CAPITAL NOMOS

DATA GOVERNANCE AND PRIVACY PROTECTION POLICY

1. INFORMATION GOVERNANCE FRAMEWORK AND PRIVACY COMMITMENT

1.1 Scope, Purpose, and Application

1.1.1 This Data Governance and Privacy Protection Policy *(the "Policy")* establishes the legal, operational, technical, cybersecurity, and compliance framework adopted by **CAPITAL NOMOS** *(the "Company," "we," "our," or "us")* governing the collection, recording, processing, storage, transfer, disclosure, retention, safeguarding, and administration of personal information, confidential records, transactional information, electronic communications, and financial data relating to individuals who access, interact with, utilize, or otherwise engage with the Company's websites, Trading Platforms, software systems, applications, communication channels *(such as our official email address support@capitalnomos.com)*, operational infrastructure, and associated digital environments *(collectively referred to as the "Platform")*.

1.1.2 This Policy operates as a supplementary and legally binding component of the Company's Conditions of Use and shall apply to all Clients, prospective Clients, authorized representatives, beneficial owners, affiliates, contractors, visitors, service providers, operational partners, and any individual or entity whose information is processed, maintained, stored, transmitted, or otherwise handled by the Company in connection with its Services, operational activities, compliance obligations, cybersecurity functions, and regulatory responsibilities.

1.1.3 The Company recognizes the importance of maintaining the confidentiality, integrity, availability, and lawful processing of information entrusted to its systems and undertakes to implement commercially reasonable administrative, organizational, operational, technical, and cybersecurity safeguards intended to protect such information against unauthorized access, misuse, disclosure, destruction, compromise, or unlawful processing.

1.1.4 This Policy governs all information processing activities conducted by the Company, whether performed electronically, digitally, manually, automatically, internally, externally, algorithmically, or through independent third-party providers acting on behalf of the Company pursuant to contractual, operational, regulatory, legal, or compliance requirements.

1.1.5 By accessing or continuing to utilize the Platform or Services of the Company, the Client acknowledges having reviewed, understood, and accepted the practices, procedures, disclosures, safeguards, and obligations contained within this Policy.

1.2 Privacy Governance and Internal Compliance Administration

1.2.1 The Company may establish, maintain, supplement, revise, and enforce internal information governance procedures, cybersecurity protocols, access management controls, monitoring systems, operational safeguards, audit mechanisms, compliance frameworks, and risk management measures intended to preserve operational integrity, lawful information processing practices, and regulatory compliance.

1.2.2 The Company reserves the right to conduct internal reviews, monitoring activities, operational investigations, compliance assessments, fraud prevention procedures, cybersecurity evaluations, and technical security inspections where reasonably necessary to:
(a) maintain system integrity;
(b) protect Client information;
(c) ensure compliance with applicable laws;
(d) prevent unauthorized activity;
(e) investigate suspicious conduct; or
(f) preserve operational security.

1.2.3 All employees, officers, consultants, contractors, affiliates, agents, operational personnel, and authorized representatives of the Company shall remain subject to confidentiality obligations, cybersecurity requirements, operational safeguards, and information governance standards established under this Policy and applicable law.

1.2.4 The Company may allocate internal and external resources for purposes including:
(a) cybersecurity enhancement;
(b) compliance administration;
(c) fraud prevention;
(d) operational risk management;
(e) technical infrastructure protection;
(f) information security monitoring;
(g) internal audits; and
(h) employee training programs.

1.2.5 Nothing contained within this Policy shall restrict the Company's authority to cooperate with regulators, supervisory bodies, financial institutions, law enforcement agencies, governmental authorities, cybersecurity specialists, or legally authorized entities where disclosure, monitoring, restriction, investigation, or enforcement actions are reasonably necessary or legally required.

2. INFORMATION COLLECTION, CLIENT VERIFICATION, AND DATA PROCESSING ACTIVITIES

2.1 Personal Information Collection and Verification Procedures

2.1.1 During onboarding, account registration, transactional processing, compliance reviews, fraud prevention activities, operational administration, cybersecurity monitoring, and service delivery functions, the Company may collect, verify, analyze, process, maintain, and store personal, financial, technical, and operational information relating to the Client.

