

ZYRO ECOSYSTEM

PRIVACY POLICY

Effective Date: September 23, 2026

Website: www.zyroecosystem.com

Version: 1.0

1. INTRODUCTION

Welcome to **ZYRO Ecosystem** ("ZYRO", "the Protocol", "the Ecosystem").

ZYRO is designed as a **decentralized, non-custodial and blockchain-based ecosystem** intended to allow users to interact directly with blockchain networks, smart contracts, decentralized applications and protocol infrastructure.

This Privacy Policy explains how privacy operates within the ZYRO Ecosystem and, importantly, the information that **ZYRO does not control or collect** as a consequence of decentralized protocol use.

ZYRO is designed around the principle:

Your wallet is yours. Your assets are yours. Your blockchain activity is yours.

ZYRO does not intend to operate a centralized user database or require users to surrender personal information merely to interact with decentralized blockchain infrastructure.

2. THE DECENTRALIZED NATURE OF ZYRO

ZYRO is designed to operate without a traditional centralized account-based architecture.

Unlike conventional platforms, ZYRO is intended to allow users to interact directly with decentralized infrastructure through:

- blockchain networks;
- smart contracts;
- decentralized applications;
- non-custodial wallets;
- decentralized exchange infrastructure;
- publicly verifiable blockchain transactions.

ZYRO does not require users to create a conventional centralized account simply to hold or interact with blockchain assets.

Where technically applicable, users interact directly with the relevant smart contracts through their own wallets.

3. NO CENTRALIZED USER DATABASE

ZYRO is designed without a centralized database containing the personal identities of all protocol users.

ZYRO does not intend to maintain a centralized profile containing information such as:

- full legal name;
- residential address;
- date of birth;
- government identification;
- bank account information;
- private keys;
- seed phrases;
- wallet passwords.

A blockchain wallet may be used to interact with the ecosystem without providing such information to the ZYRO Protocol.

4. NO MANDATORY PERSONAL IDENTIFICATION FOR PROTOCOL USE

The decentralized protocol is designed so that users can interact with blockchain infrastructure through compatible wallets.

A user may be able to:

- connect a wallet;
- view blockchain information;
- interact with smart contracts;
- transfer supported digital assets;
- interact with decentralized applications;
- use decentralized exchange functionality;

without creating a conventional identity-based account with ZYRO.

However, certain **third-party services** connected to the ecosystem may legally require identity verification.

Such requirements are imposed by the relevant service provider or applicable law and are not necessarily requirements of the decentralized ZYRO Protocol itself.

5. WALLET ADDRESSES

When you connect a blockchain wallet to a ZYRO application, your wallet address may become visible to the application and to the relevant blockchain network.

A wallet address is generally a publicly accessible blockchain identifier.

For example:

0x1234...ABCD

may be publicly visible without revealing the user's legal name.

However, blockchain activity associated with a wallet address can potentially be analyzed or linked to an individual through external information.

Users should therefore understand that blockchain addresses are generally **pseudonymous rather than completely anonymous**.

6. PUBLIC BLOCKCHAIN INFORMATION

Blockchain networks are generally transparent by design.

When you conduct a transaction on a blockchain, information such as the following may become publicly accessible:

- wallet address;
- recipient address;
- transaction amount;
- token;
- transaction hash;
- block number;
- timestamp;
- smart-contract interaction;
- gas or network fees;
- other blockchain metadata.

ZYRO does not control the underlying public blockchain ledger.

Once a transaction has been recorded on a decentralized blockchain, it may be impossible to modify, hide, or delete that record.

7. ZYRO DOES NOT CONTROL BLOCKCHAIN DATA

ZYRO does not own or control the decentralized blockchain networks on which transactions may occur.

Blockchain data is distributed among independent network participants.

Consequently:

- ZYRO cannot guarantee blockchain privacy;
- ZYRO cannot remove blockchain transactions;
- ZYRO cannot alter blockchain records;
- ZYRO cannot erase wallet history;
- ZYRO cannot guarantee anonymity.

Users should carefully consider the information they publicly associate with their wallet addresses.

8. NON-CUSTODIAL ARCHITECTURE

ZYRO is designed around a **non-custodial model**.

This means that, where applicable, users maintain control over their own:

- private keys;
- wallet credentials;
- seed phrases;
- digital assets;
- transaction approvals.

ZYRO does not intend to take custody of users' private keys or seed phrases.

ZYRO cannot access information that is not provided to the protocol or application.

