

GC EXCHANGE FZE

DIGITAL PRIME BROKERAGE

PRIVACY POLICY

Version 3 August 2026

Document Title	Privacy Policy
Applicability	GC Exchange FZE ("GCEX")
Approver	Board of Directors
Policy Owner	Compliance Officer / Data Protection Officer
Contact Person	Danielis Zelvaras
Last Revision Date	August 2026
Effective Date	September 2026
Version	3.0
Review Cycle	Annual

REGISTER OF AMENDMENTS

No.	Date	Section(s)	Description
1–2	Historic	All	GCEX applied the group privacy policy of GC Exchange Limited.
3	2026	All	Fully revised to identify GC Exchange FZE as controller and align the Policy with the UAE PDPL, VARA Regulations, Rulebooks and Directives applicable to the Firm's VA Broker-Dealer licence.

Table of Contents

1. INTRODUCTION	4
2. KEY TERMS.....	4
3. WHO THIS POLICY APPLIES TO	5
4. PERSONAL DATA WE COLLECT	5
5. HOW WE COLLECT PERSONAL DATA	6
6. PURPOSES AND LAWFUL BASES OF PROCESSING	6
7. WHO WE SHARE PERSONAL DATA WITH	9
7.1 Disclosure to VARA	10
8. INTERNATIONAL TRANSFERS	10
9. HOW WE KEEP PERSONAL DATA SECURE.....	10
10. HOW LONG WE KEEP PERSONAL DATA	11
11. COOKIES	11
12. AUTOMATED DECISION-MAKING	11
13. YOUR RIGHTS.....	11
13.1 Limitations on these rights	12
13.2 How to exercise your rights	12
13.3 Complaints	12
14. MARKETING	13
15. PERSONAL DATA BREACHES	13
16. MINORS	13
17. CONTACT US	13
18. CHANGES TO THIS POLICY	13

1. INTRODUCTION

GC Exchange FZE (“GCEX”, the “Firm”, “we”, “us” or “our”) is a company incorporated in the Dubai World Trade Centre free zone, Dubai, United Arab Emirates, with registration number 1896 and its registered office at One Central, The Offices 4, Level 8, Unit 132 Dubai World Trade Centre Dubai, UAE. GCEX is licensed and regulated by the Virtual Assets Regulatory Authority of the Emirate of Dubai (“VARA”) to carry out Virtual Asset Broker-Dealer Services under licence number VL/23/09/002. Our services are provided to clients meeting the applicable VARA investor-classification criteria.

GCEX respects your right to privacy. This Privacy Policy (the “Policy”) explains what personal data we collect, why we collect it, who we share it with, how we keep it secure, how long we keep it, and the rights you have in relation to it.

This Policy applies to personal data that we collect and process: (a) through our website at <https://www.gc.exchange/> and any related sites, portals, platforms and applications operated by GCEX; (b) when you apply for, use or interact with our products and services; and (c) through any correspondence or interaction with us by telephone, e-mail, in person, at events or otherwise. It does not apply to websites, applications or services operated by third parties, or to the processing activities of other companies in our corporate group acting as independent controllers under their own privacy policies.

This Policy is issued in accordance with Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the “PDPL”), together with any implementing regulations issued thereunder, and Part II (Personal Data Protection) of VARA’s Technology and Information Rulebook. It forms part of GCEX’s written personal data protection compliance programme.

GCEX also complies with data protection and privacy laws outside the UAE to the extent that such laws apply to its activities.

2. KEY TERMS

“Personal Data” means any data relating to an identified natural person, or a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to their biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

“Sensitive Personal Data” means any data that directly or indirectly reveals a natural person’s family or racial origin, political or philosophical opinions or religious beliefs, criminal record, biometric data, or health data.

“Processing” means any operation performed on Personal Data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, transfer, restriction, erasure or destruction.

“Controller” means the party that determines the purposes and means of Processing; **“Processor”** means a party that Processes Personal Data on behalf of, and on the instructions of, a Controller. For the Processing described in this Policy, GC Exchange FZE acts as the Controller of your Personal Data.

3. WHO THIS POLICY APPLIES TO

GCEX provides its services to clients meeting the applicable VARA investor-classification criteria. Most of the Personal Data we process therefore relates to natural persons connected with our clients and prospective clients. This Policy applies to you if you are, in particular:

- a director, officer, employee, authorised representative, authorised trader or other contact person of a client or prospective client of GCEX;
- a shareholder, controller or ultimate beneficial owner of a client or prospective client;
- an individual client onboarded in your personal capacity, where our investor classification criteria permit;
- a visitor to our website or user of our platforms and applications;
- a counterparty representative, service provider contact, or other business contact of GCEX; or
- any other individual whose Personal Data we receive in the course of conducting our licensed activities.

