PRIVACY POLICY

Last Updated June 2026

1. OUR COMMITMENT TO YOU

We understand the importance of maintaining the confidentiality and privacy of Your Information. By entrusting us with your information, we would like to assure you of our commitment to keep such information private. We have taken measurable steps to protect the confidentiality, security and integrity of Your Information.

This Privacy Policy provides an overview of how EPIDI EU LTD (the "Company") processes your personal data and sets out the information that the Company must provide to you for the purpose of the EU General Data Protection Regulation (the "GDPR") which is applicable as of 25 May 2018.

By accessing our website, using our Platform or communicating with us through any available communication channel, you acknowledge that you have read and understood this Privacy Policy. Moreover, you agree that this Policy, including any amendments will govern how we collect, store, use, share and in any other form process your personal data and your rights during our relationship and after its termination.

The information contained herein supersedes any information in relation to the processing of personal data that is included in any of the existing Agreements/Client Agreement and associated forms on matters that are covered by this Privacy Policy. The Company may revise or update this policy from time to time. The new version of this Policy will be available on the Company's website.

For the purposes of the GDPR, the Company acts as the controller of your personal data in relation to the processing activities described in this Privacy Policy.

For the purposes of this Privacy Policy:

a) Personal Data shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b) Processing shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
c) Controller shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

d) Processor shall mean a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2. COLLECTION OF INFORMATION

As part of the Company's client account opening procedures and ongoing obligations, the Company is required to comply with the legislative and regulatory framework applicable to Cyprus Investment Firms and the requirements of the Cyprus Securities and Exchange Commission (the "CySEC"). Specifically, the Company shall comply with its legal obligations under the AML Law (Law 13(I)/2018), as amended, and the AML Directive (Directive DI144-2007-08 of 2012) for the establishment on the Client's economic profile and prevention of money-laundering as well as abide with the relevant record keeping obligations under the European Commission Delegated Regulation (EU) 2017/565 (the "Delegated Regulation") and Law 87(I)/2017 for establishing the suitability and appropriateness of each Client based on the services offered by each CIF and recordings of telephone conversations, client transactions, FATCA and CRS.

Based on the above-mentioned obligations, the Company may request, collect, verify, process and retain the following categories of information for such periods as may be required by applicable laws, regulations and the Company's record-keeping obligations:

(a) Name and Surname
(b) Date of Birth
(c) Place of Birth
(d) Nationality
(e) Copy of the Passport and/or of the Identity Card
(f) Utility bill (including the full address of the client)
(g) Tax Identification Number
(h) Tax Residence
(i) Telephone number
(j) Email
(k) Profession
(l) Industry of Employment
(m) Gross Annual Income
(n) Net Worth
(o) Anticipated Turnover
(p) Bank Account Details
(q) Device Contacts
(r) Device Information and Identifiers

The Company may collect device-related information including device identifiers, mobile device information, application identifiers, operating system information, IP addresses, browser information, security information, fraud-prevention information, advertising identifiers where permitted by the operating system and applicable law, and other technical information necessary for security, analytics, attribution, fraud prevention, regulatory compliance and service improvement purposes.

Where you choose to use features such as sending assets, inviting friends, referrals, or selecting recipients from your device contacts, the Company may access contact information stored on your device, including contact names, email addresses and telephone numbers where available.

Access to device contacts is optional and will only occur where you grant the relevant permission and choose to use the applicable feature. Such information is accessed solely for the purpose of providing the requested functionality and is not used for unrelated purposes.

The Company does not access device contacts unless permission has been granted by you through your device settings or operating system permissions framework.

The Company may collect the said information directly from you (during the account opening procedure) and/or from third parties, including, without limitation, credit reference agencies, fraud prevention agencies, banks, payment service providers, electronic money institutions, other financial institutions, identity verification providers, third-party authentication service providers, sanctions screening providers and public registers.

The Company may also collect information relating to your use of the Platform, website and mobile applications, including pages viewed, features used, session activity, device information, technical logs, application events, analytics information, attribution information, trading activities, transaction activities and other information necessary to operate, secure, improve and analyse the Company's services.

The Company may also keep records relating to your trading and transaction activity, including:

i. Products you trade and their performance.

ii. Historical data about the trades and investments you have made including the amount invested.

iii. Historical data about your payment activities and your withdrawal activities.

Further to the above, the Company may also request further information to improve its Service to you (Existing or Potential Clients) or our activities (if you are our Provider for Trading Data) under our relevant Agreement or comply with Applicable Regulations.

