

CFIX Data Privacy Policy

1. INTRODUCTION

CFIX Virtual Assets Broker & Dealer Services L.L.C S.O.C (“CFIX”, “we”, “our”, or “us”) is a virtual assets broker-dealer based in the United Arab Emirates, operating under the regulatory framework of the Dubai Virtual Assets Regulatory Authority (VARA), and incorporated in the UAE under Trade Licence Number 1501218 issued by the Dubai Department of Economy and Tourism. Our registered office is Office 704, International Business Tower, Business Bay, Dubai, UAE.

CFIX takes the privacy and protection of personal data seriously. This Data Privacy Policy outlines the principles, practices, and procedures that govern how we collect, use, store, disclose, and protect personal data, as well as the rights of individuals whose data we process. It is designed to ensure compliance with the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the “PDPL”) and its Executive Regulations, the applicable VARA Rulebooks, and other applicable laws.

This Policy is published on our website in accordance with VARA’s requirements relating to the public disclosure of policies governing the protection of personal data.

2. SCOPE

This Policy applies to all personal data that CFIX processes in connection with:

- Visitors to our website and users of our online platforms;
- Prospective, current, and former clients and counterparties, and their authorised representatives, beneficial owners, and connected parties;
- Suppliers, vendors, and other business contacts; and
- Any other natural person whose personal data we receive in the course of our regulated activities.

This Policy applies to personal data in any form, whether digital or physical, and to processing activities conducted within the UAE or in cross-border contexts.

3. REGULATORY AND LEGAL FRAMEWORK

CFIX is committed to full compliance with all applicable data protection laws and regulatory guidance, including in particular:

- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and its Executive Regulations;
- UAE Federal Law No. 15 of 2020 on Consumer Protection;
- UAE Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime;
- The applicable VARA Rulebooks, including the Technology and Information Rulebook;

- Other UAE federal and emirate-level regulations relevant to our business; and
- To the extent applicable to our cross-border activities, relevant international data protection frameworks.

4. DATA CONTROLLER

CFIX Virtual Assets Broker & Dealer Services L.L.C S.O.C is the Data Controller in respect of personal data processed in connection with the services described in this Policy. Our registered office is Office 1824, Park Lane Tower, Business Bay, Dubai, UAE.

5. DATA PROTECTION PRINCIPLES

CFIX applies the following core principles when processing personal data, consistent with the PDPL and the applicable VARA Rulebooks:

Principle	Description
Lawfulness, Fairness, and Transparency	Personal data is processed lawfully, fairly, and transparently. Data Subjects are informed clearly about how and why their data is processed, the legal basis, and their rights.
Purpose Limitation	Personal data is collected for specified, explicit, and legitimate purposes only, and is not further processed in a manner incompatible with those purposes.
Data Minimisation	Only data that is adequate, relevant, and necessary for the stated purpose is collected and processed.
Accuracy	Reasonable steps are taken to ensure that personal data is accurate, complete, and up to date. Inaccurate data is corrected or securely erased without undue delay.
Storage Limitation	Personal data is retained only for as long as is necessary for the purpose of processing and to meet legal, regulatory, and contractual obligations.
Integrity and Confidentiality	Personal data is protected by appropriate technical and organisational security measures, including encryption, access controls, secure architecture, monitoring, and staff training.
Accountability	CFIX takes responsibility for, and is able to demonstrate,

Principle	Description
	compliance with these principles through documented policies, processing records, risk assessments, breach response, audits, and training.

6. PERSONAL DATA WE COLLECT

Depending on how you interact with us, we may collect the following categories of personal data:

- Identity and contact data, such as full name, date of birth, nationality, residential address, email address, and telephone number;
- Identification and verification data, including government-issued identification documents (such as passport or Emirates ID) and proof of address;
- KYC and customer due diligence data, including source of funds and source of wealth information, employment and occupation details, tax residency, politically exposed person status, and sanctions screening results;
- Financial and transactional data, such as bank account details, payment instructions, balances, order activity, transaction history, and counterparty information;
- Blockchain transaction data, including wallet addresses, transaction hashes, on-chain and off-chain transaction history, and related metadata;
- Technical and usage data, including IP addresses, device identifiers, browser type and version, operating system, login activity, and information about how you use our website and platforms;
- Communications data, including emails, chat messages, and call recordings, where lawful; and
- Cookie and tracking data, collected through cookies and similar tracking technologies, subject to your consent where required by applicable law.

7. SENSITIVE PERSONAL DATA

CFIX will only process Sensitive Personal Data (as defined under the PDPL) where the Data Subject has given explicit consent, where the processing is necessary for compliance with a legal obligation, where the processing is necessary to protect the vital interests of the Data Subject or another natural person, or where the processing is otherwise permitted under applicable law.