2.1.2 Information collected by the Company may include, without limitation:
(a) full legal name;
(b) date and place of birth;
(c) nationality and citizenship details;
(d) residential or mailing address;
(e) telephone numbers and email addresses;
(f) government-issued identification records;
(g) passport or national identity documentation;
(h) banking information;

(i) occupational details;
(j) financial profile information;
(k) tax-related information;
(l) payment details;
(m) technical device identifiers; and
(n) additional information reasonably necessary for legal, operational, regulatory, compliance, or cybersecurity purposes.

2.1.3 The Company may request supplementary documentation or declarations necessary to satisfy Know Your Customer *("KYC")*, Anti-Money Laundering *("AML")*, Counter-Terrorism Financing *("CTF")*, sanctions compliance, fraud prevention, cybersecurity, operational security, and regulatory obligations.

2.1.4 Verification documentation requested by the Company may include:
(a) government-issued identification;
(b) proof of residential address;
(c) utility bills or bank statements;
(d) corporate registration records;
(e) beneficial ownership declarations;
(f) source-of-funds evidence;
(g) source-of-wealth confirmations;
(h) tax residency certifications; and
(i) additional records deemed reasonably necessary for compliance review purposes.

2.1.5 The Company may utilize internal verification systems, sanctions databases, cybersecurity tools, fraud prevention technologies, independent compliance providers, and third-party verification services for purposes of identity validation, operational security, risk assessment, and regulatory compliance.

2.2 Automated Data Collection and Technical Monitoring

2.2.1 The Client acknowledges and accepts that the Company may automatically collect technical, analytical, behavioral, operational, and transactional information generated through interaction with the Platform or Services.

2.2.2 Automatically collected information may include:
(a) Internet Protocol *(IP)* addresses;
(b) browser configuration details;
(c) operating system information;
(d) device identifiers;
(e) access timestamps;
(f) geolocation indicators;
(g) login activity;
(h) session duration metrics;
(i) clickstream behavior;
(j) transaction patterns;
(k) device fingerprinting data; and
(l) technical usage analytics.

2.2.3 Such information may be collected through cookies, tracking technologies, server logs, cybersecurity systems, analytics tools, monitoring applications, operational surveillance technologies, and fraud prevention software for purposes including:
(a) service optimization;
(b) cybersecurity protection;
(c) fraud prevention;
(d) operational administration;
(e) compliance oversight;
(f) performance monitoring;
(g) user authentication; and
(h) system maintenance.

2.2.4 The Company may combine technical information with personal or financial information for purposes relating to:
(a) operational integrity;
(b) suspicious activity monitoring;
(c) fraud detection;
(d) cybersecurity analysis;
(e) compliance administration;

(f) service enhancement; and
(g) lawful business operations.

3. DATA SECURITY, CYBERSECURITY SAFEGUARDS, AND RECORD RETENTION

3.1 Information Security and Operational Protection Measures

3.1.1 The Company shall implement commercially reasonable cybersecurity measures, operational safeguards, encryption standards, authentication systems, monitoring technologies, access restrictions, network protections, and security procedures intended to preserve the confidentiality, integrity, availability, and lawful processing of information maintained within its systems.

3.1.2 Security measures utilized by the Company may include:
(a) multi-layer encryption technologies;
(b) Secure Socket Layer *("SSL")* protocols;
(c) multi-factor authentication *("MFA")* systems;
(d) access management controls;
(e) firewall protections;
(f) intrusion detection systems;
(g) cybersecurity surveillance technologies;
(h) threat monitoring tools;
(i) incident response procedures; and
(j) internal security audits.

3.1.3 The Company may require additional authentication procedures, identity reconfirmation measures, account recovery verification, or enhanced security checks in circumstances involving suspicious account activity, unusual access attempts, technical inconsistencies, password recovery requests, or operational security concerns.

