BOOXARO
YOUR EDGE, YOUR RULES, YOUR RESULTS.

# CLIENT DATA PROTECTION POLICY

This Client Data Protection Policy *(the "Policy")* sets forth the principles and regulatory framework under which **BOOXARO** ("the Company," "we," "our," or "us") collects, processes, stores, transfers, and protects the personal data of individuals who access or interact with our digital platforms, including but not limited to our websites, mobile applications, and associated interfaces (collectively, the "Platform"). This Policy governs all processing activities related to clients, users, or visitors (referred to as "you" or "your").

## SECTION 1: DATA ACQUISITION AND PROCESSING ACTIVITIES

**1.1** In the course of account registration, platform usage, compliance assessments, and service delivery, the Company may collect and process personal data, including but not limited to: full legal name, date of birth, nationality, contact details, residential address, government-issued identification, and financial or occupational data. This information is gathered to assess service eligibility, execute risk assessments, and fulfill contractual or statutory obligations.

**1.2** To meet Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, the Company may request supporting documentation, such as identification documents, proof of residence, and financial records. Such data shall be used strictly for identity verification, compliance checks, fraud mitigation, and risk profiling.

**1.3** By accessing or using the Platform, you consent to the automated collection of technical and behavioral data—such as device type, IP address, browser metadata, geolocation, session duration, and clickstream patterns—via cookies and similar technologies for system optimization, fraud detection, and regulatory compliance

## SECTION 2: SECURITY CONTROLS AND DATA RETENTION

**2.1** The Company implements state-of-the-art data security measures including, but not limited to, multi-tier encryption standards, SSL protocols, and continuous threat surveillance to protect the confidentiality, integrity, and availability of your personal data.

**2.2** For enhanced access security, two-factor authentication (2FA) is utilized. This requires verification via a secondary secure channel in addition to login credentials to mitigate unauthorized access.

**2.3** Personal data shall be retained only for as long as necessary to fulfill the purposes for which it was collected or as required by law. Upon expiry of the applicable retention period, the Company shall ensure the secure erasure or anonymization of such data in accordance with applicable regulations.

**2.4** In the event of account recovery or access restoration, re-verification procedures will be undertaken to confirm the identity of the account holder, thereby preventing potential impersonation or fraud.

## SECTION 3: USE, DISCLOSURE, AND CROSS-BORDER TRANSFERS OF DATA

**3.1** Personal data shall be used solely for legitimate business purposes including, but not limited to, service provision, operational management, regulatory compliance, fraud prevention, dispute resolution, and internal audits.

**3.2** The Company may engage external service providers, affiliated entities, or authorized agents to perform operational tasks on its behalf. Any such disclosure shall be governed by strict confidentiality and data protection obligations in accordance with applicable law.

**3.3** The Company may be legally compelled to disclose personal information to governmental authorities, regulatory agencies, or courts. Such disclosures will be made only when required by applicable law and duly recorded.

**3.4** The Company shall not release any personal data of one user to another unless ordered to do so by a competent legal authority. Requests for disclosure must be legally substantiated and submitted in writing.

**3.5** You expressly acknowledge that your personal data may be transmitted and stored in jurisdictions outside your country of residence. The Company will ensure that all international transfers are conducted under recognized legal safeguards that uphold equivalent levels of data protection.

## SECTION 4: RIGHTS, CONSENT, AND LEGAL DISCLAIMERS

**4.1** You have the right to request erasure of your personal data, subject to limitations imposed by legal obligations, regulatory retention requirements, and ongoing investigations related to fraud or contractual breaches. However, data subject to account recovery, dispute resolution, fraud prevention, or legal retention mandates may be exempt from erasure until such conditions are resolved

**4.2** The Company may send informational or promotional materials. You may withdraw your consent to such communications at any time without prejudice to your contractual relationship with the Company.

**4.3** You agree to indemnify, defend, and hold the Company, its affiliates, officers, and employees harmless from any third-party claims arising out of your breach of this Policy or any applicable data protection legislation.

**4.4** The failure of the Company to enforce any provision of this Policy shall not be construed as a waiver of its rights. Any waiver must be formally documented and signed by an authorized Company representative.

**4.5** The Company reserves the right to amend this Policy at its sole discretion. Updates will be posted on the Platform and take effect upon publication. Continued use of the services following such publication constitutes acceptance of the revised Policy.

## SECTION 5: ANCILLARY PROVISIONS

**5.1** Hyperlinks to external websites are provided for user convenience. The Company disclaims any liability for third-party website content or data practices. Users are advised to review the privacy policies of any external sites accessed via hyperlinks from our Platform.

**5.2** The Company shall conduct routine internal audits and reviews of its data protection framework, including breach detection, compliance validation, and risk assessments to ensure regulatory alignment and operational resilience.

**5.3** All inquiries, data access requests, or complaints must be submitted through the official communication channels listed on the Platform. Only submissions originating from a registered user email will be recognized for processing.