# TENDY

# PRIVACY POLICY

*Last Updated: 22 April 2026*

This Privacy Policy ("Policy") explains how Tendy LLC, a limited liability company incorporated under the laws of the Cayman Islands ("Tendy", "we", "us", or "our"), processes information relating to identifiable individuals ("personal data") in connection with the Tendy user interface, including our website, web app, Telegram-based experiences, and any related interfaces, features, and support channels (collectively, the "Interface"). We aim to collect and process only the minimum personal data necessary to operate, secure, and improve the Interface, and to comply with applicable law.

Tendy is a non-custodial software interface. We do not custody, hold, control, or have access to your private keys, seed phrase, or digital assets. This Policy covers data we process at the Interface layer (such as device/session data, account identifiers, support communications, and access-control signals). Blockchain transactions and public on-chain activity are recorded on public networks and are not controlled by us. Third-party services that are part of or linked to the Interface (including Hyperliquid, Telegram, and blockchain networks) may process data under their own terms and policies.

## 1. Who We Are (Controller)

For purposes of applicable data protection laws, Tendy LLC is the controller of the personal data we process under this Policy, unless we explicitly state otherwise for a specific processing activity. Third-party service providers may process personal data on our behalf as processors (or equivalent roles) under appropriate contractual safeguards.

Contact details are provided in Section 14 (Contact). Nothing in this Policy is intended to exclude or limit any mandatory rights you may have under applicable data protection laws.

## 2. Scope

This Policy applies to personal data processed when you: (i) access, visit, or use the Interface; (ii) create, enable, or use a wallet generated locally on your device through the Interface (an "In-App Wallet") and/or, where supported, connect a third-party wallet; (iii) authenticate (for example via email, Telegram, or other identity methods made available in the Interface); (iv) interact with features such as analytics, leaderboards, programs, demos, or notifications; (v) contact us for support or send us communications; or (vi) otherwise interact with us in connection with Tendy. Any In-App Wallet key generation and transaction signing occur locally on your device, and we do not receive, store, or have access to your private keys or seed phrase.

Third-party services (for example decentralized protocols such as Hyperliquid, data providers, payment processors, and infrastructure providers integrated with the Interface) operate independently. Their privacy practices are governed by their own policies and terms.

## 3. Personal Data We Collect

We aim to collect the minimum data needed to operate, secure, and improve the Interface. Depending on how you use Tendy, we may collect:

### 3.1 Information you provide

- In-App Wallet public address(es) and related public identifiers generated locally on your device and used within the Interface (for example, an address used to authenticate a session or to display account activity). Where the Interface supports third-party wallet connections, we may also

process the public address(es) you choose to connect. We do not collect, store, or have access to private keys or seed phrases.

- Authentication identifiers, such as an email address, Telegram username, Telegram user ID, or similar identifiers used for login, account access, or recovery (if applicable).
- Communications and support data, including the content of messages you send to us and associated contact information.
- Preferences and settings you configure in the Interface (for example notification preferences, display settings, risk-mode toggles, or other feature settings).
- Program participation data, including referral codes, eligibility information, and related identifiers used to administer referrals, rewards, leaderboards, or similar programs and to detect abuse or circumvention.

### 3.2 Information we collect automatically

- Device and technical data, such as device type, operating system, app/web version, browser type, language, and user-agent.
- Log and usage data, such as timestamps, pages/screens viewed, feature usage, clicks/taps, error logs, crash reports, and diagnostic events.
- Network data, such as IP address and approximate location derived from IP (for example for security, fraud prevention, and geo-restriction controls).
- Cookies and similar technologies (for web experiences), as described in Section 10 (Cookies and Similar Technologies).

### 3.3 On-chain and transactional data

If you use the Interface to initiate interactions with third-party services (including Hyperliquid), you may generate transaction-related information (for example transaction hashes, protocol interactions, orders, fills, positions, and other activity). We may display, cache, index, or otherwise process limited transaction-related information to provide the Interface experience (for example, showing activity history, positions, or performance views). Public blockchain data is generally visible to anyone and is processed by networks and third parties outside our control.

