COMPLIANCE POLICY

นโยบายการปฏิบัติตามกฎระเบียบ

VERSION 01 DECEMBER 2022

QRS GLOBAL — PRIVACY, SECURITY & COMPLIANCE POLICY

Version: 01 December 2022

Prepared by: QRS Global Compliance & Information Security Office

Note: This document is prepared using the structure and core content of an industry-standard broker privacy/security policy and expands that foundation to adopt stricter, more comprehensive, and internationally aligned controls and compliance measures.

Purpose and Objective

This Policy sets out QRS Global's commitments, principles and mandatory controls for the collection, processing, retention, disclosure and protection of Personal Data and other sensitive information in the course of our brokerage, advisory and educational services. The Policy also establishes our compliance obligations for anti-money-laundering/combating the financing of terrorism (AML/CFT), market-conduct rules, regulatory reporting, information security standards and incident response requirements. It aims to meet or exceed relevant international standards including, but not limited to, principles embodied by the EU General Data Protection Regulation (GDPR), ISO/IEC 27001 information security management principles, and applicable local regulatory regimes to which QRS Global is subject.

PRIVACY, SECURITY & COMPLIANCE POLICY

Table of Contents

PRIVACY, SECURITY & COMPLIANCE POLICY

A. PRIVACY POLICY (DATA PROTECTION & PERSONAL INFORMATION MANAGEMENT)

1. Policy Scope

1.1 Coverage of Individuals

This Policy applies to all clients (prospective, current and former), Introducing Brokers (IBs), partners, employees, contractors, consultants, temporary staff, officers, directors and any third parties whose Personal Data is collected, stored, processed, transmitted or disposed of by QRS Global or on QRS Global's behalf.

1.2 Coverage of Data Types

Applies to all Personal Data and Confidential Information, including identity, contact, financial, transaction, account, device, behavioural, performance, and special categories of data that QRS processes in connection with its brokerage, advisory and educational services and internal operations.

2. Principles and Legal Bases for Processing

QRS Global commits to processing Personal Data in accordance with the following principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Permissible lawful bases include contract performance, legal/regulatory obligations (e.g., AML/CFT, tax, sanctions), legitimate interests (balanced against individual rights) and consent where required. Where applicable local law imposes stricter grounds, those prevail.

3. Types of Data Collected and Purposes

3.1 Identity & Verification Data

Data examples: full name, date of birth, national ID/passport, tax ID, nationality, residency, identity documents, beneficial ownership information.

Purpose: onboarding, KYC/AML verification, sanctions screening, regulatory reporting and identity proofing.

3.2 Contact & Relationship Data

Data examples: address, email, phone numbers, emergency contact, communication preferences.

Purpose: account management, notifications, regulatory communications, customer service.

3.3 Financial & Transaction Data

Data examples: bank account details, deposit/withdrawal history, trade orders, balances, PSP references.

Purpose: execution and settlement of trades, reconciliation, AML monitoring, tax reporting, dispute resolution.

3.4 Device & Technical Data

Data examples: IP addresses, device IDs, browser and OS metadata, cookies, geolocation (where lawful), logs.

Purpose: platform security, fraud prevention (device/IP correlation), analytics, detection of prohibited trading patterns (e.g., latency/arbitrage misuse).

3.5 Account Behaviour & Performance Data

Data examples: trading strategies metadata, P&L history, frequency and size of trades, copy-trade relationships.

Purpose: compliance monitoring, risk management, master/IB performance assessment, platform/product improvements, permitted marketing.

3.6 Sensitive & Special Data (only where strictly necessary)

Data examples: criminal conviction records where required by law or AML investigations; limited health data for reasonable adjustments.

Purpose: statutory compliance, risk/suitability checks and investigations.

4. KYC, AML/CFT, Sanctions and Enhanced Due Diligence

QRS operates an AML/CTF programme aligned with FATF recommendations and applicable local regulation. Controls include: identity verification, beneficial ownership identification, source of funds/wealth checks, transaction monitoring, sanctions screening, PEP screening and enhanced due diligence for high-risk clients or jurisdictions. QRS documents verification evidence. Where identity or risk cannot be satisfactorily resolved, onboarding or continued account access will be refused or restricted. Suspicious activity is reported internally and to competent authorities as required. QRS reserves the right to suspend or terminate accounts pending investigation.

