

## 1. INTRODUCTION

QuantumTrade Global Market Limited is a Company incorporated and registered under the laws of Mauritius with registered number 212104GBC. The Company is licensed and regulated as an investment dealer by the Financial Services Commission under license number GB24203431 (refer to as “the Company, “QTGM”, “we”, “us”, “our”).

The Firm has appointed QuantumGlobeServe (EU) Limited, a company incorporated in Cyprus (HE 479664) with registered address at Pindo,4, Egkomi, 2409, Nicosia, Cyprus and an affiliate, to act as payment agent for the Firm.

## 2. APPLICABLE REGULATORY FRAMEWORK AND PURPOSE OF THIS POLICY

The formulation and adoption of this Policy is pursuant to and in compliance with applicable laws and regulations. This is to strengthen client protection and confidence when accessing financial services and products.

The purpose is to formulate procedures which ensure protection of non-public client information. The policy provides the manner in which the Company, its employees, agents or other relevant parties acting on its behalf, holds, treats and uses information received from actual or potential clients who intend to or partake in the products or services offered by the Company.

The Company shall not disclose the data of its clients and shall protect the confidentiality of its non-public client data. Client data shall only be utilized for the purposes specified and agreed with the financial client or as required under any applicable law.

This Policy is in addition to and does not replace or supersede any information in relation to the processing of personal data that is included in any of the existing Privacy Policy, Agreement, Partnership or Affiliates Agreement. The Company’s Privacy Policy, as amended from time to time, is published on the Company’s website and governs how the Company collects, uses, stores, discloses and transfers client’s personal data and the individual’s personal data rights during and after the termination of the business relationship.

## 3. NON-PUBLIC DATA COLLECTED AND PROCESSED

A list of non-public data collected and processed by the Company includes but is not limited to:

- Personal information such as: name, surname, residential address, e-mail address, phone number, date of birth, gender, citizenship, occupation and employment details;
- Information for the construction of client’s economic profile, including source of income and wealth, details about source of funds;
- Information on whether a client is a politically exposed person (PEPs);
- Bank account and/or credit card details or/and other payment details;
- Documents provided to the Company for verification of the client’s identity i.e., passport/identity card, utility bills and other identifiable documents of clients who are physical persons;
- Documents provided to the Company for verification of identity of clients who are legal entities such as the legal entity’s incorporation documents as applicable, financial statements, business plan, passport/ID, utility bills and other identifiable documents of directors, shareholders and authorized persons of the legal entity for verification purposes; and

- Any other information designated as confidential.

#### **4. SENSITIVE DATA COLLECTED AND PROCESSED**

The Company considers the following personal data to be “sensitive”:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person’s sex life or sexual orientation.

The Company does not customarily collect and process sensitive data from clients or potential clients during the provision of the services. Where the Company will ask you for sensitive personal data it will always tell you why and how the information will be used.

#### **5. THE PURPOSE FOR WHICH NON-PUBLIC CLIENT DATA IS COLLECTED AND USED**

The non-public client data collected by the Company are used in all stages of its business relationship with clients to be able to provide the services and products based on the client services agreement and business relationship with the clients. In other words, the Company needs to collect the data explained above for the performance of its contractual obligations towards clients. In addition, processing of personal data takes place to be able to complete our client due diligence and onboarding process, as well as to ensure the provision of high-quality services to its clients.

The Company is subject to several laws and regulations including anti-money laundering laws and financial services laws while it is under the supervision of competent authorities such as Financial Services Commission in the Republic of Mauritius whose laws, regulations and circulars apply to the Company. For this purpose, the Company is required to comply and collect certain data during the client onboarding and ongoing monitoring of clients as well as transactions and/or request information from clients for risk mitigation/management reasons.

At the beginning a client relationship, non-public client data such as without limitation full name, address and telephone number are required by the Company to authenticate/verify the identity of a client. Identifying the true identity of a client is of crucial importance for the Company, as it enables the Company to identify, assess, mitigate, prevent and investigate possible fraudulent activity.

In the course of a client relationship, non-public client data such as without limitation the risk aversion, income and profession of a client are required by the Company to assess the appropriateness of the products and services it provides to clients. In addition, using the client’s data the Company is able to manage the client’s account and/or inform the client about any products or services that may be of his/her interest. Apart from the aforesaid, the data can be used by the Company for statistical purposes with the aim of improving its products and services as well as to update clients on any issues that might arise regarding their business relationship with the Company.

Lastly, non-public client data is necessary at the stage at which a client decides to terminate its relationship with the Company. In this stage, non-public client data might be used for the purpose of resolving and/or assessing the history of a client's complaint. It is noted that non-public client data is kept by the Company for a period of 7 years from the date of the client's last transaction with the Company, in line with anti-money laundering and the requirements of our regulatory authority.