Where you provide us with Personal Data relating to other individuals (for example, your firm's directors, beneficial owners or authorised signatories), you confirm that you are authorised to do so and that you have informed those individuals of this Policy.

4. PERSONAL DATA WE COLLECT

The categories of Personal Data we collect and process include:

Identity data: full name, date and place of birth, gender, nationality, passport, Emirates ID or other government-issued identification details, photographs, and the results of identity verification checks (including liveness and biometric-based verification performed by our identity verification providers).

Contact data: residential and business address, e-mail address and telephone numbers.

Professional and role data: job title, employer, role within the client entity, and evidence of your authority to act on the client's behalf.

Due diligence data: information collected for know-your-customer ("KYC"), customer due diligence ("CDD") and enhanced due diligence ("EDD") purposes, including beneficial ownership information, source of funds and source of wealth information, tax residency and related details (including for FATCA/CRS purposes), politically exposed person ("PEP") status, and the results of sanctions, PEP and adverse media screening. This may include criminal-record-related information where required or permitted by applicable law.

Financial data: bank account details, payment records, account balances, deposits, withdrawals and transaction history.

Virtual asset data: wallet addresses, wallet ownership verification evidence, on-chain transaction data, and risk assessments or analytics scores generated by blockchain analytics tools.

Trading and suitability data: investor classification information, knowledge and experience information, appropriateness assessment inputs and outcomes, and trading activity records.

Communications data: recordings and records of telephone calls and electronic communications with GCEX relating to our services and transactions, and correspondence, complaints and support interactions. Calls and electronic communications with our staff may be recorded and monitored.

Technical and usage data: IP address, device type and identifiers, browser type, operating system, broad geographic location (such as country or city), log-in data, pages accessed and links clicked, and other information collected through cookies and similar technologies.

Marketing and preference data: your marketing preferences, subscriptions, and records of consents given or withdrawn.

We only process Sensitive Personal Data where it is necessary and permitted by applicable law — for example, biometric-based identity verification carried out with your consent as part of onboarding, or criminal-record-related information processed to meet our financial crime prevention obligations.

5. HOW WE COLLECT PERSONAL DATA

We collect Personal Data:

Directly from you — when you or your firm apply for our products or services, complete onboarding forms, register or use an account, transact with us, contact us, subscribe to communications, attend our events, or otherwise correspond with us.

From the client you represent — where a client provides us with the details of its directors, officers, beneficial owners, authorised traders or other representatives.

Automatically — when you visit our website or use our platforms, through cookies, log files and similar technologies, as described in Section 11 (Cookies).

From third parties and publicly available sources — including identity verification and screening providers, sanctions, PEP and adverse media databases, blockchain analytics providers, fraud prevention services, public registers and other public sources, other companies in our corporate group, counterparty virtual asset service providers (“VASPs”) and financial institutions, and regulators or other authorities. We only obtain Personal Data from third parties where they are legally permitted or required to disclose it to us.

6. PURPOSES AND LAWFUL BASES OF PROCESSING

Under the PDPL, Personal Data may not be processed without the consent of the data subject unless an exception applies. In addition to consent, the PDPL permits Processing where it is, among other things: necessary for the performance of a contract to which you are a party, or to take steps at your request prior to entering into a contract; necessary to comply with applicable UAE laws and regulations; necessary to protect the public interest; necessary to initiate, exercise or defend legal claims and rights; necessary to protect your interests; or related to Personal Data that you have made publicly available.

As a VARA-licensed VASP, a substantial part of our Processing is mandated by law and regulation — in particular UAE anti-money laundering and counter-terrorist financing (“AML/CFT”) legislation and the VARA Regulations, Rulebooks and Directives applicable to our licence. The table below sets out the principal purposes for which we process Personal Data and the corresponding lawful bases:

References in the table below to the performance of a contract apply only where the Data Subject is personally a party to the relevant contract, including where the Data Subject is onboarded as an individual client. Where the Data Subject is a director, ultimate beneficial owner, authorised representative, authorised trader, employee or other individual connected with a corporate client, GCEX primarily processes their Personal Data to comply with applicable legal and regulatory obligations, including KYC, AML/CFT, sanctions, Travel Rule, record-keeping and other VARA requirements. Personal Data used for ordinary business communications, account administration and platform access is processed based on consent or another condition permitted under the PDPL, as applicable.

