PRIVACY POLICY

---

1. Introduction

1.1 Purpose and Scope

Capitalvo ("Capitalvo," "we," "our," or "us") is committed to safeguarding the privacy and security of personal data entrusted to us by our clients, prospective clients, counterparties, employees, suppliers, and business partners. This Privacy Policy explains how we collect, use, process, disclose, transfer, and protect personal data in accordance with applicable data protection and privacy laws, including but not limited to:

- The **General Data Protection Regulation (EU) 2016/679 (GDPR)**;
- The **UK Data Protection Act 2018 (DPA)**;
- The **California Consumer Privacy Act (CCPA)** and **California Privacy Rights Act (CPRA)**;
- The **Personal Data Protection Act (PDPA) of Singapore**;
- The **Dubai International Financial Centre (DIFC) Data Protection Law**;
- Any other applicable local data protection or privacy regulations.

This Privacy Policy applies globally across all Capitalvo operations, regardless of where the data subject resides or where the data is processed. Where local laws provide stricter requirements, Capitalvo will comply with the higher standard.

1.2 Definition of Personal Data

"Personal Data" refers to any information relating to an identified or identifiable natural person ("Data Subject"). A Data Subject is identifiable if it can be identified directly or indirectly through identifiers such as name, identification number, location data, online identifier, or factors specific to their identity.

1.3 Categories of Personal Data

Capitalvo processes the following categories of personal data:

1. **General (Non-Sensitive) Personal Data**
    - Full name, residential and mailing address, date of birth, nationality;
    - Contact information (telephone numbers, email addresses);
    - Financial and banking details, trading account details, transaction history;
    - Employment information, education history, and other business details.
2. **Special Categories of Personal Data (Sensitive Data)**
    - Information revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership;
    - Health data, biometric data, and genetic information;
    - Data concerning criminal convictions or offences, subject to applicable law;

- National identification numbers or government-issued ID documents.

Processing of sensitive data is strictly limited to circumstances permitted by law (e.g., explicit consent, legal obligations, fraud prevention, or regulatory reporting).

1.4 Business Contact and Sole Proprietorship Data

Business-related data such as corporate email addresses or job titles may qualify as personal data when linked to an individual. For sole proprietors, business details are treated as personal data since they identify a natural person.

---

2. Legal Basis for Processing Personal Data

Capitalvo processes personal data only where a valid legal basis exists under applicable law. The legal bases include, but are not limited to:

- **Performance of a Contract**: To establish, perform, and manage contractual relationships (e.g., opening trading accounts, processing transactions).
- **Compliance with Legal and Regulatory Obligations**: To comply with applicable laws, anti-money laundering (AML) and counter-terrorist financing (CTF) regulations, sanctions screening, tax reporting, and financial regulatory obligations.
- **Legitimate Interests**: Where processing is necessary to pursue our legitimate business interests (e.g., risk management, fraud detection, service improvement), provided such interests do not override the rights and freedoms of Data Subjects.
- **Consent**: Where required by law, Capitalvo will obtain clear and explicit consent from the Data Subject before processing personal data (e.g., for marketing or certain profiling activities).
- **Legal Claims**: Where processing is necessary to establish, exercise, or defend legal claims.

---

3. Collection and Use of Personal Data

Capitalvo collects personal data through:

- Account opening forms, KYC/AML onboarding procedures, and due diligence processes;
- Electronic communications, website interactions, and trading platforms;
- Third-party service providers, background check agencies, and regulatory databases;
- Publicly available sources, subject to applicable law.

Personal data is processed for the following purposes:

- Client onboarding, account maintenance, and identity verification;
- Compliance with AML, CTF, and sanctions obligations;
- Risk management, transaction monitoring, and fraud prevention;
- Execution of trades, clearing, settlement, and related services;

- Internal administration, record-keeping, and regulatory reporting;
- Customer service, complaint handling, and dispute resolution;
- Marketing, communications, and client relationship management (subject to consent where required).

