Moonetrix

Information Privacy and Security Policy

Overview

This Policy outlines **Moonetrix's** commitment to protecting the confidentiality, integrity, and security of personal information collected from users of our digital platforms. We prioritize compliance with global data protection standards and ensure responsible handling of personal data throughout its lifecycle. Our objective is to provide transparency regarding our data practices, empower users with rights over their information, and maintain trust through robust security measures.

Scope and Application

This Policy governs all personal data processing activities undertaken by the Company in connection with its website, mobile applications, and related services (collectively, the "Platform"). It applies to all users, clients, visitors, and other individuals ("Data Subjects") whose personal information is collected, stored, or otherwise processed by the Company, irrespective of their geographic location. The Policy also extends to third parties acting on behalf of the Company in data processing roles.

Definitions

1. Personal Data: Any information that relates to an identified or identifiable individual, including name, email, identification numbers, location data, or other attributes specific to their identity.

2. Data Subject: An individual whose personal data is collected, stored, or processed by the Company. This includes clients, users, and visitors of the Platform.

3. Processing: Any operation performed on personal data, whether automated or not, including collection, storage, use, disclosure, and deletion.

4. Data Controller: The Company or any entity that determines the purposes and means of processing personal data.

5. Data Processor: A third-party entity that processes personal data on behalf of the Data Controller under specific instructions.

6. Consent: A freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which they, by a statement or clear affirmative action, signify

agreement to the processing of their personal data.
7. Cross-Border Transfer: The movement of personal data to jurisdictions outside of the Data Subject's country, which may be subject to additional legal protections.

8. Opt-Out: The process by which a Data Subject withdraws consent for certain processing activities, such as marketing communications.

Part A: Data Collection and Processing

Section 1.1: Personal Data Acquisition
As part of account creation and service provision, we lawfully gather personal data identifiers including but not limited to your full name, contact details (email, phone), date of birth, nationality, residential address, government-issued IDs, financial profile, and source of funds. This data supports eligibility verification and risk assessment procedures.

Section 1.2: Regulatory Compliance Documentation
To fulfill regulatory obligations under Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, we request supporting documentation such as identification cards, proof of address (utility bills), bank statements, and similar verification documents. These documents also facilitate lawful communications, risk detection, and fraud prevention.

Section 1.3: Technical Data Collection
By utilizing the Platform, you consent to the collection of technical data including IP addresses, geolocation coordinates, device and browser metadata, and user activity patterns. This information helps optimize Platform performance and maintain compliance with applicable laws.

Part B: Data Security Measures and Retention

Section 2.1: Security Controls
We implement advanced data security measures such as encryption protocols (including SSL/TLS), continuous network monitoring, and intrusion detection systems to safeguard your personal data from unauthorized access, alteration, or disclosure.

Section 2.2: Authentication Protocols
Multi-factor authentication (MFA) is enforced to bolster account security. This includes a secondary authentication factor delivered via secure channels, in addition to your primary login credentials.

Section 2.3: Data Retention Policy

Personal information is retained strictly for as long as necessary to fulfill the purposes for which it was collected or as mandated by legal or regulatory requirements. After such periods, data is securely deleted or anonymized following industry best practices.

Section 2.4: Account Recovery Procedures

In case of account access loss, reactivation requires identity verification to prevent fraudulent claims and ensure data integrity.

Part C: Use, Disclosure, and International Transfer of Data

Section 3.1: Purpose of Data Usage

Your personal data will be utilized exclusively for operational needs including service delivery, customer management, compliance monitoring, fraud prevention, and legal dispute resolution.

Section 3.2: Data Sharing with Third Parties

Subject to confidentiality agreements and data protection laws, we may disclose your information to trusted third-party service providers, affiliates, or agents who perform functions on our behalf.

Section 3.3: Legal Disclosure Obligations

We may disclose personal data when compelled by law, subpoena, or regulatory authorities, strictly within the bounds of applicable statutes and only to the necessary extent.

Section 3.4: Client Data Privacy Between Users

Requests for personal data pertaining to another client will be denied unless legally mandated, documented, and compliant with relevant privacy regulations. We reserve discretion to reject unfounded requests.

Section 3.5: Cross-Border Data Transfers

By accessing the Platform, you consent to your personal data being transferred and stored across jurisdictions. We ensure these transfers comply with binding international data protection instruments to safeguard your information.

Part D: Data Subject Rights, Consent, and Notifications

Section 4.1: Data Deletion Rights

You may request the deletion of your personal data at any time. However, such requests may be declined where data retention is required to comply with legal obligations, resolve disputes, enforce agreements, or prevent fraud.

Section 4.2: Marketing and Communications Preferences
We may send you promotional materials or updates, but you have the right to opt out at any time without affecting your service access.

Section 4.3: Indemnification Clause
You agree to indemnify and hold the Company harmless against any claims, liabilities, or damages arising directly from your willful violation of this Policy or applicable data protection laws.

Section 4.4: Non-Waiver of Rights
Our failure to enforce any provision does not constitute waiver of rights, unless expressly documented and authorized in writing.

Section 4.5: Amendments and Policy Updates
This Policy may be amended periodically. Changes will be published on the Platform and become effective immediately. Continued use implies acceptance of the revised terms.

Part E: Additional Provisions

Section 5.1: Third-Party Links Disclaimer
The Platform may contain links to external websites or services. We do not endorse or control third-party privacy practices and recommend reviewing their policies separately.

Section 5.2: Audit and Compliance Monitoring
The Company commits to routine audits of its privacy and security practices, including breach detection, reporting, and policy reviews to maintain compliance.

Section 5.3: Contact and Data Requests
For privacy inquiries, complaints, or to exercise your rights under this Policy, contact us via designated channels listed on the Platform. All requests must be submitted from your registered email address.