Boursium

Data Governance Policy

INTRODUCTION

This Data Governance Policy (the "Policy") establishes the principles and standards governing the collection, use, handling, storage, disclosure, transfer, retention, and protection of Personal Data by the Company.

The Policy provides a framework for the responsible management and protection of Personal Data in connection with the Company's Services, business operations, Account Holders, and other individuals whose information may be handled by the Company.

The Company is committed to maintaining appropriate standards of privacy, confidentiality, transparency, and information security and to managing Personal Data in accordance with Applicable Law, regulatory requirements, contractual obligations, and the Company's internal governance standards.

This Policy should be read together with the Company's Terms of Use and Governance and other applicable policies, agreements, notices, and disclosures issued by the Company.

CHAPTER I: PURPOSE, SCOPE AND GOVERNANCE

SECTION I.I: PURPOSE AND APPLICATION

This Policy applies to the collection, use, handling, storage, disclosure, transfer, retention, and protection of Personal Data by the Company in connection with its

Services, trading platforms, websites, applications, communication channels, and related business activities.

The Policy applies to Account Holders, prospective Account Holders, Authorized Persons, beneficial owners, business partners, website visitors, platform users, and other individuals whose Personal Data is collected, handled, or maintained by the Company.

Personal Data may be obtained through account registration, onboarding, compliance procedures, websites, trading platforms, applications, customer support, transactions, communications, and other lawful business activities, whether electronically, digitally, verbally, physically, or through third-party sources.

Certain Services, products, jurisdictions, or activities may be subject to additional privacy notices, disclosures, or regulatory requirements, which shall apply together with this Policy where relevant.

SECTION I.II: KEY TERMS AND APPLICATION

For the purposes of this Policy, **"Personal Data"** means information relating to an identified or identifiable individual, whether the individual is identified directly or can reasonably be identified through the information available to the Company.

"Data Handling" means any activity carried out in relation to Personal Data, including obtaining, recording, organizing, storing, accessing, reviewing, using, modifying, disclosing, sharing, transferring, restricting, deleting, or otherwise managing such information.

"Account Holder" means any individual or legal entity that establishes, maintains, or uses an account with the Company or otherwise enters into a business relationship with the Company in connection with its Services.

"Authorized Person" means an individual who is authorized by an Account Holder or otherwise permitted by the Company to access an account, provide instructions, receive information, or act on behalf of an Account Holder.

References to the Company may include its affiliates, subsidiaries, service providers, Authorized Persons, successors, and permitted assigns where the context permits.

Headings and section references are included for convenience and shall not affect the interpretation of this Policy.

SECTION I.III: RELATIONSHIP WITH OTHER GOVERNING DOCUMENTS

This Policy shall be read together with the Company's Terms of Use and Governance and other applicable policies, agreements, disclosures, notices, and procedures.

Nothing in this Policy shall limit any rights or obligations arising under Applicable Law, regulatory requirements, or contractual arrangements.

Where this Policy conflicts with mandatory Applicable Law or regulatory requirements, the applicable legal or regulatory requirement shall prevail to the extent required.

CHAPTER II: COLLECTION AND SOURCES OF PERSONAL DATA

SECTION II.I: TYPES OF PERSONAL DATA

The Company may collect Personal Data that is reasonably necessary for account administration, Service delivery, regulatory compliance, risk management, security, fraud prevention, and legitimate business purposes.

Depending on the nature of the Services, Account, jurisdiction, and business relationship, such information may include identification and contact details, residential information, employment information, financial information, transaction records, source of funds and source of wealth information, technical information, communication records, compliance information, and other information reasonably required by the Company.

The categories of Personal Data collected may vary depending on the Services requested, applicable legal and regulatory requirements, and the circumstances of the relationship between the Company and the relevant individual or entity.

SECTION II.II: DATA PROVIDED BY ACCOUNT HOLDERS AND VERIFICATION INFORMATION

Account Holders may provide Personal Data during account registration, onboarding, identity verification, customer support interactions, transactions, surveys, promotions, or other communications with the Company.

Information provided may include full name, date of birth, nationality, residential address, telephone number, email address, employment details, financial information, source of funds information, tax information, and other information reasonably required by the Company.

The Account Holder is responsible for ensuring that information provided to the Company is accurate, complete, current, and not misleading and shall promptly provide updated information where required.

For purposes of Know Your Customer (KYC), Anti-Money Laundering (AML), sanctions screening, fraud prevention, and other compliance requirements, the Company may request identification documents, proof of address, tax information,

source of wealth documentation, source of funds information, corporate records, beneficial ownership information, and other supporting documentation.

The Company may conduct verification directly or through authorized third-party providers and may carry out ongoing reviews or request updated documentation throughout the business relationship.