5. Use, Disclosure and Transfers of Personal Data

Personal Data is used only for stated purposes and compatible purposes. QRS may disclose Personal Data to: regulators and law enforcement; banks, payment processors and custodians; third-party processors (cloud, trade execution, AML/sanctions vendors, analytics providers) under written contracts; legal, audit and professional advisers; and parties expressly authorised by the data subject. International transfers are permitted where appropriate safeguards exist (SCCs, BCRs, adequacy, or contractual/technical compensatory controls) and after risk assessment where protections vary.

6. Third-Party Providers & Processors

QRS performs due diligence and security/privacy assessment prior to engaging processors. Contracts will require processors to: process only per QRS instructions; maintain adequate technical and organisational safeguards; support audit and compliance activities; notify QRS of breaches; and return/securely erase data at contract termination. A register of processors/subprocessors is maintained and periodically reviewed.

7. Retention and Destruction

Personal Data is retained only as long as necessary to satisfy contractual, legal, regulatory, or legitimate business purposes. Retention periods are documented in QRS's Data Retention Schedule (Annex B illustrative examples). After expiry, data is

securely destroyed or anonymised using industry-accepted methods. Certain logs and records (e.g., AML, transaction records) are retained for statutory minimums (commonly 5–10+ years depending on jurisdiction).

8. Data Subject Rights & Requests

QRS recognises data subject rights to the extent provided by law, including rights of access, rectification, erasure (subject to legal retention), restriction, objection, portability and withdrawal of consent. Requests are processed per the Data Subject Request Procedure; identity is verified; statutory timelines observed. QRS may refuse manifestly unfounded/excessive requests but will document rationale and provide recourse options.

9. Cookies, Tracking and Analytics

QRS uses cookies and similar technologies for essential operations (sessions, authentication), security (fraud detection), analytics and optional marketing. Cookie notices and opt-in mechanisms are provided where legally mandated. Persistent identifiers/cross-device tracking are used only where lawful and disclosed in notices.

B. SECURITY POLICY (INFORMATION SECURITY & CYBER RISK MANAGEMENT)

1. Security Governance

QRS's Information Security Office (ISO), in coordination with the Compliance function and senior management (CISO, CCO), governs the ISMS. Adopted frameworks include ISO/IEC 27001, NIST CSF, OWASP and AML/CTF guidance. The Board retains ultimate accountability.

2. Information Security Controls (ISMS) — Technical & Organisational Safeguards

2.1 Access Control & Identity Management

- Principle of least privilege and role-based access control (RBAC).
- Multi-Factor Authentication (MFA) on all privileged and client-facing access.
- Quarterly access reviews and privileged account management.

2.2 Cryptography & Key Management

- TLS 1.2+ (recommend TLS 1.3 when supported) for data in transit.
- Encryption at rest for critical systems and PII where applicable.
- Formal key management procedures, periodic key rotation, HSMs for sensitive keys where required.

2.3 Network, Infrastructure & Application Security

- Network segmentation, firewalls, IDS/IPS, WAFs for web services.
- Secure configuration baselines, vulnerability management and patching SLAs.
- Secure SDLC, static/dynamic analysis (SAST/DAST), code reviews and regular penetration testing.

2.4 Endpoint & Device Security

- EDR/anti-malware on endpoints, device hardening policies, managed device inventory.
- Controls for BYOD where allowed; device attestation for sensitive functions.

2.5 Logging, SIEM & Monitoring

- Centralised log collection and SIEM for real-time detection.
- Tamper-evident logs, secure retention per regulatory requirements (hot logs 90 days as minimum; longer archival per Annex).
- Alerting and escalation playbooks integrated with SOC.

2.6 Backups, Continuity & Disaster Recovery

- Encrypted, immutable backups stored across geographically separate sites.
- Regular backup verification and DR exercises.
- Business continuity plans and RTO/RPO defined for critical services.

3. Incident Response, Notification & Forensics

QRS maintains an Incident Response Plan (IRP) and SOC procedures. On suspected breaches: contain, investigate (forensics), remediate, restore and report. For confirmed Personal Data breaches, QRS will notify regulators and affected data subjects as required by law, providing required information clearly and promptly. Post-incident reviews and remedial measures are documented.