8. HOW WE COLLECT PERSONAL DATA

We collect personal data from the following sources:

- Directly from you, when you complete our onboarding forms, communicate with us, or use our services;
- Automatically, through your interaction with our website, platforms, and applications (including via cookies and similar technologies);
- From third parties, including identity verification providers, blockchain analytics providers, sanctions and PEP screening databases, public registries, and authorised representatives or agents acting on your behalf; and
- From regulators, law enforcement authorities, and other competent authorities.

9. LAWFUL BASES FOR PROCESSING

We only process your personal data where we have a valid lawful basis to do so under the PDPL. The lawful bases on which we rely include:

- Consent of the Data Subject;
- Performance of a contract with the Data Subject, or to take steps prior to entering into such a contract;
- Compliance with our legal and regulatory obligations;
- Protection of the vital interests of the Data Subject or another natural person;
- Performance of a task carried out in the public interest; and
- Legitimate interests pursued by us or by a third party, balanced against the rights and freedoms of the Data Subject.

10. PURPOSES OF PROCESSING

We process personal data for the following purposes:

- Providing virtual asset services to our clients;
- Fulfilling Know Your Customer (KYC), Customer Due Diligence, and Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) obligations;
- Account management and customer service;
- Transaction processing, monitoring, and reconciliation;
- Compliance with legal, regulatory, and reporting obligations, including obligations under the applicable VARA Rulebooks, sanctions regimes, and the FATF Travel Rule;
- Security, fraud prevention, market abuse detection, and risk management;
- Service improvement and business development, including analytics;
- Marketing communications, where you have provided your consent;
- Statistical analysis and research; and
- Establishing, exercising, or defending legal claims, and protecting our legal rights, property, and the safety of our staff, clients, and other persons.

11. AUTOMATED DECISION-MAKING AND PROFILING

CFIX may use automated systems to assess transaction risk, detect fraud, screen wallets and counterparties, and determine eligibility for certain services. Where an automated decision significantly affects you, you have the right to request human review of the decision and to contest the outcome. CFIX ensures that meaningful human intervention is available in such processes unless required otherwise by law or contractual necessity.

12. COOKIES AND TRACKING TECHNOLOGIES

Our website uses cookies and similar tracking technologies to enable essential site functionality, to remember your preferences, to support security and fraud prevention, and (subject to your consent) to perform analytics and profiling. You may manage your cookie preferences via your browser settings or via our consent management platform. Withdrawal of consent will not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal. For full details, please refer to our Cookie Policy available on our website.

13. DISCLOSURE OF PERSONAL DATA

We may share your personal data with the following categories of recipients, in each case only where the disclosure is lawful and necessary:

- VARA, the UAE Data Office, the Central Bank of the UAE, tax authorities, and other competent regulators, supervisors, and law enforcement authorities;
- Licensed custodians, banking partners, payment service providers, market makers, and liquidity providers used to deliver our services;
- Identity verification, KYC, sanctions and PEP screening, blockchain analytics, and Travel Rule service providers;
- Other licensed Virtual Asset Service Providers and financial institutions where required to comply with the FATF Travel Rule, sanctions, or other applicable obligations;
- Professional advisers (including legal, tax, audit, and compliance advisers) acting on our behalf and bound by confidentiality obligations;
- IT, hosting, communications, and security service providers acting as data processors on our behalf; and
- Any successor entity in the event of a merger, acquisition, restructuring, or sale of all or part of our business.

CFIX does not sell your personal data, and does not share your personal data with third parties for their own marketing purposes without your explicit consent.

14. CROSS-BORDER DATA TRANSFERS

Some of our service providers and group entities may be located outside the United Arab Emirates. We transfer personal data outside the UAE only where one or more of the following conditions is satisfied:

- The destination country is recognised by the UAE Data Office as providing an adequate level of data protection;
- Appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other approved legal instruments providing enforceable rights and effective legal remedies;
- The transfer is necessary for the performance of a contract with the Data Subject or for the implementation of pre-contractual measures requested by the Data Subject;
- The Data Subject has provided explicit and informed consent; or
- The transfer is required for important grounds of public interest, including law enforcement or regulatory compliance.

Where transfers are made to a jurisdiction not designated as providing an adequate level of protection by the UAE Data Office, CFI X conducts a Transfer Impact Assessment to evaluate local laws, surveillance and judicial redress regimes, and applicable technical safeguards before proceeding.

