Privacy Policy

Inverza Smart

Risk Warning: Smart Contracts and Digital Assets
Trading with smart contracts, decentralized protocols, and digital assets carries a high level of risk due to extreme market volatility, the technical complexity of blockchain architecture, and the irreversible nature of transactions, which can result in the total loss of deposited funds. You also accept that, as there are no intermediaries or central authorities, you are solely responsible for the security of your private keys and the decisions you make; therefore, it is imperative that you fully understand the technological risks.

Version Date: October 2025

Last updated: [October 2025]

This Privacy Policy describes how Inverza Smart ("we", "the Platform") collects, uses, stores, shares and protects the personal data of Customers ("User", "you") when accessing or using the website, applications, technology services, educational tools and Smart Contract-based functionalities (the "Services").

By using the Platform, the User declares that they have read and understood this Privacy Policy and accept the processing of their data in accordance with what is established herein.

1. Identity of the Responsible Party

The Platform acts as the data controller for personal data associated with the use of the Platform, including registration, verification, fraud prevention, compliance, and support. For privacy-related inquiries, you can contact us at: operations@inverzasmart.com

2. Data We Collect

The Platform may collect personal data directly (when provided by the User), automatically (through use of the site), or indirectly (by authorized providers). This data includes:

2.1. Identification data

- Name and surname Identity document (if
- applicable) Date of birth Nationality
- Address / country of residence
-
-

2.2. Contact details

- Email address Telephone number Residential
- address (when required)
-

2.3. Verification data (KYC/AML)

- Identity and authentication tests; Facial or biometric validation (if
- applicable with an authorized provider); Risk and compliance
- information; Checks against watchlists and sanctions
-

2.4. Operational and transactional data

- Transaction history and activity within the Platform; Deposits
- and withdrawals requested; Account statement, margins and
- settlements; Information associated with executed orders
-

2.5. Technical data

- IP address, browser type and device,
- operating system, date/time of access,
- security logs and session events,
- cookies and browsing data
-
-

2.6. Datos blockchain (off-chain)

The User acknowledges that certain operations performed with Smart Contracts may generate public and immutable records, such as:

- public wallet address, transaction hash,
- timestamps, and events recorded on the
- blockchain

3. Purposes of the Processing

The Platform processes personal data for the following purposes:

- Create, manage and maintain the User account

- Execute and operate Smart Contract-based technology services; perform Know Your
- Customer (KYC) verification processes; prevent fraud, unauthorized access, and illicit
- use (AML/CFT); ensure the operational security, integrity, and traceability of the
- system; manage deposits, withdrawals, and technical validations; provide user support
- and handle complaints; comply with legal, regulatory, and audit obligations; improve
- platform performance, user experience, and technical stability; and issue operational
- communications and important notices.
-
-

4. Legal Basis for Processing

Data processing is based on:

- The provision and execution of the contract with the User, compliance with operational
- and security obligations, legitimate interests related to fraud prevention, traceability and
- continuity, User consent when required (e.g., non-essential cookies).

5. External Suppliers and Authorized Third Parties

The User agrees that the Platform may share data with external providers strictly necessary for the operation of the service, including:

- KYC verification providers, AML services and transactional
- monitoring, technology infrastructure and cybersecurity
- providers, oracles or market data providers, payment
- gateways or third-party processors
-

Secure Payments – PCI DSS

Payments made on the Platform may be processed through providers certified under international security standards (e.g., PCI DSS). The Platform does not store complete card information on its servers and limits its involvement to permitted technical processing.

6. International Transfers

Given the global nature of the Platform, data may be processed or stored on servers located outside the User's country of residence. The Platform will take reasonable measures to protect information during international transfers in accordance with recognized security practices.

7. Data Retention

Personal data will only be kept for as long as necessary to:

- To provide services, maintain security and traceability, comply with internal audit and fraud
- prevention obligations, and address legal and regulatory requirements. The User acknowledges that
- blockchain (off-chain) records are permanent in nature and independent of the Platform.
-
-

8. Information Security

The Platform applies reasonable security controls to protect personal data, including:

- encryption of communications and secure
- connections, internal access control, activity
- monitoring and fraud prevention, off-chain/off-
- chain technical validations

Site protected with SSL/TLS certificate (HTTPS)

The User acknowledges that no system can guarantee absolute security against technological risks.

9. User Rights

The User may request, as appropriate:

- access to your data
- correction or updating
- deletion where appropriate

- Portability limitation or opposition as applicable The Platform may request identity
- verification to process requests and may restrict them when there are retention or
- compliance obligations.

Cookies and Similar Technologies

The Platform may use cookies:

- Technical (necessary): for login, security and operation. Analytics: to improve performance and
- experience. The User can configure cookies from their browser or from the available
- preference system.

Communications

The Platform may send operational communications (security, changes, validations, support) to the User's registered email address or dashboard. The User is responsible for keeping their information up to date.

Minors

The Services are not intended for minors. The Platform may block accounts when it detects unauthorized use by minors or impersonation.

Changes to this Policy

The Platform may update this Policy as needed due to technical improvements, operational changes, or compliance adjustments. The current version will be the one published on the official website.

Contact

To exercise your rights or make inquiries about privacy:
operations@inverzasmart.com