VSMARKETS LTD

PRIVACY POLICY

Version 2.1 | October 2026

1. INTRODUCTION

1.1 VSMarkets Ltd (the "**Company**", "**VSMarkets**", "**we**", "**us**" or "**our**") is a limited liability company incorporated in the Republic of Cyprus with registration number HE431041. The Company is authorised and regulated by the Cyprus Securities and Exchange Commission ("**CySEC**") as a Cyprus Investment Firm ("**CIF**") under licence number 434/23. The Company's registered address is 11 Riga Fereou Street, Ground Floor, 3095 Limassol, Cyprus. The Company's approved website is www.vsmarkets.com.

1.2. The Company is committed to protecting the privacy and personal data of individuals who interact with us. This Privacy Policy (the "**Policy**" or "**Privacy Policy**") explains how we collect, use, process, store and disclose personal data in connection with our website, mobile applications, trading platforms and other electronic services, the account-opening and onboarding process, and other interactions or communications with the Company.

1.3 The Company processes personal data in accordance with Regulation (EU) 2016/679 (the **"GDPR"**), the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data Law of 2018 (Law 125(I)/2018), as amended from time to time (the **"Cyprus Data Protection Law"**), and other applicable data protection legislation.

1.4 For the purposes of the GDPR and the Cyprus Data Protection Law, VSMarkets is the **data controller** in respect of the personal data covered by this Privacy Policy, unless otherwise expressly stated.

1.5 This Privacy Policy should be read together with the Company's User/Client Agreement, Cookie Policy, available on the Company's website, and any other applicable legal notices or policies.

2. SCOPE OF THIS POLICY

2.1 This Privacy Policy applies to all individuals whose personal data is collected or processed by the Company in connection with its website, electronic services, trading platform, account-opening and onboarding processes and the products and services offered by the Company. This includes, without limitation:

(a) visitors to the Company's website;

(b) individuals who create or register an account with the Company;

(c) individuals who commence but do not complete the account-opening or onboarding process;

(d) applicants and potential clients;

(e) demo-account users;

(f) existing clients; and

(g) former clients.

Such individuals are collectively referred to in this Privacy Policy as **"you"** or **"your"**.

2.2 You do not need to become an approved client or establish a business relationship with the Company for this Privacy Policy to apply. It applies from the point at which we collect or receive personal data relating to you, including where you provide personal data through an "Open Account" registration, demo, contact or similar form, even if you do not subsequently complete the onboarding process or become a client of the Company.

2.3 Certain provisions of this Privacy Policy may apply differently depending on whether you are an applicant, potential client, existing or former client, registered user, website visitor or another category of data subject, and depending on the products, services or interactions concerned.

2.4 Our services are not intended for persons under eighteen (18) years of age and we do not knowingly provide our services to, or collect personal data from, children. If we become aware that such personal data has been collected, we will take appropriate steps in accordance with applicable law.

3. PERSONAL DATA WE COLLECT

3.1 Depending on the nature of your interaction with the Company, the stage of your registration or account-opening process, the products or services requested or provided to you, and our applicable legal and regulatory obligations, we may collect and process the following categories of personal data:

