

**Thayer Brook Partners LLP (the “Firm”)
PRIVACY POLICY**

The privacy policy set forth here applies to the Firm and affiliated companies of the Firm.

Protecting Confidential Information

This policy, together with (depending upon how you access the Firm or provide data to the Firm) the Firm’s [Terms & Conditions](#) and any other documents referred to, governs how the personal data obtained by the Firm or provided to the Firm is processed by the Firm. The Firm takes reasonable and proportional steps to protect personal information and ensure that it remains private. This policy summarizes the categories of personal information that the Firm collects, how that information is handled, and how the Firm protects that information. By visiting www.thayerbrook.co.uk (the “Firm’s site”) Clients are accepting and consenting to the practices described in this policy.

For the purpose of the Data Protection Act 1998 (“the Act”) and depending on how the Firm has received data, the Firm is either the data controller or the data processor. For more information contact the Firm’s Data Protection Officer (Scott Ganis) at scott@thayerbrook.co.uk.

Other than as may be outlined within this Privacy Policy, the Firm does not disclose any non-public personal information to anyone, except as required or permitted by law.

The Firm does not sell personal information to companies that are not associated with the Firm.

Collection and Use of Personal Information

The Firm collects non-public personal information from the following sources, from clients or prospective clients (as applicable), solely for the purposes specified:

- Information received on account applications or other forms, such as name, address, federal tax identification number, income, assets and similar information. The Firm uses this information to administer accounts, process transactions requested by clients, respond to client inquiries, evaluate client investment needs, and identify other products and services that may interest clients;
- Information about client transactions with the Firm or the Firm’s affiliates, such as client account balance, transaction history and payment activity. This information is used to process transactions and ensure the accuracy of the records and reports the Firm maintains that relate to client accounts. The Firm may also collect various other types of data, such as transaction, site navigation and optional survey information, in connection with client use of online services the Firm make available, either directly or through other entities. The Firm uses this information in order to improve the quality of the services the Firm offers clients; and
- Information the Firm collects or receives during communications with clients and the Firm’s affiliates, and due diligence which may include consumer reporting agencies, such as credit relationships and credit history. The Firm uses this information to help the Firm fulfill the Firm’s regulatory obligations and determine client eligibility for the Firm products and services.

Sharing of Information Within the Firm

The information the Firm or any affiliate collects relating to client transactions, accounts, account applications, due diligence and experiences with the Firm may be shared among the Firm's affiliates.

Sharing of Information Outside the Firm

As permitted by law, the Firm may disclose some or all of the information described above with entities that are not affiliated with the Firm for the purpose of servicing the Client's account(s), improving the Firm's services, or providing products and services clients have requested from the Firm. Such companies may include:

- companies that are the source or origin of financial services offered by the Firm, such as collective investment schemes, futures commission merchants ("FCM"), banks, securities broker-dealers, mutual fund companies and insurance companies;
- nonfinancial companies, such as companies that perform services on behalf of the Firm, auditors, companies that prepare account statements for the Firm, or companies that assist the Firm in communicating or marketing its services;
- others, such as independent contractors or technical system consultants who program the Firm's software, government agencies and regulators, consumer reporting agencies, and other outside entities as permitted or required by applicable laws; or
- a third party who acquires the firm as the personal information held by the Firm will be one of the transferred assets.

Protecting the Confidentiality of Client Personal Information

All employees of the Firm are instructed to use strict standard of care regarding the confidentiality of clients' non-public personal information as outlined in the Firm's policies. Employees not adhering to the Firm's policies are subject to disciplinary action. The Firm require outside companies and independent contractors to whom the Firm provide customer information for servicing or processing to enter into a confidentiality agreement that restricts the use of the information to those purposes. The Firm maintains physical, electronic and procedural safeguards that comply with applicable laws to protect client non-public personal information. The information that the Firm collects may be transferred to, and stored at, a destination outside the European Economic Area ("**EEA**"). It may also be processed by the Firm or the Firm's suppliers operating outside of the EEA for the purposes set out above.

Client rights

Clients have the right to ask the Firm not to process their personal data for marketing purposes. Clients can exercise their right to prevent such processing by contacting the Firm at the following email address: **marketing@thayerbrook.co.uk**.

Access to information

The Act gives Clients the right to access information held about them. A Client's right of access can be exercised in accordance with the Act. Any access request may be subject to a maximum fee of £10 to meet the costs in providing the Client with details of the information the Firm holds about them.

Questions or comments about this policy should be directed to the Firm's Data Protection Officer (Scott Ganis).