PRIVACY POLICY – NPE MARKET

DRAFTED VERSION

1. INTRODUCTION

1.1 This Privacy Policy ("Policy") is issued by **NPE Market Limited**, a company registered under the laws of **Saint Lucia**, registration number **2024-00497**, having its registered office at Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros Islet, Saint Lucia, and operational office at 24th Floor, The One Tower, Barsha Heights, P.O. Box 390114, Dubai, United Arab Emirates ("NPE Market", "Company", "we", "us", "our").

1.2 The purpose of this Policy is to describe how the Company, acting as a **data controller** with respect to personal information under its possession, collects, processes, stores, transfers, and protects information pertaining to natural persons ("Client", "you", "your", "data subject") in connection with the Company's provision of Forex, CFDs, commodities, indices, metals, cryptocurrencies, and other OTC derivatives trading services.

1.3 This Policy applies to:

- Current Clients
- Prospective Clients
- Website visitors
- Users of the NPE Market trading platform
- IBs, affiliates, and partners
- Former Clients whose data is retained for compliance or legal purposes

1.4 By registering on our website, submitting documents, opening an account, using our platform, or interacting with the Company, you acknowledge that you have read and understood this Privacy Policy and that you consent to the data processing practices described herein.

1.5 This Policy does **not** apply to any third-party websites or services linked from our website, payment providers, or external parties not under our direct control.

2. DEFINITIONS

For purposes of this Policy:

- **"Personal Data"** means any information relating to an identified or identifiable natural person.
- **"Processing"** means any operation performed on personal data including collection, storage, use, transfer, disclosure, modification, or deletion.
- **"Data Controller"** means the entity that determines the purposes and methods of processing personal data.
- **"Data Subject"** means an individual whose personal data is processed.

- **“Third Parties”** means service providers, partners, banks, payment processors, regulatory bodies, or affiliates to whom the Company may disclose personal information.

While certain terminology originates from GDPR, the Company is **not subject to EU GDPR** unless explicitly required by client jurisdiction.

3. CATEGORIES OF PERSONAL DATA WE COLLECT

In order to provide our services, comply with regulatory standards, and ensure the integrity of our operations, NPE Market collects a range of personal information. Each category serves a specific legal, operational, or compliance purpose, and is processed in strict accordance with this Policy.

3.1 Identification and Verification Data

To establish a business relationship and verify your identity as required by Know-Your-Customer (KYC) and anti-money laundering (AML) regulations, we collect identification data such as your name, date of birth, nationality, residential address, and other demographic details. We also request copies of government-issued identification documents, including passports, national IDs, and driving licenses. Proof of address documents—such as utility bills or bank statements—are collected to confirm residency. In some cases, we may use video or biometric verification to authenticate your identity. This information ensures that we meet regulatory obligations, prevent illicit activity, and protect both the Company and clients from fraud or impersonation.

3.2 Contact Information

We collect contact data including your email address, phone number, and communication preferences. This information is used to contact you regarding account activity, verification procedures, platform updates, security alerts, or any obligations arising from our contractual relationship. Accurate contact information is essential for us to maintain effective communication and provide timely notifications related to your trading activities.

3.3 Financial and Trading Information

To deliver trading services, process transactions, and prevent financial abuse, we collect information relating to your trading accounts and financial activity. This includes account numbers, balances, positions, deposits, withdrawals, and trade history. We may collect details about your payment methods and bank accounts; however, we do not store sensitive card details. This data enables us to execute your trades, provide statements, ensure proper functioning of your account, and comply with regulatory requirements related to trade monitoring, audit trails, and financial reporting.

3.4 AML, KYC, and Regulatory Compliance Data

In accordance with international AML/CTF standards and the Company's legal obligations, we collect information intended to assess financial risk and verify the legitimacy of your funds. This may include your employment status, source of wealth, source of funds, tax residency, financial profile, FATCA or CRS information, and PEP (Politically Exposed Person) status. These data points help us identify potential risks, detect suspicious activity, and fully comply with anti-money-laundering regulations applicable to OTC financial service providers.