- **Identity data:** full name or parts thereof, date and place of birth, nationality, gender, tax identification information, national identification number, identification document details and copies, photographs, signature and other information used to identify or verify you. Where remote identity-verification tools are used, this may also include images, video recordings, facial images, liveness-check information and other verification data generated during the identity-verification process.
- **Contact data:** residential, correspondence or billing address, email address, telephone number and other contact details.
- **Account and profile data**: username, authentication information, account preferences, language preferences, registration and onboarding status, client classification and related account or platform settings.
- **Economic, appropriateness and target-market data**: occupation, employment status, education, source and level of income, wealth, source of funds, source of wealth, assets, liabilities, financial commitments, investment objectives, investment horizon, risk tolerance, capacity for loss, trading knowledge and experience and other information required for appropriateness, suitability or product-governance and target-market purposes, where applicable.
- **Financial and payment data**: bank account details, payment card or other payment-method information, payment instructions, payment history and information relating to deposits, withdrawals and other transfers.
- **Transaction and service data**: trading activity, orders, transactions, positions, balances, product use, account activity, deposits, withdrawals, fees and charges, requests, inquiries, complaints and other information generated in connection with services provided or requested.
- **Screening and compliance data**: information relating to sanctions, politically exposed person ("PEP") status, close connections and related persons where relevant, adverse media, fraud prevention, tax reporting, FATCA and CRS information, identity-verification and liveness-check results, document-verification results and other customer due-diligence or regulatory compliance information.
- **Risk assessment data**: client risk scores, risk categorisation, fraud-risk indicators and information used for AML/CFT, sanctions, fraud or other regulatory risk assessments.
- **Technical and usage data**: IP address, device identifiers, login data, browser type and version, time-zone settings and location, operating system, platform, cookie identifiers, website or application activity and other information about how you access and use our electronic services. Where applicable, this may include device and technical information collected during remote

identification or verification processes, as well as session or screen-recording information where such technology is lawfully used.

- **Communication data**: communications between you and the Company, including emails, telephone communications, electronic messages, chats, correspondence, call recordings where applicable and lawful, CRM notes and other records of communications with us.
- **Marketing and preference data**: communication preferences, subscriptions, marketing consents or objections, campaign interactions, survey responses, feedback and product or service preferences.

3.2 We may also generate or derive personal data about you in the course of your interaction or relationship with us, including internal assessments, compliance records, onboarding status, risk classifications and other information generated in connection with the provision or proposed provision of our services.

3.3 We do not intentionally seek to collect or process special categories of personal data unless such processing is necessary and lawful. Where remote identity-verification technology involves the processing of biometric data for the purpose of uniquely identifying or authenticating you, including through facial recognition or liveness-verification technology, or where another special category of personal data is processed, the Company will ensure that an appropriate condition under Article 9 of the GDPR and any other applicable legal requirements are satisfied.

3.4 We only collect and process personal data that is relevant and reasonably necessary for the purposes described in this Privacy Policy and for compliance with our legal and regulatory obligations.

4. HOW WE COLLECT PERSONAL DATA

4.1 Most of the personal data we process is provided directly by you, including when you visit or use our website or Services, register or create an account, commence or complete an account-opening or onboarding application, provide information or documentation, or communicate with us.

4.2 We may also receive personal data about you from third parties and publicly accessible sources, including banks and payment service providers, identity-verification, KYC, screening and fraud-prevention providers, credit-reference providers where applicable, public authorities and registers, analytics providers, advertising networks and other lawful sources.

4.3 When you use our website, platform, applications or other electronic services, we may automatically collect Technical and Usage Data through cookies, server logs and similar technologies. Further information is available in our Cookie Policy.

4.4 We may periodically request that you confirm, update or correct personal data previously provided to us in order to ensure that our records remain accurate and up to date and to comply with applicable legal and regulatory requirements.

4.5 Certain personal data is required in order for us to comply with our legal and regulatory obligations or is necessary for us to process your application, enter into or perform a contract with you or provide requested services. Where such information is required and you do not provide it, we may be unable to process or approve your application, open or maintain an account or provide some or all of our services.

5. PURPOSES AND LAWFUL BASES FOR PROCESSING

5.1 We process personal data only where we have a lawful basis under the GDPR. Depending on the relevant processing activity, the principal lawful bases we rely on are:

a) your consent;
b) performance of a contract or taking steps at your request before entering into a contract;
c) compliance with a legal obligation; and
d) our legitimate interests or those of a third party, where those interests are not overridden by your interests, rights and freedoms.

