PRIVACY & DATA PROTECTION POLICY

Version 3.0 | May 2026 | Confidential

www.qrsfx.com

compliance@qrsfx.com

QRS FX — PRIVACY & DATA PROTECTION POLICY (Version 3.0) | May 2026

QRS FX — PRIVACY & DATA PROTECTION POLICY Version 3.0 | Effective: May 2026 | Compliant with Thailand PDPA B.E. 2562

Document Type	Privacy and Data Protection Policy — Client-Facing
Version	3.0
Effective Date	May 2026
Supersedes	All previous versions of QRS FX Privacy Policy
Review Schedule	Annual — next review due May 2027
Data Controller	QRS FX and its group entities
Data Protection Officer (DPO)	dpo@qrsfx.com | appointed under PDPA Section 41(2)
Applies To	All natural persons who are or have been QRS FX clients, Introducing Brokers, Strategy Providers, or website visitors
Related Documents	QRS FX Trading Policy (v3.0); QRS FX Trading Compliance Policy (v3.0)
Lodge a Complaint	dpo@qrsfx.com first; then Thailand PDPC at www.pdpc.or.th

THAILAND PDPA COMPLIANCE STATEMENT

This document is QRS FX's Privacy and Data Protection Policy as required under the Thailand Personal Data Protection Act B.E. 2562 (PDPA) and operates in conjunction with the Cybersecurity Act B.E. 2562 and the Royal Decree on Computer-Related Crimes (No. 2) B.E. 2568 (2025). It sets out how QRS FX collects, uses, stores, protects, and processes personal data and meets all 8 categories of PDPA requirements applicable to data controllers operating in Thailand. QRS FX has formally designated a Data Protection Officer (DPO) under PDPA Section 41(2) on the basis that QRS FX qualifies as a financial institution business engaged in the large-scale processing of personal data and the regular monitoring of data subjects.

SECTION 1 — WHO WE ARE AND HOW TO CONTACT US

1.1 Data Controller

QRS FX is the Data Controller for all personal data collected and processed in connection with QRS FX trading accounts, Introducing Broker partnerships, Strategy Provider activities, and website usage. As Data Controller, QRS FX determines the purposes and means of processing your personal data within the meaning of the Thailand Personal Data Protection Act B.E. 2562 ("PDPA").

1.2 Data Protection Officer (DPO) — Mandatory Appointment

In accordance with PDPA Section 41(2) and the PDPC Notification on Designation of Data Protection Officers (effective 13 December 2023), QRS FX has formally designated a Data Protection Officer. The DPO appointment is required on three independent grounds:

- QRS FX engages in core activities involving the regular and large-scale monitoring of data subjects (trade pattern monitoring, behavioral analytics, fraud prevention).
- QRS FX qualifies as a financial institution business under the PDPC's sectoral notification.
- QRS FX processes sensitive personal data within the meaning of PDPA Section 26 (including biometric data collected during identity verification).

The DPO is responsible for advising QRS FX on PDPA compliance, monitoring policy adherence, coordinating with the PDPC, and serving as the point of contact for data subject inquiries.

1.3 Contact Details

General Enquiries	support@qrsfx.com
Data Protection Officer (DPO)	dpo@qrsfx.com
Compliance Department	compliance@qrsfx.com
Security Incidents	security@qrsfx.com
Complaints	complaints@qrsfx.com
Website	www.qrsfx.com
Thailand PDPC (Regulator)	www.pdpc.or.th

1.4 Language

This Privacy Policy is published in English and Thai. Both versions are equally authoritative. In the event of any discrepancy between the English and Thai versions, the Thai version prevails where required by Thai law; otherwise, the English version prevails. The Thai version is available at www.qrsfx.com/privacy and on request from dpo@qrsfx.com.

