VENOR LTD.

Trading as : Venor Markets

Registered in Saint Lucia | International Clients

PRIVACY POLICY

Website Publication | Client Onboarding | KYC / AML

Version	1.0
Effective Date	01-05-2026
Jurisdiction	Saint Lucia
Status	Final Document

Prepared for Website Publication | 2026

Important Notice

This Privacy Policy explains how Venor Ltd., trading as Venor Markets, collects, uses, stores, shares and protects personal data when you visit our Website, open an Account, complete onboarding, submit KYC documents, use our client portal, deposit or withdraw funds, access the Trading Platform, communicate with us, or use our Services.

This Policy is designed to be read together with the Client Agreement, AML / KYC Notice, Deposit and Withdrawal Policy, Risk Disclosure Statement, Complaints Handling Policy and any other applicable policy or notice issued by the Company.

1. Who We Are and Scope of this Policy

1.1 This Privacy Policy is issued by Venor Ltd., a company registered in Saint Lucia under registration number [Registration Number], having its registered office at - Ground floor, the Sotheby building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia, and operating under the trading name Venor Markets.

1.2 In this Policy, the Company may be referred to as "the Company", "we", "us" or "our". The person whose personal data is processed may be referred to as "you", "your" or "Client".

1.3 For the KYC/AML, trading account, payment, website, client portal and related Services we provide, the Company acts as the data controller or equivalent decision-maker in respect of your personal data, meaning we determine the purposes and means of processing. Certain service providers, including identity verification providers and payment providers, may act as processors on our behalf, or as independent controllers for their own compliance purposes.

1.4 This Policy applies to personal data which may be collected through our Website, client portal, onboarding forms, KYC process, payment and withdrawal process, Trading Platform, mobile applications, communications, support channels, marketing channels and any related Services.

1.5 This Policy is intended to describe how we process personal data, subject to applicable data protection laws, including the Saint Lucia Data Protection Act, 2011 (as amended), to the extent applicable to the Company and the relevant processing activity, and any other data protection or privacy laws that apply to particular Clients, Services or processing activities.

1.6 This Policy should be read together with the Client Agreement, AML/KYC Notice, Deposit and Withdrawal Policy, Risk Disclosure Statement, Complaints Handling Policy and any other applicable policy or notice issued by the Company.

1.7 This Policy does not replace the privacy policy of any third-party service provider. Third-party providers may also process personal data under their own privacy notices, especially where you interact with their systems directly or where they are required to process data for their own legal, security, compliance or fraud-prevention purposes.

2. Personal Data We Collect

2.1 We may collect and process the following categories of personal data, depending on your interaction with us and the Services you use:

- **Identity data:** including name, date of birth, nationality, citizenship, gender, photograph, signature, identity document details and copies of passports, national IDs, residence cards or driving licenses.
- **Contact data:** including residential address, email address, telephone number, country of residence and communication preferences.
- **KYC and verification data:** including selfie images, liveness checks, video verification, document authenticity checks, biometric or facial-comparison outputs where permitted, verification status, fraud indicators and screening results.
- **Financial and economic profile data:** including employment, occupation, income range, source of funds, source of wealth, bank account information, payment details, wallet details and trading experience.
- **Trading and account data:** including Account number, account type, trading history, orders, transactions, positions, profits, losses, balances, margin information, leverage, platform logs, IP logs and device records.
- **Payment and withdrawal data:** including deposit and withdrawal requests, payment method, payment provider references, bank details, card information tokenized by payment providers, crypto wallet addresses, blockchain transaction hashes and payment status.
- **Technical data:** including IP address, device identifiers, browser type, operating system, login history, session data, application logs and cybersecurity information.
- **Communications data:** including emails, chat messages, support tickets, call recordings, video calls, complaint records and other approved communication records where used.
- **Marketing and preference data:** including consent choices, campaign responses, referral source, affiliate or introducer information, communication preferences and opt-out requests.
- **Compliance and risk data:** including sanctions screening, politically exposed person checks, adverse media checks, fraud risk indicators, internal risk scoring, chargeback risk, investigation records and regulatory records.
- **Special category or sensitive data:** where contained in documents or verification material you provide, including biometric or facial-comparison data and any sensitive information that may appear in identity documents, proof of address documents, financial records or compliance records.