The Company records any communications, electronic, by telephone, in person or otherwise, that we have with you in relation to the services that were provided by the Company to you and the relationship with you. Such recordings may be retained, reviewed, disclosed and processed where required for regulatory compliance, dispute resolution, fraud prevention, legal proceedings, internal investigations and the provision of services.

3. USE OF THE INFORMATION

The Company will collect, use, store, process and otherwise handle your personal data in accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR"), applicable Cyprus data protection legislation and any other applicable laws and regulations relating to the processing and protection of personal data.

The Company will collect and process personal data only for specified, explicit and legitimate purposes and will ensure that such data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Personal data will not be processed in a manner that is incompatible with those purposes unless otherwise permitted or required by applicable law.

The Company may transfer personal data to countries outside the European Economic Area ("EEA"), including to service providers, payment service providers, electronic money institutions, cloud infrastructure providers, technology providers, group companies and other authorised third parties where necessary for the provision of services, compliance with legal or regulatory obligations or other legitimate business purposes. Where such transfers occur, the Company shall implement appropriate safeguards in accordance with applicable data protection laws, including adequacy decisions adopted by the European Commission, Standard Contractual Clauses or any other lawful transfer mechanism recognised under applicable law.

The Company may process personal data for client onboarding, identity verification, know-your-customer ("KYC") procedures, anti-money laundering ("AML") compliance, sanctions screening, FATCA and CRS reporting, suitability and appropriateness assessments, account administration, regulatory compliance, fraud prevention, security monitoring, service improvement, analytics, attribution, marketing performance measurement, registration conversion analysis, deposit conversion analysis, first-time deposit attribution, transaction monitoring, risk management and the provision of investment and ancillary services.

4. CONTACTING YOU

The Company may contact you by telephone, email, SMS, push notification, post, in-platform messaging or any other available communication channel for purposes related to the administration of your account, the provision of services, compliance with legal and regulatory obligations, security notifications, transaction confirmations, customer support, updates to agreements, policies or disclosures, and any other matters relating to the Company's relationship with you.

Where required by applicable law, the Company will obtain your consent before sending marketing communications. If you consent, the Company and its Affiliates may contact you from time to time by telephone, email, SMS, push notification, post or other communication channels to provide information regarding products, services, promotions, events, market updates, surveys or other information which may be of interest to you.

You may withdraw your consent to receive marketing communications at any time by updating your communication preferences within the Platform, using any unsubscribe mechanism provided in the communication, or by contacting the Company directly. The withdrawal of consent shall not affect the lawfulness of processing carried out prior to such withdrawal and shall not affect communications that the Company is required to send for legal, regulatory, security or operational purposes.

5. DISCLOSURE OF INFORMATION

As part of using your personal information for the purposes set out above, we may disclose your information to:

(a) Service providers and specialist advisers who have been contracted to provide the Company with IT, cloud hosting, telecommunications, cybersecurity, financial, regulatory, compliance, legal, accounting, audit, consultancy, administrative and other support services.

(b) Partners, Introducers or Tied Agents with whom the Company has established business relationships and who provide services to or on behalf of the Company.

(c) Regulatory authorities, governmental bodies, supervisory authorities, law enforcement agencies, tax authorities, courts, tribunals, dispute resolution bodies and any other competent authority where disclosure is required or permitted by applicable law or regulation.

(d) Any person, organisation or representative authorised by you.

(e) Relevant authorities, financial institutions, fraud prevention agencies, sanctions screening providers and other organisations for the purposes of investigating, detecting, preventing or reporting fraud, money laundering, terrorist financing, sanctions breaches or other illegal or unlawful activities.

(f) Trade repositories, reporting mechanisms, approved reporting entities, execution venues, liquidity providers, custodians, brokers, counterparties, clearing organisations and similar entities where required for the provision of services or compliance with legal and regulatory obligations.

(g) The Company's directors, officers, employees, contractors, consultants, auditors and professional advisers who require access to such information for the performance of their duties, the provision of services, regulatory compliance, internal administration, risk management, fraud prevention, dispute resolution and the efficient operation of the Platform.

(h) Payment Processing Providers

To facilitate deposits, withdrawals, payment verification, fraud prevention, anti-money laundering (AML), know-your-customer (KYC), transaction monitoring and regulatory compliance obligations, the Company may share relevant personal information with its payment processing partners and electronic money institutions ("EMIs"), including but not limited to Hero Payments and Nuvei.

The information shared may include, where necessary and applicable, your name and surname, contact details, date of birth, identification and verification documents, payment card information (where applicable), bank account details, transaction details, device, security and fraud-prevention information, and any additional information required to process a deposit, withdrawal, refund, chargeback investigation, fraud investigation, regulatory review or compliance assessment.