3.5 Technical and Platform Usage Data

When you access our websites, trading platforms, or mobile applications, we collect technical data such as IP addresses, device identifiers, operating systems, browser types, access times, and platform usage logs. We use this information for cybersecurity, fraud prevention, platform optimization, session management, and identification of unusual login activity. Technical data is essential to ensure the security and stability of our trading environment and to protect both users and the Company from unauthorized or malicious activity.

3.6 Optional and Voluntarily Submitted Data

From time to time, you may provide additional personal information through surveys, feedback forms, marketing opt-ins, or participation in promotions. You may also provide preferences regarding trading instruments, educational content, or communication methods. Submission of such data is optional and is processed only with your consent for customer experience enhancement or product development.

4. LEGAL BASES FOR PROCESSING PERSONAL DATA

Although NPE Market is an offshore entity and not legally bound by GDPR, we voluntarily adopt internationally recognized principles that help define the legal foundations on which personal data is processed. Doing so increases transparency, supports best business practices, and enhances client trust.

4.1 Processing Necessary for Performance of a Contract

When you open an account or register with NPE Market, you enter into a contractual relationship with the Company. To fulfill our obligations under that agreement, we must process your personal data to verify your identity, operate your trading account, process your deposits and withdrawals, execute trades, and provide access to our trading platforms and support services. Without this information, we cannot deliver the products and services you request.

4.2 Processing Necessary for Compliance with Legal Obligations

As a financial services provider, we are subject to AML, CTF, fraud prevention, taxation, and financial reporting regulations. These obligations require us to collect, verify, store, and analyze personal data for purposes such as identity verification, risk assessment, sanctions screening,

transaction monitoring, and maintaining records for regulatory inquiries. Failure to collect this data would place the Company in breach of mandatory compliance standards.

4.3 Processing for Legitimate Interests

We may process personal data to advance our legitimate business interests, provided these interests do not override your rights. Such interests include protecting our systems, preventing unauthorized access, enhancing cybersecurity, maintaining platform performance, investigating suspicious activity, improving customer service, developing new features, performing analytics, and defending legal claims. These activities are essential for the stability, reliability, and lawful operation of our business.

4.4 Processing Based on Consent

Where required, such as in the case of marketing communication or certain optional features, we process personal data only after obtaining your explicit consent. You retain the right to withdraw this consent at any time. Withdrawal of consent does not affect the lawfulness of prior processing carried out before the withdrawal.

5. PURPOSES OF DATA PROCESSING

We process personal data for clearly defined purposes aligned with our business operations and regulatory obligations. These purposes are intentional, necessary, and consistent with best practices in financial services.

5.1 Establishing and Managing Your Account

We use personal data to review your application, confirm your identity, assign an account number, configure account settings, and provide you access to trading environments. Without processing your identification and financial information, we cannot engage in a contractual relationship or legally permit trading activity.

5.2 Delivering and Improving Our Services

Data is used to execute your trades, assess market exposure, maintain account security, process deposits and withdrawals, and manage ongoing operations of the trading platform. We may analyze platform usage to improve stability, optimize features, and enhance user experience.

5.3 Ensuring Legal and Regulatory Compliance

We process data to comply with AML/CTF regulations, monitor for suspicious behavior, produce required reports, prevent fraud, respond to regulatory inquiries, meet audit obligations, and uphold industry standards for dealing with financial crime.

5.4 Safeguarding the Platform and Your Account

Technical data helps us protect the platform from unauthorized access, cyberattacks, and

abuse. We monitor access patterns, verify device integrity, assess login behavior, and detect irregularities that may indicate account compromise or misuse.

5.5 Communications and Notifications
We use your personal data to provide important notifications such as account updates, trade confirmations, margin calls, security alerts, service-related messages, or changes to terms. Such communication is essential for safe and effective account management.

