BROKERZA

PERSONAL DATA PROTECTION POLICY

(Incorporated by Reference into and Forming an Integral Part of the Usage Terms and Policies)

1. Scope, Application, and Legal Basis

1.1 Framework and Purpose

This Personal Data Protection Policy (hereinafter referred to as the **"Policy"**) establishes the principles, standards, and procedures governing the collection, processing, storage, use, disclosure, and protection of personal data obtained by the Company in the course of providing its services. This Policy is designed to ensure compliance with applicable data protection laws, international regulatory standards, and internal risk management practices.

1.2 Integration with Main Agreement

(a) This Policy shall be read in conjunction with, and shall constitute an integral and legally binding component of, the Company's Usage Terms and Policies (the "Main Agreement").

(b) By accessing or using the Company's services, platforms, or systems, you expressly acknowledge and agree to the practices described herein.

(c) In the event of any inconsistency between this Policy and the Main Agreement, the interpretation that best supports regulatory compliance and operational integrity shall prevail.

1.3 Scope of Application

(a) This Policy applies to all personal data collected through the Company's website, trading platforms, mobile applications, communication channels, and associated digital environments (collectively, the **"Platform"**).

(b) It applies to all Clients, prospective Clients, and any individuals interacting with the Company's services.

2. Collection of Personal Data

2.1 Categories of Personal Information

(a) During account registration and ongoing service use, the Company collects personal data necessary to establish, verify, and maintain Client relationships.
(b) Such data may include, but is not limited to:

- Full legal name, contact details, and identification information;
- Date of birth, nationality, and residency status;
- Financial background, employment details, and source of funds;
- Trading preferences, experience, and account-related information.

2.2 Identity Verification and Compliance Requirements

(a) In order to comply with regulatory obligations, including anti-money laundering (AML) and Know Your Customer (KYC) requirements, the Company may require submission of official identification documents.
(b) These may include passports, national identification cards, proof of address, and other supporting documentation.
(c) The Company reserves the right to verify such information through internal processes or third-party verification providers.

2.3 Accuracy and Updating of Information

(a) You are obligated to ensure that all personal data provided is accurate, complete, and up to date.
(b) Failure to maintain accurate information may result in restrictions, suspension, or termination of services.

3. Technical and Automated Data Collection

3.1 System-Generated Data

(a) The Company automatically collects technical and usage-related data during your interaction with the Platform.
(b) This includes, but is not limited to:

- IP addresses and device identifiers;
- Browser type, operating system, and network data;

- Access times, navigation patterns, and interaction logs.

3.2 Cookies and Tracking Technologies

(a) The Company utilizes cookies and similar tracking mechanisms to enhance user experience, improve system performance, and analyze usage behavior.
(b) By accessing the Platform, you consent to the use of such technologies unless disabled through your device settings.

3.3 Analytical and Performance Monitoring

(a) Collected data may be used for internal analytics, system optimization, fraud detection, and service improvement initiatives.

4. Purpose and Legal Grounds for Processing

4.1 Operational and Service Delivery Purposes

Personal data is processed for purposes including:
(a) Account creation, management, and service delivery;
(b) Execution of transactions and operational functions;
(c) Customer support and communication.

4.2 Regulatory and Compliance Purposes

(a) The Company processes personal data to comply with applicable legal and regulatory obligations, including AML, KYC, and fraud prevention measures.

4.3 Risk Management and Security

(a) Data may be used to detect, prevent, and investigate unauthorized or unlawful activities, including fraud, abuse, and system breaches.

4.4 Legal Proceedings and Dispute Resolution

(a) Personal data may be processed where necessary for the establishment, exercise, or defense of legal claims.

5. Data Sharing and Disclosure

5.1 Disclosure to Service Providers and Affiliates

(a) The Company may share personal data with affiliated entities, service providers, financial institutions, and technology partners for operational purposes.
(b) Such entities are required to maintain confidentiality and comply with applicable data protection obligations.

5.2 Disclosure to Authorities

(a) Personal data may be disclosed to governmental, regulatory, or law enforcement authorities where required by law, legal process, or regulatory obligation.

5.3 Restrictions on Client-to-Client Information Requests

(a) Requests for information relating to other Clients shall not be granted unless legally required.
(b) The Company retains absolute discretion in determining whether such disclosure is permissible.

6. Data Security and Protection Measures

6.1 Security Framework

(a) The Company implements industry-standard security measures designed to protect personal data against unauthorized access, alteration, disclosure, or destruction.

6.2 Authentication Controls

(a) Multi-factor authentication mechanisms may be deployed to enhance account security and prevent unauthorized access.

6.3 Encryption and Transmission Protection

(a) Sensitive data is protected through encryption protocols during transmission and storage to ensure confidentiality and integrity.

6.4 Monitoring and Threat Detection

(a) Continuous monitoring systems are employed to identify suspicious activities and respond to potential security threats.

6.5 Incident Response and Breach Management

(a) In the event of a data security incident, the Company shall take appropriate measures to contain, investigate, and mitigate the impact, in accordance with applicable legal requirements.

7. Data Retention and Disposal

7.1 Retention Period

(a) Personal data shall be retained only for as long as necessary to fulfill the purposes outlined in this Policy and to comply with legal and regulatory obligations.

7.2 Secure Disposal

(a) Upon expiration of the retention period, data shall be securely deleted, anonymized, or otherwise disposed of in accordance with internal policies.

8. International Data Transfers

8.1 Cross-Border Processing

(a) Personal data may be transferred to, stored, and processed in jurisdictions outside your country of residence.

8.2 Safeguards

(a) The Company shall implement appropriate safeguards to ensure that such transfers comply with applicable data protection laws and maintain adequate levels of data protection.

9. Client Rights and Data Requests

9.1 Access and Correction Rights

(a) You may request access to your personal data and request correction of inaccurate or incomplete information, subject to verification procedures.

9.2 Data Deletion Requests

(a) Requests for deletion of personal data may be submitted, subject to legal, regulatory, and operational retention requirements.
(b) Certain data may be retained notwithstanding such requests where required by law.

10. Third-Party Services and External Links

10.1 External Platforms

(a) The Platform may contain links to third-party websites or services.
(b) The Company does not control and is not responsible for the privacy practices or content of such external platforms.

11. Marketing and Communications

11.1 Consent to Communications

(a) By using the Company's services, you consent to receiving communications relating to services, updates, and promotional materials.

11.2 Opt-Out Rights

(a) You may withdraw consent for marketing communications at any time through available opt-out mechanisms.

12. Limitation of Liability Relating to Data

12.1 Scope of Limitation

(a) The Company shall not be liable for indirect, incidental, or consequential damages arising from unauthorized access, data breaches, or system vulnerabilities beyond its reasonable control.

(b) The Company does not guarantee absolute security of data transmissions over the internet.

13. Indemnification

13.1 Client Responsibility

(a) You agree to indemnify and hold harmless the Company from any claims, damages, or liabilities arising from:

- Your misuse of the Platform;
- Breach of this Policy;
- Violation of applicable laws or third-party rights.

14. Policy Amendments and Continuing Consent

14.1 Right to Modify

(a) The Company reserves the right to amend or update this Policy at any time.

14.2 Acceptance of Changes

(a) Continued use of the Company's services following any updates shall constitute acceptance of the revised Policy.