4. Monitoring, Trading Surveillance & Prohibited Conduct Detection

Automated and manual surveillance detect market abuse and prohibited conducts (arbitrage abuse, wash trading, layering, manipulation), suspicious deposit/withdraw patterns, multi-accounting, VPN/proxy misuse and other fraud. Alerts feed a case management workflow; investigations may result in restrictions, penalties, fund actions and regulatory reporting per trading agreements and policy.

5. Third-Party & Vendor Security (Due Diligence and Contracts)

Third parties are assessed by security, privacy and operational criteria. Critical vendors require assurance (SOC2, ISO27001) and contractual controls: data processing obligations, security SLAs, audit rights, breach notification timelines and exit/transition clauses.

6. Business Continuity, DR and Resilience Testing

Continuity plans, failover architectures, and DR runbooks are maintained. Regular tabletop exercises and semi-annual DR tests validate recovery capability and business impact considerations.

7. Audits, Testing & Assurance

Periodic internal audits and independent external reviews are conducted across security, privacy, AML/CFT and trading compliance. Annual external penetration tests and quarterly vulnerability scans are performed; remediation tracked with SLAs. Vendor assurance is reviewed regularly.

8. Data Protection Impact Assessments (DPIA)

DPIAs are mandatory for high-risk processing (e.g., large-scale profiling, systematic monitoring, new data flows or transfers). Outcomes and mitigating controls are documented and approved prior to deployment.

C. COMPLIANCE POLICY (LEGAL, REGULATORY & ETHICAL CONDUCT)

1. Regulatory Compliance Framework & Licensing

QRS shall comply with applicable licensing requirements and obligations of supervisory authorities in operating jurisdictions. The Compliance function maintains oversight and reporting lines to senior management and the Board.

2. AML/CTF Operational Programme & Reporting

QRS maintains an AML/CTF programme covering client risk segmentation, transaction monitoring, STR filing, sanctions screening, ongoing KYC and enhanced due diligence for higher risk relationships. All suspicious activity is escalated and if required reported to authorities in accordance with local law.

3. Fair Trading & Market Conduct (Prohibited Activities)

Prohibited behaviors include arbitrage abuse, latency exploitation, wash trading, layering, front-running, spoofing, identity misrepresentation, and collusive conduct. Robust surveillance and sanctions are applied where contraventions are proven.

4. Recordkeeping & Evidence Preservation

QRS preserves trading records, communications, transactional logs, AML checks and surveillance evidence as required by applicable law and regulatory expectations to ensure auditability and dispute resolution capability.

5. Client Communication Standards & Complaint Handling

QRS communicates clearly and accurately to clients. A formal complaint process captures, investigates and resolves complaints with defined SLA targets; unresolved matters may be escalated to regulators or dispute bodies. Communication relating to regulatory or contractual obligations may be delivered without prior consent where lawful.

6. Employee & Partner Obligations (Confidentiality, Conduct, Training)

All personnel and partners must observe confidentiality obligations and the QRS Code of Conduct.

Mandatory annual training is required for data protection, AML/CFT, security awareness and role-based courses for specialised roles. Phishing simulations and targeted assessments measure effectiveness.

7. Governance, Accountability & Roles (Board, CCO, CISO, DPO)

- Board: ultimate accountability.
- Chief Compliance Officer (CCO): operational oversight of compliance programmes.
- Chief Information Security Officer (CISO): oversees ISMS and incident response.
- Data Protection Officer (DPO): appointed when required by law; otherwise, a senior compliance lead performs DPO-equivalent duties.
- Records of Processing Activities (RoPA), DPIAs, risk registers and audit trails are maintained.

8. Policy Review, Amendments & Publication

Policy is reviewed at least annually and after material business, technology or legal changes. Amendments are Board-approved and published; materially adverse changes impacting data subjects are communicated per law.

9. Enforcement, Sanctions & Remedies

Policy violations by employees may result in disciplinary action up to termination. Third-party breaches may trigger contractual remedies and termination. Clients violating trading rules or engaging in illicit activities may face account restrictions, fund confiscation/reversal, and legal actions per contractual terms.