5.2 The principal purposes for which we process personal data, the typical categories of personal data involved and the corresponding lawful bases are set out in the below table. A processing activity may rely on more than one lawful basis where appropriate:

Purpose / activity	Typical data used	Principal lawful basis
Create and administer your registration or account and process an account-opening or onboarding application.	Identity, Contact, Account/Profile, Technical and Usage Data	Article 6(1)(b): taking steps at your request before entering into a contract and/or performance of a contract.
Communicate with you regarding your registration or account-opening application, including its status, outstanding information or steps, technical issues, and whether you require assistance completing the onboarding process.	Identity, Contact, Account/Profile, Technical and Communication Data	Article 6(1)(b), where necessary to take steps at your request before entering into a contract; and/or Article 6(1)(f), our legitimate interests in administering applications, facilitating the onboarding process and providing appropriate operational support.
Verify your identity and carry out KYC, AML/CFT, sanctions, PEP, fraud-prevention, document-verification, liveness and client-risk checks.	Identity, Contact, Screening/Compliance, Risk Assessment, Financial, Technical and Communication Data	Article 6(1)(c): compliance with applicable legal and regulatory obligations. Where special-category or biometric data is processed, an appropriate condition under Article 9 GDPR will also be relied upon where required.
Assess your economic profile, knowledge and experience, appropriateness, target-market information and client categorisation, where applicable.	Economic/Appropriateness/Target-Market, Identity and Account/Profile Data	Article 6(1)(c): compliance with applicable investment-services, product-governance and other regulatory obligations; and Article 6(1)(b) where also necessary for services requested by you.
Provide and administer our investment and ancillary services and process orders, transactions, deposits, withdrawals, payments, fees and charges.	Identity, Contact, Financial/Payment, Transaction/Service, Technical and Account/Profile Data	Article 6(1)(b): performance of a contract; and Article 6(1)(c) where applicable legal or regulatory obligations apply.

Purpose / activity	Typical data used	Principal lawful basis
Manage our relationship with you, provide customer and operational support and respond to inquiries, requests and complaints.	Identity, Contact, Account/Profile, Transaction/Service, Technical and Communication Data	Article 6(1)(b) and/or Article 6(1)(f), our legitimate interests in administering our relationship and providing appropriate customer and operational support.
Send service, security, regulatory and other operational communications concerning your registration, application, account or use of our services.	Contact, Communication and Account/Profile Data	Article 6(1)(b), Article 6(1)(c) and/or Article 6(1)(f), depending on the nature and purpose of the communication.
Record, retain and, where applicable, monitor communications and maintain appropriate records of services, activities and transactions.	Identity, Contact, Communication and Transaction/Service Data	Article 6(1)(c): compliance with applicable investment-services and record-keeping obligations; Article 6(1)(f) for appropriate operational records not legally mandated.
Prevent and detect fraud, financial crime, cyber-security threats, misuse or other unlawful activity and protect our systems, services, rights and property.	Identity, Contact, Screening/Compliance, Risk Assessment, Technical/Usage, Financial and Transaction/Service Data	Article 6(1)(c) and/or Article 6(1)(f), our legitimate interests in fraud prevention, security and protection of our business and users.
Administer, analyse, maintain and improve our business, website, platforms, products and services.	Technical/Usage, Account/Profile and aggregated or anonymised data	Article 6(1)(f), our legitimate interests in operating, analysing and improving our business and services; consent where required for non-essential cookies or similar technologies.
Send marketing communications, promotional content, offers or information about our products and services.	Identity, Contact, Marketing/Preference, Account/Profile and Usage Data	Consent where required by applicable law; otherwise Article 6(1)(f), legitimate interests, where direct marketing is legally permitted. Applicable direct-marketing and electronic-communications requirements will also be observed. You may object to direct marketing at any time.
Establish, exercise or defend legal claims, enforce our rights and comply with lawful requests from regulators, courts or public authorities.	Any personal data relevant to the matter	Article 6(1)(c) and/or Article 6(1)(f).

5.3 Communications relating to the administration, progress or completion of a registration, account-opening or onboarding application, including communications intended to identify outstanding information or steps, technical difficulties or to determine whether you require assistance with the onboarding process, are operational communications and are distinct from direct marketing communications. Such communications may be made through the contact details provided by you,

including by email, telephone, SMS, platform message or other appropriate communication channel, subject to applicable law.