3.1.4 While commercially reasonable safeguards are implemented, the Client acknowledges that no cybersecurity framework, communication network, electronic storage environment, or digital infrastructure can guarantee absolute protection against unauthorized access, malicious software, cyberattacks, interception, operational disruption, or technical compromise.

3.2 Record Retention and Information Preservation

3.2.1 The Company shall retain personal information, verification materials, transactional records, communications, operational logs, account-related data, and compliance documentation only for such periods as are reasonably necessary to:
(a) fulfill contractual obligations;
(b) satisfy legal or regulatory requirements;
(c) resolve disputes;
(d) prevent fraud;
(e) support cybersecurity investigations;
(f) conduct operational reviews; or
(g) protect the legitimate interests of the Company.

3.2.2 Upon expiration of the applicable retention period, the Company may securely delete, anonymize, archive, destroy, or otherwise dispose of information in accordance with applicable legal obligations, operational requirements, and cybersecurity standards.

3.2.3 The Company reserves the right to retain information beyond standard retention periods where reasonably necessary in connection with:
(a) regulatory investigations;
(b) legal proceedings;
(c) fraud prevention activities;
(d) cybersecurity assessments;
(e) compliance reviews; or
(f) enforcement actions.

CAPITAL NOMOS

4. USE, DISCLOSURE, AND CROSS-BORDER TRANSFER OF INFORMATION

4.1 Authorized Processing and Operational Use of Information

4.1.1 Personal information collected by the Company shall be processed solely for legitimate operational, contractual, legal, compliance, cybersecurity, fraud prevention, regulatory, and lawful business administration purposes.

4.1.2 Such processing activities may include:
(a) account administration;
(b) service delivery;
(c) identity verification;
(d) transaction processing;
(e) customer support;
(f) fraud prevention;
(g) cybersecurity protection;
(h) operational analytics;
(i) legal enforcement;
(j) compliance monitoring;
(k) internal audits; and
(l) regulatory reporting.

4.1.3 The Company may engage affiliates, operational vendors, payment processors, infrastructure providers, cybersecurity consultants, compliance partners, cloud hosting providers, contractors, and authorized third-party service providers to perform operational functions on its behalf.

4.1.4 Any disclosure of information to third-party providers shall occur subject to confidentiality obligations, cybersecurity safeguards, operational controls, contractual protections, and applicable legal requirements.

4.2 Regulatory Disclosure and International Data Transfers

4.2.1 The Company may disclose personal information where reasonably necessary to comply with:
(a) applicable laws;
(b) court orders;
(c) governmental directives;
(d) regulatory obligations;
(e) compliance investigations;
(f) supervisory requests; or
(g) lawful enforcement actions.

4.2.2 The Company shall not disclose the personal information of one Client to another Client except where disclosure is required under applicable law, judicial proceedings, arbitration procedures, regulatory mandates, or lawful enforcement requirements.

4.2.3 The Client acknowledges and accepts that personal information may be processed, stored, transmitted, or accessed in jurisdictions outside the Client's country of residence.

4.2.4 International data transfers may occur where reasonably necessary for:
(a) cloud hosting services;
(b) operational continuity;
(c) payment processing;
(d) compliance administration;
(e) cybersecurity monitoring;
(f) technical support; or
(g) lawful business operations.

4.2.5 The Company shall undertake commercially reasonable efforts to ensure that international transfers are conducted under safeguards reasonably designed to maintain appropriate standards of confidentiality, operational security, cybersecurity protection, and regulatory compliance.

5. CLIENT RIGHTS, CONSENT MANAGEMENT, AND LEGAL DISCLAIMERS

5.1 Data Subject Rights and Consent Administration

5.1.1 Subject to applicable legal limitations, operational requirements, regulatory obligations, fraud prevention activities, and ongoing compliance procedures, the Client may request:
(a) access to personal information;
(b) correction of inaccurate information;
(c) restriction of processing activities;
(d) withdrawal of marketing consent; or
(e) erasure of personal information where legally permissible.

