# PRIVACY POLICY

## 1.Introduction

1.1. In2Markets Ltd. (hereinafter referred to as “the Company,” “we,” “our”) is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data when you interact with our website www.in2markets.com (the "Website"). We use cookies to provide you with a better, more personalized experience and improve our services.

1.2. By using our website, you consent to the use of cookies in accordance with this policy. If you do not agree to the use of cookies, you should adjust your browser settings or refrain from using our website.

1.3. This Privacy Policy may be updated periodically, and we will notify you of any significant changes by posting an updated version on our website.

## 2. Who We Are

2.1. In2Markets Ltd. is a Cyprus Investment Firm (CIF), incorporated under the laws of the Republic of Cyprus with company registration number HE 333743, and is authorized and regulated by the Cyprus Securities and Exchange Commission (CySEC) under license number 263/14. The Company operates in accordance with the applicable laws and regulatory framework governing the provision of investment services and the conduct of financial activities within the European Union.

2.2. The Company specializes in the provision of investment services related to Contracts for Difference (CFDs). We offer our services to retail clients, professional clients, and eligible counterparties, enabling them to trade CFDs on a wide range of financial instruments across both domestic and international markets.

2.3. The registered office of the Company is located at: In2Markets Ltd, Chrysanthou Mylona, 16 B, AVENUE COURT, 3030, Limassol, Cyprus. We are fully committed to safeguarding your personal data and ensuring its processing is conducted in full compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and other applicable data protection laws.

## 3. Types of Clients and Data Collection

3.1. Retail Clients:

Retail clients are individual investors who use the Company’s services for personal investment purposes. The personal data we collect from retail clients may include:

- ✓ Personal Identification Information:

  Full name, date of birth, nationality, and contact information (email, phone number, residential address).

- ✓ Financial Information:

  Income, assets, liabilities, and financial goals.

- ✓ Risk Profile:

  Information regarding the client’s risk tolerance, trading experience, and knowledge of financial instruments.

- ✓ Identification Documents:

  Passport, national ID, proof of address, and other documents required for compliance with anti-money laundering (AML) regulations.

3.2. Professional Clients:

Professional clients are individuals or entities that possess sufficient knowledge and experience in trading financial instruments and are classified as such under regulatory criteria.

The personal data collected from professional clients may include:

- ✓ Business Information:

Corporate details, business address, and company registration number.

- ✓ Financial Information:

Company's financial position, balance sheets, and asset declarations.

- ✓ Investment Experience:

Specific trading history and expertise in financial markets.

- ✓ Legal or Regulatory Information:

Information required to assess the client's eligibility as a professional client under CySEC's regulatory framework.

3.3. Eligible Counterparties:

Eligible counterparties are typically institutional clients, such as banks, investment firms, and insurance companies, which are subject to lower levels of regulatory protection.

The personal data collected from eligible counterparties may include:

- ✓ Business and Regulatory Information:

Documents proving classification as an eligible counterparty (e.g., financial institutions, regulated entities).

- ✓ Transaction and Trading Data:

Detailed data on significant trading activities and prior investment transactions.

3.4. The extent of personal data collection and processing is tailored to the classification of each client type. Retail clients undergo comprehensive suitability assessments, while professional clients and eligible counterparties are subject to simplified due diligence in line with the applicable regulatory framework. We apply the principle of data minimization to ensure that only data necessary for the specific legal and regulatory purpose is collected.

## 4. How We Collect Your Data

4.1. The Company collects personal data through the following means:

- ✓ Direct Collection:

Information provided by you when you create an account with us, fill out forms, and provide documents for verification (KYC/AML).

- ✓ Third-Party Sources:

Information collected from third-party verification sources, such as payment processors, identity verification services, or credit reporting agencies, to meet regulatory obligations.

- ✓ Automated Collection:

Data collected automatically through your interactions with our website, such as IP addresses, device information, and browser activity (via cookies and web tracking technologies).

4.2. By using our services, you consent to the collection and processing of your personal data as described in this Privacy Policy.