9. PRIVATE KEYS AND SEED PHRASES

ZYRO will never legitimately request your:

- private key;
- seed phrase;
- recovery phrase;
- wallet password;
- hardware-wallet PIN;
- authentication secret.

You should never provide these credentials to anyone claiming to represent ZYRO.

Anyone who obtains a private key or seed phrase may potentially gain control over the associated blockchain assets.

Protect your wallet credentials at all times.

10. SMART CONTRACT INTERACTIONS

ZYRO may use smart contracts to provide decentralized functionality.

When a user interacts with a smart contract:

1. the user's wallet initiates the transaction;
2. the user reviews the transaction;
3. the user authorizes the transaction;
4. the blockchain processes the transaction;
5. the resulting transaction becomes part of the blockchain record.

ZYRO does not have unilateral control over transactions that have been independently authorized and confirmed by the relevant blockchain network.

11. NO CENTRALIZED TRANSACTION CONTROL

ZYRO's decentralized architecture is designed so that blockchain transactions are not processed through a traditional centralized account database.

Transactions are validated according to the rules of the relevant blockchain network and smart contracts.

Accordingly, ZYRO generally cannot:

- reverse confirmed blockchain transactions;
- cancel blockchain transfers;
- recover assets sent to the wrong address;
- change blockchain ownership records;
- freeze assets solely through a centralized account system.

Users are responsible for confirming transaction details before signing.

12. INFORMATION ZYRO MAY RECEIVE TECHNICALLY

Although ZYRO does not intend to maintain a centralized identity database, certain information may technically become available when users interact with decentralized applications.

Depending on the application architecture, this may include:

- wallet address;
- blockchain network;
- transaction information;

- smart-contract interactions;
- browser information;
- device information;
- IP address;
- connection information;
- application usage information.

Some of this information may be generated automatically by web browsers, RPC providers, node providers, hosting infrastructure, analytics services or other technical components.

The availability of such information does not necessarily mean that ZYRO possesses or controls it as a centralized personal profile.

13. RPC AND INFRASTRUCTURE PROVIDERS

Decentralized applications may use blockchain infrastructure providers, including RPC endpoints, node providers or other technical infrastructure.

When a wallet or application connects to an RPC or node provider, that provider may potentially observe technical information such as:

- IP address;
- wallet address;
- requested blockchain data;
- network information;
- timestamps.

Such providers operate independently and may have their own privacy policies.

Users should review the privacy practices of infrastructure providers used by their wallets or applications.

14. WEBSITE INFORMATION

The ZYRO website may contain informational pages describing the ecosystem, blockchain infrastructure, products and developments.

Simply visiting the website may result in certain technical information being processed by standard internet infrastructure.

This may include:

- IP address;
- browser type;
- operating system;
- device information;
- requested pages;
- timestamps;
- technical error information.

Such information may be processed by hosting or infrastructure providers rather than by a centralized ZYRO user database.

15. COOKIES

The ZYRO website may use essential technical technologies required to operate the website.

ZYRO's decentralized applications should minimize unnecessary tracking technologies.

Where analytics or optional cookies are used, the relevant application or website should provide appropriate notice and controls where required by applicable law.

ZYRO's objective is to avoid unnecessary collection of user information.

16. NO SALE OF PERSONAL INFORMATION

ZYRO does not intend to sell personal information as a business model.

ZYRO is designed around decentralized protocol usage rather than the monetization of user identity information.

The protocol's objective is to provide blockchain infrastructure and decentralized functionality rather than create centralized advertising profiles of users.

17. NO CENTRALIZED USER PROFILING

ZYRO does not intend to build centralized behavioral profiles of protocol users for advertising or unrelated commercial purposes.

The protocol is designed to minimize the collection of personal information and allow users to interact through blockchain addresses rather than conventional identity profiles.

18. DECENTRALIZED EXCHANGE — HYDEX

HYDEX, as a decentralized exchange component of the ecosystem, is intended to operate through blockchain infrastructure and smart contracts.

Where HYDEX operates in a non-custodial decentralized manner:

- users connect their own wallets;
- users retain control of their assets;
- transactions are authorized by users;

- trades are executed through applicable smart contracts;
- blockchain transactions are publicly verifiable.

HYDEX does not need to maintain a conventional centralized account balance for every user where the relevant architecture is genuinely non-custodial.

19. ZYRO WALLET

The ZYRO Wallet is intended to provide users with a means of interacting with blockchain assets and decentralized applications.

Where the wallet operates as a non-custodial wallet:

- private keys remain under user control;
- ZYRO does not hold user funds;
- ZYRO does not receive users' seed phrases;
- blockchain transactions are authorized by the user.