SECTION 2 — WHAT PERSONAL DATA WE COLLECT

2.1 Categories of Personal Data

QRS FX collects and processes the following categories of personal data. The collection is limited to what is necessary for the purposes set out in Section 4 (the principle of data minimization):

Category	Examples	Source
Identity Data	Full legal name, date of birth, nationality, passport or national ID number, photograph.	Provided by client at registration
Contact Data	Email address, phone number, residential address, postal address.	Provided by client at registration

Financial Data	Bank account details, deposit and withdrawal history, account balance, trading history. (Treated as sensitive — see Section 11.)	Provided by client and generated by trading activity
Document Data	Copies of passport, national ID, driving license, proof of address, bank statements, source of wealth documents.	Provided by client for KYC
Biometric Data	Selfie images and short videos collected during identity verification; facial geometry data derived from such images for liveness and matching checks. (Treated as sensitive — see Section 11.)	Provided by client at registration with explicit consent
Technical Data	IP address, device fingerprint, device ID, MT5 Terminal ID, browser type, operating system, login timestamps, session data.	Collected automatically
Trading Data	All orders placed including cancelled, executed trades, position history, MT5 account ID, leverage used, profit and loss records.	Generated by trading activity
Communication Data	Email and chat communications with QRS FX, support ticket content, telephone call recordings where applicable.	Generated by client interactions
Compliance Data	KYC status, AML screening results, sanctions check results, compliance investigation notes, Politically Exposed Person (PEP) status.	Generated by compliance processes
Marketing Data	Marketing preferences, promotion participation history, referral source.	Provided by client or collected during registration
Monitoring Data	IP logs, device logs, trade pattern analysis outputs, Client ID cross-reference records, Expert Advisor activity logs, behavioral ML/AI pattern detection outputs, cross-account correlation analysis results.	Generated by compliance monitoring

2.2 Sensitive Personal Data — Section 26 PDPA

Certain categories of data we collect fall within the scope of “sensitive personal data” under PDPA Section 26 and require explicit consent. Section 11 of this Policy sets out QRS FX’s specific treatment of sensitive personal data, including biometric data collected during identity verification and financial data.

2.3 Data We Do Not Collect

QRS FX does not collect: payment card PIN numbers; banking passwords; full payment card numbers (only a masked reference token is retained); special category data we have no operational need for (including political opinions, religious or philosophical beliefs, sexual behavior, genetic data, and trade union membership), except where required by law. We encourage clients never to share passwords or PINs with any party, including with anyone purporting to represent QRS FX.

2.4 Data Minimization

QRS FX applies the data minimization principle. We collect only personal data that is adequate, relevant, and limited to what is necessary for the purposes set out in this Policy. We periodically review our collection practices to remove data fields that are no longer required.

SECTION 3 — LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA

Under the Thailand PDPA, QRS FX must have a valid legal basis under PDPA Sections 24 (general personal data) and 26 (sensitive personal data) for each category of personal data processing. The table below sets out the legal basis QRS FX relies upon for each processing activity:

Processing Activity	Legal Basis (PDPA)	Details
Account registration and KYC	Contractual necessity plus Legal obligation (Sections 24(3), 24(6))	Required to enter and fulfil the client agreement. Also required by AML law.
Biometric verification (selfie / liveness)	Explicit consent (Section 26)	Explicit consent is collected at registration. Refusal means the account cannot be opened, since identity verification is a regulatory prerequisite.
Processing deposits and withdrawals	Contractual necessity (Section 24(3))	Required to perform payment services under the client agreement.
Executing and recording trades	Contractual necessity (Section 24(3))	Required to perform the core trading service.

AML screening and sanctions checks	Legal obligation (Section 24(6))	Required under Thailand AMLO regulations and international sanctions compliance obligations.
IP, device, and trade pattern monitoring	Legitimate interest plus contractual consent (Sections 24(5), 24(3))	QRS FX has a legitimate interest in preventing fraud and Prohibited Practice exploitation. Client provides explicit consent at account opening.
Behavioral ML / AI pattern detection	Legitimate interest (Section 24(5))	Detection of automated systems, AI Analysis Software, and patterns consistent with platform exploitation.
Cross-account correlation analysis	Legitimate interest (Section 24(5))	Detection of coordinated trading rings and multi-account abuse.
Same-IP / Same-Device aggregation	Legitimate interest (Section 24(5))	Aggregation of orders from shared identifiers for fraud prevention. See Trading Policy Section 3.4.
Marketing communications	Consent (Section 19)	QRS FX sends marketing only where the client has opted in. Consent may be withdrawn at any time.
Regulatory reporting and SARs	Legal obligation (Section 24(6))	Required under AML and financial regulation obligations.
Compliance investigations	Legitimate interest plus Legal obligation	Protecting QRS FX's business and meeting legal obligations to investigate suspected Prohibited Practices.
Record retention	Legal obligation (Section 24(6))	Required by financial regulation, AML law, and PDPA recordkeeping rules.