Purpose	Personal Data Typically Involved	Lawful Basis
Client onboarding and due diligence — verifying your identity; conducting KYC, CDD and EDD; identifying beneficial owners; investor classification; assessing appropriateness.	Identity, contact, professional, due diligence, financial and virtual asset data.	Compliance with legal obligations under UAE AML/CFT legislation and the VARA Regulations, Rulebooks and Directives; Processing necessary to protect the public interest; and, where the Data Subject is an individual client, performance of a contract or steps taken at the Data Subject's request before entering into a contract.
Providing our Broker-Dealer Services — opening and administering accounts; receiving, transmitting and executing orders; settlement; client reporting; client support.	Identity, contact, financial, virtual asset, trading and communications data.	Compliance with applicable legal and regulatory obligations; performance of a contract where the Data Subject is an individual client or is otherwise personally a party to the relevant agreement; and, where applicable, consent or another condition permitted under the PDPL for the Processing of Personal Data relating to representatives of corporate clients.
Financial crime prevention — sanctions, PEP and adverse media screening; ongoing transaction monitoring; blockchain analytics (know-your-transaction); wallet ownership verification; investigating and reporting suspicious activity to the UAE	Identity, due diligence, financial, virtual asset and transaction data; screening results.	Compliance with legal obligations; Processing necessary to protect the public interest.

Purpose	Personal Data Typically Involved	Lawful Basis
Financial Intelligence Unit (goAML); targeted financial sanctions compliance and reporting.		
Virtual asset transfers — sharing required originator and beneficiary information with counterparty VASPs and financial institutions (“Travel Rule”), and verifying ownership of self-hosted wallets, in each case where applicable.	Identity, account, wallet address and transaction data.	Compliance with legal obligations.
Regulatory compliance and cooperation — maintaining regulatory records; making reports and notifications to VARA and other competent authorities; enabling VARA’s access to information; audits, inspections and inquiries.	All categories described in Section 4, as relevant.	Compliance with legal obligations, including under the VARA Regulations, Rulebooks and Directives.
Recording and monitoring communications — recording telephone and electronic communications relating to our services and transactions.	Communications data; identity and contact data.	Compliance with applicable legal and regulatory obligations; consent where required; establishment, exercise or defence of legal claims and rights
Risk management and internal governance — compliance monitoring, internal and external audit, management and board reporting, business continuity, systems testing.	Relevant categories described in Section 4.	Compliance with applicable legal and regulatory obligations under the VARA Rulebooks; establishment, exercise or defence of legal claims and rights, where applicable.
Complaints handling and dispute resolution.	Identity, contact, account and communications data.	Compliance with legal obligations; performance of a contract; establishment, exercise or defence of legal claims.
Security and fraud prevention — protecting our platforms, systems, premises, staff and clients; detecting and preventing fraud and misuse.	Technical, usage, identity and transaction data.	Compliance with applicable legal and regulatory obligations; Processing necessary to protect the public interest; establishment,

Purpose	Personal Data Typically Involved	Lawful Basis
		exercise or defence of legal claims and rights, where applicable.
Legal claims — establishing, exercising or defending legal claims and rights.	Relevant categories described in Section 4.	Establishment, exercise or defence of legal claims and rights.
Marketing and events — sending you updates, insights, product information and event invitations.	Identity, contact and marketing preference data.	Your consent, which you may withdraw at any time (see Section 14).
Website operation, analytics and improvement.	Technical and usage data; cookies.	Your consent for non-essential cookies and analytics; provision of the website and functionality you request for strictly necessary cookies.

Where we ask you to provide Personal Data in order to comply with a legal requirement or to enter into or perform a contract with you, we will make this clear at the relevant time. If you do not provide the Personal Data we require, we may be unable to onboard you or the client you represent, or to provide or continue providing our services.

7. WHO WE SHARE PERSONAL DATA WITH

We disclose Personal Data to the following categories of recipients, in each case only where there is a lawful basis to do so and subject to appropriate safeguards:

Group companies — other companies in the GCEX corporate group, where necessary for onboarding, service delivery, technology and operational support, risk management, compliance and internal governance.

Service providers and Processors — third parties that process Personal Data on our behalf and on our instructions, including providers of identity verification and screening services, sanctions and PEP databases, blockchain analytics, trading platform and wallet infrastructure technology, cloud hosting and IT services, communications recording and archiving, and payment and banking services. We require our Processors to implement appropriate technical and organisational security measures and to process Personal Data only in accordance with our documented instructions and applicable data protection law.

Counterparties to your transactions — counterparty VASPs, banks, liquidity providers and other financial institutions, where required to execute and settle transactions or to comply with applicable Travel Rule or wallet verification requirements.

Professional advisers and auditors — legal, accounting, tax, audit and other professional advisers, subject to duties of confidentiality.

