraws consent or as otherwise required by law.

3. COOKIES

3.1. The Interface utilizes cookies and similar client-side tracking technologies to provide services, remember user preferences, collect aggregated performance metrics, and enhance services.

3.2. We utilize a cookie consent banner to respect your privacy preferences. On Infrastructure, these technologies are categorized as follows:

Strictly Necessary – required for the operation, technical routing, and security of the Interface. Always on and cannot be toggled off without disrupting Interface access;

Functional – preserves user-defined technical parameters across sessions to enhance interface usability. Stored within your client browser (localStorage).

Analytical – measures Interface performance, diagnoses technical errors. Are processed in aggregate using pseudonymous identifiers (cookie IDs). Wallet addresses, amounts and recipients are never sent to analytics and not correlated with Public Addresses.

The Operator does not place marketing or behavioral advertising cookies on the Interface domain.

3.3. Cookies include:

Name	Service	Type	Category	Purpose	Retention

yetitrade_cc_settings	yetiTrade (cookie banner)	Cookie	Strictly necessary	Stores the visitor's cookie consent choice: accepted categories, time, and consent ID.	~182 days
_ga	Google Analytics 4	Cookie	Analytics	Distinguishes visitors with a random client ID.	2 years
_ga_<STREAM_ID>	Google Analytics 4	Cookie	Analytics	Keeps the session state for the yetiTrade data stream.	2 years
yetitrade.swap-settings	yetiTrade	Local storage	Functional	Remembers swap settings between visits (slippage mode, slippage tolerance, transaction deadline). Contains no wallet address or personal data.	Until cleared
WALLETCONNECT_DEEPLINK_CHOICE	WalletConnect (Reown)	Local storage	Strictly necessary	Pairing and session data when a wallet connects through WalletConnect.	Until cleared
base-acc-sdk.store	Base Account SDK	Local storage	Strictly necessary	Library start-up state, only if this wallet is used.	Until cleared
ph_<PROJECT_KEY>_posthog	PostHog	Local storage	Analytics	Random visitor ID, session ID, and event properties.	Until cleared or consent withdrawn
__ph_opt_in_out_<PROJECT_KEY>	PostHog	Local storage	Analytics	Records that the visitor withdrew Analytics consent, so the choice is respected on the next visit.	Until cleared

3.5. Except for strictly necessary technical scripts, you may manage your cookies by clicking the "Manage cookie preferences" link located in the footer of the Interface.

Additionally, you manage or block cookies and local storage directly through your browser settings by:

- By clearing your browser cache and localStorage, which will reset all interface preferences and disconnect your wallet from the session, or
- Blocking third-party analytics scripts or utilizing privacy-focused browser extensions (e.g., ad-blockers, script-blockers), which will not impact your ability to connect your wallet or execute on-chain swaps through the Interface.

4. THIRD-PARTY INFRASTRUCTURE

4.1. The Interface utilizes third-party service providers to ensure the secure and compliant routing of blockchain interactions. The Operator executes strict data processing agreements (where applicable) ensuring these third parties are legally restricted from utilizing the routed data for their independent commercial benefit.

4.2. The Interface incorporates edge computing providers to deliver content and defend against advanced cyberattacks. The reverse proxy architecture ensures these providers act merely as transient network conduits.

4.4. The Interface links to and interacts with independent third-party services that are not operated or controlled by the Operator. These include non-custodial wallet software providers, public blockchain RPC node providers, Layer-2 sequencers, block explorers, and external market pricing indexers. The Operator bears no responsibility or liability for the data processing practices or performance of such third-party services, which are governed by their respective terms and privacy policies.

4.4.1. When you view balances or configure transactions through the Interface, your browser or connected digital wallet executes read calls to public or third-party Remote Procedure Call (RPC) nodes via the Operator's proxy infrastructure. The Operator does not log, or aggregate your IP address with your Public Address during RPC calls. Your interactions with RPC node providers are governed strictly by their respective independent privacy notices.

4.4.2. To establish cryptographic communication with your non-custodial wallet, the Interface integrates open-source connection protocols and third-party software development kits. Establishing a session may transmit ephemeral network connection parameters directly to these relayers to facilitate Web3 socket handshakes, operating independently of the Operator's infrastructure.

4.5. The Operator may disclose relevant technical metadata or interaction records to competent judicial, administrative, or regulatory authorities where required to satisfy mandatory legal obligations, comply with valid legal process, or protect the integrity and security of the Interface.

4.6. The Interface fetches token metadata, visual icons, and market price charts via direct client-side API calls to third-party data indexers and content delivery networks. Loading these visual assets may expose your transient IP address to third-party asset hosts purely for rendering media within your browser session.

