4XC

4xc.com

LEGAL DOCUMENTATION

PRIVACY POLICY

4XC is a trade name of 4XC (Seychelles) Ltd, a company registered in Seychelles under number 8428661-1 and licensed by the Financial Services Authority (FSA) under License number SD139.

PRIVACY POLICY

For clients, prospective clients, corporate representatives and website users.

Version	1.0
Effective date	6 July 2026
Registered company number	8428661-1
FSA securities-dealer licence	SD139
Contracting entity	4XC (Seychelles) Ltd
Business/contact address	Office 3, Room B11, 1st Floor, Providence Complex, Providence, Mahé, Seychelles

- *Authorised and regulated by the Seychelles Financial Services Authority as a Securities Dealer.*
- *+44 8000 66 8165 | support-sc@4xc.com | www.4xc.com/sc*

CONTENTS

1. About this Privacy Policy
2. Who we are and how to contact us
3. Who this Policy applies to
4. Personal data we collect
5. How we obtain personal data
6. How and why we use personal data
7. Sensitive and special-category data
8. Corporate applicants and connected persons
9. Automated processing, profiling and monitoring
10. Communications and marketing
11. Cookies and similar technologies
12. Sharing personal data
13. International transfers
14. Data retention
15. Security and confidentiality
16. Your data-protection rights
17. Complaints and regulatory contact
18. Personal data breaches
19. Children
20. Changes to this Policy

1. ABOUT THIS PRIVACY POLICY

This Privacy Policy explains how 4XC (Seychelles) Ltd (the "Company", "4XC", "we", "us" or "our") collects, uses, stores, shares and otherwise processes personal data in connection with its websites, portals, applications, account-opening processes, trading platforms, products, services and communications.

It is intended to provide a clear and accurate description of our processing and international data-transfer activities in accordance with the laws of the Republic of Seychelles, including the Seychelles Data Protection Act, 2023, and the regulatory requirements applicable to our business.

This Policy should be read with the Client Service Agreement, applicable account-opening terms, Risk Disclosure Statement, Order Execution Policy, Conflicts of Interest Policy, Complaints Handling Policy and Cookie Policy. If a separate notice is presented at the point where data is collected, that notice supplements this Policy.

2. WHO WE ARE AND HOW TO CONTACT US

4XC (Seychelles) Ltd is incorporated in Seychelles under company number 8428661-1 and is licensed by the Seychelles Financial Services Authority as a Securities Dealer under license number SD139.

Registered office: Office 3, Room B11, 1st Floor, Providence Complex, Providence, Mahé, Seychelles.

For the purposes of the Seychelles Data Protection Act, 2023, 4XC (Seychelles) Ltd is the data controller for the personal data described in this Policy, except where another entity is identified as a separate or joint controller.

Data Protection Contact: The Data Protection Contact is responsible for receiving and coordinating data-protection queries, requests and complaints relating to this Policy. If the Company is required to designate, or elects to designate, a Data Protection Officer under Applicable Law, the appointed officer's current business contact details will be published in this Policy and made available to data subjects and the Seychelles Information Commission.

If you have any questions about this Policy or wish to exercise your data protection rights, please contact our designated data protection contact at complaints-sc@4xc.com.

3. WHO THIS POLICY APPLIES TO

This Policy applies to personal data relating to:

- individual clients, prospective clients, former clients and website or application users;
- directors, shareholders, ultimate beneficial owners, partners, trustees, protectors, beneficiaries, senior managing officials and other persons connected with a corporate applicant or client;
- authorized representatives, signatories, attorneys, traders, decision-makers and primary contacts;
- introducing brokers, agents, counterparties, payors, payees and other persons involved in a transaction or business relationship;
- complainants, witnesses and persons communicating with us; and
- any other individual whose personal data we process in connection with our regulated activities.

A company or other legal entity is not itself a data subject, but this Policy applies to personal data about natural persons connected with that entity.