5.6 Marketing and Promotions (Optional)
With your consent, we may use your data to send promotional materials, educational content, or product updates. You may opt out at any time using links provided in our communications.

6. COOKIES AND TRACKING TECHNOLOGIES

Cookies are small text files stored on your device that help us improve website functionality, personalize your experience, and analyze performance.

6.1 Purpose of Cookies
Cookies allow us to remember your preferences, maintain login sessions, enhance loading speeds, provide a consistent user experience, and understand how visitors interact with our website. They help identify errors, optimize user journeys, and improve performance of both web and mobile platforms.

6.2 Types of Cookies Used
We may use essential cookies required for platform operation, analytical cookies for performance measurement, preference cookies to remember user settings, and security cookies to detect fraudulent or unauthorized behaviour.

6.3 Managing Cookies
You may disable cookies in your browser settings. However, disabling essential cookies may impair access to the trading platform or reduce website functionality.

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

To operate effectively and comply with legal, technical, and regulatory standards, certain personal data must be shared with trusted third parties. We do so carefully, responsibly, and only when necessary.

7.1 Service Providers and Vendors
We may share data with third-party service providers who support our operations, including KYC verification vendors, AML screening firms, payment processors, banks, liquidity providers,

cloud hosting services, CRM operators, and technical infrastructure providers. These parties act under binding confidentiality obligations and process data only according to our instructions.

7.2 Legal, Regulatory, and Government Authorities

Where legally required, we may disclose data to courts, law enforcement agencies, financial regulators, tax authorities, or other governmental bodies. Such disclosure occurs only when mandated by law or necessary to protect our legal rights.

7.3 Internal Departments and Affiliates

Access to personal data is restricted to authorized personnel involved in compliance, risk management, payments, IT security, customer support, and senior management. Access is granted strictly on a "need-to-know" basis.

7.4 Protection Against Fraud and Abuse

We may disclose data to fraud prevention agencies, investigation partners, cybersecurity auditors, or other specialized entities for the purpose of preventing or investigating fraudulent activities, market abuse, or platform misuse.

7.5 No Sale of Personal Data

Under no circumstances do we sell or trade personal data for commercial gain.

8. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Because we operate globally, your data may be processed or stored in jurisdictions outside your country of residence. These transfers are necessary for platforms, infrastructure, support services, payment processing, and global operations.

8.1 Jurisdictions Involved

Data may be transferred to data centres or partners located in Saint Lucia, the UAE, the EU, Asia, or the United States. Such jurisdictions may have different levels of data protection, but we ensure that your information is handled securely.

8.2 Safeguards for International Transfers

We only work with third parties who provide adequate data protection standards, contractual safeguards, or recognized information security frameworks. By using our services, you authorize such international transfers as required for the execution of your agreement.

8.3 Operational Necessity

These transfers enable our trading platforms to function efficiently and allow us to provide uninterrupted, high-quality service to clients worldwide.

9. DATA SECURITY MEASURES

Protecting your personal data is a core operational priority. We apply a combination of administrative, technical, and organizational measures to prevent unauthorized access, loss, alteration, or misuse of personal information.

9.1 Technical Protection Measures

We use advanced encryption technologies for data transmission and storage, secure server environments, firewalls, intrusion detection and prevention systems, anti-malware protection, and multi-factor authentication for sensitive access points. We continuously monitor our systems for anomalies, attacks, and unauthorized behavior.

9.2 Organizational and Administrative Controls

Only authorized employees with a legitimate operational need may access personal data. Each employee is bound by confidentiality obligations and trained in data protection practices. Internal procedures govern access permissions, audit trails, data segmentation, and secure disposal of information once retention periods expire.

9.3 Incident Prevention and Response

We implement strict cybersecurity standards to minimize the risk of data breaches or unauthorized access. In the event of a suspected incident, we follow a structured incident response protocol designed to protect affected clients, secure systems, and meet any legal notification obligations in applicable jurisdictions.