4.7. We share necessary data, or facilitate direct connections, with the following partners to run the Interface:

Third-Party Partner	Purpose / Function
Cloudflare	To provide DNS routing and edge security protection for our API.
AWS CloudFront	To act as a Content Delivery Network (CDN) for hosting.
Reown (WalletConnect), Coinbase	To facilitate secure session connections with your non-custodial wallet. For Coinbase, transferred outside EEA under 4.1
Google Analytics, PostHog	To analyze Interface usage, optimize user flows, and diagnose technical performance. Transferred outside EEA under 4.1.
Typeform	To securely process API key request forms.
1Password	To authenticate and securely deliver API keys.
Slack	To route internal technical alerts and user support notifications.

5. DATA SUBJECT RIGHTS

5.1. In accordance with Chapter III of Regulation (EU) 2016/679 (GDPR) and corresponding global privacy legislation, Users residing in applicable jurisdictions are granted statutory rights regarding their personal data, including:

- Right of Access (Article 15 GDPR): The right to obtain confirmation as to whether personal data concerning you is being processed and receive a copy of such off-chain data.
- Right to Rectification (Article 16 GDPR): The right to request the correction or completion of inaccurate off-chain personal data.
- Right to Erasure (Article 17 GDPR): The right to request the deletion of off-chain personal data held on Operator-controlled infrastructure.
- Right to Restriction of Processing (Article 18 GDPR): The right to request the restriction of processing of off-chain personal data under statutory conditions.
- Right to Data Portability (Article 20 GDPR): The right to receive off-chain personal data provided to the Operator in a structured, commonly used, and machine-readable format.
- Right to Object (Article 21 GDPR): The right to object at any time to the processing of personal data based on legitimate interests (Article 6(1)(f) GDPR).
- Right to Lodge a Complaint (Article 77 GDPR): The right to lodge a complaint with a competent Supervisory Authority, in particular in the EU Member State of your habitual residence, place of work, or place of the alleged infringement.

5.2. Under GDPR Article 17, data subjects possess the right to request the deletion of personal data. The Operator will comply with all valid erasure requests pertaining to any off-chain data stored on servers physically or virtually controlled by the Operator. However, the Operator disclaims any technical or legal

ability to enforce the right to erasure, the right to rectification of processing upon data that has been broadcasted to a public blockchain network pursuant to GDPR Article 17(3)(b), (e).

5.4. The User interacting with the Interface must independently acknowledge the immutable, permanent, public, and transparent nature of cryptographic blockchain technology before initiating any transaction. On-chain data is technically exempt from traditional centralized compliance capabilities.

6. INTERNATIONAL DATA TRANSFERS

6.1. The Interface is deployed as a globally accessible infrastructure. By accessing the Interface, the User acknowledges that any transient off-chain technical data routed through the reverse proxy network may be transmitted to servers located in the United States or other global jurisdictions that may not provide the exact statutory equivalents of data protection found in the country of residence of the User.

6.2. Where the Operator engages in international transfers of data originating from the EEA or the UK, such transfers are safeguarded by the EU-US Data Privacy Framework (DPF) or Standard Contractual Clauses (SCCs) approved by the European Commission.

7. SECURITY AND DATA RETENTION

7.1. The Operator implements commercially reasonable, industry-standard administrative, technical, and physical safeguards designed to protect the integrity of the Interface. This includes encrypted transit protocols (HTTPS) and edge-layer security routing. However, the Operator does not control the security of the personal hardware, local network, operating system, or non-custodial wallet application utilized by the User. The User bears sole responsibility for securing their cryptographic private keys and mnemonic phrases.

7.2. The Operator adheres to a strict policy of non-retention for transient data. Public Addresses screened for compliance purposes are evaluated asynchronously in real-time; the Operator does not maintain historical, localized databases of a transaction history beyond what is required to render the active session on the Interface.

8. AUTOMATED DECISION-MAKING AND PROFILING

8.1. Pursuant to Article 13(2)(f) and Article 22 of the GDPR, the Operator does not engage in automated decision-making or profiling that produces legal effects concerning Users or similarly significantly affects them.

8.2. Automated screening checks performed by third-party blockchain analytics providers upon wallet connection are strictly limited to technical cross-referencing of Public Addresses against static sanctions lists and threat intelligence databases for risk defense and security routing. Such screening does not involve behavioral profiling, credit scoring, or automated contract execution decisions.

9. CHILDREN'S PRIVACY

9.1. The Interface is strictly intended for adult users and is not directed to or intended to attract individuals under eighteen (18) years of age (or the legal age of digital consent in your jurisdiction).

9.2. The Operator does not knowingly solicit, collect, process, or maintain personal data from children under 18 years of age (or under 13/16 years of age under applicable U.S. and EU statutory frameworks). If the Operator discovers or is notified that personal data of a child has been unintentionally collected off-chain, the Operator will promptly delete such data from its systems.

10. POLICY MODIFICATIONS AND CONTACT INFORMATION

10.1. The Operator reserves the right, at its sole discretion, to modify or update this Policy at any time to reflect changes in global regulatory frameworks or technological updates. All modifications will be updated on this page with a revised "Last Updated" date. Continued use of the Interface following such updates constitutes acknowledgment of the revised Policy.

10.2. For any queries pertaining to this Policy, please contact us at info@nexodedao.com.