SECTION 4 — HOW WE USE YOUR PERSONAL DATA

4.1 Primary Purposes

QRS FX uses personal data for the following primary purposes:

- Opening and managing your trading account.
- Verifying your identity and conducting Know-Your-Client (KYC) checks, including biometric liveness verification.
- Processing deposits, withdrawals, and other financial transactions.
- Executing and maintaining records of all trading activity.
- Providing customer support and responding to enquiries.
- Conducting Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions compliance checks.
- Monitoring trading activity for compliance with the QRS FX Trading Policy, including behavioral ML / AI pattern detection, cross-account correlation analysis, and Same-IP / Same-Device aggregation.
- Administering the Social Trading platform and calculating Strategy Provider performance fees.
- Communicating account-related information including policy changes.
- Investigating and enforcing the QRS FX Trading Policy and Trading Compliance Policy.

4.2 Secondary Purposes — With Consent Only

With your separate, granular, and revocable consent, QRS FX may use your personal data for: sending marketing communications about QRS FX products, promotions, and events; conducting client satisfaction surveys; and inviting you to participate in research panels. You may withdraw any of these consents independently at any time without affecting your account.

4.3 Automated Decision-Making and Profiling

QRS FX uses automated systems for the following purposes:

- Sanctions list screening — automated name and identifier matching against international sanctions registers.
- Trade pattern flagging — automated detection of patterns consistent with Prohibited Practices as defined in the Trading Policy Section 4.
- Margin and stop-out calculation — automated calculation based on account balance, position size, and instrument leverage.

- Behavioral ML / AI pattern detection — automated detection of automated trading systems, AI Analysis Software, and exploitation patterns.
- Cross-account correlation analysis — automated identification of accounts that may be linked or coordinated.

HUMAN REVIEW GUARANTEE: No significant compliance decision affecting a client's account (including suspension, restriction, termination, fee imposition, or claw back) is taken solely on the basis of automated processing. Every significant compliance decision is reviewed by a qualified compliance officer prior to action. Clients may request human review of any automated flag that has resulted in an enforcement action by emailing dpo@qrsfx.com.

SECTION 5 — YOUR RIGHTS UNDER THE THAILAND PDPA

Under the Thailand Personal Data Protection Act B.E. 2562, you have the following eight rights in relation to your personal data. All requests should be submitted to dpo@qrsfx.com. QRS FX will respond within 30 days. We may request additional information to verify your identity before processing a request.

Right	What This Means	Limitations
Right to Access	Request a copy of all personal data QRS FX holds about you, including account data, KYC records, trade history, communication records, and monitoring data.	We may redact third-party information or withhold data where disclosure would prejudice an active investigation or legal proceedings.
Right to Rectification	If any personal data we hold about you is inaccurate or incomplete, you have the right to request correction, including updating contact details, name changes, and correcting errors.	Identity-related corrections require re-verification of identity documents.
Right to Erasure	Request deletion of your personal data where: data is no longer needed for the original purpose; you withdraw consent; or data was unlawfully processed.	Can not be fulfilled where QRS FX has a legal obligation to retain data (such as the 7-year AML retention). Erasure of trading records is not possible for live or recently closed accounts.
Right to Restriction	Request that QRS FX restricts processing of your data — for example, while a rectification request	Restriction may delay QRS FX's ability to process withdrawals or maintain active account services.

	is being assessed, or where you contest the accuracy of data.	
Right to Data Portability	Request a copy of your personal data in a structured, machine-readable format for data you provided to us based on contractual necessity or your consent.	Only applies to data you provided to us. Does not apply to data we generated (such as compliance investigation notes or monitoring outputs).
Right to Object	Object to processing based on legitimate interest grounds, including the monitoring activities described in Section 4.3 of this Policy.	Objecting to compliance monitoring may prevent QRS FX from offering trading services, as monitoring is necessary for policy enforcement and fraud prevention.
Right to Withdraw Consent	Where QRS FX processes data based on your consent (such as marketing or biometric verification), you may withdraw consent at any time by emailing dpo@qrsfx.com or updating preferences in the QRS FX portal.	Withdrawal does not affect the lawfulness of processing prior to withdrawal. Withdrawal of consent for mandatory compliance monitoring or biometric verification may require account closure.
Right to Complain	Submit a complaint to the Thailand Personal Data Protection Committee (PDPC) at www.pdpc.or.th if you believe your data rights have been violated.	We encourage you to first raise the complaint with QRS FX's Data Protection Officer at dpo@qrsfx.com before escalating to the PDPC.

