PRIVACY POLICY

1. INTRODUCTION

Your privacy is very important to us. We are committed to protecting and respecting your personal data. This Privacy Policy describes what types of personal data we collect about you when you choose to use our services, how we will use your personal data, when and with whom we share it and how we keep it safe. It also details your rights regarding processing of your personal information and how you may exercise them. Please take the time to read and understand this policy

Should the Company decide to amend or revise this privacy statement, the Company may do so at any time with no prior consent of any User. The Company will post those changes to this privacy statement through the Website so that the User becomes aware of any changes. It is advised that this policy is checked for updates. Any personal information we hold will be governed by our most current privacy notice. If we make changes we consider to be important, we will communicate them to you.

Please note that this notice is addressed to customers and potential customers. If you are an QFS employee, a contractor to QFS or a third-party service provider, your personal information will be used in connection with your employment contract, your contractual relationship or in accordance with our separate policies which are available by contacting us.

Any reference to 'us', 'our', 'we' or 'QFS' in this privacy notice is a reference to any company within the QFS Group as the context requires unless otherwise stated.

Similarly, any reference to 'you', 'your', 'yours' or 'yourself' in this privacy notice is a reference to any of our customers and potential customers as the context requires unless otherwise stated.

By accessing our websites including using any of the communication channels to contact us, we consider that you have read and understood the terms of this notice and how we process any information you disclose to us including personal data prior to becoming a client. Once you open an account with us, you agree that this notice, 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 business relationship and after its termination

2. WHAT KIND OF PERSONAL INFORMATION DO WE COLLECT AND STORE?

As part of our business we collect personal data from customers and potential customers for legitimate business purposes that include the following:

- name, surname and contact details
- date of birth and gender
- information about your income and wealth including details about your assets and liabilities, account balances, trading statements, tax and financial statements
- profession and employment details
- location data
- knowledge and experience in trading, risk tolerance and risk profile

- IP address, device specifications and other information relating to your trading experience
- Bank account, e-wallets and credit card details
- details of your visits to our Website or our Apps including, but not limited to, traffic data, location data, weblogs and other communication data.

We use cookies to store and collect information about your use of our Website. Cookies are small text files stored by the browser on your equipment's hard drive. They send information stored on them back to our web server when you access our Website. These cookies enable us to put in place personal settings and load your personal preferences to improve your experience. You can remove persistent cookies by following directions provided in your Internet browser's "help" file. We also keep records of your trading behaviour, including a record of:

- products traded
- historical data about the trades and investments you have made including the amount invested
- your preference for certain types of products and services

We are required by law to identify you if you are opening a new account or adding a new signatory to an existing account. Anti-money laundering laws require us to sight and record details of certain documents (i.e. photographic and non-photographic documents) to meet the standards, set under those laws. Identification documentation, as required under anti-money laundering legislation or other legislation relevant to the services we provide to you, includes:

(a) passport;
(b) driver's licence;
(c) national identity card (if applicable);
(d) utility bills;
(e) trust deed (if applicable);
(f) a credit check on the individual; or
(g) other information we consider necessary to our functions and activities.

If you are a corporate client we are required to collect additional information such as corporate documents of address, shareholders, directors, officers including additional personal information on the Shareholders and Directors. We have the right to ask any additional information we deem necessary to be compliant with our legal and regulatory requirements.

We obtain this information in a number of ways through your use of our services and websites, the account opening applications, our demo sign up forms, website cookies, and similar tracking technology built into our Websites and Apps, subscribing to news updates and from information provided in the course of our ongoing relationship.

We may also collect this information about you from third parties either through bought-in third party marketing lists, publicly available sources, social media platforms, introducing brokers and

affiliates, bankers and credit card processors, subscription-based intelligence databases and other third-party associates.

We may ask for other personal information voluntarily from time to time (for example, through market research, surveys or special offers). If you choose not to provide the information we need to fulfil your request for a specific product or service, we may not be able to provide you with the requested product or service.

We may record any communications, electronic, by telephone, in person or otherwise, that we have with you in relation to the services we provide to you and our relationship with you. These recordings will be our sole property and will constitute evidence of the communications between us. Such telephone conversations may be recorded without the use of a warning tone or any other further notice.

3. WHO MAY WE DISCLOSE PERSONAL INFORMATION TO?

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

- other companies within the QFS group who provide financial and other services;
- third party apps providers when you use our apps, communication systems and trading platforms which are provided to us by third parties;
- service providers and specialist advisers who have been contracted to provide us with services such as administrative, IT, analytics and online marketing optimization, financial, regulatory, compliance, insurance, research or other services;
- introducing brokers and affiliates with whom we have a mutual relationship;
- Payment service providers and banks processing your transactions;
- auditors or contractors or other advisers auditing, assisting with or advising on any of our business purposes;
- courts, tribunals and applicable regulatory authorities as agreed or authorised by law or our agreement with you
- government bodies and law enforcement agencies where required by law and in response to other legal and regulatory requests;
- any third-party where such disclosure is required in order to enforce or apply our Terms and Conditions of Service or other relevant agreements;
- anyone authorised by you.