5.4 Where we rely on legitimate interests, we consider the nature and purpose of the processing, your reasonable expectations and the potential impact on your rights and freedoms. Where appropriate, we carry out a balancing assessment before relying on this lawful basis.

5.5 Where we rely on your consent, you may withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal or processing which we carry out on another lawful basis.

5.6 We will use personal data for the purposes for which it was collected. Where we intend to process personal data for another purpose, we will assess whether that purpose is compatible with the original purpose and, where required by applicable law, provide you with further information regarding such processing as required by law.

6. COOKIES

6.1 We may use cookies and similar technologies to operate and secure our website and electronic services, remember your preferences, understand how our services are used and, where permitted, support analytics, personalisation and marketing activities.

6.2 Strictly necessary cookies may be used without your consent where they are required to provide a service requested by you or to ensure the security and functionality of our website and electronic services. Analytics, advertising and other non-essential cookies or similar technologies will be used only in accordance with applicable law and, where required, with your consent.

6.3 Further information about the types of cookies and similar technologies we use, their purposes, duration, providers and how you can manage or withdraw your preferences is available in our Cookie Policy, available on the Company's website, and through our cookie preference tool, where applicable.

7. HOW DO WE SHARE YOUR PERSONAL DATA

7.1 We do not share your personal information with third parties, except as described in this Privacy Policy.

7.2. We may share personal data with companies within our wider group or with affiliated or related entities where reasonably necessary for the provision or support of our services, operational or administrative purposes, compliance with legal or regulatory obligations, or other legitimate business purposes, subject to applicable data-protection requirements and appropriate safeguards.

7.3 We may also engage third-party service providers, professional advisers and other partners to assist us in operating our business, providing our services, administering or processing your account or application, complying with our legal and regulatory obligations, protecting our legitimate interests or otherwise where permitted or required by applicable law. Depending on the circumstances, recipients of your personal data may include:

Category of Recipient	Purpose
Regulatory, governmental and public authorities	To comply with legal, regulatory, reporting, tax, AML/CFT, law-enforcement and other statutory obligations, including disclosures to regulators, courts and other competent authorities.

Identity-verification and compliance providers	To conduct identity and document verification, remote identification and liveness checks, sanctions and PEP screening, adverse-media checks, fraud prevention, AML/CFT checks, credit or similar verification where applicable, and risk assessment.
Banks, payment service providers and other financial institutions	To process deposits, withdrawals, payments and transfers, verify payment information and support fraud-prevention and financial controls.
Trading, execution, custody and other investment-service providers	To provide or support trading, order execution, liquidity, custody, settlement, transaction reporting, investment transfers, corporate actions and other investment or ancillary services.
Technology and operational service providers	To provide IT, hosting, cloud storage, cyber-security, CRM, analytics, business intelligence, communications, customer support, call-recording or monitoring and other operational or technology services.
Professional advisers and assurance providers	To provide legal, audit, accounting, compliance, insurance, research, consultancy and other professional or advisory services.
Introducing brokers, affiliates and other business partners	To support the introduction, administration or servicing of clients or potential clients, where applicable and where such sharing is lawful.
Marketing and communications providers	To support communications, advertising or marketing activities where such processing is lawful and consistent with your preferences and applicable direct-marketing requirements.
Persons authorised by you or acting on your behalf	To give effect to your instructions or communicate with an authorised representative, agent or other person whom you have authorised to act on your behalf.

7.4 We may also disclose personal data where necessary to establish, exercise or defend legal claims, enforce our contractual or legal rights, prevent or investigate fraud or other unlawful activity, or in connection with a genuine merger, acquisition, restructuring, financing, transfer of business or other corporate transaction, subject to appropriate confidentiality and data-protection safeguards.