5.1.2 Requests relating to deletion or restriction of personal information may be denied or delayed where retention remains necessary for:
(a) AML compliance;
(b) fraud prevention;
(c) dispute resolution;
(d) legal proceedings;
(e) cybersecurity investigations;
(f) contractual enforcement; or
(g) regulatory obligations.

5.1.3 The Company may distribute operational notices, informational communications, educational materials, compliance updates, promotional communications, or service-related announcements through electronic communication channels. The Client may withdraw consent for promotional communications at any time without affecting the underlying contractual relationship.

5.1.4 Subject to applicable legal, regulatory, operational, cybersecurity, fraud prevention, and compliance obligations, the Client may request the restriction or limitation of specific processing activities relating to their personal information where:
(a) the accuracy of such information is contested;
(b) the processing activity is alleged to be unlawful;
(c) the information is no longer required for operational purposes but remains necessary for legal claims; or
(d) an objection to processing is pending review by the Company.

5.1.5 The Company reserves the right to deny or postpone any restriction request where continued processing is reasonably necessary for:
(a) compliance with legal obligations;
(b) fraud prevention;
(c) cybersecurity protection;
(d) dispute resolution;
(e) operational security; or
(f) legitimate business administration.

5.1.6 The Client may object to specific categories of information processing activities conducted by the Company where such processing is based primarily upon operational, analytical, commercial, or marketing interests rather than mandatory legal obligations.

5.1.7 Upon receipt of a valid objection request, the Company may evaluate whether overriding legal, compliance, cybersecurity, operational, fraud prevention, or legitimate business grounds justify continuation of the relevant processing activity.

5.1.8 Subject to identity verification procedures and applicable legal limitations, the Client may request access to certain personal information maintained by the Company in a structured and commonly used electronic format where such disclosure is operationally feasible and legally permissible.

5.1.9 The Company reserves the right to withhold, redact, restrict, or refuse disclosure of information where such disclosure may:
(a) compromise cybersecurity measures;
(b) expose confidential operational systems;
(c) affect third-party rights;
(d) interfere with fraud prevention activities;
(e) violate legal restrictions; or
(f) undermine regulatory obligations.

5.1.10 The Client acknowledges and accepts that the Company may utilize automated systems, algorithmic tools, fraud detection technologies, risk assessment models, cybersecurity analytics, transaction monitoring systems, and operational review mechanisms for purposes including:
(a) compliance administration;
(b) suspicious activity detection;
(c) operational security;
(d) account monitoring;
(e) fraud prevention;
(f) transaction review; and
(g) service optimization.

5.1.11 Such automated assessments may contribute to decisions involving:
(a) account verification;
(b) withdrawal restrictions;
(c) transaction reviews;
(d) enhanced due diligence;
(e) account suspension;
(f) fraud prevention actions; or
(g) operational risk management measures.

5.1.12 The Company may, where reasonably appropriate and legally permissible, conduct supplementary human review of automated assessments prior to implementation of material account restrictions or enforcement measures.

5.2 Legal Disclaimers and Enforcement Rights

5.2.1 The Client agrees to indemnify and hold harmless the Company, its affiliates, officers, employees, contractors, agents, and representatives against liabilities, claims, damages, losses, penalties, costs, or expenses arising from:
(a) breach of this Policy;
(b) misuse of the Platform;
(c) violation of applicable privacy laws; or
(d) unauthorized disclosure of information attributable to the Client.

5.2.2 Failure by the Company to enforce any provision of this Policy shall not constitute a waiver of its rights, remedies, protections, or enforcement authority under applicable law or contractual obligations.

5.2.3 The Company reserves the right to amend, revise, supplement, replace, suspend, update, or otherwise modify this Policy where reasonably necessary for legal, regulatory, operational, cybersecurity, technological, or commercial purposes.

5.2.4 Continued use of the Company's Services following publication of amendments to this Policy shall constitute acknowledgment and acceptance of the revised provisions.