HOW TO EXERCISE YOUR RIGHTS: Email dpo@qrsfx.com with your full name, account number, and a clear description of your request. For requests concerning sensitive personal data, identity verification by a secondary channel (such as a video call) may be required. QRS FX will respond within 30 days, extendable once by a further 30 days for complex requests with prior written notice to the data subject.

SECTION 6 — WHO WE SHARE YOUR DATA WITH

6.1 Categories of Recipients

QRS FX may share your personal data with the following categories of recipients. Every external recipient (other than government authorities acting under legal compulsion) is subject to a written Data Processing Agreement (DPA) that obliges them to apply data protection standards at least equivalent to the Thailand PDPA:

Recipient	Purpose	Basis
Liquidity Providers	Necessary to execute client orders. Limited to trade data required for execution.	Contractual necessity
Payment Processors	Necessary to process deposits and withdrawals. Limited to payment details required for the transaction.	Contractual necessity
KYC and Identity Verification Providers	Conducting identity checks, document verification, and biometric matching under DPAs.	Legal obligation plus contractual necessity
Sanctions Screening Providers	Screening client names and identifiers against international sanctions lists.	Legal obligation
IT and Cloud Service Providers	Hosting, maintenance, and security of QRS FX systems. Subject to strict DPAs with security audit rights.	Legitimate interest
External Auditors	Annual financial and security audits. Access is read-only and limited in scope.	Legitimate interest plus legal obligation
Financial Commission (FinCom)	Only where a client dispute has been formally submitted to FinCom.	Legitimate interest plus legal proceedings
Regulatory Authorities and Law Enforcement	Where required by law, court order, or regulatory request, including filing of SARs with the Thailand AMLO.	Legal obligation

Introducing Brokers (IBs)	Only with client consent and limited to account opening confirmation and basic account status. No trading data, financial details, or sensitive personal data.	Consent plus contractual necessity

6.2 No Sale of Personal Data

QRS FX does not sell personal data to any third party for any commercial purpose. QRS FX does not allow third-party advertisers, data brokers, or affiliate networks to access client personal data. QRS FX does not permit retargeting client personal data for the benefit of any third-party advertiser.

6.3 Data Processor Obligations

All QRS FX data processors are required, under their respective Data Processing Agreements, to:

- Process personal data only on documented instructions from QRS FX.
- Implement technical and organizational security measures equivalent to those described in Section 9 of this Policy.
- Engage sub-processors only with QRS FX's prior written authorization.
- Notify QRS FX without undue delay of any personal data breach and in any event within 24 hours of becoming aware of the breach.
- Return or delete all personal data on termination of the Data Processing Agreement.
- Submit to audits and inspections by QRS FX or by an auditor mandated by QRS FX.

SECTION 7 — INTERNATIONAL DATA TRANSFERS

7.1 Transfer Safeguards — PDPA Sections 28 and 29

QRS FX may transfer personal data to jurisdictions outside Thailand in connection with its operations. PDPA Sections 28 and 29 apply to all such transfers. Where personal data is transferred to a jurisdiction that has not been recognized by the Thailand PDPC as providing adequate data protection, one of the following safeguards must be in place:

- Standard Contractual Clauses (SCCs) approved by the Thailand PDPC or, where applicable, equivalent SCCs recognized under PDPA Section 28.
- Binding Corporate Rules (BCRs) where transfers occur within the QRS FX group of companies.

- Explicit, informed, and unambiguous consent of the data subject for a specific one-time transfer, with full disclosure of the recipient jurisdiction and the risks involved.
- Necessity for the performance of a contract between the data subject and QRS FX (such as transferring trade data to a non-Thai liquidity provider as required to execute the client's order).
- Necessity for compliance with a legal obligation (such as transfer to a foreign regulator under a mutual legal assistance treaty).