Regulators, authorities and law enforcement — VARA, the UAE Data Office, the UAE Financial Intelligence Unit, law enforcement bodies, courts, tax authorities (including under FATCA/CRS) and

other competent authorities, where disclosure is required or permitted by applicable law or regulation, to exercise, establish or defend legal rights, or to protect your vital interests or those of another person.

Corporate transactions — prospective or actual purchasers, investors or successors (and their advisers) in connection with a merger, acquisition, reorganisation or transfer of all or part of our business, subject to confidentiality obligations and applicable law.

Other persons with your consent to the disclosure.

Disclosure to VARA

As a VARA-licensed VASP, GCEX is required under Part II of VARA's Technology and Information Rulebook to take all steps — including providing notifications and obtaining consents — necessary to enable VARA to have access to any information relating to GCEX's compliance with its personal data protection obligations, regardless of where that information is stored. Accordingly, by engaging with GCEX or using our services, you acknowledge and, where required, consent to the disclosure of your Personal Data to VARA upon its request, irrespective of the jurisdiction in which the data is held. GCEX will provide such access in the manner and within the timelines communicated by VARA.

We do not sell your Personal Data.

8. INTERNATIONAL TRANSFERS

GCEX is part of an international group and works with service providers and counterparties located in a number of jurisdictions. Your Personal Data may therefore be transferred to, stored in, or accessed from countries outside the UAE, including jurisdictions in which our group companies and technology providers operate.

Where we transfer Personal Data outside the UAE, we do so in accordance with the PDPL. This means we transfer Personal Data: (a) to jurisdictions recognised as providing an adequate level of protection for Personal Data; or (b) in the absence of such adequacy, subject to appropriate safeguards — such as contracts or binding agreements requiring the recipient to protect the Personal Data to the standards required by the PDPL — or another condition permitted by the PDPL, including your express consent, or where the transfer is necessary for the performance of a contract or for the establishment, exercise or defence of legal claims.

Irrespective of where your Personal Data is stored, it remains subject to this Policy, and GCEX remains able to provide VARA with access to information as described in Section 7.1.

9. HOW WE KEEP PERSONAL DATA SECURE

We implement appropriate technical and organisational measures, proportionate to the risks of the Processing, to protect Personal Data against unauthorised access, disclosure, alteration, loss, misuse or destruction. These measures are maintained under GCEX's technology governance and information security framework, which is overseen by senior management in accordance with VARA's Technology and Information Rulebook, and include:

holding Personal Data in secure facilities and, where held electronically, on secure servers with encrypted transmission links;

access controls, authentication (including multi-factor authentication where applicable), password protection and segregation of duties, with access granted strictly on a need-to-know basis;

classification of client and compliance data as confidential or restricted confidential information, with enhanced controls for the most sensitive records;

logging, audit trails, monitoring, vulnerability assessments and penetration testing;

due diligence on, and contractual security obligations for, service providers that process Personal Data on our behalf;

staff confidentiality obligations, data protection and information security training, and periodic access reviews;

10. HOW LONG WE KEEP PERSONAL DATA

We retain Personal Data for as long as necessary to fulfil the purposes described in this Policy and to comply with our legal and regulatory obligations. As a VARA-licensed VASP, GCEX is subject to record-keeping requirements under the VARA Rulebooks and UAE AML/CFT legislation. In general, records relating to clients, due diligence, transactions and regulatory compliance are retained for a minimum of eight (8) years from the end of the relevant business relationship, or from the date of the relevant record or transaction, as applicable. Certain records, such as recordings of communications, are retained for the periods specified in the applicable VARA requirements.

11. COOKIES

Our website uses cookies and similar technologies, including strictly necessary cookies and, subject to consent where required, analytics and marketing cookies. Further information about the cookies used and available preference controls is provided in our Cookie Policy.

12. AUTOMATED DECISION-MAKING

We use automated tools to support identity verification, sanctions and PEP screening, blockchain analytics and other onboarding checks. GCEX does not make decisions producing legal or similarly significant effects based solely on automated Processing. Material onboarding, client-classification and appropriateness decisions are subject to meaningful human review.

Where a decision that produces legal effects or otherwise significantly affects you is based solely on automated Processing, you have the right, in accordance with the PDPL, to contest the decision, to express your point of view, and to request a review of the decision by a member of our staff. To exercise this right, please contact us using the details in Section 17.