2.2 We do not intentionally collect personal data from minors. Our Services are intended only for persons who are at least 18 years old or the age of legal majority in their jurisdiction, whichever is higher.

3. How We Collect Personal Data

3.1 We may collect personal data directly from you when you complete forms, open an Account, upload documents, communicate with us, place orders, deposit or withdraw funds, use the Trading Platform, submit complaints or otherwise use the Services.

3.2 We may collect personal data automatically through the Website, client portal, Trading Platform, security systems and analytics tools.

3.3 We may collect personal data from third parties, including identity verification and KYC providers; payment gateways, payment service providers, banks and wallet providers; sanctions, PEP, adverse media, fraud-prevention and compliance screening providers; platform providers, CRM providers, liquidity providers and technology vendors; introducing brokers, affiliates and referral partners; and public records, government databases, company registries and other lawful sources.

4. How We Use Personal Data

4.1 We may use personal data for any one or more of the following purposes, depending on the Services used, onboarding stage, Account activity, payment method, risk profile, applicable law, service-provider requirements and our internal policies:

- to receive, review and process Account applications;
- to verify identity, support onboarding and KYC checks, and where relevant, support AML/CFT checks, sanctions screening, PEP screening, adverse media review and due diligence;
- to assess or support assessment of eligibility, client categorization, appropriateness, risk profile and account restrictions;
- to provide, operate and administer Accounts, the client portal, Trading Platform and related Services;
- to process or support deposits, withdrawals, refunds, payment investigations, chargebacks, payment reversals and payment-provider requests;
- to execute, record, settle, reconcile, review or report transactions;
- to provide client support, respond to enquiries and investigate complaints;
- to detect, prevent, review or investigate suspected or actual fraud, account abuse, prohibited trading, payment abuse, market abuse, cyber incidents, identity abuse and suspicious activity;
- to support compliance with legal, regulatory, tax, AML/CFT, sanctions, audit, accounting and record-keeping obligations, where applicable;
- to communicate important account notices, policy updates, risk warnings, operational alerts and service communications where applicable;
- to send marketing communications where permitted and subject to your preferences and any consent required by applicable law;
- to improve our Website, systems, security, products, Services and user experience;
- to protect the rights, property, reputation, legal position and security of the Company, Clients, staff, service providers and third parties;
- to establish, exercise or defend legal claims and enforce agreements.

5. Legal Bases and Client Consent

5.1 Depending on the applicable law, Services used, onboarding stage, payment method, risk profile and purpose of processing, we may process personal data on one or more of the following bases: performance of a contract with you or steps taken before entering into a contract; compliance with legal, regulatory, AML/CFT, sanctions, tax or reporting obligations where applicable; our legitimate interests including risk management, fraud prevention, platform security, service improvement, dispute resolution and enforcement of legal rights; your consent where consent is required or appropriate; and establishment, exercise or defense of legal claims.

5.2 By submitting documents, completing onboarding, using the Website, using the Trading Platform, depositing funds, withdrawing funds or communicating with us, you acknowledge and agree that, we may process personal data for the purposes described in this Policy.

5.3 Consent is not the only basis on which we may process personal data. Certain processing may be necessary for contract performance, AML/KYC or related compliance purposes, sanctions screening, fraud prevention, payment processing, security, record keeping and legal claims. If you withdraw consent where consent is required for a specific activity, we may be unable to provide or continue providing the relevant Service, including opening or maintaining an Account.