7.2 Liquidity Providers and Payment Processors

QRS FX's liquidity providers and payment processors may be located outside Thailand. All such providers are required, as a condition of their Data Processing Agreement with QRS FX, to apply data protection standards at least equivalent to the Thailand PDPA. QRS FX maintains a register of all data processors and their applicable safeguards.

7.3 Cross-Border Transfer Inventory

A list of all jurisdictions to which QRS FX may transfer personal data, together with the applicable transfer safeguard, is available on request from dpo@qrsfx.com. QRS FX updates this inventory at least quarterly.

SECTION 8 — DATA RETENTION

8.1 Retention Schedule

QRS FX retains personal data only for as long as necessary for the purpose for which it was collected, or as required by law. At the end of the retention period, personal data is permanently deleted from all QRS FX systems, including backups. This schedule is aligned with the Record Retention Schedule in the Trading Compliance Policy Section 7.1:

Data Category	Retention Period	Reason
Identity and KYC documents	7 years from account closure	AML regulations, PDPA record-keeping
Biometric verification data (selfie, liveness)	Until verification is completed plus 7 years from account closure	AML regulations plus dispute resolution
Full trade history	7 years from account closure	Regulatory requirement, dispute resolution

Financial transaction records	7 years from account closure	AML law, accounting obligation
Account communication records	7 years from account closure	Dispute resolution, regulatory compliance
Compliance investigation records	7 years from conclusion	Legal proceedings preparation
Suspicious Activity Reports (SARs)	7 years from filing	AML legal obligation — must not be deleted
Monitoring logs (IP, device, trade pattern, ML/AI outputs)	7 years from account closure	PDPA compliance monitoring basis, legal proceedings
Marketing preferences and consent records	Until consent withdrawn plus 3 years	Proof of consent under PDPA
Social Trading performance data	7 years from last activity	Contractual plus regulatory records
Website analytics (anonymized)	2 years	Legitimate interest — anonymized, cannot identify individuals
Security incident records and breach register	10 years from incident closure	Regulatory reporting and post-incident review

8.2 Deletion Procedure

At the end of the retention period, personal data is deleted from production systems within 30 days and from encrypted backup storage on the next scheduled backup rotation cycle (which is no longer than 90 days). Deletion is logged and verifiable. SAR filings and other records subject to mandatory non-deletion obligations under AML law are retained beyond the 7-year period only to the extent legally required.

SECTION 9 — DATA SECURITY

9.1 Technical Security Measures

QRS FX implements the following technical security measures to protect personal data against unauthorized access, modification, disclosure, or destruction:

- All data in transit is encrypted using TLS 1.2 or higher; TLS 1.3 is preferred for new client connections.
- All data at rest is encrypted using AES-256 encryption.
- Trading platform access by QRS FX staff requires multi-factor authentication (MFA) without exception.
- Client passwords are stored using industry-standard hashing algorithms (bcrypt or equivalent with appropriate work factors). QRS FX staff cannot view client passwords.
- Access to personal data is restricted to staff with a documented legitimate need, enforced by role-based access controls (RBAC) reviewed at least quarterly.
- All system access is logged in tamper-evident audit logs and monitored for unauthorized access attempts.
- Payment card data is tokenized; QRS FX does not store full payment card numbers.
- Production environments are network-segmented from corporate development, and testing environments.
- Annual penetration testing is conducted by an independent qualified third party. Material findings are remediated promptly.
- Vulnerability scanning of QRS FX infrastructure is conducted at least monthly.

9.2 Organizational Security Measures

- All QRS FX staff with access to personal data complete annual PDPA, AML, and information security training.
- All staff are bound by written confidentiality obligations that survive termination of employment.
- Background checks are conducted on all staff with access to sensitive personal data or financial systems.
- A security incident response plan is maintained, tested at least annually, and reviewed after every significant incident.
- Vendor security assessments are conducted before engaging any third-party data processor.
- Physical access to QRS FX premises and data centres is restricted by access control systems and is logged.

