PRIVACY POLICY

3 September 2019

1. Policy Statement

Privacy is fundamental to our relationship with clients. We are committed to maintaining the confidentiality, security and integrity of our clients' information. A client's right to privacy extends to all mediums of communication, including written correspondence, online chat and other electronic media, telephone conversations and in-person meetings.

During the course of its business, Y TREE will collect, store and process personal data about its customers, suppliers and other third parties. Y TREE aims to treat this data in a correct, transparent and lawful way in order to inspire confidence in our organisation.

This document lays out in simple terms the type of data Y TREE collects in the course of business, why we collect this data, how we use and store data, and who it is available to.
We adhere to the following principles with respect to personal data:

- Personal data is collected for a specific reason, and is limited to what is necessary
- We are transparent in the way in which personal data is processed, handled and stored
- We will never share personal data with a third party for financial gain (i.e. sell data)
- Client data is compartmentalised, and is only accessible to those who need it
- We take appropriate steps to ensure that personal data is either kept up to date or deleted
- Client data is stored securely at all times

All Y TREE employees are obliged to comply with the data protection & usage policy when processing personal data on the company's behalf. Any breach of this policy may result in disciplinary action.

2. Types And Scope Of Data We Collect

With their consent, we collect personal data from our clients. This includes data we receive directly from our clients (either in paper format, by email or specified within our technology interface) and data we receive from other sources (e.g. from a client's investment providers, or from service providers such as banks or credit institutions).

Presently, the only third party source from which we receive client specific data is from Yapily Limited ("Yapily"). Yapily provides an interface which is connected to over 2,500 banking institutions and acts as an

interface with our clients' bank accounts in order to supply client bank balances and transaction data to our platform, with clients' permission.

We process client data, with their consent, in order to provide tailored investment advice. To achieve this, we amalgamate client data with asset and exposure data from other service providers (such as Reuters).

With their consent (in the case of clients / prospective clients) and with legitimate business interests (in the case of employees / prospective employees), we also collect and store personal data. We may, at our discretion, collect data on employees' data usage, website browsing history and review any communications (phone calls, email, instant messages) made on company property, with a view to ensuring the safety and security of client information, and to ensure that employees are compliant with the relevant regulatory requirements in the jurisdiction in which they are operating.

3. How We Store And Process Data

Client and employee data may be held on paper, a personal computer or other media, and is subject to legal safeguards specified in The General Data Protection Regulation (EU) 2016/679 ("GDPR"). In the UK, GDPR is enforced by the Information Commissioner's Office ("ICO").

If you request to link bank current account or credit cards to your Y TREE account, Y TREE will request this data from your bank or provider via a third party organisation, Yapily. Yapily are a company specialising in the aggregation of financial data. In order to retrieve this data efficiently, Yapily may retain and store your personal information.

We may also share client data with local and foreign regulators, governments, law enforcement authorities, advisors, courts, tribunals and arbitrators as required by law.

4. Who Is Responsible For Client Data Protection?

The GDPR requires that companies meeting certain criteria must appoint a Data Protection Officer ("DPO"). Y TREE is not required to appoint a DPO under the GDPR, but we have decided to do so voluntarily. Our DPO can be contacted at :

Data Protection Officer
Y TREE Limited
2 Stephen Street
London W1T 1AN
Tel: +44 203 457 0551
Email: dpo@y-tree.com

Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
Our DPO acts as a contact point for the ICO, and particularly in the event of a data security breach. They cooperate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

5. Your Rights

The GDPR provides the following rights for individuals:

The right to be informed
Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

The right of access
Individuals have the right of access to personal data held about them.

The right to rectification
Individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. Y TREE has one calendar month to respond to a request. In certain circumstances, Y TREE can refuse a request for rectification.

The right to erasure
Also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. Y TREE has one month to respond to a request. The right is not absolute and only applies in certain circumstances.

The right to restrict processing
Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, Y TREE is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. Y TREE has one calendar month to respond to a request.

The right to data portability
The right to data portability allows individuals to obtain and re-use their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to object
The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Objections can be made verbally or in writing and Y TREE will have one calendar month to respond to an objection.

Rights in relation to automated decision making and profiling
The GDPR has provisions on (i) automated individual decision-making (making a decision solely by automated means without any human involvement); and (ii) profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Y TREE does not presently undertake either of these activities.

More information about these rights can be found at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

6. How can I request a copy of my data or request that it is permanently deleted?

To request a copy of your personal data, or to exercise any of the rights specified in section 5 above, we ask that you contact either our Data Protection Officer, or your adviser, in writing (either electronically or otherwise).

7. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data.

We put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to another organisation that processes data if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

We also maintain data security by protecting the confidentiality, integrity and availability of the personal data, as defined as follows:

- Only people who are authorised to use the data may access it
- Personal data should be accurate and suitable for the purpose for which it is processed
- Personal data is encrypted and stored centrally in a secure virtual environment, and is not typically stored on individual machines (except for short periods of time in relation to the activity being undertaken by an authorised individual)

Our security procedures include:

- We encrypt client data using AES 256-bit encryption
- Personal data relating to clients of Y TREE is kept segregated and separately encrypted from transaction data. Transaction data is anonymised using a unique client reference number
- A clear desk policy - no client personal information is to be left in view. Such documents should be stored in secure locations such as a locked filing cabinet
- Entry controls to Y TREE's physical work space
- Confidential paper documents which are no longer required will be shredded
- Data users must ensure that confidential data is not visible to passers by on their screen, and to lock computers when not in use

8. Transferring Personal Data to a Country Outside of the EEA

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Currently, Y TREE does not send any personal data outside of the EEA. However, should we have the need to do so in future, it is our responsibility to ensure that we only transfer data to organisations that have provided adequate safeguards, such as appropriately secure levels of data encryption and storage. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

9. Data Retention

As a regulated financial services firm, Y TREE has a number of regulatory requirements relating to the retention of client data. Most notably, we are required to retain client records relating to MiFiD business for a period of 5 years. Y TREE reserves the right to retain client records for longer periods of time than specified under FCA regulations up to an indefinite period. This does not affect an individual's right to request that their data is deleted, subject to GDPR.

10. Changes to this Policy

We keep this Privacy Policy under regular review. We reserve the right to amend this policy at any time. Where appropriate, we will notify subjects of those changes electronically.