We endeavour to disclose only the minimum personal data that is required to perform their contractual obligations to us. Our third-party service providers are not permitted to share or use personal data we make available to them for any other purpose than to provide services to us.

Our websites or our apps may have links to external third-party websites. This Privacy Policy does not apply to those other sites which we link to and the Company is not responsible for any personal information collected by third parties via those other sites. Please check with each third party as to their privacy practices and procedures.

4. WHEN AND HOW DO WE OBTAIN YOUR CONSENT?

We may process your personal data for one or more lawful bases of processing ("Lawful Basis") depending on the specific purpose for which we are using your data.

The Lawful basis are the following:

- to perform our contractual obligations towards you
- to be compliant with the legal and regulatory requirements
- to pursue our legitimate interests

Where the use of personal information does not fall under one of these three Lawful basis we require your consent. Such consent shall be freely given by you and you have the right to withdraw your consent at any time by contacting us using the contact details set out in this privacy notice or by unsubscribing from email lists.

5. MANAGEMENT OF PERSONAL INFORMATION

We are committed to safeguarding and protecting personal data and will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to protect any personal data provided to us from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

We require organizations outside of QFS who handle or obtain personal information acknowledge the confidentiality of this information, undertake to respect any individual's right to privacy and comply with the all relevant data protection laws and this privacy notice.

In brief, the data protection measures we have in place are the following:

- we train our employees who handle personal information to respect the confidentiality of customer information and the privacy of individuals
- requiring our employees to use passwords and two-factor authentication when accessing our systems;
- relevant employees only have access to the personal data required for the purposes of the tasks they handle;
- We apply data encrypting technologies during data transmission during internet transactions and client access codes transmitted across networks
- employing firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses entering our systems;
- using dedicated secure networks or encryption when we transmit electronic data for purposes of outsourcing.

6. HOW DO WE STORE PERSONAL INFORMATION AND FOR HOW LONG?

QFS makes efforts to maintain the appropriate safeguards in order to ensure that the security, integrity and privacy of the data and personal information that you have provided is not misused.

Such measures and safeguards include encryption during data transmission, strong authentication mechanisms and the separation of machines and data to provide secure areas. While such systems and procedures reduce the risk of security breaches, they do not provide absolute security. Therefore the Company cannot guarantee that our service will be immune from any wrongdoings, malfunctions, unlawful interceptions or unauthorized access to the information stored therein and to other information security risks, or that your private communications on or through our service will remain private. We may need to maintain records for a significant period of time. For example, we are subject to investment services and anti-money laundering laws which require us to retain copies and evidence of the actions taken by us in regard to your identity verification, sources of incomes and wealth, monitoring of your transactions, telephone, chat and email communications, orders and trades history, handling of your complaints and records that can demonstrate that we have acted in line with regulatory code of conduct throughout the business relationship. These records must be maintained for a prolonged period after our business relationship with you has ended or even longer if required by our Regulators.

Where you have opted out of receiving marketing communications we will hold your details on our list so that we know you do not want to receive these communications.

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers or Affiliate companies. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy.

When we transfer your data to other third parties outside the EEA, we may in some cases rely on applicable standard contractual clauses, binding corporate rules, the EU-US Privacy Shield or any other equivalent applicable arrangements.

If you would like a copy of such arrangements, please contact us using the contact details below.

7. YOUR RIGHTS

Please note that these rights do not apply in all circumstances. You are entitled to:

(a) request access to your personal data (commonly known as a "data subject access request");

(b) request correction of the personal data that we hold about you;

(c) request erasure of your personal data. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request;

(d) object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms;

(e) request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful, but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it;

(f) request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information (i.e. not to hard copies) which you initially provided consent for us to use or where we used the information to perform a contract with you; and

(g) withdraw consent at any time where we are relying on consent to process your personal data. To withdraw constant, kindly address your quires to complaince@quantixfs.com

We will endeavour to respond to all requests within 30 days. Occasionally, it may take us longer than 30 days if your request is particularly complex or you have made a number of requests. In this case, we will notify you within 30 days of the receipt of your request and keep you updated.

We may charge you a reasonable fee to you when a request is manifestly unfounded, excessive or repetitive, or we receive a request to provide further copies of the same data. In this case we will send you a fee request which you will have to accept prior to us processing your request. Alternatively, we may refuse to comply with your request in these circumstances.

8. WHAT IF YOU HAVE A QUERRY OR A COMPLAINT?

If you have a concern about any aspect of our privacy practices, you have the right to contact us to make a query or a complaint by email at complaince@quantixfs.com

We try to respond to all requests within 30 days. Occasionally, it may take us longer than 30 days if your request is particularly complex or you have made a number of requests. In this case, we will notify you within 30 days of the receipt of your request and keep you updated.

If you are not satisfied with our response to your complaint, you have the right to lodge a complaint with our supervisory authorities. Alternatively, you also have the right to lodge a complaint with the data protection authority of your country of residence.