SECTION II.III: INFORMATION FROM THIRD-PARTY SOURCES

Where permitted by Applicable Law, the Company may obtain Personal Data from financial institutions, identity verification providers, regulatory databases, sanctions screening services, public records, governmental authorities, business partners, and other lawful sources.

Information obtained from third parties may be combined with information provided directly by an Account Holder for verification, compliance, fraud prevention, security, and risk-management purposes.

The Company may also obtain information concerning beneficial owners, directors, officers, Authorized Persons, representatives, or other individuals associated with an Account Holder where reasonably necessary for account administration, verification, compliance, or risk-management purposes.

SECTION II.IV: TECHNICAL INFORMATION, COOKIES AND DIGITAL INTERACTIONS

When individuals access the Company's websites, trading platforms, applications, or other digital Services, the Company may automatically collect technical, operational, and device-related information, including IP addresses, browser information, device identifiers, operating system information, network information, login activity, usage patterns, and platform interactions.

Such information may be used for security monitoring, fraud prevention, analytics, Service improvement, operational management, and regulatory or compliance purposes.

The Company may use cookies, web beacons, software development kits (SDKs), analytics tools, and similar technologies to maintain functionality, facilitate authentication, remember preferences, improve navigation, monitor performance, enhance security, and analyze the use of its digital Services.

Individuals may manage or restrict certain cookie settings through their browser or device settings. Restricting cookies or similar technologies may affect the functionality of certain Services.

SECTION II.V: COMMUNICATION AND INTERACTION RECORDS

The Company may collect and retain records of communications, correspondence, inquiries, complaints, support requests, telephone conversations, electronic communications, platform messages, and other interactions with Account Holders and other individuals interacting with the Company.

Such records may be used for quality assurance, dispute resolution, compliance monitoring, fraud prevention, Service improvement, training, legal proceedings, security, and operational purposes.

Communications may be monitored, recorded, stored, and reviewed to the extent permitted or required by Applicable Law.

CHAPTER III: USE AND DATA HANDLING PURPOSES

SECTION III.I: DATA HANDLING FOR SERVICE ADMINISTRATION

The Company may collect, use, handle, store, transfer, disclose, and otherwise manage Personal Data for legitimate contractual, operational, legal, regulatory, compliance, security, risk-management, and business purposes.

Personal Data may be handled to establish, maintain, administer, support, and manage Accounts and Services, including account registration, onboarding, identity verification, transaction processing, account maintenance, customer support, communication management, platform administration, and Service delivery.

The Company may use Personal Data to communicate with Account Holders regarding account activity, Service updates, operational matters, security notifications, and other information relating to the Account Holder's relationship with the Company.

Data Handling may be carried out through automated, electronic, manual, or other lawful methods and shall be undertaken for purposes reasonably connected with the Company's activities and obligations.

SECTION III.II: LEGAL, REGULATORY AND COMPLIANCE REQUIREMENTS

The Company may handle Personal Data where necessary to comply with Applicable Law, regulatory requirements, licensing obligations, governmental requests, judicial orders, and other legal or compliance requirements.

Such activities may include Know Your Customer (KYC) procedures, Anti-Money Laundering (AML) compliance, sanctions screening, fraud prevention, transaction monitoring, tax reporting, regulatory reporting, investigations, audits, and other compliance activities.

The Company may retain and review Personal Data for periods necessary to satisfy legal, regulatory, compliance, recordkeeping, and reporting obligations.

Boursium

SECTION III.III: SECURITY, FRAUD PREVENTION AND RISK MANAGEMENT

Personal Data may be handled to detect, prevent, investigate, and respond to fraud, financial crime, unauthorized activity, cybersecurity threats, suspicious transactions, account misuse, and other security-related risks.

The Company may use automated monitoring systems, screening tools, risk assessments, investigative procedures, and other controls to identify unusual activity, assess risks, protect its systems, and safeguard Account Holders and business operations.

The Company may verify information and take appropriate measures where necessary to protect the security and integrity of its Services and operations.

SECTION III.IV: BUSINESS OPERATIONS AND SERVICE IMPROVEMENT

The Company may handle Personal Data to improve its Services, products, technological infrastructure, operational processes, user experience, and business performance.

Such activities may include analytics, Service optimization, performance monitoring, quality assurance, product development, system testing, operational reviews, and internal reporting.

Where permitted by Applicable Law, information may be aggregated, anonymized, or otherwise transformed into a form that does not directly identify individuals for analytical and statistical purposes.

SECTION III.V: MARKETING AND COMMUNICATIONS

Where permitted by Applicable Law, the Company may use Personal Data to provide newsletters, educational materials, market updates, promotional offers, product announcements, event invitations, surveys, and other marketing communications.

Marketing communications may be delivered through email, telephone, SMS, platform notifications, mobile applications, websites, or other permitted communication channels.