## 4. Why We Use Personal Data

We use personal data for the following purposes:

- To provide and operate the Interface, including enabling access, maintaining sessions, and delivering requested features.
- To secure the Interface and prevent abuse, including detecting fraud, account compromise, suspicious activity, and enforcing our Terms of Use.
- To apply and enforce jurisdictional restrictions and sanctions controls (for example, geo-blocking and other risk-based controls intended to restrict access by Restricted Persons), where reasonably necessary and proportionate. We do not conduct full KYC/AML unless explicitly stated in the Interface.
- To support users, respond to inquiries, and provide operational communications (for example, security alerts, account-related messages, and service notices).
- To improve, debug, and develop the Interface, including analytics, testing, and internal research.
- To administer rewards, referral programs, or incentive features, including abuse prevention, fraud detection, and verification of eligibility where applicable.

- To send notifications via Telegram or other channels, including service and product updates, and (where permitted by applicable law) marketing communications, in accordance with your choices, preferences, and any required opt-in/opt-out mechanisms.
- To comply with legal obligations and to protect our rights, users, and the Interface (including responding to lawful requests and enforcing claims).

**5. Legal Bases for Processing Personal Data**

Where applicable data protection laws require a legal basis for processing, we rely on one or more of the following bases (or their equivalents):

Performance of a contract. We generally process personal data where such processing is necessary to perform our contract with you under our Terms of Use. For example, we process certain data to enable your access to and use of the Interface, to maintain sessions, to provide requested features, and to facilitate your interactions with third-party services through the Interface. We may also process certain information to apply and enforce access restrictions and risk-based controls, which is necessary to provide the Interface responsibly and to reduce legal, security, and compliance risks.

Consent. Where required by applicable law, and with your consent, we may use certain data (including usage and device data) to tailor features and content, to remember preferences, and to present the Interface in the most effective manner for your device. We may also use consent-based analytics to better understand user experience and improve the Interface. You may withdraw consent at any time (this does not affect processing before withdrawal).

Legitimate interests. We may process personal data in our legitimate interests to operate, secure, and maintain the Interface, including to prevent fraud and abuse, detect and investigate suspicious activity, protect accounts and Interface security, conduct troubleshooting, perform testing and research, maintain system stability, and carry out internal analytics and statistical analysis to optimize, improve, and develop the Interface. We take steps intended to ensure that such processing is proportionate and appropriately balanced against your rights and interests.

Legal obligations. We may process your information as necessary to comply with applicable legal obligations and lawful requests, to enforce our Terms of Use and other applicable policies, and to protect or defend the Interface, our rights, and the rights and safety of our users or others.

**6. Sharing of Personal Data**

In certain circumstances, we may share your personal data with third parties with your consent, as necessary to provide the Interface, or as otherwise required or permitted by applicable law, including (without limitation) the following categories of recipients:

Service providers and processors. We may share personal data with third parties that process data on our behalf in order to operate, secure, support, and improve the Interface. These may include, for example, infrastructure and hosting providers, security and fraud-prevention vendors, analytics and product telemetry providers, customer support tools, communications providers, and contractors assisting with development, debugging, and maintenance. Where you use Telegram-based features, relevant Telegram-related infrastructure may also process certain identifiers and message-routing data as part of delivering those features.

Screening and compliance vendors. Where used, we may share certain data with screening, risk, and compliance vendors to help apply access restrictions and risk controls (for example sanctions screening, fraud detection, abuse prevention, and geo-restriction controls). Such providers may assist with functions such as IP-based geo-blocking and security analytics.

Third-party services. The Interface enables user-initiated interaction with independent third-party services (including Hyperliquid and other decentralized protocols, data providers, payment processors, and infrastructure providers). When you choose to use or interact with such services through the Interface, those third parties may process data under their own terms and policies. We do not control their privacy practices, and you are responsible for reviewing their policies.

Professional advisors. We may share personal data with our professional advisors (such as lawyers, auditors, accountants, and consultants) where necessary in our legitimate interests or to comply with legal obligations.

