

DYNK.io

Privacy Policy

Effective Date: May 2026

DYNK.io (“dynk.io,” “we,” “our,” or “us”) operates a non-custodial NFT wallet marketplace on Solana. This Privacy Policy explains how we collect, use, store, share, and protect information about you when you use our website, web application, mobile application, and related services (collectively, the “Services”).

By accessing or using the Services, you agree to the practices described in this Privacy Policy. If you do not agree, please do not use the Services.

A note on blockchain data: Certain information — including wallet addresses, NFT ownership records, transaction amounts, and smart contract interactions — is recorded on the Solana blockchain. Blockchain records are public, permanent, and cannot be deleted or altered by dynk.io or anyone else.

1. Information We Collect

1.1 Information You Provide Directly

- **Email address:** required to create an account, receive one-time passcodes (OTP), and communicate with you.
- **Password:** stored as a salted bcrypt hash — your plaintext password is never stored.
- **MPIN:** a numeric PIN used for in-app authentication, stored as a hash.
- **Profile information:** display name or other optional profile details you choose to provide.
- **Referral codes:** if you participate in our referral programme, your referral relationships are recorded.

1.2 Authentication Credentials

- **Social sign-in (Google, Facebook, Apple):** when you sign in via a social provider, we receive an identity token and basic profile information (name, email) from that provider via Firebase Authentication. We do not receive or store your social media password.
- **Passkeys / WebAuthn:** if you register a passkey, we store only the credential ID and public key on our servers. The private key never leaves your device.
- **Biometric authentication:** Face ID and Touch ID checks are handled entirely on your device by the operating system. We do not receive or store biometric data.

1.3 Wallet and Blockchain Data

When you use the Services, we create and manage multi-chain wallets on your behalf through web3Auth, a third-party managed wallet provider. The following information is associated with your account:

- **Wallet addresses:** Solana, Ethereum, Polygon, and BNB Smart Chain wallet addresses assigned to your account and embedded in your NFT metadata.
- **NFT ownership records:** which NFT wallets you own, their metadata, pre-loaded balances, and listing history.
- **Transaction history:** on-platform transactions including NFT purchases, sales, auction bids, token transfers, and exchange orders.
- **Exchange orders:** sell orders you create (DYNK amount, minimum SOL price, expiry). Buy orders from other chains are identified by an anonymised identity hash, not your personal identity.
- **On-chain activity:** we receive webhook notifications from Helius and Alchemy about on-chain events related to your wallets and NFTs. This data is public on the Solana blockchain.

1.4 Information Collected Automatically

- **Log data:** IP address, browser type, operating system, pages visited, timestamps, and HTTP request metadata collected by our servers.
- **Device information:** device model, OS version, app version, and unique device identifiers collected by the mobile app.
- **Session data:** JWT session tokens used to maintain your login state.
- **Push notification tokens:** Firebase Cloud Messaging tokens used to send push notifications to your device.
- **Cookies and local storage:** we use browser local storage to maintain your authenticated session on the web app. We do not use third-party advertising cookies.

1.5 Files You Upload

If you upload files through the Services (for example, a profile image), these are stored in AWS S3. We retain these files for as long as your account is active or as necessary to provide the Services.

2. How We Use Your Information

We use the information we collect for the following purposes:

- **Providing the Services:** creating and managing your account, operating NFT wallet minting and marketplace functions, processing exchange orders, and facilitating token purchases.
- **Authentication and security:** verifying your identity via email OTP, social sign-in, passkeys, MPIN, and biometrics; detecting and preventing fraud and abuse.
- **Wallet management:** creating and maintaining your multi-chain wallets; displaying balances and transaction history.
- **Gasless transactions:** sponsoring Solana transaction fees on your behalf for certain operations (relist, delist, auction, bid).
- **Order settlement:** matching and settling exchange orders between buyers and sellers using our settlement authority service.

- **Auction management:** running timed auctions, tracking bids, and notifying participants of outcomes.
- **Communications:** sending email OTP codes, account notifications, auction alerts, order updates, and service announcements. We do not send marketing emails without your explicit consent.
- **Push notifications:** sending real-time alerts about your NFTs, bids, orders, and wallet activity via Firebase Cloud Messaging.
- **Customer support:** responding to your support requests and enquiries.
- **Referral programme:** tracking referral relationships and attributing referral rewards.
- **Legal compliance:** complying with applicable laws, regulations, and court orders; responding to lawful requests from authorities.
- **Service improvement:** analysing aggregated, anonymised usage data to improve the Services.

3. How We Share Your Information

We do not sell your personal information. We share your information only in the circumstances described below.

3.1 Third-Party Service Providers

- **Firebase (Google):** social authentication and push notifications. See Google's privacy policy at policies.google.com.
- **AWS (Amazon Web Services):** cloud hosting (EC2), file storage (S3), and cryptographic key management (KMS). Our infrastructure runs on AWS in the EU (Stockholm) region.
- **Helius / Alchemy:** Solana blockchain indexing and webhook delivery for on-chain event monitoring.
- **Metaplex:** NFT metadata standard. NFT metadata URIs point to publicly accessible JSON stored off-chain.