7.5 Where a third-party service provider processes personal data on our behalf, we require it to process such data only for the agreed purposes and in accordance with our instructions, and to maintain appropriate confidentiality, security and data-protection safeguards. Where a recipient processes personal data as an independent controller, its own privacy terms may also apply to that processing.

7.6 Where required by applicable law or by the terms applicable to a particular service provider, we may provide additional information about specific third-party providers and their privacy practices in this Privacy Policy or through another appropriate privacy notice.

8. INTERNATIONAL TRANSFERS

8.1 Some of the recipients of your personal data, including companies within our wider group, affiliated or related entities and third-party service providers, may be located outside the European Economic Area ("**EEA**"). Where personal data is transferred outside the EEA, we will ensure that the transfer is carried out in accordance with applicable data-protection law, including Chapter V of the GDPR.

8.2 Depending on the country and recipient concerned, we may rely on an adequacy decision of the European Commission or implement appropriate safeguards, such as the European Commission's

Standard Contractual Clauses, together with supplementary measures where required. We may also rely on another lawful transfer mechanism or applicable derogation permitted under the GDPR where appropriate.

8.3 You may contact the Company's Data Protection Officer at dpo@vsmarkets.com for further information regarding international transfers of your personal data and the safeguards applied.

9. SECURITY AND CONFIDENTIALITY

9.1 We implement appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Such measures may include encryption, access controls, authentication measures, logging and monitoring, network and endpoint security controls, segregation of access, business-continuity arrangements and incident-response procedures.

9.2 Access to personal data is limited to employees, officers, contractors and service providers who have a legitimate business need to access it and who are subject to appropriate confidentiality and data-protection obligations.

10. COMMUNICATIONS, CALL RECORDING AND MONITORING

10.1 We may keep records of communications between you and the Company, including emails, electronic messages, chats, written correspondence, CRM records and where applicable, recordings of telephone or other electronic communications.

10.2 Telephone conversations and electronic communications between you and the Company may be recorded, retained and monitored where required or permitted by applicable law and regulatory requirements, including for regulatory compliance, record-keeping, security, fraud prevention, complaints handling, quality assurance, training and evidential purposes.

10.3 Where required by applicable law, we will provide appropriate notice that a telephone conversation or other communication may be recorded. Such notice may be provided through this Privacy Policy, the Client Agreement, the account-opening or onboarding documentation, an electronic notice or other appropriate means.

10.4 Access to recordings and communication records is restricted to authorised persons, and such records will be retained and protected in accordance with applicable legal, regulatory and data-protection requirements and the retention periods described in this Privacy Policy.

11. AUTOMATED DECISION-MAKING AND PROFILING

11.1 We may use automated processing and profiling in connection with certain regulatory, compliance, risk-management and service-related activities, including identity verification, fraud prevention, AML/CFT and client-risk assessments, appropriateness and target-market assessments.

11.2 Automated processing may be used to assess information provided by you or otherwise lawfully obtained by us and may contribute to decisions concerning your application, account, access to particular products or services, the level of due diligence required or other risk and compliance measures.

11.3 Where a decision is based solely on automated processing and produces legal effects concerning you or otherwise significantly affects you, we will only carry out such processing where permitted by

applicable law and will implement the safeguards required under the GDPR. Where applicable, these safeguards may include the right to request human intervention, express your point of view and contest the decision.

12. RETENTION OF PERSONAL DATA

12.1 We retain personal data only for as long as is necessary for the purposes for which it was collected or otherwise processed, taking into account our legal, regulatory, accounting, tax and reporting obligations and the need to establish, exercise or defend legal claims.

12.2 Where you become a client of the Company, your personal data and records relating to the business relationship will generally be retained for at least five (5) years following the termination of the business relationship. Certain categories of information may be retained for a longer period where this is required or permitted by applicable law or regulatory requirements.

12.3 Where you register with us, commence an account-opening or onboarding application or otherwise provide personal data to us but do not subsequently become a client, we will generally retain the relevant personal data for five (5) years following the closure, rejection, withdrawal or abandonment of your application or your last substantive interaction with us, as applicable. This enables us to maintain an appropriate regulatory and compliance audit trail, prevent and investigate fraud or financial crime, address complaints or disputes and establish, exercise or defend legal claims.

