Bronetix

Data Privacy and Information Security Policy

Bronetix

This Data Privacy and Information Security Policy (the **"Policy"**) sets out the principles, controls, and safeguards adopted by the Company to govern the lawful handling, protection, and confidentiality of personal information processed through the Company's digital environment, including its websites, applications, systems, and related technological infrastructure (collectively, the **"Platform"**).

This Policy applies to all individuals whose personal data is processed by the Company, including clients, users, prospective clients, and visitors (collectively, **"Data Subjects"**).

Article 1: Categories of Personal Data and Lawful Processing

1.1. In the course of providing services, administering accounts, performing regulatory checks, and maintaining operational functionality, the Company may process personal information such as identification details, contact information, demographic data, residency records, employment or financial disclosures, and government-issued documentation, where lawfully required.

1.2. Information collected is processed strictly for defined and legitimate purposes, including identity verification, eligibility assessment, regulatory compliance, contractual performance, fraud prevention, risk management, and dispute resolution.

1.3. In addition to information provided directly by Data Subjects, the Company may automatically collect technical and usage data—including device identifiers, IP addresses, access timestamps, session activity, and platform interaction metrics—through cookies or similar technologies to ensure system integrity, security monitoring, and service optimization.

Article 2: Information Security Controls and Retention Standards

2.1. To preserve the confidentiality, accuracy, and availability of personal data, the Company implements administrative, technical, and organizational safeguards, including encryption technologies, secure network protocols, controlled access permissions, and continuous monitoring against unauthorized intrusion.

2.2. Enhanced authentication mechanisms, such as multi-factor verification, may be applied to protect account access and reduce the risk of unauthorized use or identity compromise.

2.3. Personal data is retained only for the period necessary to fulfill the purpose for which it was collected or to comply with applicable legal, regulatory, or contractual retention obligations, after which such data is securely erased, anonymized, or archived in accordance with lawful standards.

2.4. Where account restoration, credential recovery, or access reinstatement is requested, the Company may require renewed identity verification to prevent impersonation, fraud, or misuse.

Article 3: Use, Disclosure, and Cross-Border Transfer of Data

3.1. The Company processes personal data solely for legitimate operational and compliance-related activities, including service delivery, system administration, audit functions, legal defense, and internal risk controls.

3.2. Certain processing activities may be conducted by affiliated entities, external service providers, or professional advisers engaged by the Company. Any such engagement is governed by contractual confidentiality obligations and data protection commitments consistent with applicable law.

3.3. Where disclosure of personal data is required by statute, court order, regulatory directive, or lawful authority request, the Company shall comply strictly within the scope mandated and maintain appropriate records of such disclosures.

3.4. Personal data is not disclosed to other users of the Platform and shall only be shared where legally justified or contractually required.

3.5. Due to the international nature of digital services, personal data may be processed or stored outside the Data Subject's country of residence. The Company ensures that cross-border transfers are conducted under lawful transfer mechanisms providing adequate levels of data protection.

Article 4: Data Subject Rights, Consent, and Legal Safeguards

4.1. Subject to applicable legal limitations, Data Subjects may request access to, correction of, restriction on processing of, or deletion of their personal data. Requests may be declined

or deferred where retention is required for regulatory compliance, fraud prevention, or legal proceedings.

4.2. The Company may communicate service-related, administrative, or promotional messages where legally permitted. Consent for non-essential communications may be withdrawn at any time without affecting contractual rights or service eligibility.

4.3. Data Subjects agree to indemnify the Company against losses arising from inaccurate information provided, misuse of data rights, or violations of applicable data protection laws attributable to the Data Subject.

4.4. Any failure by the Company to exercise a right or enforce a provision under this Policy shall not constitute a waiver unless expressly confirmed in writing.

4.5. The Company may revise this Policy periodically. Amendments take effect upon publication through official channels, and continued use of the Platform constitutes acknowledgment and acceptance of the updated Policy.

Article 5: Compliance Monitoring and External Interactions

5.1. Links to external websites or services are provided for informational purposes only. The Company bears no responsibility for the data practices or content of third-party platforms.

5.2. Ongoing internal reviews, audits, and risk assessments are conducted to ensure compliance with data protection laws, cybersecurity standards, and internal governance requirements.

5.3. Requests, complaints, or inquiries relating to personal data must be submitted through official Company communication channels. The Company may require verification of identity before responding.

Article 6: Personal Data Breach Management

6.1. In the event of a verified personal data breach, the Company shall promptly assess the incident, implement containment measures, notify competent authorities and affected individuals where legally required, and take corrective action to mitigate potential harm.

Article 7: Data Minimization and Purpose Restriction

7.1. The Company adheres to the principles of data minimization and purpose limitation, ensuring that only information strictly necessary for lawful business purposes is collected, processed, and retained.

Article 8: Third-Party Accountability

8.1. All third-party vendors or partners with access to personal data must satisfy equivalent data protection and information security standards and are contractually bound to process data lawfully and confidentially.

Article 9: Access, Rectification, and Processing Controls

9.1. Data Subjects may request confirmation of whether their personal data is being processed and may seek correction or limitation of processing where appropriate. The Company shall respond within legally prescribed timeframes.