Privacy Policy & Personal Data Protection Standards

Governance, Encryption, Retention, and Data Subject Rights under Global Privacy Frameworks

DOC REF: STX-POL-PRV-2026-V5 | STANDARD REGULATORY SPECIFICATION | EFFECTIVE: 2026 EDITION

1. General Provisions & Commitment to Confidentiality

1.1. StarX Options Global (the "Company", "we", "our", or "us") is dedicated to protecting the confidentiality, privacy, and integrity of the personal data of all registered users, prospective clients, and website visitors (the "Client" or "you").

1.2. This Privacy Policy (the "Policy") delineates the principles, lawful bases, categories of information collected, security mechanisms, and retention protocols governing your personal data when you access `https://starxoptions.com`, utilize our web terminals, or engage with our mobile progressive web applications (PWAs).

1.3. We operate under strict compliance with internationally recognized data protection principles, including provisions aligned with the General Data Protection Regulation (GDPR) and global privacy standards. We categorically declare that **we do not sell, rent, monetize, or disclose your personal data to third-party marketing brokers**.

2. Categories of Information Collected

2.1. *Identification & Contact Data:* During registration and customer due diligence, we collect your full legal name, date of birth, residential address, nationality, email address, and verified telephone number.

2.2. *Regulatory KYC Verification Dossiers:* Copies of government-issued identification cards, passports, driver's licenses, biometric facial selfies, proof of address utility bills, and verifiable bank statement disclosures.

2.3. *Financial & Transactional Records:* Deposit intent timestamps, payment rail types (UPI, Cryptocurrency, EPS), truncated card identifiers, transaction reference numbers (UTR, blockchain tx hashes), withdrawal requests, account balances, and historical trade order books.

2.4. *Technical Telemetrics & Device Telemetry:* Internet Protocol (IP) addresses, browser type, operating system version, screen resolution, device fingerprint hashes, hardware acceleration specs, language preferences, and network latency timestamps collected automatically upon terminal connection.

3. Depersonalized & Analytical Information

3.1. The Company processes depersonalized, aggregated technical metrics that cannot be linked directly to any identifiable natural person. These metrics are utilized exclusively to measure platform concurrency, optimize WebSocket data streaming, identify software bugs, and safeguard server infrastructure against Distributed Denial of Service (DDoS) attacks.

4. Lawful Grounds & Purposes of Data Processing

4.1. We process personal data solely under established lawful bases:

- **Contractual Performance:** To establish your trading account, execute digital option contracts, calculate payouts, and process deposit and withdrawal instructions;
- **Legal & Statutory Compliance:** To satisfy mandatory Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and international sanctions screening obligations;

- **Legitimate Commercial Interests:** To detect market abuse, prevent multi-account bonus fraud, investigate cybersecurity incidents, and enhance platform trading latency;
- **Explicit Consent:** Where you provide voluntary consent for optional customer service surveys or platform feature announcements.

5. Cookie Policy & Tracking Technologies

5.1. Cookies are small encrypted data files stored on your local browser to enable core platform features, session continuity, and security verification.

5.2. Types of Cookies Deployed:

- **Strictly Necessary Security Cookies:** Essential for user authentication, memory-only session tokens, and Cloudflare bot defense challenges;
- **Functional & Preference Cookies:** Remembering your chosen chart indicator layouts, timezone preferences, sound effects, and display currency;
- **Performance Telemetry Cookies:** Measuring WebSocket round-trip ping times and interface rendering performance.

5.3. You may adjust your browser settings to refuse or delete cookies; however, disabling strictly necessary cookies will render the Trading Terminal unable to authenticate your session or execute trade orders.

6. Sharing & Disclosure of Personal Data to Third Parties

6.1. The Company restricts access to your personal data strictly to authorized personnel bound by non-disclosure agreements. We share data with external entities solely under the following conditions:

- **Licensed Acquiring & Payment Processors:** Necessary transaction metadata is transmitted to payment service providers, UPI aggregators, and banking partners solely to execute deposit and withdrawal settlements;
- **Automated KYC & Identity Verification Vendors:** Identity document images are processed via encrypted API pipelines by audited identity verification providers solely for anti-fraud validation;
- **Judicial & Regulatory Authorities:** We may disclose information if compelled by a lawful, valid court order, subpoena, or statutory inquiry issued by a recognized judicial body investigating serious criminal offenses.

7. International Data Transfers & Cybersecurity Architecture

7.1. All personal data and financial records are encrypted in transit using Transport Layer Security (TLS 1.3) with modern cryptographic cipher suites and stored at rest utilizing Advanced Encryption Standard (AES-256) encryption within hardened, tier-IV data center server clusters.

7.2. Sensitive private cryptographic keys and master database access tokens are governed under hardware security modules (HSM) and strict Maker-Checker dual-authorization operational protocols.

8. Data Retention & Archival Limits

8.1. We retain your personal data for the entire duration of your active account relationship with the Company.

8.2. Following voluntary account termination or administrative closure, all identification records, KYC verification dossiers, and financial ledgers are retained in encrypted archival storage for a mandatory statutory duration of **five (5) years** in compliance with global Anti-Money Laundering legislation. Upon the expiration of this statutory period, data is securely and permanently purged.

9. Client Data Subject Rights

9.1. Subject to applicable statutory regulations, the Client possesses the following rights regarding personal data:

- **Right of Access:** You may request an electronic copy of all personal records and transaction logs maintained on your profile;
- **Right to Rectification:** You may request immediate correction of outdated or inaccurate personal details;
- **Right to Erasure ("Right to be Forgotten"):** You may request the deletion of your account and personal data, subject to the Company's mandatory statutory AML archival obligations;
- **Right to Restrict Processing:** You may request the restriction of processing while a data accuracy dispute is investigated.

10. Inquiries, Data Protection Officer & Policy Amendments

10.1. Any formal inquiries, data subject access requests, or privacy grievances should be directed to our designated Data Protection Secretariat at `privacy@starxoptions.com`.

10.2. The Company reserves the right to amend this Policy periodically. In the event of material modifications, registered Clients will be notified via terminal alert or website announcement at least fourteen (14) calendar days prior to effective implementation.

ISSUED & GOVERNED BY:
StarX Options Global Technology Operations
Legal & Compliance Secretariat
Digital Asset & Financial Markets Division
Portal: https://starxoptions.com
Inquiries: compliance@starxoptions.com

CLIENT ACKNOWLEDGEMENT:
By registering an account, depositing capital, or placing a transaction order on StarX Options, the Client unconditionally certifies complete understanding and legally binding consent to all terms, operational rules, and risk provisions set forth herein.