9.3 Client Responsibilities and Mandatory Two-Factor Authentication

MANDATORY 2FA: All QRS FX client accounts are required to enable two-factor authentication (2FA) on the trading portal and on the MT5 platform where supported. Accounts that have not enabled 2FA within 30 days of account opening will be restricted from initiating withdrawals until 2FA is activated. This is a security minimum, not an optional convenience.

Clients are otherwise responsible for maintaining the security of their own account credentials. QRS FX requires clients to:

- Use a strong unique password — minimum 12 characters with a mix of upper case, lower case, digits, and symbols.
- Never share login credentials with any third party, including any person claiming to represent QRS FX.
- Notify QRS FX immediately at security@qrsfx.com if you suspect unauthorized access to your account.
- Not access QRS FX services from shared or public devices without first clearing all session data on logout.

SECTION 10 — DATA BREACH NOTIFICATION

10.1 QRS FX Obligations

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, QRS FX will comply with the following procedure:

Timeframe	Action Required
Within 24 hours of detection	Internal escalation to the Data Protection Officer and the Chief Compliance Officer. Initiation of containment measures and forensic preservation.
Within 72 hours of becoming aware	Notification to the Thailand Personal Data Protection Committee (PDPC), including nature of the breach, categories and approximate number of data subjects affected, contact details of the DPO, likely consequences, and measures taken or proposed.
Without undue delay	Notification to affected data subjects directly where the breach is likely to result in a high risk to their rights and freedoms. Notification will include what happened, what data was involved, what QRS FX is doing to address it, and what steps the individual can take to protect themselves.
Within 14 days	Coordinated notification to relevant data processors, liquidity providers, payment processors, and Introducing Brokers whose operations may be affected by the breach.

Ongoing	Documentation of the breach, response actions, and outcomes in QRS FX's breach register. Conduct of a post-incident review by the DPO and implementation of any required improvements to prevent recurrence.

10.2 Incident Severity Classification

Severity	Criteria	Notification
CRITICAL	Unauthorized disclosure of sensitive personal data (biometric, financial) affecting any data subjects, or unauthorized access to client funds.	PDPC + affected data subjects + law enforcement (where applicable)
HIGH	Unauthorized disclosure of non-sensitive personal data affecting more than 100 data subjects, or any disclosure of identity documents.	PDPC + affected data subjects
MEDIUM	Unauthorized disclosure of non-sensitive personal data affecting fewer than 100 data subjects, with no biometric, financial, or identity-document content.	PDPC notification at QRS FX's discretion based on risk assessment; affected data subjects notified
LOW	Internal access control violation or near-miss with no actual data disclosure.	Internal documentation only; reviewed in quarterly compliance report

10.3 Reporting a Suspected Breach

If you believe your QRS FX account data has been compromised or accessed without authorization, take the following steps immediately:

- Contact QRS FX at security@qrsfx.com with the subject line "SECURITY INCIDENT".
- Change your account password immediately via the QRS FX portal.
- Enable two-factor authentication if it is not already active.
- Do not delete suspicious emails, messages, or screenshots — these may be needed for forensic investigation.

- Do not take public action (such as social media posts) regarding the suspected breach until QRS FX has confirmed receipt and provided initial guidance, as premature public statements may impede investigation or escalate harm to other affected clients.

SECTION 11 — SENSITIVE PERSONAL DATA AND BIOMETRIC DATA

11.1 Section 26 PDPA — Categories of Sensitive Data

Under PDPA Section 26, certain categories of personal data are treated as "sensitive personal data" and require explicit consent for processing (or a specific statutory exception). The PDPC has confirmed that the following categories qualify as sensitive personal data:

- Racial or ethnic origin.
- Political opinions.
- Cult, religious, or philosophical beliefs.
- Sexual behavior.
- Criminal records.
- Health data.
- Disability.
- Trade union information.
- Genetic data.
- Biometric data.
- Financial information (as confirmed by the PDPC for regulated financial sectors).

11.2 Biometric Data — Special Treatment

QRS FX collects biometric data in two specific contexts only:

- Identity verification at account opening: a selfie image and a short liveness video, processed to derive facial geometry data for matching against the client's submitted identity document.
- Re-verification: a refreshed selfie or liveness check where required under Section 1.3 of the Trading Compliance Policy.