5.4 Where biometric, facial-comparison, liveness, video verification or enhanced identity verification is used, you may be asked to provide specific consent or acknowledgment through the relevant verification flow. If you do not provide required verification data, we may be unable to open or maintain your Account or process transactions.

6. KYC, AML, Sanctions and Identity Verification

6.1 We may use personal data to conduct, support or document identity verification, KYC, AML/CFT, sanctions, PEP, adverse media, fraud-prevention and other due diligence checks before, during or after the client relationship, depending on the Services used, Account activity, payment activity, risk profile, applicable law, service-provider requirements and our internal policies.

6.2 We may use third-party identity verification, onboarding, KYC, AML/CFT, sanctions-screening or fraud-prevention providers to support verification or compliance-related purposes, including verifying identity documents, performing liveness or selfie checks, comparing images, detecting document fraud, screening against relevant databases, generating verification outputs and supporting compliance monitoring.

6.3 Where an identity verification or compliance provider processes your personal data, such processing may include identity document data, photograph or selfie data, liveness data, facial-comparison outputs, device information, verification status, fraud indicators, screening results and related verification information.

6.4 Biometric, facial-comparison, liveness, selfie and video verification data may be collected, processed, reviewed, stored, shared or used for identity verification, onboarding, KYC checks, AML/CFT compliance, sanctions screening, fraud prevention, account security, duplicate-account detection, document authenticity checks, payment verification, dispute handling, legal claims and regulatory obligations. We do not use such data for unrelated marketing or general profiling.

6.5 We may request additional documents or information at any time for onboarding, verification, payment, risk-management, compliance, legal, fraud-prevention or account-

administration purposes, including proof of address, proof of payment method, source of funds, source of wealth, bank statements, corporate documents, beneficial ownership details and explanations of trading or payment activity.

6.6 If we cannot complete, validate or satisfy any verification, due diligence, service-provider, payment, legal, risk-management or internal-policy requirement that applies to your Account or activity, we may refuse onboarding, restrict Account access, delay deposits, delay withdrawals, place the Account in close-only mode, return funds to source, terminate the relationship or take any other action permitted under our Client Agreement and policies.

6.7 We may be unable to provide detailed reasons for certain checks, delays, restrictions or reports where doing so would breach law, AML obligations, sanctions obligations, security requirements, confidentiality obligations or third-party restrictions.

7. Payment Processing and Funding Data

7. Payment Processing and Funding Data

7.1 The Company exclusively accepts deposits and processes withdrawals through cryptocurrency. The Company does not accept deposits or process withdrawals by credit card, debit card, bank transfer, wire transfer, electronic money transfer or any other fiat payment method.

7.2 We may process payment-related personal data for the purposes of accepting crypto deposits, processing crypto withdrawals, verifying wallet ownership, reconciling funds, reviewing payment and transaction activity, preventing fraud, supporting AML/KYC or sanctions-related checks, conducting blockchain analytics and on-chain due diligence, resolving disputes, complying with legal or service-provider requirements and administering the Account.

7.3 We may use one or more crypto-payment providers, cryptocurrency treasury platforms, wallet infrastructure providers or on/off-ramp providers in connection with the Services. Such providers may independently collect, store and process personal data under their own terms and privacy notices, including for transaction monitoring, fraud prevention, sanctions screening, wallet screening, blockchain analytics and legal compliance. We are not responsible for the privacy practices of any crypto-payment provider where it acts independently of us as a data controller.

7.4 In connection with crypto deposits and withdrawals, we may process wallet addresses, blockchain transaction hashes, on-chain analytics results, wallet ownership evidence, wallet screening outputs, counterparty wallet information, transaction amounts, timestamps and related compliance, payment, risk-management, dispute-handling or account-administration information.

7.5 Where required or permitted, payment-related data may be shared with crypto-payment providers, blockchain analytics providers, sanctions screening providers, AML/CFT compliance providers, regulators, authorities, auditors, legal advisers and other parties where necessary for payment processing, compliance, risk-management, dispute-handling, legal or account-administration purposes.