15. RETENTION OF PERSONAL DATA

We retain your personal data only for as long as is necessary to fulfil the purposes for which it was collected, to comply with our legal and regulatory obligations, to resolve disputes, and to enforce our agreements. As a regulated VASP, CFI X is required to retain certain records for prescribed minimum periods. The principal retention periods we apply are:

- Client onboarding and KYC records: a minimum of ten (10) years following the termination of the client relationship;
- Transaction records: a minimum of eight (8) years from the date of the transaction;
- Marketing and communication consents: until the consent is withdrawn; and
- Other personal data: for the period necessary for the purpose for which it was collected, or for any longer period required by applicable law.

Where personal data is no longer required, it will be securely deleted, anonymised, or destroyed.

16. SECURITY OF PERSONAL DATA

CFI X implements appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage. These measures include encryption of data in transit and at rest, role-based access controls, multi-factor authentication, network and endpoint security controls, secure logging and audit trails,

vendor due diligence, employee training, regular security testing (including threat-led penetration testing where applicable), and incident response procedures. Despite these safeguards, no system can be guaranteed to be completely secure; in the event of a personal data breach, CFIx will respond in accordance with its incident response procedures and applicable notification obligations.

17. PERSONAL DATA BREACH NOTIFICATION

In the event of a personal data breach that is likely to pose a risk to the rights and freedoms of Data Subjects, CFIx will notify the UAE Data Office within seventy-two (72) hours of becoming aware of the breach, where required. Where the breach is likely to result in a high risk to the rights, freedoms, or personal security of affected Data Subjects, CFIx will notify those Data Subjects without undue delay. CFIx will also notify VARA in accordance with the timelines set out in the applicable VARA Rulebooks. The notification will include the nature and scope of the breach, the categories and approximate number of affected Data Subjects, the likely consequences of the breach, the measures taken or proposed to address the breach, and the contact details of the Data Protection Officer.

18. YOUR RIGHTS AS A DATA SUBJECT

Subject to the conditions and exemptions set out in the PDPL, you have the following rights in relation to your personal data:

- Right to information: to be informed clearly, concisely, and transparently about how your personal data is collected, used, stored, shared, and protected;
- Right of access: to obtain confirmation of whether we are processing your personal data and, if so, to obtain a copy of that data and information about the processing;
- Right to rectification: to request the correction or completion of inaccurate or incomplete personal data;
- Right to erasure: to request the deletion of your personal data where the data is no longer needed, consent has been withdrawn, processing is unlawful, or erasure is otherwise legally required;
- Right to restriction of processing: to request that we limit the processing of your personal data in certain circumstances, such as where the accuracy of the data is contested;
- Right to data portability: where processing is based on consent or contract and is carried out by automated means, to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller, where technically feasible;
- Right to object: to object to the processing of your personal data on grounds relating to your particular situation, including for direct marketing or profiling;

- Rights related to automated decision-making and profiling: not to be subject to decisions based solely on automated processing that significantly affect you, and to request human intervention;
- Right to withdraw consent: where processing is based on your consent, to withdraw your consent at any time, without affecting the lawfulness of prior processing; and
- Right to lodge a complaint: with the UAE Data Office, VARA, or other competent supervisory authority.

To exercise any of these rights, please contact our Data Protection Officer using the details below. We will acknowledge your request within five (5) business days and respond to it within thirty (30) calendar days, subject to lawful exemptions and to any extension permitted under applicable law. We may need to verify your identity before responding to your request.

19. CHILDREN'S DATA

Our services are not directed at children. CFI does not knowingly collect or process personal data from individuals under the age of 18 without verified parental or guardian consent. If you become aware that personal data of a minor has been provided to us, please contact us so that we may take appropriate action, which may include deleting the data.

20. REPORTING PRIVACY CONCERNS

CFIX maintains a secure and confidential channel through which any individual may report a suspected misuse or unlawful access to personal data. Reports may be submitted through the channels listed under "Contact Us" below, or through our online ethics portal. CFI will investigate all reports promptly and maintains a strict non-retaliation policy for individuals who report concerns in good faith.

21. CHANGES TO THIS POLICY

CFIX reviews this Policy at least annually, and may update it from time to time to reflect changes in our practices, in applicable law, or in regulatory requirements. The latest version will always be available on our website, and the "Last Updated" date below will be revised accordingly. Where changes are material, we will provide additional notice as required under applicable law.

22. CONTACT US

Questions, requests, and complaints relating to this Policy or to our processing of your personal data may be directed to our Data Protection Officer:

Email: dpo@cfix.com

Address: Data Protection Officer, CFI Virtual Assets Broker & Dealer Services L.L.C S.O.C, Office 704, International Business tower, Business Bay, Dubai, UAE

Telephone: +971 4 7706717



Website: www.cfix.com

If you are not satisfied with our response, you have the right to lodge a complaint with the UAE Data Office or other competent supervisory authority. You may also escalate concerns relating to our regulated activities to the Virtual Assets Regulatory Authority (VARA) of Dubai.