Account Holders may withdraw consent to receive marketing communications or modify their communication preferences in accordance with the Company's procedures and Applicable Law.

Withdrawal of marketing consent shall not affect the Company's ability to communicate with an Account Holder regarding account administration, security matters, regulatory obligations, or contractual requirements.

SECTION III.VI: LEGAL PROCEEDINGS AND CORPORATE TRANSACTIONS

The Company may handle Personal Data where reasonably necessary to establish, exercise, defend, investigate, enforce, or protect legal rights, contractual rights, regulatory obligations, or legitimate business interests.

Such activities may include dispute resolution, litigation, arbitration, regulatory investigations, internal investigations, debt recovery, compliance reviews, enforcement actions, and other legal or regulatory proceedings.

Personal Data may also be handled or disclosed in connection with mergers, acquisitions, restructurings, reorganizations, financing arrangements, asset transfers, business sales, investments, joint ventures, or other legitimate corporate transactions.

Where appropriate, Personal Data may be provided to professional advisers, auditors, consultants, investors, financial institutions, transaction counterparties, or other parties involved in such activities, subject to appropriate confidentiality and security measures.

CHAPTER IV: DISCLOSURE AND TRANSFER OF PERSONAL DATA

SECTION IV.I: SERVICE PROVIDERS, BUSINESS PARTNERS AND CORPORATE GROUP

The Company may disclose Personal Data to third-party service providers, contractors, vendors, consultants, professional advisers, operational partners, affiliates, subsidiaries, parent entities, associated companies, successors, and Authorized Persons where reasonably necessary to provide Services or support the Company's business activities.

Such parties may assist with information technology, cloud hosting, payment processing, identity verification, compliance, cybersecurity, customer support, analytics, financial services, administration, and other operational functions.

Personal Data may also be disclosed to banks, payment service providers, liquidity providers, custodians, brokers, intermediaries, and other financial or business partners where necessary to facilitate transactions, account operations, Service delivery, compliance, or risk-management activities.

The Company shall take reasonable steps to ensure that recipients of Personal Data are subject to appropriate confidentiality, security, and data protection obligations where required.

Boursium

SECTION IV.II: REGULATORY, GOVERNMENTAL AND LEGAL DISCLOSURES

The Company may disclose Personal Data to regulators, supervisory authorities, governmental agencies, tax authorities, financial intelligence units, licensing bodies, courts, tribunals, law enforcement agencies, and other competent authorities where required or permitted by Applicable Law.

Such disclosures may occur in connection with regulatory reporting, investigations, audits, inspections, licensing requirements, enforcement actions, judicial proceedings, compliance reviews, or other legal and regulatory matters.

The Company may also disclose Personal Data where reasonably necessary to establish, exercise, defend, investigate, enforce, or protect legal or contractual rights, prevent fraud or financial crime, address security incidents, or protect the Company, Account Holders, or third parties.

The Company may make disclosures without prior notice where permitted or required by Applicable Law.

SECTION IV.III: INTERNATIONAL TRANSFERS

Personal Data may be transferred, stored, handled, or disclosed in jurisdictions outside the Account Holder's country of residence where necessary for operational, technological, administrative, regulatory, security, compliance, or business purposes.

Such transfers may involve affiliates, service providers, financial institutions, business partners, or other authorized third parties located in different jurisdictions.

The Company shall take reasonable steps to implement appropriate safeguards designed to protect Personal Data during international transfers where required by Applicable Law.

SECTION IV.IV: THIRD-PARTY SERVICES AND AUTHORIZED DISCLOSURES

The Company's websites, platforms, applications, or communications may contain links to third-party websites, applications, resources, products, or services.

The Company does not control and shall not be responsible for the privacy practices, content, security measures, or policies of third-party services. Individuals are encouraged to review the applicable privacy notices and terms before providing Personal Data to third parties.

The Company may disclose Personal Data where an Account Holder or other relevant individual has provided consent or otherwise authorized such disclosure, subject to the scope of the authorization and any continuing legal, contractual, regulatory, or operational obligations.

CHAPTER V: DATA SECURITY AND ACCOUNT HOLDER RESPONSIBILITIES

SECTION V.I: SECURITY FRAMEWORK AND PROTECTIVE MEASURES

The Company is committed to maintaining reasonable administrative, technical, physical, and organizational safeguards designed to protect Personal Data against unauthorized access, disclosure, misuse, alteration, loss, destruction, or other unlawful handling.

Security measures may include internal policies, access controls, monitoring systems, risk assessments, personnel training, secure infrastructure, encryption, secure communication protocols, firewalls, and other safeguards considered appropriate by the Company.

The Company may use encryption technologies, Secure Socket Layer (SSL), Transport Layer Security (TLS), secure servers, and other technical measures to protect Personal Data during transmission and storage.