4. PERSONAL DATA WE COLLECT

Depending on your relationship with us, we may process the following categories of personal data:

Category	Examples
Identity and personal details	Name, title, date and place of birth, age, gender where relevant, nationality, citizenship, photograph, signature, identity-document details and identifiers.
Contact and address details	Residential, registered and operational addresses, telephone numbers, email addresses and communication preferences.
Corporate and authority information	Position, relationship to an entity, direct and indirect ownership, nature of control, authority to act, powers of attorney, board or signatory information and organizational structure.
Tax and regulatory information	Tax residence, tax identification numbers, regulatory status, license details, declarations and information required for regulatory reporting.
Financial and economic information	Income, revenue, net worth, source of funds, source of wealth, employment, occupation, business activity, bank and payment details, expected activity and financial capacity.
KYC, AML/CFT and screening information	Passports, national identity cards and proof-of-address documents such as utility bills or bank statements; identity-verification results, liveness checks, sanctions and PEP screening, adverse-media or fraud indicators, risk ratings, due-diligence records, monitoring alerts and information relevant to suspicious-activity assessments.
Biometric and other sensitive data	Facial images, liveness or biometric matching data and, where relevant and lawful, information that may reveal political exposure, criminal allegations or convictions, health or vulnerability information.
Account, trading and transaction data	Account numbers, platform identifiers, orders, trades, positions, deposits, withdrawals, payment history, account balances, pricing, margin, leverage, transaction counterparties and audit trails.
Knowledge and appropriateness information	Trading experience, qualifications, knowledge-check responses, product knowledge, appropriateness outcomes, warnings and restrictions.
Communications and complaints	Emails, chats, support tickets, correspondence, documents, complaint information and recordings or transcripts of calls and online meetings where recording is notified or otherwise permitted.
Technical and online data	IP address, device identifiers, browser and operating-system information, login and security logs, session data, portal activity, website usage and cookie or similar-technology data.
Marketing and preference data	Marketing choices, consent records, campaign responses, event participation and preferences.
Derived or inferred data	Risk classifications, fraud or security flags, behavioral indicators, transaction-monitoring results and other conclusions generated from the information described above.

5. HOW WE OBTAIN PERSONAL DATA

We may obtain personal data:

- directly from you, including through forms, documents, telephone calls, emails, chats, meetings, websites, portals, applications and trading platforms;
- from a corporate applicant, client, representative, authorized person, introducing broker or other person who provides information about you;
- from public registers, company registries, regulatory databases, court records, official publications and publicly available sources;
- from identity-verification, fraud-prevention, credit-reference, sanctions, PEP, adverse-media and authentication service providers;
- from banks, payment service providers, card schemes, financial institutions, counterparties, liquidity providers, exchanges and trading or technology providers;
- from group entities, professional advisers, auditors, insurers, agents and service providers; and
- automatically when you use our websites, portals, applications or trading systems.

Where personal data is not obtained directly from you, we will provide information about the processing, where required by law, subject to lawful exemptions such as confidentiality, legal restrictions and financial-crime reporting obligations.

6. HOW AND WHY WE USE PERSONAL DATA

We process personal data only where we have a lawful basis. The applicable basis depends on the purpose and circumstances of the processing.

Account opening and relationship management	Assess applications; verify identity and authority; create, administer, support and close accounts; maintain records and communicate with you.	Steps requested before entering a contract; performance of a contract; legal obligations; legitimate interests.
Providing trading and related services	Receive and execute instructions; operate platforms; process deposits and withdrawals; calculate pricing, margin and charges; issue statements and confirmations.	Performance of a contract; legal obligations; legitimate interests in delivering and safeguarding services.
KYC, AML/CFT, sanctions and regulatory compliance	Due diligence, screening, client risk classification, source-of-funds and wealth checks, transaction monitoring, suspicious-activity investigation and regulatory reporting.	Legal obligations; substantial public interest under Seychelles law; legitimate interests in preventing crime and protecting the financial system.
Biometric identity verification	Facial/liveness checks and identity matching to verify that an applicant is the holder of an identity document.	Explicit consent where required; legal obligations or substantial public interest where permitted by law; fraud-prevention and security interests.
Appropriateness and risk management	Assess knowledge, experience and financial profile; provide warnings; apply risk controls; monitor exposure and product eligibility.	Legal and regulatory obligations; performance of a contract; legitimate interests in responsible service provision and risk management.
Security, fraud prevention and service integrity	Authenticate users; secure accounts and systems; investigate misuse; maintain logs; prevent unauthorised access and protect clients, staff and systems.	Legal obligations; legitimate interests; protection of legal rights and vital interests where relevant.
Complaints, enquiries and legal claims	Respond to support requests and complaints; record investigations and outcomes; defend, establish or exercise legal rights.	Legal obligations; performance of a contract; legitimate interests; administration of justice.
Business operations and improvement	Quality assurance, training, audit, reporting, service development, testing, statistics and operational management using the minimum data necessary.	Legitimate interests; legal obligations; consent where required.
Marketing and client engagement	Provide product information, newsletters, invitations and offers, and measure campaign effectiveness.	Consent where required; otherwise legitimate interests where permitted, with an unconditional right to opt out.
Corporate transactions	Due diligence and transfer of relevant records in connection with a merger, acquisition, restructuring, financing, sale or transfer of business or assets.	Legitimate interests; legal obligations; performance of contractual arrangements.