6. CYBERSECURITY INCIDENT RESPONSE AND OPERATIONAL SECURITY MEASURES

6.1 Cybersecurity Monitoring and Threat Prevention

6.1.1 The Company may implement continuous cybersecurity monitoring systems, threat detection technologies, intrusion prevention mechanisms, vulnerability assessments, penetration testing procedures, operational surveillance protocols, and incident response frameworks intended to safeguard the confidentiality, integrity, availability, and operational security of the Platform, Client information, internal systems, and associated digital infrastructure.

6.1.2 The Company reserves the right to temporarily suspend, isolate, delay, restrict, or terminate access to any account, transaction, communication channel, Platform functionality, or operational system where cybersecurity threats, unauthorized access attempts, malicious activity, technical vulnerabilities, data compromise risks, or operational security concerns are identified or reasonably suspected.

6.2 Incident Investigation and Containment Procedures

6.2.1 In the event of an actual, suspected, or potential cybersecurity incident, data compromise event, unauthorized disclosure, operational intrusion, malware attack, phishing

attempt, or technical breach affecting the Company's systems or Client information, the Company may undertake such actions as it reasonably deems necessary to:
(a) investigate the incident;
(b) contain operational risks;
(c) prevent further unauthorized activity;
(d) preserve evidence;
(e) secure operational systems;
(f) protect Client assets; and
(g) comply with legal or regulatory obligations.

6.2.2 Such measures may include:
(a) temporary account suspension;
(b) password resets;
(c) enhanced identity verification;
(d) transaction restrictions;
(e) communication delays;
(f) forensic investigations;
(g) emergency operational controls;
(h) access revocation; or
(i) system maintenance procedures.

6.3 Notification and Regulatory Cooperation

6.3.1 Where required under applicable law, regulatory obligations, or operational necessity, the Company may notify affected Clients, financial institutions, cybersecurity specialists, supervisory authorities, regulators, law enforcement agencies, or relevant third parties regarding cybersecurity incidents or operational security events.

6.3.2 The timing, scope, content, and manner of any notification issued by the Company shall remain subject to:
(a) legal restrictions;
(b) operational security considerations;
(c) investigative confidentiality;
(d) cybersecurity containment measures; and
(e) regulatory guidance.

6.4 Client Security Responsibilities

6.4.1 The Client remains solely responsible for maintaining the confidentiality and security of:
(a) passwords;
(b) login credentials;
(c) authentication devices;
(d) email accounts;
(e) access codes; and
(f) communication channels associated with the Platform.

6.4.2 The Client undertakes to immediately notify the Company upon becoming aware of:
(a) unauthorized access;
(b) suspected credential compromise;
(c) phishing attempts;
(d) suspicious communications;
(e) malware exposure; or
(f) cybersecurity incidents affecting the Client's devices or account.

6.4.3 The Company shall not be liable for losses arising from the Client's failure to maintain appropriate cybersecurity safeguards, password confidentiality, device protection, or account security practices.

7. ANCILLARY PROVISIONS

7.1 External Resources, Audits, and Communication Procedures

7.1.1 The Platform may contain hyperlinks, integrations, references, or access points to third-party websites, software systems, applications, or external services maintained independently from the Company.

7.1.2 The Company does not control and shall not assume responsibility for the privacy practices, cybersecurity measures, operational standards, or content maintained by third-party platforms.

7.1.3 The Company may conduct periodic operational reviews, cybersecurity assessments, penetration testing procedures, compliance evaluations, risk management audits, and internal investigations intended to strengthen its information governance framework and operational resilience.

7.1.4 All requests relating to:
(a) personal information access;
(b) correction requests;
(c) privacy complaints;
(d) consent withdrawal;
(e) security concerns; or
(f) compliance inquiries

shall be submitted through the Company's officially designated communication channels.

7.1.5 For operational security, verification, and compliance purposes, the Company may require that requests originate from the Client's registered email address or verified communication channel before such requests are processed.