No electronic transmission, storage system, or information security program can be guaranteed to be completely secure. Account Holders acknowledge that electronic communications, internet transmissions, and information systems involve inherent risks.

SECTION V.II: ACCESS CONTROLS AND ACCOUNT SECURITY

The Company may require Account Holders to use multi-factor authentication (MFA), two-factor authentication (2FA), security verification procedures, authentication devices, or other access controls when accessing Accounts or sensitive information.

Access to Personal Data shall be restricted to authorized personnel, service providers, and Authorized Persons who require such access for legitimate business, operational, compliance, security, or regulatory purposes.

The Company may implement role-based access controls, authentication procedures, account monitoring, and other safeguards designed to prevent unauthorized access.

Where an Account Holder is unable to access an Account due to lost credentials, security concerns, technical issues, or other circumstances, the Company may

require identity verification, security confirmations, supporting documentation, or other information before restoring access.

The Company may refuse, delay, suspend, or restrict account recovery where identity verification cannot be satisfactorily completed.

Account Holders remain responsible for maintaining the confidentiality and security of their passwords, credentials, authentication devices, and account access methods.

SECTION V.III: SECURITY MONITORING AND INCIDENT RESPONSE

The Company may conduct ongoing security monitoring, vulnerability assessments, audits, testing procedures, and risk-management activities to identify and address potential security threats.

Security monitoring may include the review of system activity, account access logs, network traffic, operational alerts, authentication events, and other security-related information.

The Company may engage independent security professionals, consultants, auditors, or specialized service providers to assist with security assessments and compliance reviews.

Where an actual or suspected security incident occurs, the Company may investigate, contain, mitigate, restrict access, suspend Services, conduct forensic reviews, engage external specialists, or notify affected parties where required by Applicable Law.

Security incidents may include unauthorized access, data breaches, cybersecurity attacks, system compromises, malware infections, accidental disclosures, or other events affecting the confidentiality, integrity, or availability of Personal Data.

The Company may modify, strengthen, or replace its security measures where reasonably necessary to address emerging threats, technological developments, regulatory requirements, or operational risks.

SECTION V.IV: ACCOUNT HOLDER SECURITY RESPONSIBILITIES

Account Holders shall take reasonable measures to protect their Personal Data, devices, passwords, authentication credentials, and communication channels.

Account Holders should promptly notify the Company of any suspected unauthorized access, cybersecurity incident, security breach, fraudulent activity, or misuse of account credentials.

Account Holders should maintain appropriate software, security settings, antivirus protection, and other safeguards necessary to protect their devices and information.

Failure to maintain reasonable security practices may increase the risk of unauthorized access, data loss, identity theft, fraud, or other adverse consequences.

CHAPTER VI: RETENTION, DATA RIGHTS AND POLICY ADMINISTRATION

SECTION VI.I: RETENTION AND DISPOSAL

The Company shall retain Personal Data for as long as reasonably necessary to provide Services, comply with legal and regulatory obligations, resolve disputes, enforce contractual rights, support legitimate business operations, and satisfy applicable recordkeeping requirements.

Retention periods may vary depending on the nature of the information, applicable legal requirements, regulatory obligations, and operational needs.

When Personal Data is no longer required to be retained, the Company may securely delete, anonymize, archive, or otherwise dispose of it in accordance with Applicable Law and its internal procedures.

SECTION VI.II: DATA RIGHTS AND REQUESTS

Subject to Applicable Law and regulatory requirements, individuals may request access to Personal Data maintained by the Company concerning them.

Individuals may request the correction, updating, or amendment of inaccurate, incomplete, or outdated Personal Data.

Individuals may request deletion of Personal Data where such deletion is permitted by Applicable Law and does not conflict with the Company's legal, regulatory, contractual, security, or compliance obligations.

The Company may refuse, limit, or defer a request where permitted or required by Applicable Law or where necessary to protect legal, regulatory, security, or operational interests.

SECTION VI.III: POLICY AMENDMENTS

Boursium

The Company reserves the right to amend, revise, supplement, replace, or update this Policy from time to time for legal, regulatory, operational, technological, security, or business reasons.

Amendments may become effective upon publication through the Company's official communication channels unless otherwise specified.

Account Holders and other relevant individuals are responsible for periodically reviewing this Policy and any updates published by the Company.

SECTION VI.IV: CONTACT AND GOVERNANCE

Questions, requests, complaints, or inquiries relating to this Policy may be submitted through the Company's official communication channels.

Website: https://boursium.com/

Email: support@boursium.com

The Company may update its official contact details from time to time. Updated contact information shall become effective upon publication through an official communication channel.

This Policy shall be interpreted together with the Company's Terms of Use and Governance and other applicable policies, agreements, disclosures, and notices.

Where this Policy conflicts with mandatory Applicable Law, the applicable legal or regulatory requirement shall prevail to the extent required.