3.2 Public Blockchain

Wallet addresses, NFT ownership, transaction amounts, and all smart contract interactions are recorded on the Solana blockchain (currently devnet; mainnet on launch). This data is public, permanent, and visible to anyone. We have no ability to delete or modify on-chain data.

3.3 Legal Requirements

We may disclose your information if required to do so by law, or in the good-faith belief that disclosure is necessary to comply with a legal obligation, protect our rights or property, prevent fraud, or protect the safety of our users or the public.

3.4 Business Transfers

If dynk.io is involved in a merger, acquisition, or sale of assets, your information may be transferred as part of that transaction. We will notify you before your information is transferred and becomes subject to a different privacy policy.

4. Blockchain Data and Immutability

The following data is written to the Solana blockchain when you use the Services and cannot be deleted:

- NFT mint addresses, ownership transfers, listing and sale events
- Exchange sell orders, settlement records, and MatchNonce accounts
- Token transfer events
- Auction creation, bid, and settlement events

Because blockchain data is public and permanent, we recommend you consider this before engaging in any on-chain activity. Your email address and off-chain account data are not written to the blockchain.

5. Data Retention

- **Account data (email, password hash, MPIN hash):** retained for the life of your account. Deleted within 30 days of a verified account deletion request, subject to legal hold obligations.
- **Transaction history:** retained indefinitely to support dispute resolution, regulatory compliance, and audit trails. On-chain records are permanent regardless.
- **Log data and IP addresses:** retained for up to 90 days for security monitoring and debugging.
- **Push notification tokens:** retained until you log out, uninstall the app, or revoke notification permissions.
- **Uploaded files (AWS S3):** retained for the life of your account. Deleted within 30 days of account deletion.
- **Support messages:** retained for up to 2 years for quality assurance and dispute resolution.
- **Social auth tokens:** stored only for the duration of your session; not persisted server-side.

6. Security

We take security seriously and implement the following measures:

- Passwords and MPINs are stored as salted bcrypt hashes — never in plaintext
- Cryptographic private keys for managed wallets are handled by AWS KMS and Web3auth — dynk.io staff cannot access your private keys directly
- All data in transit is encrypted via HTTPS/TLS
- JWT tokens are used for session authentication with short expiry windows
- The exchange settlement authority key is a separate, limited-permission backend key distinct from administrative credentials
- Two-factor authentication (email OTP) is required for sensitive account actions

- Passkey / WebAuthn authentication provides phishing-resistant login on supported devices

Despite these measures, no system is completely secure. We cannot guarantee absolute security of your information. If you believe your account has been compromised, contact us immediately at contact@dynk.io.

7. Your Rights

Depending on your location, you may have the following rights regarding your personal information:

- **Access:** request a copy of the personal information we hold about you.
- **Correction:** request correction of inaccurate or incomplete information.
- **Deletion:** request deletion of your account and associated off-chain personal data (subject to legal hold obligations and the permanent nature of on-chain data).
- **Portability:** request your personal data in a structured, machine-readable format.
- **Objection:** object to processing of your personal data in certain circumstances.
- **Withdrawal of consent:** where processing is based on consent (e.g. marketing communications), withdraw consent at any time without affecting prior processing.
- **Complaints:** lodge a complaint with your local data protection authority.

To exercise any of these rights, contact us at contact@dynk.io. We will respond within 30 days.

8. Children's Privacy

The Services are not directed to children under the age of 18. We do not knowingly collect personal information from anyone under 18. If you believe we have inadvertently collected information from a minor, please contact us at privacy@dynk.io and we will delete it promptly.

9. International Data Transfers

dynk.io operates infrastructure on AWS in the EU (Stockholm / eu-north-1) region. However, some third-party service providers — including Firebase — may process data in other jurisdictions. Where data is transferred outside your country of residence, we take steps to ensure appropriate safeguards are in place in accordance with applicable law.

10. Third-Party Links and Services

The Services integrate with third-party services including Firebase, and the Solana blockchain. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy policies of any third-party services you interact with through our platform.

11. Cookies and Tracking Technologies

The web application uses browser local storage to maintain your authenticated session (JWT token). We do not use third-party advertising cookies or tracking pixels, and we do not use analytics tools that share your data with advertising networks.

The mobile application uses device storage to persist your session and preferences. You can clear app data at any time through your device settings.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. When we do, we will update the effective date at the top of this document and, where changes are material, notify you by email or via an in-app notice. Your continued use of the Services after such changes constitutes acceptance of the updated policy.

13. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or your personal data, please contact us:

Email: contact@dynk.io

Website: www.dynk.io

Data controller: dynk.io

This Privacy Policy was last updated in June 2026 and applies to all users of dynk.io web, mobile, and API services.