## **6. SECURITY PRACTICES AND PROCEDURES TO SAFEGUARD NON-PUBLIC CLIENT DATA**

The Company implements the required procedures for safeguarding the security, integrity, and confidentiality of information, considering the nature of the information to be stored.

Agents or third parties that assist the Company to provide its services to clients shall maintain the confidentiality of non-public client data and use such information only in the course of providing their services, based on the Company's directions.

The Company monitors the activities of agents and third parties acting on its behalf on the basis of the relevant agreements that are in place for each business relationship.

The security of non-public client data is of utmost importance for the Company. For this reason, the Company implements a number of procedures on the accessibility and protection of data.

Specifically, non-public client data is only accessible by employees who need the specific information in order to operate, develop or improve the Company's services. Such individuals are bound by confidentiality and are subject to internal disciplinary procedures in case they fail to meet their obligations.

The accessibility of non-public client information by employees is based on the following principles:

- a. Differentiation of the access rights depending on job responsibilities;
- b. Protect systems using technical measures at the network, system and application levels, as well as organizational measures;
- c. Responsibility measures for the illegal rendering of the information to the employees of the Company and by individuals outside the Company;
- d. Ensure confidentiality of information by using data encryption and access control.

## **7. COLLECTION OF NON-PUBLIC CLIENT DATA**

### **7.1. Processing of data**

The processing of non-public client data is carried out through the information processing systems used by the Company. The data collected from clients are only processed and analyzed by the employees of the Company, and by persons who have the required authority and rights to use such data. The Company treats unauthorized access to data by employees as a serious violation of the Company's internal policies and procedures. To this end, any unauthorized access to non-public client data by employees is subject to disciplinary procedures, without prior notice

The Client can request from the Company to restrict and/or terminate the processing of his/her Personal Data at any time and the Company shall duly consider such request based on the applicable laws and regulations.

### **7.2. Intended recipients**

The intended recipients of non-public client data shall be the employees of the Company, persons who possess the required rights and authority to access such data. In addition, any agent's or third parties acting on behalf of the Company should be considered as intended recipients of the data only in case such data is required in the course of providing their services, based on their agreement with the Company.

### **7.3. Non-public client data rights**

The Client may exercise the following rights in relation to the non-public data the Company holds by sending an email at [cs@quantumtrade.com](mailto:cs@quantumtrade.com).

Every client has the right to review his/her non-public client data stored by the Company, upon request to the Company.

Every client has the right to correct or amend his/her non-public client data stored by the Company, upon request to the Company.

## **8. STORAGE OF NON-PUBLIC CLIENT DATA**

The Company undertakes all reasonable and appropriate organizational, physical and technical measures for the protection of non-public client data against unlawful access, destruction, misuse or accidental loss.

Non-public client data are being stored on the various databases of the Company located on the Company's server and cloud. In case of third-party service providers, non-public client data are being stored in their servers and cloud. In selecting a third-party service provider, the Company will assess their reputation, experience in handling confidential data as well as the jurisdiction in which the third-party service provider is operating. The Client acknowledges that when the Company uses a third-party service provider, the Company needs to rely on the provider's infrastructure and internal organizational process.

For safeguarding the Company's recorded data from possible loss, the Company implements consistent, reliable and documented back up procedures. The back up procedure is automatic and takes place in different ways and frequency depending on the criticality level of the relevant business application system.

The Company keeps client's non-public client data on record for a period of seven (7) years from the date of the last transaction of the client with the Company. In case there is an investigation against any client the documents will be kept according to the instructions of the investigating authority.

The Company will be able to retrieve the relevant documents/data without undue delay and present them at any time to the local authorities if requested.

## **9. DISCLOSURE OF NON-PUBLIC CLIENT DATA**

The Company may disclose non-public client data to a third party in the following circumstances:

- a. If the client has been informed about the disclosure and he/she has consented in writing to the disclosure.
- b. If the third party to which the data will be disclosed has been authorized by the client to obtain the data from the Company.
- c. If the Company is required to disclose the non-public client data under mandated regulatory reporting or under any other law or by a court order.

**10. VOLUNTARY DISCLOSURE**

Apart from the above circumstances, the Company might disclose the client's non-public data to third parties, on the basis that the client has voluntarily consented to this Policy, as described in section 11 below.

**11. CLIENT CONSENT**

At the stage of establishing a business relationship with the client, the Company obtains the client voluntary consent to this policy. Such consent is obtained before the offering of any services to the client.

**12. HOW TO CONTACT US**

The Client can extend any questions or requests he/she might have in relation to his/her data stored by the Company by sending an email at [cs@quantumtradeglobal.com](mailto:cs@quantumtradeglobal.com).