Fulcrum Asset Management LLP

Privacy Policy

July 2018

1. Introduction

This policy sets out Fulcrum Asset Management LLP ("**Fulcrum**" or "**the Firm**")'s commitment to data protection, and individual rights and obligations to personal data. Where applicable, it draws on the new rules and principles under the General Data Protection Regulation ("**GDPR**")[1]. Under the regulation, Fulcrum would be listed as a 'Controller' and a 'Processor' of personal data given it is domiciled in the EU and processes personal data in the EU.

In the course of Fulcrum's business, any client[2] personal data held by the Firm is held in a secure and fully protected manner at all times. Fulcrum has previously adopted exisiting policies and procedures in order to comply with the U.S. Securities and Exchange Commission's (SEC), Commodity Futures Trading Commission's (CFTC) privacy rules.

Any questions about this policy, or requests for further information, should be directed to the Firm's Compliance Department.

2. Data protection principles

The Firm processes client personal data in accordance with the following data protection principles:

- The Firm processes personal data lawfully, fairly and in a transparent manner.
- The Firm collects personal data only for specified, explicit and legitimate purposes.
- The Firm processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Firm keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Firm keeps personal data only for the period necessary for processing.
- The Firm adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Personal information is collected through the following sources: (i) subscription documents, (ii) Investor questionnaires and (iii) provided by the client in writing, in person, by telephone, electronically or by any other means.

Such information may include, but is not limited to, name, address, nationality, tax identification number, financial and investment qualifications and through investments with Fulcrum (either through a pooled investment vehicle or as a separately managed account).

In some cases, the Firm needs to process data to ensure that it is complying with its legal and compliance obligations.

---

1 REGULATION (EU) 2016/679

2 In this document, the Firm defines 'client' as an investor who is a natural person or, in the case of a corporate entity, its directors, members, employees, shareholders, agents, interns and any other personnel.

In other cases, the Firm has a legitimate interest in processing personal data before, during and after the end of the contractual relationship. Processing client data allows the company to:

- Provide products and services to clients such as managing transactions, engaging with transfer agents, meeting tax requirements and performance of any other tasks necessary as part of the ordinary course of the business relationship.
- Market to relevant potential clients or existing clients concerning new products or services via email, telephone, post or in person and ensuring client records are up-to-date for those purposes.
- Onboard new clients and comply with our compliance requirements such as AML/KYC. This could include obtaining information from third-party data solution providers, credit agencies and law enforcement; and
- respond to and defend against legal claims.

Fulcrum will update client-related personal data promptly if an individual advises that his/her information has changed or is inaccurate. The individual is responsible for updating Fulcrum of any changes.

Personal data gathered during the business relationship is held in the client's dedicated file (in hard copy or electronic format, or both), and on CRM systems. The Firm will hold client-related personal data for seven years after the client relationship has ended.

The Firm keeps a record of its processing activities in respect of client-related personal data in accordance with the requirements of GDPR.

a. **Client and Individual rights**

As data subjects, clients have a number of rights in relation to their personal data. They can require Fulcrum to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Firm's legitimate grounds for processing data (where the Firm relies on its legitimate interests as a reason for processing data);
- process a subject access request;
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Firm's legitimate grounds for processing data.

To ask the Firm to take any of these steps, the client and or individual should send the request to the Firm's Compliance Department at compliance@fulcrumasset.com.

3. Impact assessments

Some of the processing that the Firm carries out may result in risks to privacy. Where processing would result in a high risk to client's rights and freedoms, the Firm will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

4. Data breaches

If Fulcrum discovers that there has been a breach of client-related personal data that poses a risk to the rights and freedoms of clients, it will report it to the Information Commissioner within 72 hours of discovery. The Firm will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of clients, it will tell affected clients that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

5. Disclosure of Non-Public Personal Information and international data transfers (SEC/CFTC requirement)

Fulcrum does not sell nor rent client information. Fulcrum does not disclose personal information about its investors to non-affiliated third parties or to affiliated entities, except as permitted by law. However, Fulcrum may share personal information in the following situations:

1. To service providers in connection with the administration and servicing of the client or a pooled investment vehicle whereby the client is an investor and Fulcrum is the investment adviser, which may include attorneys, accountants, auditors and other professionals.

2. To affiliated companies in order to provide the client with ongoing personal advice and assistance with respect to products and services purchased through Fulcrum and to introduce the clients to other products or services that may be of value to the client.

3. To respond to a subpoena or court order, judicial process or request from regulatory authorities;

4. To protect against fraud, unauthorised investments (such as money laundering), claims or other liabilities; and

5. Upon the consent of a client to release such information, including authorisation to disclose such information to persons acting in a fiduciary or representative capacity on behalf of the client.

Where the Firm engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical measures to ensure the security of data.

Client-related personal data may be transferred to countries outside the EEA. Any data transferred outside the EEA will be on the basis of declaration of adequacy of the jurisdiction or any other allowable data transfer strategies.

6. Disposal of Non-Public Personal Information (SEC/CFTC requirement)

It is essential that Fulcrum dispose of such client personal information in a secure fashion when it is no longer required for record keeping requirements. In general, Fulcrum will have methods to shred physical documents as well as the erasure and over-writing of electronic media.

7. Operating Procedures and Compliance Review (SEC/CFTC requirement)

It is Fulcrum's policy to require that all employees, financial professionals and companies that provide services on behalf of Fulcrum, keep client information confidential.

Fulcrum maintains safeguards to protect investor information from unauthorised access and use. These measures include computer safeguards and secured files and buildings.

Fulcrum restricts access to personal and account information of investors to those employees who need to know that information in the course of their job responsibilities. Fulcrum's employees/partners may work with, review, examine, inspect, have access to, or obtain personal information only for the purpose of fulfilling their responsibilities to the client or investor and should otherwise hold the information in strict confidence.

Fulcrum's Data Protection Privacy Policy applies to both current and former clients and it is provided to all new investors and managed account clients as well as existing clients and investors on at least an annual basis.