## 5. How We Use Your Data

5.1. The Company processes your personal data for the following lawful purposes:

- ✓ To perform our contractual obligations: open and manage trading accounts, execute transactions, and provide support;

- ✓ To comply with legal obligations: fulfil regulatory requirements, including anti-money laundering, tax, and investor protection rules;

- ✓ To meet regulatory and supervisory requirements: including reporting obligations under CySEC and other authorities;
- ✓ To serve legitimate interests: protect systems, prevent fraud, and ensure business continuity;
- ✓ To ensure the physical security of the Company's premises. The Company operates a restricted-range CCTV system installed at the entrance of its office. The camera is positioned to capture only individuals approaching the office door and does not record public areas or unrelated passers-by. Video footage is used solely to prevent unauthorized access or detect criminal activity. Access to recordings is limited to authorized personnel, and data is retained for a strictly limited period. This processing is carried out based on the Company's legitimate interest in protecting its physical infrastructure and complies with Article 6(1)(f) of the GDPR.
- ✓ To provide direct marketing communications: only with your explicit consent (opt-in) as required by GDPR.

5.2. Your data will not be processed for any purpose that is incompatible with those described above unless required by law or with your prior consent.

## 6. No Children's Data Collection

6.1. Our services are intended only for individuals aged 18 and older. We do not knowingly collect or process personal data of children. If we become aware that we have collected such data, we will take immediate steps to delete the data and disable the relevant account.

## 7. Cookies

7.1. The Company uses cookies to improve your experience on the Website. Cookies allow us to remember your preferences and help analyse web traffic.

7.2. For more information on the type of cookies we use and how to control or delete them, please refer to our Cookies Policy.

## 8. Sharing and Disclosure of Personal Data

8.1. In the course of providing services, the Company may share personal data with:

- ✓ Third-Party Service Providers:

  Such as payment processors, IT service providers, and legal consultants.
- ✓ Regulatory Bodies:

  Including CySEC, law enforcement, and tax authorities for compliance with legal obligations.
- ✓ Business Transfers:

  In the case of mergers, acquisitions, or business transitions, personal data may be transferred to a successor or affiliate.

8.2. All third parties granted access to personal data are contractually bound to maintain confidentiality and apply appropriate technical and organizational measures to ensure data protection in accordance with Article 28 of the GDPR.

## 9. Personal Data Transfers Outside the EEA

9.1. The Company may transfer personal data outside the European Economic Area (EEA), subject to adequate safeguards. These safeguards include using Standard Contractual Clauses or other legal measures to ensure the continued protection of your data.

## 10. Client Records Retention Periods

10.1. We retain your personal data for at least five (5) years following the end of our business relationship, or longer if required by law or regulation. In certain cases, data may be retained for up to seven (7) years or more if required to fulfil tax, regulatory, or legal obligations.

## 11. Personal Data Rights

11.1. You have the following rights under the GDPR:

- ✓ Right of Access: Request confirmation of whether we process your personal data and receive a copy of such data.
- ✓ Right to Rectification: Request correction of any inaccurate or incomplete data.
- ✓ Right to Erasure ("Right to be Forgotten"): Request deletion of data under specific legal grounds.
- ✓ Right to Restriction: Request that we limit the processing of your data.
- ✓ Right to Data Portability: Receive your data in a structured, commonly used, machine-readable format and request transfer to another provider.
- ✓ Right to Object: Object to processing based on legitimate interests or for direct marketing purposes.

11.2. You may exercise your rights by contacting us via the contact information provided in section 15. We may require verification of your identity before processing your request. You may also withdraw your consent to marketing at any time by following the unsubscribe instructions or updating your preferences.

## 12. Automated Decision-Making and Profiling

12.1. We may use automated systems to assess your risk profile and determine product suitability in compliance with MiFID II requirements. However, decisions with significant legal or similar effects are not made solely through automated processing. You have the right to request human intervention, express your point of view, and contest a decision.

## 13. Confidentiality and Security of Personal Data

13.1. The Company takes all necessary measures to protect personal data. This includes encryption of sensitive data and secure storage on password-protected servers. The Company also applies physical security measures, including a limited-range CCTV system installed at its premises. The system is configured to avoid capturing excessive or irrelevant data and serves solely to protect Company property.

13.2. Personal data will not be disclosed except as required by law or regulatory bodies.

## 14. Amendments to this Privacy Policy

14.1. The Company reserves the right to amend this Privacy Policy. Any updates will be posted on our website, and significant changes will be communicated to you directly.

## 15. Contact Us

15.1. If you have any questions about this Privacy Policy or wish to exercise your rights, please contact us at:

Email: compliance@in2markets.com

Website: www.in2markets.com

Phone: +35726221007

Address: Chrysanthou Mylona, 16 B, AVENUE COURT, 3030, Limassol, Cyprus

***Version 1.01: 30.05.2025***