Loss of a private key or recovery phrase may result in permanent loss of access to assets.

ZYRO cannot guarantee recovery of lost wallet credentials.

20. ZYRO PAYMENT SERVICES

Future ZYRO payment products may involve third-party infrastructure.

If a payment product is genuinely decentralized and non-custodial, blockchain transactions may occur directly between users, merchants and smart contracts.

However, certain payment infrastructure may require regulated intermediaries.

Examples may include:

- card issuers;
- banking partners;

- payment processors;
- fiat conversion providers;
- compliance providers.

Those entities may collect personal information independently.

Their privacy policies will apply to the information they collect.

21. ZYRO PAYMENT CARD

If the ZYRO Payment Card is provided through a regulated third-party issuer or payment network, the card provider may require information such as:

- identity information;
- address;
- date of birth;
- payment information;
- tax information;
- KYC documentation.

Such information may be collected directly by the relevant regulated provider.

A card issuer's collection of personal information should not be interpreted as ZYRO operating a centralized identity database for the decentralized protocol.

The applicable card provider's privacy policy will govern its processing of personal information.

22. THIRD-PARTY APPLICATIONS

ZYRO may interact with third-party applications and protocols.

These may include:

- blockchain explorers;
- wallets;
- RPC providers;
- decentralized applications;
- payment providers;
- infrastructure providers;
- analytics providers;
- exchanges;
- card providers.

Third-party services operate independently.

ZYRO does not control how independent third parties collect or process information.

Users should review the relevant third-party privacy policies before using those services.

23. DECENTRALIZED GOVERNANCE

Where governance functionality is implemented, participation may occur through blockchain-based mechanisms.

Governance participation may create publicly visible records such as:

- wallet address;
- proposal participation;
- votes;
- delegation;
- transaction records.

These records may be permanently available on the blockchain.

Users should consider this before participating in public on-chain governance.

24. DATA MINIMIZATION

ZYRO's privacy philosophy is based on **data minimization**.

The ecosystem seeks to collect or process only information reasonably necessary for:

- operating decentralized applications;
- maintaining security;
- providing technical functionality;
- complying with applicable legal obligations where relevant;
- responding to voluntary communications.

The decentralized architecture is intended to reduce unnecessary centralized collection of personal information.

25. USER RESPONSIBILITY

Users are responsible for understanding the public nature of blockchain networks.

Users should:

- protect private keys;
- protect seed phrases;
- verify wallet addresses;
- review smart-contract permissions;
- verify transaction details;
- understand blockchain transparency;
- review third-party applications;
- avoid sharing sensitive information publicly.

ZYRO cannot protect information that a user voluntarily publishes on a public blockchain or external website.

26. SECURITY

Although decentralized architecture can reduce certain forms of centralized data risk, it does not eliminate cybersecurity risks.

Users may encounter:

- phishing websites;
- malicious smart contracts;
- fake ZYRO accounts;
- fraudulent applications;
- wallet-draining attacks;
- malicious browser extensions;
- compromised devices;
- social-engineering attacks.

Users should verify that they are interacting with official ZYRO resources before signing transactions.

27. NO GUARANTEE OF ANONYMITY

ZYRO does not represent that use of the ecosystem provides complete anonymity.

Blockchain activity can potentially be analyzed using:

- public blockchain explorers;
- transaction-analysis tools;
- publicly available information;
- exchange records;
- other external datasets.

A wallet address that appears anonymous may potentially become associated with a real-world identity through information obtained elsewhere.

Users should treat blockchain activity as **public and potentially traceable**.

28. DATA RETENTION

ZYRO does not maintain a centralized database of blockchain transactions for the purpose of replacing the blockchain's public ledger.

Blockchain transaction records are maintained by the applicable decentralized network.

Because blockchain records may be immutable, information recorded on-chain may remain permanently available.

ZYRO cannot independently delete information from a decentralized blockchain network.

29. DELETION REQUESTS

Where personal information is held by a centralized service operated by or on behalf of ZYRO, applicable privacy laws may provide rights to request deletion or correction.

However, information permanently recorded on a public blockchain generally cannot be deleted by ZYRO.

For example, ZYRO cannot remove:

- confirmed blockchain transactions;
- wallet addresses appearing in blockchain records;
- token transfers;
- smart-contract interactions;
- on-chain governance votes.

This limitation is inherent to decentralized blockchain architecture.

30. INTERNATIONAL USERS

ZYRO is designed as a global blockchain ecosystem.

Users may access decentralized infrastructure from different jurisdictions.

Different countries may have different privacy, digital-asset, financial and data-protection laws.