---

4. Data Sharing and Transfers

4.1 Disclosure to Third Parties

Capitalvo may share personal data with:

- Regulatory and supervisory authorities, tax authorities, and law enforcement agencies;
- Auditors, consultants, professional advisers, and external legal counsel;
- Payment processors, banks, custodians, and clearing institutions;
- Technology service providers (IT systems, cloud hosting, cybersecurity providers);
- Affiliates, subsidiaries, and group companies.

4.2 International Data Transfers

Where personal data is transferred across borders, including outside the European Economic Area (EEA) or United Kingdom, Capitalvo ensures that adequate safeguards are implemented, such as:

- European Commission or UK adequacy decisions;
- Standard Contractual Clauses (SCCs);
- Binding Corporate Rules (BCRs);
- Other legally recognized transfer mechanisms.

---

5. Data Retention

Personal data is retained only as long as necessary to fulfil the purposes for which it was collected or as required by law, including regulatory retention requirements. For example:

- AML/KYC data may be retained for at least five (5) years after the business relationship ends;
- Transaction data may be retained for statutory limitation periods applicable under financial regulations.

Data that is no longer required will be securely deleted or anonymized.

---

6. Data Protection Principles

Capitalvo adheres to the following principles in processing personal data:

1. **Lawfulness, Fairness, and Transparency**: Data is processed lawfully and fairly, with clear information provided to Data Subjects.
2. **Purpose Limitation**: Data is collected for specific and legitimate purposes only.
3. **Data Minimization**: Only the minimum data necessary is collected.
4. **Accuracy**: Data is maintained in an accurate and up-to-date form.
5. **Storage Limitation**: Data is retained no longer than necessary.
6. **Integrity and Confidentiality**: Data is secured with technical and organizational measures.
7. **Accountability**: Capitalvo demonstrates compliance with applicable laws and standards.

---

7. Security of Processing

Capitalvo implements robust technical and organizational measures, including:

- Encryption, pseudonymization, and secure storage solutions;
- Access controls, role-based restrictions, and monitoring systems;
- Intrusion detection, firewalls, and anti-malware tools;
- Business continuity and disaster recovery systems;
- Regular security audits, penetration testing, and employee training.

---

8. Data Subject Rights

Depending on applicable law, Data Subjects have the following rights:

- **Right of Access**: To obtain confirmation of whether Capitalvo processes personal data and to receive a copy.
- **Right to Rectification**: To correct inaccurate or incomplete data.
- **Right to Erasure (Right to be Forgotten)**: To request deletion of personal data, subject to regulatory requirements.
- **Right to Restriction of Processing**: To request limitations on how data is processed.
- **Right to Data Portability**: To receive data in a structured, machine-readable format for transfer.
- **Right to Object**: To object to processing for marketing or legitimate interests.
- **Right to Withdraw Consent**: Where processing is based on consent.
- **Right to Lodge a Complaint**: With a supervisory authority in the relevant jurisdiction.

Requests will be handled promptly, in accordance with legal timeframes.

---

9. Profiling and Automated Decision-Making

Capitalvo may use automated processing, including profiling, for:

- Fraud detection and AML monitoring;
- Creditworthiness and suitability assessments;
- Personalized marketing and client engagement.

Where automated decisions have legal or significant effects, Capitalvo ensures that appropriate safeguards are in place, including human intervention upon request.

---

10. Data Protection by Design and by Default

Capitalvo incorporates privacy and data protection principles into all business processes and technological systems by:

- Embedding security and privacy safeguards at the design stage;
- Ensuring default settings minimize data collection;
- Conducting regular risk and impact assessments;
- Reviewing measures periodically to ensure ongoing compliance.

---

11. National and Local Law Compliance

Capitalvo complies with all applicable privacy regulations in the jurisdictions where it operates. Where local laws impose stricter requirements than international standards, Capitalvo will comply with the higher requirement.

---

12. Updates to this Privacy Policy

This Privacy Policy may be updated periodically to reflect legal, regulatory, or operational changes. The most recent version will always be available on our website.

---

13. Contact Information

For questions, requests, or complaints regarding this Privacy Policy or data processing practices, please contact:

Data Protection Officer (DPO)
Email: **privacy@capitalvo.com**

Capitalvo takes all privacy concerns seriously and will respond to inquiries in a timely and professional manner.
