

Storm Trade Privacy Policy

Last Updated: October 28, 2025

1. Introduction

At Storm Trade (“**Storm Trade**”, “**Storm**”, “**we**”, “**us**”, or “**our**”), we recognize the importance of privacy and data protection. Storm Trade is a perpetual futures exchange built on the dvAMM (Dynamic Virtual Automated Market Maker) concept on **The Open Network (TON)** blockchain. Because our Services are decentralized by design, we aim to process the minimum amount of information necessary to operate, secure, and improve them.

This Privacy Policy explains how we collect, use, share, secure, and retain information when you use our websites, decentralized applications (dApps), APIs, smart-contract interfaces, and any related features (collectively, the “**Services**”). By using the Services, you acknowledge you have read and understood this Privacy Policy.

2. Data Controller and Contact

For purposes of this Privacy Policy, the data controller is **Storm Trade** operating under the laws of the **Republic of Seychelles**.

Contact: **Telegram bot @storm_support_bot**

3. What We Collect (Data Minimization)

We collect only what is necessary to provide and protect the Services:

- **Network identifiers (IP address):** Used for abuse monitoring, network security, DDoS mitigation, traffic routing (including compliance geofencing), and basic analytics.
- **Technical telemetry** (limited): Browser/user agent, device type, timestamps, and basic performance metrics (e.g., error codes) to maintain functionality and reliability.
- **Support communications:** If you contact us (e.g., via email), we process the information you provide (email address, message content, attachments) to handle your request.
- **On-chain information (wallet addresses & transactions):** Interactions with our smart contracts are **public by default** on the TON blockchain. This data is not collected by us

privately; it is published and persisted by the blockchain network and accessible to anyone.

We do not collect your name, postal address, date of birth, or other direct identifiers through the dApp. We do not perform custodian account creation: you retain control of your wallet and private keys.

3.1 Cookies and Local Storage

We may use strictly necessary cookies or local storage to remember non-personal settings (e.g., interface preferences) and to protect the Service from abuse. We do **not** use them to build behavioral profiles.

4. Legal Bases for Processing

Where required by applicable law, we rely on the following legal bases:

- **Legitimate interests:** securing our infrastructure, preventing misuse, operating core functionality, and improving the Services.
- **Legal obligations:** complying with applicable laws, regulations, and lawful requests.
- **Consent:** where expressly required (e.g., certain optional analytics or user-initiated features).

5. How We Use the Information

We use the above information to:

- Operate and maintain the Services and smart-contract interfaces;
- Protect the Services and users (fraud, abuse, spam, DDoS prevention);
- Comply with legal or regulatory obligations (including geofencing if applicable);
- Conduct aggregate, **anonymized** usage and performance analysis to improve stability and user experience;
- Provide user support and address inquiries.

5.1 Anonymized and Aggregated Data

We may analyze or publish aggregated, de-identified statistics (e.g., uptime, request volumes). Such reports do not identify individuals.

6. Data Sharing and Disclosures

We do **not** sell your personal information. We may share limited information (primarily IP address and technical telemetry) with:

- **Service providers (“processors”)** such as cloud hosting, security, DDoS protection, logging/monitoring, or analytics strictly necessary to run the Services. These providers process data only under our instructions and applicable data-protection terms.
- **Legal and compliance recipients** when required to comply with law, enforce our terms, or protect rights, property, users, or the integrity of the Services.
- **Business transfers:** If we are involved in a merger, acquisition, or asset transfer, permitted information may be transferred as part of that transaction, subject to this Policy.

Third-Party Platforms. If you follow links to, or connect your wallet through, third-party sites, RPC providers, wallets, bridges, or block explorers, those parties act as independent controllers of any information they process. Their policies govern your use of their services.

7. International Transfers

We may process and store information with providers located in multiple jurisdictions. Where required, we implement appropriate contractual safeguards (e.g., standard contractual clauses) and technical and organizational measures to protect data when transferred internationally.

8. Security

Security is integral to privacy. We employ commercially reasonable administrative, technical, and organizational measures to help protect information against unauthorized access, alteration, disclosure, or destruction. However, **no** method of transmission or storage is completely secure, and on-chain data is public by design.

Wallet keys. We never have access to your private keys. You are responsible for securing your wallet and seed phrases.

9. Retention

- **IP addresses and telemetry** are retained only as long as needed for the purposes outlined above (e.g., operating and securing the Services) and to meet legal requirements or resolve disputes.
- **Support communications** are retained as long as necessary to address the request and for legitimate business or legal purposes.
- **On-chain data** follows blockchain persistence and cannot be altered or deleted by us.

We periodically review retention to avoid keeping data longer than necessary.

10. Your Rights

Depending on your jurisdiction, you may have rights such as access, rectification, deletion, restriction, objection, portability, or withdrawal of consent (where processing is based on consent). Because on-chain data is public and immutable, it cannot be edited or removed by us. For off-chain data (e.g., IP logs or support tickets), you can contact **Telegram bot @storm_support_bot** to exercise your rights, subject to verification and applicable law.

11. Children

The Services are intended for individuals **18 years or older**. We do not knowingly collect information from children under 13 (or under the age of digital consent in your jurisdiction). If you believe a child has provided information to us, please contact **Telegram bot @storm_support_bot** so we can address the issue.

12. Third-Party Links and Interfaces

Our interfaces may reference or route to third-party resources (wallets, RPC nodes, explorers, analytics, social networks). We are not responsible for their practices. Review their privacy policies before use.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in technology, law, or our Services. When we do, we will revise the “Last Updated” date above and, where legally required, provide additional notice. Your continued use of the Services after changes take effect constitutes acceptance of the updated Policy.

14. Governing Law and Dispute Resolution

This Privacy Policy is governed by the laws of the **Republic of Seychelles**, without regard to conflict-of-law rules. You agree to first attempt to resolve any privacy-related dispute informally by contacting **Telegram bot @storm_support_bot**. Subject to applicable law, disputes that cannot be resolved informally may be brought in the competent courts of the Republic of Seychelles.

15. Contact Us

If you have questions about this Privacy Policy or our data practices, contact:
Telegram bot @storm_support_bot