REVEXIUM

Personal Data Protection and Confidentiality Policy

REVEXIUM

This **Personal Data Protection and Confidentiality Policy** (the "Policy") establishes the regulatory framework, operational standards, and protective measures implemented by the Company for the collection, processing, storage, transfer, and safeguarding of personal data belonging to individuals accessing or interacting with the Company's digital platforms, including websites, mobile applications, and related interfaces (collectively, the "Platform"). This Policy governs all personal data processing activities pertaining to clients, users, or visitors (hereinafter referred to as "you" or "your").

Article 1: Data Collection and Processing

1.1 During account registration, utilization of the Platform, compliance verification, and service provision, the Company may gather personal data including, but not limited to: full legal name, date of birth, nationality, contact information, residential address, government-issued identification, and financial or employment-related details. Such data are collected for eligibility verification, risk evaluation, regulatory compliance, and contractual fulfillment.

1.2 To comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, the Company may request supporting documents such as identity proofs, residence verification, and financial statements. These materials are strictly utilized for identity authentication, compliance checks, fraud prevention, and risk profiling.

1.3 By accessing or using the Platform, you provide consent to automated collection of technical and behavioral data, including device information, IP address, browser metadata, geolocation, session duration, and activity logs, through cookies and similar tracking technologies, for purposes of system optimization, fraud detection, and compliance obligations.

Article 2: Security, Access Control, and Data Retention

2.1 The Company employs advanced security protocols, including multi-layer encryption, SSL, and continuous threat monitoring, to ensure the confidentiality, integrity, and availability of your personal data.

2.2 Two-factor authentication (2FA) is implemented to enhance account security, requiring secondary verification in addition to login credentials, thereby mitigating unauthorized access risks.

2.3 Personal data are retained only for as long as necessary to fulfill the purposes of collection or as mandated by law. Upon expiration of the retention period, data will be securely deleted or anonymized in accordance with applicable regulations.

2.4 In circumstances of account recovery or access reinstatement, the Company will conduct identity verification procedures to prevent fraudulent activity or impersonation.

Article 3: Data Usage, Sharing, and International Transfers

3.1 Personal data are exclusively utilized for legitimate business purposes including service delivery, operational management, regulatory compliance, fraud prevention, dispute resolution, and internal auditing.

3.2 The Company may engage external service providers, affiliated entities, or authorized agents to perform operational functions. All data disclosures are governed by binding confidentiality obligations and applicable data protection laws.

3.3 The Company may be legally obligated to disclose personal data to governmental authorities, regulatory agencies, or judicial entities. Any such disclosures are strictly in accordance with legal requirements and are duly documented.

3.4 Personal data shall not be shared with other users unless required by law. Requests for disclosure must be legally valid and provided in written form.

3.5 You acknowledge that personal data may be transferred and stored internationally. The Company ensures that all cross-border transfers adhere to recognized legal frameworks maintaining equivalent levels of data protection.

Article 4: Rights, Consent, and Legal Disclaimers

4.1 You retain the right to request erasure of personal data, subject to statutory obligations, ongoing investigations, or regulatory retention requirements. Certain data related to account recovery, dispute resolution, fraud prevention, or legal mandates may be exempt until applicable conditions are resolved.

4.2 The Company may send informational or promotional communications. You may withdraw consent to receive such communications at any time without affecting your contractual relationship.

4.3 You agree to indemnify and hold the Company, its affiliates, officers, and employees harmless from any third-party claims arising from violations of this Policy or applicable data protection regulations.

4.4 Failure by the Company to enforce any provision of this Policy does not constitute a waiver of rights. Waivers must be formalized in writing by an authorized Company representative.

4.5 The Company reserves the right to amend this Policy at its discretion. Updates will be published on the Platform and become effective immediately. Continued use of the Platform signifies acceptance of any changes.

Article 5: Ancillary and Compliance Measures

5.1 External website links are provided for convenience. The Company disclaims responsibility for third-party content or privacy practices. Users are encouraged to review the privacy policies of external websites.

5.2 The Company will conduct regular internal audits, risk assessments, and compliance reviews to ensure ongoing adherence to applicable data protection regulations and operational resilience.

5.3 All inquiries, requests for data access, or complaints must be submitted through the official communication channels provided on the Platform. Only submissions originating from registered user accounts will be considered valid.

Article 6: Breach Notification Protocol

6.1 In the event of a confirmed data breach, the Company shall promptly assess the scope, notify affected individuals and regulatory authorities as required by law, and take remedial measures to mitigate potential harm.

Article 7: Data Minimization and Purpose Limitation

7.1 The Company commits to collecting only data strictly necessary for legitimate business purposes and to retain it solely for the duration required to achieve those purposes.

Article 8: Third-Party Vendor Compliance

REVEXIUM

8.1 All third-party service providers engaged by the Company must demonstrate compliance with equivalent data protection standards, with contractual obligations ensuring confidentiality and lawful processing.

Article 9: User Access and Rectification Rights

9.1 Users may request access to, correction of, or restriction on processing of their personal data. The Company shall respond to such requests in compliance with applicable legislation within a reasonable timeframe.