Where we rely on legitimate interests, we consider whether the processing is necessary and proportionate and whether your rights and interests override those interests. We do not require consent for processing that is necessary to comply with law or perform a contract. Where consent is the basis, it must be informed, freely given and explicit where required, and may be withdrawn without affecting processing already carried out lawfully.

7. SENSITIVE AND SPECIAL-CATEGORY DATA

Some information used in our identity-verification and compliance processes is subject to additional legal protection. This may include biometric data used to confirm identity and information obtained through PEP, sanctions, fraud, adverse-media or criminal-record checks. A person's status as a politically exposed person does not mean that we seek or infer that person's political opinions. We do not intentionally request other categories of sensitive personal data that are not relevant to account opening or service provision. If such information is incidentally contained in a document or communication, we will use it only where necessary and permitted by law.

We process such information only when necessary and permitted by law, including where you have provided explicit consent, where processing is required for substantial public interest or regulatory compliance, where necessary for legal claims or where another lawful exception applies. Access is restricted and enhanced safeguards are applied.

Where identity verification includes facial comparison, selfie or liveness checks, we and our identity-verification service providers may process facial images and biometric data to confirm identity, prevent impersonation and fraud, and meet legal and regulatory obligations. A service provider may perform the technical processing on our behalf, while we may receive and retain verification results, risk indicators and supporting records. Before biometric verification begins, we will provide a dedicated notice identifying the provider, the purpose and legal basis of the processing, relevant retention and international-transfer information, and the available choices or rights. Where required by law, we will obtain explicit consent before biometric processing. We do not use biometric data for marketing or advertising purposes.

8. CORPORATE APPLICANTS AND CONNECTED PERSONS

Where an application or account relates to a company, partnership, trust, foundation or other organization, we process personal data about its connected persons. The organization and the person submitting information must ensure that they are authorized to provide it, that it is accurate, and that the relevant individuals are informed about this Policy or otherwise receive the information required by law.

We may contact connected persons directly to verify identity, ownership, control, authority, instructions or regulatory information. We may also require independent verification from reliable records and sources.

9. AUTOMATED PROCESSING, PROFILING AND MONITORING

We may use automated systems, decision rules and analytical tools to support identity verification, sanctions and PEP screening, fraud prevention, client risk classification, transaction monitoring, security monitoring and appropriateness assessments. These tools may generate scores, matches, alerts, warnings, restrictions or recommendations for review.

We do not ordinarily make decisions that produce legal or similarly significant effects solely by automated means without appropriate safeguards. Where an automated outcome materially affects an application or account, we will provide human review or another safeguard where required by law, unless we are prohibited from doing so by financial-crime or other legal restrictions.

You may contact us for information about significant automated processing and to request human review where applicable. We may be unable to disclose information that would compromise security, fraud-prevention, sanctions or AML/CFT controls.

10. COMMUNICATIONS AND MARKETING

We may contact you by email, telephone, SMS, messaging service, post, portal notification or other agreed channel to administer your account, provide required notices, respond to requests, support our services and meet legal or regulatory obligations.

Marketing communications will be sent only where permitted by law. Where consent is required, marketing consent will be requested separately from acceptance of the Client Service Agreement and will not be a condition of receiving the core service. You may withdraw consent or opt out at any time by using the unsubscribe mechanism or contacting us. We may retain a minimal suppression record to respect your preference.

Service, security, regulatory and account communications are not marketing and may continue while you have an account or while we are required to contact you.

11. COOKIES AND SIMILAR TECHNOLOGIES

Our websites, portals and applications may use cookies, software development kits, pixels, local storage and similar technologies for essential security and functionality, preference management, performance measurement, analytics and, where permitted, advertising or campaign measurement.