7.6 You acknowledge that cryptocurrency transactions are recorded on a public or decentralised blockchain ledger. Certain transaction data — including wallet addresses and transaction hashes — may be publicly visible on the blockchain and is technically beyond our ability to alter, restrict or erase once broadcast. We may retain related records as

necessary for AML/KYC, sanctions screening, fraud prevention, dispute handling, legal claims and account administration.

7.7 You are solely responsible for ensuring that the cryptocurrency wallet used for deposits and withdrawals is owned and controlled by you. We may require wallet ownership verification as part of our KYC, AML or payment-verification process. Deposits from wallets that cannot be verified as belonging to you, or from wallets flagged by blockchain analytics or sanctions screening tools, may be rejected, held, returned or escalated for further review.

8. Website, Technical Data and Cookies

This section currently covers essential and security cookies only, as the website is in its initial stage of publication. This section will be updated when analytics, marketing, affiliate or other non-essential cookies or tracking technologies are introduced.

8.1 We may collect technical data when you visit or use our Website, client portal, mobile applications, Trading Platform or other systems.

8.2 Technical data may include IP address, device type, browser, operating system, session logs, login times, failed login attempts, platform logs, approximate location derived from IP, device identifiers, security logs and basic usage data.

8.3 We may use technical data for the purposes of operating the Website and Platform, maintaining security, preventing fraud, troubleshooting issues, improving Services, monitoring performance, supporting investigations, supporting compliance, enforcing agreements and meeting legal or service-provider requirements.

8.4 At this stage of our website, we use only essential and security cookies that are strictly necessary for the Website and client portal to function, for login and session management, for account security, for fraud prevention and for compliance purposes. Essential and security cookies may be placed without separate consent as they are necessary for the operation of the Services.

8.5 We do not currently use analytics, advertising, marketing or non-essential cookies or tracking technologies. When such technologies are introduced, we will update our Cookie Policy and, where required by applicable law, provide appropriate cookie choices.

8.6 You may manage cookies through your browser settings. Blocking, deleting or disabling essential or security cookies may affect Website or portal functionality, including login, onboarding, account access, session security, payment pages and other core Services. This may cause delays, failed actions or other consequences, including financial, payment-related or trading-related loss. We are not responsible for losses arising from disabling cookies necessary for the operation, security or integrity of the Services, except where liability cannot be excluded under applicable law.

9. Sharing Personal Data with Third Parties

9.1 We may share personal data with third parties where necessary, appropriate or permitted for any one or more of the purposes described in this Policy, including:

- KYC, AML, sanctions, PEP, adverse media, onboarding, identity verification and fraud-prevention providers;
- payment gateways, wallet providers, electronic money institutions and crypto-payment providers;
- Trading Platform providers, CRM providers, bridge providers, liquidity providers, hosting providers, cloud providers, cybersecurity providers and IT support providers;
- communications providers, email providers, SMS providers, chat tools, call systems and notification services;
- introducing brokers, affiliates, partners and referral sources where permitted and relevant;
- auditors, accountants, lawyers, consultants and professional advisers;
- regulators, authorities, courts, law enforcement agencies, tax authorities and dispute-resolution bodies;
- group companies, affiliates, successors, purchasers or merged entities in connection with restructuring, future licensing, regulatory migration, sale, merger, acquisition or business transfer.

9.2 Where applicable, we require or expect service providers to process personal data for authorized purposes and to apply appropriate confidentiality and security measures, subject to their role, contractual terms and applicable law.

9.3 Where a service provider acts as our processor, we seek to ensure that appropriate contractual terms are in place. Where a provider acts as an independent controller, it may process personal data under its own privacy notice and legal responsibilities.

9.4 We may disclose personal data where required by law, court order, regulator, competent authority, payment provider, bank, liquidity provider or other lawful request.