13. YOUR RIGHTS

Subject to the conditions and exemptions set out in the PDPL (in particular Articles 13 to 18) and other applicable law, you have the following rights in relation to your Personal Data:

Right to information and access to obtain confirmation of whether we process your Personal Data and information about that Processing, including the purposes of Processing, the categories of Personal Data concerned, the recipients or categories of recipients, the applicable retention periods or criteria, cross-border transfers and related safeguards, automated Processing and, where your Personal Data was not collected directly from you, available information concerning its source.

Right to obtain a copy and data portability — to receive a copy of your Personal Data in a structured, commonly used, machine-readable format, and to request its transfer to another controller where technically feasible and where the conditions of the PDPL are met.

Right to rectification — to request correction of inaccurate Personal Data and completion of incomplete Personal Data. Where we correct our records, we will take reasonable steps to notify third parties to whom the data has been disclosed.

Right to erasure — to request deletion of your Personal Data in the circumstances provided for in the PDPL.

Right to restriction — to request that we restrict the Processing of your Personal Data in the circumstances provided for in the PDPL.

Right to object / request cessation of Processing — to object to Processing in the circumstances provided for in the PDPL, including Processing for direct marketing purposes.

Rights relating to automated decision-making — as described in Section 12.

Right to withdraw consent — where Processing is based on your consent, to withdraw that consent at any time. Withdrawal does not affect the lawfulness of Processing carried out before withdrawal, and does not affect Processing carried out on another lawful basis. If you withdraw consent, we may be unable to provide certain features or services for which the Processing is essential.

Limitations on these rights

These rights are not absolute. As a regulated VASP, we are required by law to retain certain records and to carry out certain Processing irrespective of an objection or a request for erasure or restriction — for example, records maintained under VARA record-keeping requirements and UAE AML/CFT legislation. In limited circumstances, applicable law may also prevent us from confirming or disclosing certain information, including in connection with financial crime prevention and reporting obligations. Where we are unable to action a request, we will explain why to the extent the law permits us to do so.

How to exercise your rights

You may exercise your rights, free of charge, by contacting us at compliance@gc.exchange, marked for the attention of the Data Protection Officer. We may need to verify your identity before acting on a request. We will respond without undue delay and within the timeframes required by applicable law.

Complaints

If you have a concern about how we process your Personal Data, we encourage you to contact us first so that we can address it. You also have the right to lodge a complaint with the UAE Data Office, the federal data protection authority established under Federal Decree-Law No. 44 of 2021, in accordance with the procedures prescribed under the PDPL. In addition, you may raise concerns regarding our conduct as a licensed VASP with VARA.

14. MARKETING

We will only send you direct marketing communications — such as market updates, product information and event invitations — where we have your consent or are otherwise permitted to do so under applicable law. You can opt out at any time by clicking the “unsubscribe” link in any marketing e-mail we send you, or by contacting us using the details in Section 17. Opting out of marketing does not affect service, regulatory or administrative communications that we need to send you in connection with your relationship with GCEX.

15. PERSONAL DATA BREACHES

GCEX maintains incident management, breach reporting and escalation procedures. In the event of a Personal Data breach that may prejudice your privacy or the confidentiality of your Personal Data, we will notify the UAE Data Office and, where required, affected individuals, in accordance with the PDPL. As required by VARA’s Technology and Information Rulebook, we will also notify VARA as soon as possible, and in any event within twenty-four (24) hours, following any notification made by us to a data regulator or to a data subject of an incident affecting, or potentially affecting, Personal Data.

16. MINORS

Our services are not intended for, or directed at, individuals under the age of eighteen (18). We do not knowingly collect Personal Data from minors. If you believe that a minor has provided us with Personal Data, please contact us and we will take appropriate steps, including deletion where permitted and subject to applicable legal and regulatory retention obligations..

17. CONTACT US

GC Exchange FZE is the Controller of your Personal Data. In accordance with VARA’s Technology and Information Rulebook and the PDPL, GCEX has appointed a Data Protection Officer, who is responsible for overseeing compliance with this Policy and applicable data protection law and who acts as our contact point for VARA on personal data matters.

Controller	GC Exchange FZE, One Central, The Offices 4, Level 8, Unit 132 Dubai World Trade Centre, Dubai
Regulatory Status	Licensed by the Virtual Assets Regulatory Authority (VARA) for Virtual Asset Broker-Dealer Services — licence number VL/23/09/002
Data Protection Officer	E-mail: compliance@gc.exchange

Questions, comments and requests regarding this Policy or your Personal Data are welcomed and should be addressed to the contact details above.

18. CHANGES TO THIS POLICY

We review this Policy at least annually and may update it from time to time in response to legal, regulatory, technical or business developments. When we make changes, we will update the version number and effective date above, and we will take appropriate measures to inform you, consistent with the significance of the changes. The current version of this Policy is available on our website at all times.