Non-essential technologies will be used only in accordance with applicable consent requirements. Details of the technologies in use, their purposes, duration and available controls are provided in the Cookie Policy and cookie-preference tool displayed on the relevant website or application.

12. SHARING PERSONAL DATA

We disclose only the personal data reasonably necessary for the relevant purpose and may share it with the following categories of recipients, where permitted or required by law:

- identity-verification, authentication, KYC, sanctions, PEP, adverse-media, fraud-prevention and transaction-monitoring providers;
- onboarding, client-relationship management, document-management, client-support and communications providers;
- trading-platform, market-data, technology, software, connectivity and cybersecurity providers;
- banks, payment service providers, card schemes and other financial institutions involved in deposits, withdrawals and payment verification;
- liquidity providers, counterparties, brokers, exchanges, execution venues and other parties required to provide or settle trading services;
- the Seychelles Financial Services Authority, Financial Intelligence Unit, Information Commission, tax authorities, courts, law-enforcement bodies and other competent authorities or international organisations where disclosure is required or permitted;
- auditors, lawyers, accountants, tax advisers, insurers, consultants and other professional advisers subject to confidentiality obligations;
- group companies, affiliates and shared-service entities where necessary for lawful business operations, compliance, risk management and service provision;
- introducing brokers, agents and authorised representatives where the disclosure is necessary for the relationship, is authorised by you or is otherwise permitted by law;
- hosting, cloud, backup, email, telephony, call-recording, analytics and website-service providers;
- marketing or research providers where permitted and subject to your choices; and
- a potential buyer, successor, financier or adviser in connection with a corporate transaction

Where we engage processors to process personal data on our behalf, we require them by written agreement to process personal data only on our documented instructions, maintain confidentiality, implement appropriate security measures, assist us in responding to data-subject requests where required, and return or delete personal data at the end of the service relationship unless retention is required by law. We maintain appropriate records of our processors and other recipients of personal data and take reasonable steps to ensure that any changes to service providers do not materially reduce the protections described in this Policy.

13. INTERNATIONAL TRANSFERS

Our services are international. Personal data may be accessed, processed or stored outside Seychelles by group entities, financial institutions, technology providers, trading infrastructure, professional advisers or other recipients described in this Policy.

We transfer personal data outside Seychelles only where the recipient ensures a comparable level of protection for the rights and freedoms of data subjects, or where the transfer is otherwise expressly permitted or authorised under applicable law. Written data-processing and confidentiality terms, security requirements, intra-group arrangements, cross-border privacy rules and contractual safeguards may support this assessment, but they do not replace the statutory requirement for comparable protection.

We assess the nature of the data, the purpose and duration of processing, the laws and practices of the destination, any applicable cross-border privacy arrangements and the technical and organizational safeguards applied. We limit transfers to what is necessary and maintain an internal register of relevant countries or regions, recipient categories and transfer safeguards. You may request current information about the applicable safeguards and, where required, the location of sensitive data processing by contacting the Data Protection Contact.

14. DATA RETENTION

We retain personal data only for as long as necessary for the purposes for which it was collected and to meet legal, regulatory, accounting, fraud-prevention, dispute-resolution and evidential requirements. When retention is no longer required, data is securely deleted, anonymized, archived or access restricted as appropriate. Where legal or regulatory obligations prescribe minimum retention periods, those periods take precedence over general retention principles.

Record category	General retention approach
Active accounts and relationship records	For the duration of the relationship and any additional period required to administer the account and meet legal obligations.
KYC/AML, account-opening, transaction, account-file and business-correspondence records	Generally, at least seven years from the relevant transaction, termination of the business relationship or account closure, or longer where required by law, regulatory direction, investigation, sanctions or legal proceedings.
Closed accounts	Identity, account, transaction and correspondence records are generally retained for at least seven years after closure.
Incomplete, withdrawn or rejected applications	For the period necessary to meet AML/CFT, fraud-prevention, audit, complaint and legal-claim requirements, ordinarily not longer than seven years unless a longer period is justified or required.
Complaints and complaint-related call recordings	Generally, at least seven years after the complaint is resolved, or longer where required by law or regulatory requirements.
Other communications and call recordings	For the period required for account administration, legal and regulatory compliance, quality assurance, complaint handling or evidential purposes, subject to applicable retention requirements.
Marketing records	Until consent is withdrawn or you opt out, plus a minimal suppression record to ensure no further marketing is sent.
Website and cookie data	For the periods stated in the Cookie Policy or cookie-preference tool.
Investigations, legal holds and claims	Until the relevant investigation, regulatory inquiry, audit, legal hold, litigation or limitation period has ended and any resulting obligations have been satisfied.