10. Contact & Responsible Officers

Chief Compliance Officer (CCO): compliance@qrsglobal.com

Chief Information Security Officer (CISO): infosec@qrsglobal.com

Data Protection / Privacy Enquiries: privacy@qrsglobal.com

Postal and regulatory contact details will be published on the corporate website and client documentation.

Annex A — Minimum Technical & Organisational Safeguards (Synopsis)

- MFA for privileged and client-facing access.
- RBAC and quarterly access reviews.
- TLS 1.2+ in transit; encryption at rest for critical PII.
- Secure key management; HSMs where required.
- Quarterly vulnerability scanning; annual penetration testing.
- SIEM with hot log retention (e.g., 90 days) and secure archival (e.g., 7 years) for regulatory logs.
- Immutable encrypted backups across multiple geographic locations.

- SAST/DAST in CI/CD and code review gates.
- Semi-annual BC/DR tests and periodic supplier security assessments.

Annex B — Sample Data Retention Periods (Illustrative)

- Transaction/trade records: minimum 7 years (or as local law requires).
- KYC/KYB records & AML checks: 7–10 years after account closure (subject to local law).
- Security incident logs and investigation records: 7 years.
- Marketing opt-in records: retained while opt-in active + statutory period.
- All retention periods are subject to regulatory minima in the relevant jurisdiction; QRS maintains a formal Data Retention Schedule.

Effective Date & Acceptance

By opening or maintaining an account, accessing our platforms, or using QRS Global services, clients acknowledge they have read and accept this Policy to the extent permitted by applicable law. Specific consents and notices are provided during onboarding and via account settings. The Policy is effective from the date above until superseded.

ADDITIONAL PROVISIONS

1. Data Breach Assessment and Notification Timeline

In the event of a suspected or confirmed Personal Data Breach, the Company shall conduct an initial assessment within 72 hours of becoming aware of the incident. Notifications to regulators and affected individuals will be made in accordance with applicable laws and within legally required timeframes. All breach investigations, findings and remedial actions shall be documented.

2. Consent Withdrawal and Preference Management

Individuals may withdraw their consent at any time without affecting the lawfulness of processing carried out prior to the withdrawal. The Company shall provide accessible mechanisms for managing communication preferences, opting out of optional processing activities, and submitting consent-related requests.

3. Automated Decision-Making and Profiling Disclosure

Certain monitoring, fraud detection and trading surveillance systems may utilise automated processes. However, no adverse action, account restriction, penalty or enforcement measure is taken solely on the basis of automated decision-making. A qualified compliance officer will review and validate any automated alert before a final determination is made.

4. Anti-Fraud, Multi-Account and Identity Misuse Policy

The use of multiple accounts, identity obfuscation techniques, device masking, VPN/proxy manipulation, or coordinated behaviours intended to evade risk controls, exploit latency or manipulate trading outcomes is strictly prohibited.

The Company may correlate accounts using device identifiers, IP addresses, behavioural analytics and other security intelligence to prevent fraud and misuse.

5. Governing Law and Jurisdiction

This Policy, and any dispute arising out of or in connection with it, shall be governed by and interpreted in accordance with the laws of the Union of Comoros. Parties irrevocably submit to the non-exclusive jurisdiction of the competent courts of the Union of Comoros.

6. Data Transfer Impact Assessments (DTIA)

For cross-border data transfers to jurisdictions without an adequate level of data protection, the Company shall conduct a Data Transfer Impact Assessment to evaluate risks and implement appropriate safeguards, including technical, contractual or organisational measures, before such transfers occur.

7. User Authentication and Account Security Responsibilities

Users are responsible for maintaining the confidentiality of their credentials and for using strong, unique passwords. The sharing of login details is prohibited. The Company shall not be liable for losses arising from compromised accounts resulting from inadequate password management or user negligence.

8. Legal Basis and Retention Justification

Retention periods applied by the Company are based on statutory requirements, regulatory guidelines, and operational needs. For example:

- AML/KYC records: retained for 7–10 years after account closure (depending on jurisdictional requirements).
- Trading and transactional data: retained for minimum 7 years to comply with regulatory and audit obligations.
- Complaint and dispute records: retained until all matters are fully resolved.