12.4 Personal data may be retained for longer than the periods referred to above where required or permitted by applicable law or regulatory requirements, at the request of a competent authority, or where reasonably necessary in connection with AML/CFT obligations, fraud prevention, an investigation, complaint, dispute, litigation or the establishment, exercise or defence of legal claims.

12.5 Once personal data is no longer required for any lawful purpose, it will be securely deleted, destroyed or anonymised in accordance with the Company's applicable retention and deletion procedures.

13. YOUR RIGHTS

13.1 Subject to the conditions, limitations and exceptions provided under applicable law, you may have the following rights:

a) **Right of access:** to obtain confirmation as to whether we process your personal data and to receive a copy of such data and related information;
b) **Right to rectification**: to request correction of inaccurate or completion of incomplete personal data;
c) **Right to erasure**: to request deletion of your personal data where the applicable legal conditions are met;
d) **Right to restriction:** to request restriction of the processing of your personal data in certain circumstances;
e) **Right to data portability**: to receive certain personal data in a structured, commonly used and machine-readable format and, where technically feasible, to have it transmitted to another controller;
f) **Right to object**: to object to processing based on legitimate interests, including profiling based on those interests;

g) **Right to object to direct marketing:** to object at any time to the processing of your personal data for direct-marketing purposes, including related profiling;
h) **Right to withdraw consent**: where processing is based on consent, to withdraw your consent at any time, without affecting the lawfulness of processing carried out before withdrawal; and
i) **Rights relating to automated decision-making:** where applicable, to exercise the rights available to you under applicable law in relation to decisions based solely on automated processing.

13.2 The exercise of these rights is subject to applicable legal and regulatory requirements. In particular, we may be required or permitted to continue retaining or processing certain personal data notwithstanding a request for erasure, restriction or objection, including where necessary to comply with legal or regulatory obligations or to establish, exercise or defend legal claims.

13.3 To exercise any of your rights or raise any concerns regarding the processing of your personal data, please contact our Data Protection Officer using the contact details set out in Clause 16 of this Policy. We may request information necessary to verify your identity before acting on your request. We will respond without undue delay and, in any event, within one month of receiving your request, subject to any extension permitted by applicable law.

13.4 You also have the right to lodge a complaint with the competent data-protection supervisory authority. Further information regarding the relevant supervisory authority is provided in Clause 16 of this Policy.

14. PERSONAL DATA BREACHES

14.1 We maintain appropriate procedures to identify, assess, contain and respond to personal data breaches. Where required by the GDPR or other applicable law, we will notify the competent supervisory authority and, where a breach is likely to result in a high risk to your rights and freedoms, we will also notify you without undue delay.

15. UPDATES TO THIS POLICY

15.1 We may update this Privacy Policy from time to time. The current version will be published on www.vsmarkets.com.

15.2 Where an update is material, we will provide additional notice where required by applicable law or where otherwise appropriate. Such notice may be provided through the contact details or electronic services used in our relationship with you, including by email, Client Portal, Trading Platform or other appropriate communication channel.

16. CONTACT DETAILS AND SUPERVISORY AUTHORITY

16.1 If you have any questions about this Privacy Policy, our processing of your personal data, wish to exercise any of your data-protection rights or raise a privacy-related concern, please contact:

- Data Protection Officer: dpo@vsmarkets.com
- Office Address: 11 Riga Fereou Street, Ground Floor, 3095 Limassol, Cyprus
- Website: www.vsmarkets.com

16.2 The competent supervisory authority in Cyprus is the Office of the Commissioner for Personal Data Protection. Further information is available at www.dataprotection.gov.cy.

17. LANGUAGE

17.1 This Privacy Policy may be made available in languages other than English. In the event of any inconsistency between the English version and a translated version, the English version will prevail to the extent permitted by applicable law.