Users are responsible for determining whether use of particular ZYRO services is permitted in their jurisdiction.

Where a third-party regulated service is involved, that provider may impose additional requirements based on the user's jurisdiction.

31. CHILDREN

ZYRO's blockchain and financial technology services are not intended for individuals who are below the minimum legal age required to use the applicable service.

Users must comply with applicable age and legal requirements in their jurisdiction.

32. PRIVACY OF THE DECENTRALIZED PROTOCOL

The fundamental privacy model of ZYRO can be summarized as follows:

Information	Centralized ZYRO Protocol
Legal name	Not required for basic protocol interaction
Residential address	Not required for basic protocol interaction
Government ID	Not required for basic protocol interaction
Bank account	Not required for basic protocol interaction

Private key	Never requested
Seed phrase	Never requested
Wallet address	May be publicly visible
Blockchain transactions	Publicly recorded
Smart-contract activity	Publicly verifiable
Blockchain balances	Generally publicly visible
On-chain governance activity	Potentially public
Third-party KYC	May apply to regulated third-party services

33. THE ZYRO PRIVACY PRINCIPLE

ZYRO's decentralized philosophy can be summarized in one principle:

Minimize centralized data. Maximize user control. Preserve blockchain transparency.

The ecosystem is designed so that users do not need to surrender their identity simply to participate in decentralized blockchain activity.

34. PRIVACY AND TRANSPARENCY

Privacy and transparency are not necessarily contradictory.

ZYRO seeks to distinguish between:

Personal Identity

Information that can identify an individual.

and

Blockchain Transparency

Information necessary for a decentralized network to verify transactions.

A blockchain can make transactions publicly verifiable without necessarily requiring the user's legal name to be published.

This is an important distinction in the ZYRO architecture.

35. CHANGES TO THIS PRIVACY POLICY

As the ZYRO ecosystem develops, the technical architecture may evolve.

New products may introduce additional privacy considerations.

ZYRO may therefore update this Privacy Policy when:

- new decentralized applications are launched;
- new infrastructure is introduced;
- legal requirements change;
- privacy practices change;
- new ecosystem functionality becomes available.

The latest version will be published through the official ZYRO website.

36. CONTACT AND COMMUNITY COMMUNICATION

Because ZYRO is designed as a decentralized ecosystem, communication may take place through public community channels.

If a user voluntarily contacts ZYRO through:

- email;
- support channels;
- community platforms;
- social media;

- governance forums;

the information voluntarily provided may be visible to or processed by the relevant platform.

Users should avoid publishing private keys, passwords, seed phrases or other confidential information in public channels.

37. NO PRIVATE KEY ACCESS

For avoidance of doubt:

ZYRO WILL NEVER ASK YOU FOR YOUR PRIVATE KEY.

ZYRO WILL NEVER ASK YOU FOR YOUR SEED PHRASE.

ZYRO WILL NEVER ASK YOU TO SEND YOUR WALLET RECOVERY PHRASE.

ZYRO WILL NEVER REQUIRE YOU TO TRANSFER ASSETS TO AN INDIVIDUAL CLAIMING TO BE A ZYRO REPRESENTATIVE.

If someone requests such information, treat the request as potentially fraudulent.

38. FINAL PRIVACY STATEMENT

ZYRO is designed as a **decentralized, non-custodial and transparent blockchain ecosystem**.

The fundamental architecture is intended to reduce dependence on centralized identity databases and allow users to interact with blockchain infrastructure through their own wallets.

ZYRO does not intend to:

- require personal identity for ordinary decentralized protocol interaction;
- custody user private keys;
- custody seed phrases;
- create centralized profiles of all blockchain users;
- sell user identity information;

- control public blockchain records.

At the same time, users should understand that decentralization does not mean complete anonymity.

Blockchain transactions are generally public, permanent and potentially traceable.

Users remain responsible for protecting their own wallet credentials and understanding the privacy implications of interacting with public blockchain networks.

39. OFFICIAL ZYRO WEBSITE

For official information, users should rely only on verified ZYRO communication channels.

Official Website: www.zyroecosystem.com

Users should independently verify URLs, smart-contract addresses and official communication channels before connecting wallets or signing transactions.

ZYRO ECOSYSTEM

DECENTRALIZED BY DESIGN

NON-CUSTODIAL BY PRINCIPLE

TRANSPARENT BY NATURE

PRIVACY CONSCIOUS BY ARCHITECTURE

Your wallet. Your keys. Your assets. Your choice.

© 2026 ZYRO Ecosystem. All rights reserved.