



INFORMATION PRIVACY AND DATA PROTECTION POLICY

Last Updated: April 14, 2026

1. INTRODUCTORY PROVISIONS

1.1 Purpose and Legal Framework

This Information Privacy and Data Protection Policy (*the “Policy”*) establishes the principles, standards, and legal framework governing the collection, processing, storage, use, and protection of personal data by the Company.

This Policy is designed to ensure that all personal information is handled in a lawful, fair, and transparent manner, in accordance with applicable data protection laws, regulatory requirements, and recognized industry standards.

It applies to all individuals who access, interact with, or utilize the Company’s website, applications, platforms, and related digital services (*collectively referred to as the “Platform”*).

1.2 Scope of Application

This Policy applies to all personal data collected directly from Clients or indirectly through their interaction with the Platform, including but not limited to account registration, financial transactions, communications, and system usage.

1.3 Acceptance and Acknowledgment

By accessing or using the Company’s services, the Client confirms that they have read, understood, and agreed to the terms set forth in this Policy, including the collection and processing of their personal data in accordance with its provisions.



1.4 Relationship with Other Agreements

This Policy forms an integral component of the Company's overall legal framework and shall be interpreted in conjunction with the General Service Agreement, AML and CTF Compliance Policy, Risk Assumption and Disclosure Statement, and other related policies.

2. COLLECTION AND PROCESSING OF PERSONAL DATA

2.1 Categories of Personal Data Collected

The Company may collect and process various categories of personal data necessary for the provision of services, regulatory compliance, and operational efficiency.

2.1.1 Identity and Contact Information

Personal data may include, but is not limited to:

- ❑ Full legal name;
- ❑ Date of birth;
- ❑ Nationality and residential address;
- ❑ Email address and telephone number;
- ❑ Government-issued identification details.

2.1.2 Financial and Transactional Information

The Company may collect financial information such as source of funds, income details, transaction history, and account activity for compliance and risk management purposes.

2.1.3 Technical and Usage Data

The Company may automatically collect technical data including IP addresses, geolocation data, device identifiers, browser information, and usage patterns through interaction with the Platform.

2.1.4 Legal Basis for Processing

Personal data shall be processed based on:

- ☐ Contractual necessity;
- ☐ Legal and regulatory obligations;
- ☐ Legitimate business interests;
- ☐ Client consent, where applicable.

2.2 Verification and Compliance Requirements

To comply with regulatory requirements, including Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, the Company may request supporting documentation such as identity verification records, proof of address, and financial documentation.

2.3 Purpose Limitation Principle

All personal data collected shall be used strictly for specified, legitimate purposes, including service delivery, compliance monitoring, fraud prevention, and system optimization.

3. DATA SECURITY, STORAGE, AND RETENTION

3.1 Information Security Measures

The Company implements comprehensive technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, or destruction.

These measures include encryption technologies, secure communication protocols, and continuous monitoring systems.

3.2 Authentication and Access Controls

The Company may implement enhanced authentication mechanisms, including two-factor authentication (2FA), to safeguard account access and protect user data.



3.3 Data Retention Policy

Personal data shall be retained only for the duration necessary to fulfill its intended purpose or to comply with legal and regulatory obligations.

Upon expiration of the retention period, such data shall be securely deleted or anonymized.

3.4 Data Breach Response

In the event of a data breach or security incident, the Company shall take appropriate steps to investigate, mitigate, and resolve the issue, including notifying affected parties where required by law.

3.5 Account Recovery and Verification Procedures

Where access to an account is compromised or lost, the Company shall require identity re-verification prior to restoring access, to ensure continued protection against unauthorized activity.

4. DATA USE, DISCLOSURE, AND INTERNATIONAL TRANSFERS

4.1 Use of Personal Data

Personal data shall be used solely for operational and compliance-related purposes, including service delivery, account management, fraud detection, regulatory reporting, and customer support.

4.2 Disclosure to Third Parties

The Company may share personal data with authorized third-party service providers, affiliates, or agents strictly for operational, legal, or compliance purposes, subject to appropriate safeguards.



4.3 Legal and Regulatory Disclosure

Personal data may be disclosed to regulatory authorities, law enforcement agencies, or courts where required by applicable laws or legal processes.

4.4 Restriction on Third-Party Requests

Requests for information relating to other Clients shall be rejected unless supported by valid legal authority and compliant with applicable data protection laws.

4.5 Cross-Border Data Transfers

Personal data may be transferred across international jurisdictions. The Company shall ensure that such transfers are conducted in accordance with appropriate safeguards to maintain adequate data protection standards.

4.6 Data Minimization Principle

The Company shall limit the collection and processing of personal data to what is strictly necessary for the purposes outlined in this Policy.

5. CLIENT RIGHTS, CONSENT, AND COMMUNICATIONS

5.1 Data Subject Rights

Clients may exercise rights relating to their personal data, including access, correction, deletion (*subject to limitations*), and restriction of processing where applicable.

5.2 Right to Erasure and Limitations

Requests for deletion of personal data shall be honored except where retention is required for legal compliance, dispute resolution, or fraud prevention.

5.3 Marketing Communications

The Company may provide marketing communications or service updates. Clients may opt out of non-essential communications at any time.

5.4 Consent and Withdrawal

Where data processing is based on consent, Clients may withdraw such consent at any time, subject to legal or contractual limitations.

5.5 Indemnification

The Client agrees to indemnify and hold the Company harmless from any claims arising from misuse of the Platform or violation of applicable data protection laws.

5.6 Non-Waiver of Rights

Failure by the Company to enforce any provision of this Policy shall not constitute a waiver of its rights.

6. GENERAL AND MISCELLANEOUS PROVISIONS

6.1 Third-Party Platforms

The Platform may contain links to external websites or services. The Company does not assume responsibility for the privacy practices of such third parties.

6.2 Internal Audits and Compliance Monitoring

The Company may conduct periodic audits and reviews of its data protection systems and procedures to ensure compliance with this Policy and applicable laws.

6.3 Communication Channels

All inquiries or requests relating to personal data must be submitted through the Company's official communication channels and from registered Client contact details.



6.4 Policy Amendments

The Company reserves the right to amend this Policy at its discretion. Changes shall take effect upon publication, and continued use of services constitutes acceptance.

6.5 Data Protection Contact Point

The Company may designate a responsible officer or department to oversee data protection matters and handle Client inquiries or regulatory requests.