These providers may collect, store, verify, process, transfer and retain such information in accordance with their own privacy policies, regulatory obligations, anti-money laundering requirements, fraud prevention procedures and applicable laws.

By initiating a deposit, withdrawal, payment transaction or related payment service through the Platform, you acknowledge that your personal data may be shared with and processed by such third-party payment providers for the purposes described above.

The Company takes reasonable steps to ensure that all payment processing providers engaged by the Company maintain appropriate technical, organisational and security measures to protect personal data and comply with applicable data protection laws.

(i) Analytics, Attribution and Marketing Measurement Providers

The Company may use analytics, attribution and marketing measurement service providers, including AppsFlyer, Google Ads, Google Analytics for Firebase and similar analytics, attribution and marketing measurement providers, to understand how users discover, install and use the Platform, measure the effectiveness of advertising campaigns, improve products and services, prevent fraud and evaluate business performance.

The information shared with such providers may include device identifiers, application identifiers, operating system information, campaign attribution data, event information relating to application usage, registration completion, account activation, deposits, first-time deposits, transaction status and other analytics events necessary to measure user acquisition and service performance.

Where supported by the operating system and permitted by the user, the Company may process advertising identifiers and similar device identifiers (including the Apple Identifier for Advertisers ("IDFA"), Google Advertising ID and equivalent technologies) for attribution, analytics, fraud prevention, advertising measurement and marketing performance purposes.

The Company does not share passwords, payment card numbers, bank account credentials or other authentication credentials with such providers.

Where required by applicable law, including the GDPR, the Company will obtain any necessary consent before collecting or sharing information for analytics, attribution or advertising measurement purposes. Where consent is not required, the Company may process such information on the basis of its legitimate interests, including improving services, measuring marketing effectiveness, preventing fraud and maintaining the security and integrity of the Platform.

Such providers may process personal data on the Company's behalf in accordance with contractual arrangements, applicable data protection laws and their respective privacy policies.

The Company requires organisations outside the Company that handle or obtain personal information to maintain its confidentiality, respect individuals' privacy rights and comply with applicable data protection laws and this Privacy Policy.

6. INTERNATIONAL DATA TRANSFERS

The Company may transfer personal data to countries outside the European Economic Area ("EEA"), including to service providers, payment service providers, electronic money institutions, cloud infrastructure providers, technology providers, group companies, analytics providers and other authorised third parties where necessary for the provision of services, compliance with legal or regulatory obligations, fraud prevention, security monitoring or other legitimate business purposes.

Where such transfers occur, the Company shall implement appropriate safeguards in accordance with applicable data protection laws, including adequacy decisions adopted by the European Commission, Standard Contractual Clauses ("SCCs"), binding corporate rules or any other lawful transfer mechanism recognised under applicable law.

The Company will take reasonable steps to ensure that any recipient of personal data outside the EEA maintains appropriate technical, organisational and security measures designed to protect personal data and process it in accordance with applicable data protection laws.

By using the Company's services, website or Platform, you acknowledge that your personal data may be transferred, stored or processed in jurisdictions outside your country of residence where necessary for the purposes described in this Privacy Policy.

7. YOUR CONSENT

The Company may process personal data on the basis of consent, contractual necessity, compliance with legal and regulatory obligations, legitimate interests or any other lawful basis permitted under applicable data protection laws, depending on the nature and purpose of the processing activity.

Where the processing of personal data is based on consent, such consent will be obtained in accordance with applicable data protection laws and may be provided through the Client Agreement, Platform settings, website interfaces, application permissions, marketing preferences or any other lawful mechanism made available by the Company.

Where consent is relied upon, you have the right to withdraw that consent at any time by updating your preferences through the Platform where available or by contacting the Company at compliance@epidi.com. Withdrawal of consent shall not affect the lawfulness of any processing carried out prior to such withdrawal.

Where required by applicable law, the Company will ensure that consent is freely given, specific, informed and unambiguous and is provided through a clear affirmative action.

The Company will not make consent a condition of service where such consent is not necessary for the provision of the relevant service.

In certain circumstances, the Company may process personal data without obtaining consent where permitted by applicable law, including where:

(a) Processing is necessary for compliance with a legal or regulatory obligation to which the Company is subject.

(b) Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

(c) Processing is necessary to protect the vital interests of the data subject or another natural person.

(d) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a competent authority.

(e) Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests, rights or fundamental freedoms of the data subject.