QRS FX applies the following specific safeguards to biometric data:

(a) Explicit Consent: Biometric data is collected only with the client's explicit, granular, and informed consent given separately from the general account opening consent. The consent screen clearly identifies the type of biometric data collected, the purpose, the retention period, and the consequences of refusal.

(b) Voluntariness: Consent for biometric verification is voluntary. Where a client declines biometric verification, QRS FX offers an alternative identity verification path using documentary evidence and, where required, a supervised video call with a QRS FX compliance officer. No financial inducement is offered for providing biometric data, as this would invalidate consent under PDPC guidance.

(c) Purpose Limitation: Biometric data is used solely for identity verification and AML compliance. It is not used for marketing, profiling, behavioral advertising, or any secondary purpose.

(d) Storage and Encryption: Biometric data is stored separately from other client data, encrypted at rest with AES-256, and accessible only to compliance personnel performing identity verification tasks.

(e) Vendor Governance: Where QRS FX engages a third-party biometric verification provider, the provider is bound by a Data Processing Agreement that specifically prohibits the use of QRS FX clients' biometric data for any purpose other than the verification task instructed by QRS FX.

(f) Right to Withdraw: Clients may withdraw consent for biometric data processing at any time by emailing dpo@qrsfx.com. Withdrawal will not affect the lawfulness of processing prior to withdrawal but may, depending on regulatory requirements, require account closure if alternative verification is no longer available.

11.3 Financial Data as Sensitive Personal Data

The PDPC has confirmed that financial information processed by regulated financial institutions falls within the scope of sensitive personal data. QRS FX treats financial data (bank account details, deposit and withdrawal history, account balance, trading P&L) with the same elevated safeguards as other sensitive personal data, including explicit consent at account opening, encryption at rest, restricted access, and the data subject rights set out in Section 5 of this Policy.

SECTION 12 — COOKIES AND WEBSITE DATA

12.1 Cookie Types

QRS FX's website uses the following categories of cookies. In accordance with PDPC guidelines on consent, the cookie banner offers "Accept all" and "Reject all" options with equal prominence, with granular sub-category consent available:

Cookie Type	Purpose	Can Be Disabled?
Strictly Necessary	Required for the website to function: session management, login, security, fraud prevention. Cannot be disabled without breaking the site.	No
Functional	Remembering your preferences, language settings, and login state across sessions.	Yes — via cookie preferences
Analytics	Understanding how visitors use the website. Data is aggregated and anonymized.	Yes — opt-in required
Marketing	Tracking the effectiveness of QRS FX advertising campaigns. Only active if you consent.	Yes — opt-in required

12.2 Consent Logging

All cookie consent decisions are logged with a timestamp and stored as evidence of consent for a minimum of 3 years after the consent expires or is withdrawn, in accordance with PDPA recordkeeping obligations.

SECTION 13 — CHILDREN'S PRIVACY

QRS FX's trading services are not directed at, and are not lawfully available to, persons under the age of 20 years (the age of majority under the Thai Civil and Commercial Code). QRS FX does not knowingly collect personal data from, or open trading accounts for, anyone under the age of 20.

13.1 PDPA Minor Consent Framework

Under the Thailand PDPA, where personal data is collected from a minor, consent is governed by the Civil and Commercial Code Section 27:

- Persons under 10 years of age: consent must be obtained from the holder of parental authority in all cases.
- People 10 to 20 years of age (and not sui juris by marriage or capacity): consent must be obtained both from the minor and from the holder of parental authority, except for acts the minor is permitted to do independently under the Civil and Commercial Code.

- People 20 years of age and above: own consent is sufficient.

13.2 Account Opening — Minimum Age 20

Notwithstanding the PDPA minor consent framework, QRS FX does not open trading accounts for persons under the age of 20 regardless of parental consent, because (i) trading activity carries financial risk; (ii) margin trading involves obligations that minors are not legally capable of incurring under Thai law; and (iii) AML and tax reporting obligations apply to the account holder personally.

13.3 If We Become Aware

If QRS FX becomes aware that personal data has been collected from a person under the age of 20 without the appropriate consent, that data will be deleted as soon as reasonably practicable, the related trading account (if any) will be closed, and the funds returned to the original source by AML rules. Anyone who believes QRS FX may hold data of a minor should contact dpo@qrsfx.com immediately.