10. Cross-Border Transfers

10.1 We may transfer, store and process personal data in countries other than your country of residence. Such countries may not provide the same level of data protection as your jurisdiction.

10.2 Cross-border transfers may occur because our service providers, technology providers, KYC providers, payment providers, platform providers, cloud providers, affiliates, advisers or other third parties who may be located in different jurisdictions.

10.3 Where required by applicable law, we will use appropriate safeguards for cross-border transfers, which may include contractual safeguards, due diligence on service providers, technical and organizational measures, or equivalent lawful transfer mechanisms.

10.4 By using our Services and submitting personal data, you acknowledge that your personal data may be transferred internationally as described in this Policy.

11. Data Security and Confidentiality

11.1 We take reasonable technical, organizational and administrative measures to protect personal data against unauthorized access, loss, misuse, alteration, disclosure or destruction.

11.2 Measures may include access controls, password controls, encryption where appropriate, secure transmission, logging, monitoring, staff confidentiality obligations, vendor due diligence and incident-response procedures.

11.3 No website, platform, system, email, internet transmission, blockchain transaction or electronic storage method is completely secure. We cannot guarantee absolute security of personal data.

11.4 You are responsible for keeping your login credentials, email account, device, two-factor authentication method and payment credentials secure. You must notify us immediately if you suspect unauthorized access, identity theft, device compromise or any other security incident affecting your Account.

11.5 If we become aware of a personal data breach that is likely to result in a material risk to your rights, freedoms or interests, we will take reasonable steps to investigate, contain and remediate the breach and, where required by applicable law, notify affected individuals and/or competent authorities without undue delay.

12. Data Retention

12.1 We retain personal data for as long as necessary for the purposes for which it was collected and for any longer period required or permitted by applicable law, AML requirements, sanctions obligations, tax rules, audit requirements, contractual obligations, regulatory expectations, dispute resolution or legal proceedings.

12.2 We will retain KYC/AML records, transaction records, payment records, Account records and related communications for a minimum of five (5) years following the termination of our business relationship, or longer where required or permitted by applicable law, legal claims, investigations, audits, sanctions obligations, tax obligations, dispute handling or compliance obligations.

12.3 When personal data is no longer required, we may delete, anonymize, archive or restrict access to it in accordance with our internal retention practices and applicable law.

12.4 We may be unable to delete certain information immediately where retention is required for AML, sanctions, tax, legal, audit, dispute, fraud-prevention or regulatory purposes.

13. Client Rights

13.1 Depending upon verification of your identity, you may have rights under the Saint Lucia Data Protection Act, 2011 (as amended), to request access to personal data, correction of inaccurate data, deletion of data, restriction of processing, objection to processing, withdrawal of consent, or information about how personal data is processed.

13.2 Your rights may be limited where processing is required for AML, sanctions, fraud prevention, legal claims, tax, regulatory, audit, contractual or security purposes.

13.3 Where personal data is connected to blockchain transactions, public wallet addresses, transaction hashes or records on a public or decentralized ledger, such records may be technically impossible for us to erase, alter or delete. In such cases, we may retain related records as necessary for compliance, AML/KYC, sanctions screening, fraud prevention, dispute handling, legal claims and account administration.

13.4 We may require proof of identity and additional information before responding to a rights request. Requests should be sent to the contact details set out in **Section 20** of this Policy. We will respond within the timeframe required by applicable law or, where no specific timeframe applies, within a reasonable period.

13.5 Withdrawing consent does not affect processing that occurred before withdrawal and does not prevent processing that is necessary for contract performance, legal obligations, AML/KYC obligations, sanctions screening, fraud prevention, payment processing, legal claims or record keeping.

14. Marketing Communications

14.1 We may send you service communications, account notices, policy updates, risk warnings and operational messages. These are not marketing communications and may be necessary for the Services.