The Company may rely on one or more lawful bases for processing personal data depending on the specific processing activity, including for anti-money laundering ("AML") compliance, know-your-customer ("KYC") procedures, sanctions screening, FATCA and CRS reporting, fraud prevention, security monitoring, regulatory reporting, account administration, analytics, attribution, marketing performance measurement and the provision of investment and ancillary services.

8. MANAGEMENT OF YOUR PERSONAL INFORMATION AND SAFEGUARD MEASURES

The Company has implemented appropriate technical, organisational and administrative measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, misuse or any other unlawful form of processing.

The Company maintains internal policies, procedures, controls and employee training programs to promote the protection of personal data and information security. Employees, contractors, service providers and authorised representatives who process personal data on behalf of the Company are required to maintain confidentiality and comply with applicable data protection, information security and regulatory requirements.

Access to personal data is restricted to individuals who require such access for the performance of their duties, the provision of services, regulatory compliance, fraud prevention, risk management, customer support, system administration or other legitimate business purposes.

The Company may store personal data using secure electronic systems, cloud infrastructure, secure servers, backup systems and, where necessary, physical records. The Company takes reasonable steps to protect personal data from misuse, loss, unauthorised access, disclosure, alteration or destruction.

While the Company uses reasonable efforts to protect personal data, no method of transmission over the internet or electronic storage system can be guaranteed to be completely secure. Accordingly, the Company cannot guarantee the absolute security of information transmitted to or from the Platform, website, mobile application or other electronic communication channels.

The Company will retain personal data for as long as necessary to fulfil the purposes for which it was collected, including the provision of services, compliance with legal and regulatory obligations, dispute resolution, fraud prevention, enforcement of agreements and the protection of the Company's legal rights.

Where a business relationship exists between you and the Company, personal data will generally be retained for the duration of that relationship and for a period thereafter as required by applicable laws and regulations. In many cases, this may be at least five (5) years following the termination of the business relationship.

The Company may retain personal data for longer periods where required or permitted by applicable law, regulatory requirements, court orders, ongoing investigations, legal proceedings, anti-money laundering obligations, tax obligations or other legitimate business purposes. Retention periods will be determined based on the nature of the information, the purposes for which it was collected and the applicable legal and regulatory requirements.

9. CHANGE OF INFORMATION

You may inform the Company at any time that your personal information has changed, is inaccurate, incomplete or outdated, or that you wish to exercise any of your applicable data protection rights, by contacting the Company through the Platform, by email at compliance@epidi.com or through any other communication channel made available by the Company.

The Company will review and respond to such requests in accordance with applicable data protection laws and regulatory obligations and will correct, update, restrict, erase or otherwise process personal data where required or permitted by applicable law.

The Company may retain certain personal data where required to comply with legal, regulatory, tax, anti-money laundering, fraud prevention, record-keeping, dispute resolution or other legitimate business obligations, including obligations imposed by applicable financial services regulations.

10. RIGHT OF ACCESS

Subject to applicable law, you have the right to request confirmation as to whether the Company processes your personal data and, where that is the case, to obtain access to such personal data and information relating to its processing.

This may include information regarding the categories of personal data processed, the purposes of processing, the recipients or categories of recipients to whom the personal data has been disclosed, the envisaged retention period, the source of the data where it was not collected directly from you and the safeguards applied in connection with any international transfers.

You also have the right to request a copy of the personal data held by the Company and to request the correction of any inaccurate or incomplete personal data.

To exercise your right of access, please contact the Company at compliance@epidi.com. The Company may request information necessary to verify your identity before responding to any request.

11. QUESTIONS AND COMPLAINTS

If you have any questions regarding this Privacy Policy, wish to access, update, correct or delete your personal information, wish to exercise any of your data protection rights, have a complaint regarding the processing of your personal data or have any questions regarding the security of the Company's Platform, website or services, you may contact the Company at compliance@epidi.com.

The Company will endeavour to investigate and respond to any request, enquiry or complaint within a reasonable timeframe and in accordance with applicable laws and regulations.

If you are not satisfied with the Company's response or believe that your personal data has been processed unlawfully, you have the right to lodge a complaint with the Commissioner for Personal Data Protection of the Republic of Cyprus or any other competent data protection supervisory authority in accordance with applicable law.

12. UPDATE OF THIS POLICY

The Company may amend, revise or update this Privacy Policy from time to time to reflect changes in applicable laws, regulations, technologies, business practices, services or data processing activities.

Material changes will be communicated through the Platform, website, email or other appropriate communication channels where required by applicable law.

The latest version of this Privacy Policy will always be available on the Company's website and, where applicable, through the Platform. You are encouraged to review this Privacy Policy periodically to remain informed about how the Company collects, uses and protects your personal data.