SECTION 14 — DATA PROTECTION IMPACT ASSESSMENT AND VULNERABILITY DISCLOSURE

14.1 Data Protection Impact Assessment (DPIA)

Although PDPA does not currently mandate Data Protection Impact Assessments (DPIAs), QRS FX conducts DPIAs as a matter of best practice before initiating any new processing activity that is likely to result in a high risk to the rights and freedoms of data subjects. Activities that automatically trigger a DPIA at QRS FX include:

- Any new processing of biometric data or other sensitive personal data under PDPA Section 26.
- Any new automated decision-making or profiling system that may produce significant effects on data subjects.
- Any new large-scale monitoring of behavioral data, including ML / AI pattern detection systems.
- Any new cross-border data transfer arrangement involving sensitive personal data.
- Any material changes to a data processor relationship or to the categories of data shared with a data processor.

Each DPIA is reviewed by the DPO and signed off by the Chief Compliance Officer before the relevant processing activity commences. DPIA records are retained for 7 years.

14.2 Vulnerability Disclosure and Security Research

QRS FX welcomes responsible security research and vulnerability disclosure. Security researchers who identify potential vulnerabilities in QRS FX systems are invited to report them as follows:

(a) Report Channel: Email security@qrsfx.com with the subject line "VULNERABILITY DISCLOSURE." Include: a description of the vulnerability, the steps to reproduce, the affected system or URL, and any proof-of-concept that does not involve the personal data of any QRS FX client.

(b) Good-Faith Safe Harbour: QRS FX will not pursue legal action against a security researcher who: (i) acts in good faith; (ii) does not access, modify, or exfiltrate the personal data of any QRS FX client beyond what is strictly necessary to demonstrate the vulnerability; (iii) does not publicly disclose the vulnerability before QRS FX has had a reasonable opportunity to remediate it (90 days unless agreed otherwise); and (iv) does not attempt to disrupt QRS FX services or hold them to ransom.

(c) Response Commitment: QRS FX will acknowledge receipt of a vulnerability report within 2 business days, provide an initial assessment within 10 business days, and provide regular updates until the issue is resolved.

SECTION 15 — CROSS-REFERENCE TO RELATED QRS FX POLICIES

This Privacy and Data Protection Policy operate alongside the following QRS FX policies. In the event of any inconsistency, this Policy prevails on matters of personal data protection; the relevant other policy prevails on its own subject matter:

Related Policy	Subject Matter
QRS FX Trading Policy (v3.0)	Trade execution, prohibited practices (Section 4 A–W + X), enforcement framework (Section 5), monitoring activities and client consent (Section 3), Same-IP / Same-Device aggregation (Section 3.4).
QRS FX Trading Compliance Policy (v3.0)	KYC standards, AML, deposits and withdrawals, slippage compensation, incident claims (7-day window), set-off rights, monitoring consent, record retention, sanctions, IB obligations, copy trading.
QRS FX Cookie Notice	Detailed cookie consent options, cookie inventory, and cookie management interface. Available at www.qrsfx.com/cookies.
QRS FX Client Agreement	Contractual terms governing the trading relationship, including dispute resolution and limitation of liability.

SECTION 16 — UPDATES TO THIS POLICY

QRS FX reviews and updates this Privacy and Data Protection Policy at minimum annually, with the next scheduled review in May 2027. Material changes will be notified by all active clients by email at least 14 days before the change takes effect. The updated Policy will be published at www.qrsfx.com/privacy. Continued use of QRS FX services after the effective date constitutes acceptance of the updated Policy.

Where a change introduces a new processing activity that requires additional consent (such as a new biometric verification method), QRS FX will request fresh explicit consent before that processing commences in respect of existing clients.

Version	3.0
Effective Date	May 2026
Next Review Due	May 2027
Data Controller	QRS FX and its group entities
Data Protection Officer (DPO)	dpo@qrsfx.com
Security Incidents	security@qrsfx.com
Complaints	complaints@qrsfx.com
Thailand PDPC	www.pdpc.or.th
Related Documents	QRS FX Trading Policy v3.0; QRS FX Trading Compliance Policy v3.0

— END OF QRS FX PRIVACY AND DATA PROTECTION POLICY —