
Data retention policy



Risk warning: Smart contracts and digital assets

Trading with smart contracts, decentralized protocols, and digital assets carries a high risk due to extreme market volatility, the technical complexity of blockchain architecture, and the irreversible nature of transactions, which can lead to the total loss of deposited funds. Furthermore, you acknowledge that, in the absence of intermediaries or central authorities, you are solely responsible for the security of your private keys and the decisions you make; therefore, it is crucial that you fully understand the technological risks.

Last updated: [October 2025]

1. Introduction and objective

This data retention policy establishes the criteria, principles and general guidelines applicable to the retention, storage, blocking and deletion of information processed by Inverza Smart (hereinafter, the “Platform”), in accordance with its general terms of use, its privacy policy, the technological nature of its services and the use of an infrastructure based on blockchain, smart contracts and immutable records.

The objective of this policy is:

- Ensure responsible, proportionate, and secure data management. Define retention periods that
- meet the operational, security, and integrity objectives of the ecosystem. Consider the specific characteristics of data stored in decentralized and immutable technologies. Adopt general
- international standards for security and privacy protection.

-

2. Scope of the policy

This policy applies to all information processed by Inverza Smart, including:

- Personal data of users, investors, and partners. Technical and operational data generated by
- the use of the platform. Records of interactions with smart contracts. Information relating to
- verification processes, operational integrity, and abuse prevention.

-

It applies to all processing environments, including web applications, mobile applications, technology infrastructure, internal systems, and blockchain networks used by the Platform.

3. General principles of retention

Inverza Smart manages data retention according to the following general principles:

I. Proportionality

Inverza Smart retains personal and technical data only for as long as reasonably necessary to fulfill the specific purposes for which it was collected. These purposes include, but are not limited to, platform operation, ecosystem security, transaction traceability, incident management, and preserving technological integrity. The retention period is determined based on the nature of the data, its purpose, the associated risk level, and its operational relevance. Once the purpose has been fulfilled, the data is deleted, anonymized, or blocked, except for data whose retention is necessary for technical, security, or system integrity reasons.

II. Minimization

Inverza Smart applies the principle of data minimization, limiting data collection and storage to what is strictly necessary for the platform's proper functioning. Excessive, irrelevant, or disproportionate data is not retained for operational, security, or ecosystem protection purposes. This principle applies to both personal and technical/operational data, including data used for monitoring, internal auditing, abuse prevention, and risk analysis, in order to minimize the disclosure of unnecessary information.

III. Security

Throughout its lifecycle, from collection to deletion or blocking, data is protected by reasonable technical and organizational measures designed to preserve its confidentiality, integrity, and availability. These measures include access control, encryption, system segmentation, continuous monitoring, and internal incident management procedures, in accordance with international information security standards and best practices in the technology sector.

IV. Integrity and traceability

Data retention helps preserve the integrity, consistency, and traceability of records associated with user activity within the platform.



This is especially relevant in the context of transactions executed through smart contracts, where traceability is essential for verification, technical auditing, and the analysis of historical events. Maintaining these records ensures that transactions can be reliably reconstructed, verified, and analyzed without undue alteration, thus contributing to the transparency and stability of the ecosystem.

V. Technological Differentiation

Inverza Smart acknowledges that some data, due to its technological nature and the use of decentralized infrastructures such as blockchain, cannot be modified, erased, or deleted once recorded. In particular, data stored on blockchain networks or generated by smart contracts is inherently immutable and not under the direct control of the Platform. In these cases, the Data Retention Policy applies, which distinguishes between data stored in centralized systems and data recorded in a decentralized manner, and implements reasonable mitigation and management measures, taking into account existing technical limitations. It is understood that some data, due to its technological nature, cannot be modified or deleted.

4. Data categories and retention periods I.

Identification and contact data

These include name, identity document, contact details and basic user data.

- **Storage period:**

- Throughout the duration of the relationship with the User, the data may be stored or
- subsequently blocked for a reasonable period for security purposes, incident resolution and internal management.

II. Verification and Operational Integrity Data (KYC/AML)

They include information used for processes of identification, risk assessment and integrity of ecosystems.

- **Storage period:**

- As long as the account remains active.

- Once the relationship has ended, this data may be kept blocked for reasonable periods for the purposes of internal audit, fraud prevention, litigation management and historical risk analysis.

III. Technological and operational data

These elements include access logs, technical metadata, activity logs, cryptographic identifiers, and data generated by the use of the platform.

- **Storage period:**

- Data is retained only as long as necessary for system operation, security, and monitoring. Afterward, it may be anonymized, aggregated, or deleted when no longer needed, except for
- data required for technical traceability.

IV. Data recorded on the blockchain and smart contracts

These include transactions, events, blockchain addresses, and any information recorded on blockchain networks as part of the execution of smart contracts.

- **Nature of the data:**

- This data is immutable, decentralized, and not directly controlled by Inverza Smart.

- **Storage period:**

- Permanent, in accordance with the nature of blockchain technology.

Inverza Smart cannot modify, delete, or cancel these records once they have been confirmed on the network.

5. Blocking, anonymizing, and deleting

When the data is no longer needed for its original purpose:

- Blocking them may limit their use. They may be anonymized or aggregated, provided it is
- technically feasible. They may be removed from centralized systems, except for those whose
- retention is necessary for reasons of technical or operational integrity.

Deletion does not apply to data recorded on the blockchain.

6. User requests and technical limitations

The User may request the erasure or restriction of the processing of their data in accordance with the general principles of data protection. However, the User acknowledges that:

- The use of blockchain and smart contracts has inherent technical limitations. Some data cannot
- be modified or deleted. Deletion is limited to data stored in centralized systems under the
- platform's control.

7. Security measures during detention

During storage periods, Inverza Smart implements reasonable security measures, such as:

- Data encryption. Access control and system segmentation. Continuous monitoring and
- incident detection. Credential and privilege management. Internal incident response
- procedures. These measures comply with general international information security
- standards and best practices in the technology sector.
-
-

8. Transfers and storage

The data held by Inverza Smart may be stored, processed or managed by technology providers, digital infrastructure providers, cloud storage services and specialized information security solutions, always under reasonable conditions of confidentiality, integrity, availability and control.

The platform adopts selection criteria aimed at ensuring that these providers apply security practices that comply with international standards in the technology sector, particularly in terms of access control, data protection mechanisms, internal security policies and measures to prevent unauthorized access.

Data transfers are strictly limited to what is necessary for the operation, maintenance, security, and continuity of the technological ecosystem. Inverza Smart does not perform unnecessary, large-scale, or indiscriminate data transfers, nor does it retain data without a clearly defined operational, technical, or security purpose.

When information is processed in distributed environments or infrastructures located in different regions, Inverza Smart will take reasonable measures to ensure an adequate level of protection, in accordance with general privacy principles and industry best practices.

9. Policy Review and Update

Inverza Smart may review, modify or update this data retention policy periodically or exceptionally in the following cases:

- Significant technological changes are introduced to the platform or its infrastructure. The blockchain architecture, smart contracts, or registration and traceability mechanisms are modified. Improvements, adjustments, or new practices are identified regarding information security and confidentiality. Operational needs arising from the evolution of the ecosystem or risk management are detected.
-

Any updates will be published through the Platform's official channels and will take effect immediately upon publication. Continued use of the services implies knowledge and acceptance of the current version of the Policy.

10. Acceptance

Continued use of the Platform implies knowledge and acceptance of this Data Retention Policy, which forms an integral part of the Inverza Smart documentation framework.

Inverza Smart “The union of the traditional and digital financial worlds”