14.2 Where permitted, we may send marketing communications about products, services, promotions, market information, educational materials or Company updates. We will rely on consent where required by applicable law, or on legitimate interests with an easy opt-out where permitted.

14.3 You may opt out of marketing communications using the unsubscribe method provided or by contacting us. Opting out of marketing does not stop important service, legal, compliance or account communications.

14.4 Marketing communications must not be treated as investment advice, personal recommendations or guarantees of outcome.

15. Automated Screening and Monitoring

15.1 We and our service providers may use automated tools to support identity verification, document checks, liveness checks, facial-comparison checks, sanctions screening, PEP screening, adverse media screening, fraud detection, risk monitoring, payment monitoring, account security, transaction monitoring, onboarding review and compliance support.

15.2 Automated tools may generate alerts, risk scores, verification outcomes or recommendations for manual review. We may restrict, delay or review Accounts, deposits, withdrawals or activity based on automated or manual indicators, including verification, risk, payment, fraud-prevention, compliance, legal, security or service-provider indicators.

15.3 Where required by applicable law, you may have the right to request human review of certain automated decisions. Such requests may be subject to legal, AML, sanctions, fraud-prevention and security limitations.

16. Third-Party Websites and Services

16.1 Our Website, client portal or communications may contain links to third-party websites, platforms, applications or services. We are not responsible for the privacy practices, content, security or data handling of third-party websites or services that we do not control.

16.2 You should review the privacy policies of third-party services before submitting personal data to them.

17. Minors

17.1 Our Services are not intended for minors. You must not open an Account or use the Services unless you are at least 18 years old.

17.2 If we become aware that personal data of a minor has been provided to us without lawful basis, we may delete the data, reject the Account application, close the Account or take any other appropriate action, as per company policy.

18. Changes to this Privacy Policy

18.1 We may update this Privacy Policy from time to time to reflect changes in our business, Services, technology, service providers, legal obligations, regulatory expectations, payment methods, onboarding processes or data practices.

18.2 Updated versions will be published on the Website, client portal or otherwise notified to you. Your continued use of the Website, Account, Trading Platform or Services after publication of an updated Policy constitutes acknowledgment of the updated Policy.

19. Governing Law and Jurisdiction

19.1 This Privacy Policy is governed by and shall be construed in accordance with the laws of Saint Lucia, including the Saint Lucia Data Protection Act, 2011 (as amended), and any other applicable data protection or privacy laws of Saint Lucia.

19.2 Any dispute arising from or in connection with this Privacy Policy, including questions regarding its existence, validity or termination, shall be subject to the jurisdiction of the courts of Saint Lucia.

19.3 Clients located in other jurisdictions acknowledge that their personal data may be processed in accordance with the laws of Saint Lucia and, where applicable, the laws of the jurisdiction in which relevant service providers are located.

20. Contact Details and Privacy Complaints

20.1 If you have questions, requests or complaints regarding this Privacy Policy or our handling of personal data, please contact us at:

Legal Entity	Venor Ltd.
Trading Name	Venor Markets
Registered Office	Ground floor, The Sotheby building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia.
Privacy / Data Contact	support@venormarkets.com
Website	www.venormarkets.com
Client Support	support@venormarkets.com

20.2 You should provide sufficient information to allow us to identify you and understand your request or complaint. If applicable law gives you the right to complain to a data protection authority or regulator, you may exercise that right subject to the applicable rules in Saint Lucia.

Acknowledgement

By visiting the Website, submitting personal data, opening an Account, completing onboarding, uploading KYC documents, depositing funds, withdrawing funds, accessing the Trading Platform or using the Services, you acknowledge that you have read and understood this Privacy Policy and that your personal data may be collected, used, processed, stored, shared, reviewed or verified for any one or more of the purposes described in this Policy.

During onboarding, account opening, payment processing or identity verification, the Company may require you to actively confirm, through a checkbox, electronic acceptance, consent screen or similar method, that you have read and understood this Privacy Policy.