PRIVACY POLICY

Clandestin Ecosystem (QRM)

1. Introduction & Scope

This Privacy Policy explains how information is handled within the Clandestin ecosystem, including activities related to QRM tokens, signal validation, and participation in the decentralized network ("Platform").

The Clandestin ecosystem values privacy, transparency, and security. Participation is designed to be anonymous, borderless, and compliant with global privacy standards.

2. Data Collection Principles

- The Platform does not collect, store, or process personal data such as names, addresses, identification numbers, or biometric data.
- Participation requires only a Solana-compatible wallet address. Wallet addresses are public by design and are not considered personal identifiers under this Policy.
- No cookies, trackers, or profiling mechanisms are embedded within the ecosystem's validation or distribution processes.

3. Use of Information

- The only information recorded on-chain consists of wallet addresses, validation events, and token transfers, as required for the functioning of the network.
- This information is immutable, publicly auditable, and forms part of the decentralized ledger.
- No off-chain user profiling, data resale, or commercial exploitation of participant data occurs.

4. Data Security & User Responsibility

- Security of participation is based on the user's responsibility to safeguard private keys and wallet credentials.
- The ecosystem does not provide custodial services and cannot restore or recover lost private keys.
- Participants are strongly encouraged to use secure storage methods for keys and to avoid sharing credentials with third parties.

5. No Personal Data / Anonymity Statement

- Participation in the Clandestin ecosystem is anonymous by default.
- Users are identified only through cryptographic wallet addresses.
- In compliance with GDPR, CCPA, and similar regulations, no personal data is collected, processed, or stored.

- Because no personal data is retained, rights such as access, correction, or deletion do not apply.

6. Limitation of Liability

- The ecosystem disclaims liability for any losses, breaches, or damages resulting from user negligence, compromised wallets, or third-party exploits.
- Users accept full responsibility for their participation and acknowledge that blockchain records are permanent and beyond unilateral modification.
- No party within the ecosystem guarantees absolute immunity from external threats, though the design minimizes exposure by not holding personal data.

7. Governing Law & Jurisdiction

This Privacy Policy applies globally and is intended to align with the principles of international privacy frameworks.

Disputes concerning privacy shall be resolved through decentralized arbitration or community consensus mechanisms, rather than through national courts, wherever possible.