These periods are general criteria. A shorter or longer retention period may apply where required or permitted by applicable law, regulatory requirements, court order, ongoing investigation, complaint, legal claim or other legitimate business necessity. We periodically review retained data and securely delete, anonymize or otherwise dispose of it when it is no longer required.

15. SECURITY AND CONFIDENTIALITY

We apply risk-based technical and organizational measures intended to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access, misuse or interference. Measures may include:

- role-based access controls, authentication and least privilege access;
- encryption or other protection for data in transit and at rest where appropriate;
- logging, monitoring, audit trails and security-event detection;
- resilience, backup, recovery and business continuity controls;
- confidentiality duties, staff training and disciplinary controls;
- vendor due diligence and contractual security requirements;
- regular testing, assessment and improvement of controls; and
- secure deletion, anonymization or restriction of data when no longer required.

No system can be guaranteed completely secure. You are responsible for keeping passwords and access credentials confidential and for notifying us promptly of suspected unauthorized access.

16. YOUR DATA-PROTECTION RIGHTS

Subject to Seychelles law and lawful restrictions, you may ask us to:

- receive information about how and why we use your personal data and obtain access to the personal data we hold about you, including available information about its source, purposes, retention and disclosures required by law;
- correct personal data that is inaccurate, incomplete or out of date;
- request deletion or restriction of processing where the legal conditions are met;
- object to processing for a specific purpose, including direct marketing;
- withdraw consent at any time where processing is based on consent; and
- receive personal data in a structured, machine-readable and interoperable format, or request transfer to another controller, where applicable.

Your access rights may include information about recipients who accessed your personal data during the period specified by Seychelles law. You may also lodge a complaint with the Information Commission and seek any compensation or judicial remedy available under Seychelles law.

To exercise a right, contact the Data Protection Contact and describe your request. We may request information necessary to verify your identity and authority. Rights may be restricted where necessary to comply with AML/CFT, sanctions, legal-professional privilege, regulatory investigations, suspicious-transaction reporting, security, the rights of others or another lawful exemption. We will explain any restriction unless prohibited by law.

Requests are normally free of charge. A reasonable fee may be charged, or a request may be refused, where it is manifestly unfounded or excessive, as permitted by law.

17. COMPLAINTS AND REGULATORY CONTACT

If you have a concern about how we process your personal data, please always contact us first so that we have an opportunity to address your concern.

If you remain dissatisfied, you may lodge a complaint with the Information Commission of Seychelles or another competent supervisory authority where you have that right under applicable law.

Information Commission of Seychelles
P.O. Box 1342, KLA Residence
3rd Floor, Room 9, Mont Fleuri, Seychelles
Email: enquiries@infocom.sc
Telephone: +248 4303188

18. PERSONAL DATA BREACHES

We maintain procedures to identify, investigate, contain and document personal-data breaches. We will notify the Information Commission without undue delay and no later than 72 hours after becoming aware of a personal data breach and will explain any delay where notification is made later. Where a breach is likely to affect a significant number of individuals and their rights and freedoms, we will promptly inform the affected individuals, subject to any lawful exemption. Where a security breach results in the unauthorized disclosure of non-public consumer data, we will also report it to the Seychelles Financial Services Authority as the appropriate Competent Authority and to the affected financial consumers within 24 hours, as required by applicable financial-consumer law. Notifications will describe the nature and likely consequences of the breach and the measures taken or proposed.

19. CHILDREN

Our trading services are not intended for persons under 18 years of age. We do not knowingly open accounts for minors. If we learn that we have collected a minor's personal data without a valid legal basis or required parental or guardian consent, we will take appropriate steps to restrict or delete it, subject to legal retention requirements.

20. CHANGES TO THIS POLICY

We may update this Policy to reflect changes in law, regulation, technology, services, providers or processing practices. The current version will be published on our website with its effective date. Where a change is material, we will provide additional notice through an appropriate channel before or when the change takes effect, where practicable and required.