Authorities and law enforcement. We may disclose personal data to authorities, regulators, courts, law enforcement, or other third parties where we believe disclosure is necessary or appropriate to: (i) comply with applicable law, lawful requests, or legal process; (ii) enforce our Terms of Use and other policies; (iii) investigate, prevent, or take action regarding suspected or actual fraud, security incidents, abuse, or unlawful activity; or (iv) protect the rights, property, and safety of the Interface, our users, or others.

Corporate transactions. We may share personal data in connection with a corporate transaction, such as a merger, acquisition, reorganization, financing, or sale of assets, including during due diligence and as part of any transfer to a successor entity, subject to appropriate safeguards.

International transfers. Your personal data may be transferred to, stored in, or otherwise processed in countries other than the country where you live, including in locations where our service providers or partners operate. Where required by applicable law, we will take steps designed to ensure that such transfers are subject to appropriate safeguards and that your personal data remains protected in accordance with this Policy.

## 7. Retention

We retain personal data only for as long as necessary to fulfill the purposes described in this Policy, including to comply with legal, accounting, and reporting obligations; to resolve disputes; to enforce agreements; and to maintain security and fraud-prevention controls. Retention periods vary depending on the type of data and why we process it. We may retain and use aggregated or de-identified information for longer periods where permitted by law.

## 8. Your Rights and Choices

Depending on your location and applicable data protection laws, you may have certain rights regarding your personal data, including:

- Access: request information about the personal data we hold about you.
- Correction: request correction of inaccurate or incomplete personal data.
- Deletion (erasure): request deletion of personal data in certain circumstances.
- Objection / cease processing: object to or require us to cease processing in certain circumstances (for example processing based on legitimate interests, or for direct marketing).
- Restriction: request that we restrict processing in certain circumstances.
- Portability: request a copy of certain personal data in a structured, commonly used, machine-readable format, where applicable.
- Rights in relation to automated decision-making: where applicable, request information about and, where applicable, request human review of automated decisions.
- Withdraw consent: where we process based on consent, you may withdraw consent at any time (this does not affect processing before withdrawal).

To exercise your rights, contact us using the details in Section 14. We may need to verify your identity before responding. Some rights are subject to limitations and exceptions under applicable law.

### 9. Marketing and Notifications

If you receive marketing communications or Telegram-based notifications, you can opt out by using in-product controls, adjusting Telegram notification settings, or contacting us. We may still send important service-related messages (for example security notices or major service changes). For further details, please see our Marketing Consent & Notifications Policy.

### 10. Cookies and Similar Technologies

For web-based experiences, we may use cookies or similar technologies to operate the Interface, help keep you signed in, remember preferences, and support security and analytics. Some cookies are strictly necessary for the Interface to function. Where required by law, we will request your consent for non-essential cookies and provide choices. You can also control cookies through your browser settings, though disabling certain cookies may impact functionality.

### 11. Security

We implement reasonable administrative, technical, and organizational measures designed to protect personal data. However, no security measures are perfect, and we cannot guarantee absolute security. You are responsible for securing your device(s), credentials, and any wallet keys. Because Tendy is non-custodial, we cannot recover private keys or reverse protocol-level actions.

### 12. Children's Privacy

The Interface is not intended for individuals under 18 years of age (or the age of majority in your jurisdiction). We do not knowingly collect personal data from children. If we become aware that we have collected personal data from a child, we will take reasonable steps to delete it.

### 13. Third-Party Links and Services

The Interface may link to or integrate third-party services (including Hyperliquid and other decentralized protocols, payment processors, data providers, messaging platforms such as Telegram, and social platforms). We do not control how third parties process personal data. If you choose to use such services, review their privacy policies and terms.

### 14. Contact

For questions, requests, or complaints about this Policy or our data practices, contact:

**Tendy LLC**

Email: contact@tendy.me

### 15. Changes to This Policy

We may update this Policy from time to time. If we make material changes, we will update the "Last Updated" date at the top of this Policy and, where required by applicable law, provide additional notice. Changes apply from the effective date of the updated Policy.