ALBEMARLE
ASSET MANAGEMENT

GDPR - POLICIES & PROCEDURES

1. SCOPE OF POLICY / REGISTRATION

1.1 This Policy relates to the collection and processing of Personal Data by Albemarle Asset Management Limited (the "Firm") in relation to its directors, employees, customers or potential customers, suppliers and any other category of person whose personal data is collected and processed by the Firm.

1.2 The Firm makes no distinction between the rights of Data Subjects who are directors, and those who are not. All are treated equally under this Policy.

1.3 The Policy applies equally to Personal Data held in manual and automated form.

1.4 To the extent that there are inconsistencies between this Policy and Relevant Legislation, then the Relevant Legislation shall prevail and this Policy shall be construed accordingly.

1.5 Under the Data Protection Act individuals and organisations that process personal information need to register with the Information Commissioner's Office (ICO), unless they are exempt. By going through the following questions you will be able to decide if you – as an individual or on behalf of your business or organisation – need to register with the ICO.

2. DEFINITIONS

2.1 For the avoidance of doubt, and for consistency in terminology, the following definitions will apply in this Policy.

Term	Definition
Controller	the organisation which determines the purposes and means of the processing of Personal Data.
Data	this includes both automated and manual data. Automated data means data held on computer or stored with the intention that it is processed on a computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
GDPR	General Data Protection Regulation ((EU) 2016/679).
Personal Data	any information relating to an individual who can be identified, directly or indirectly from such data. For example: name, residential address, email address and financial details. Descriptions of individuals with sufficient specificity will also be considered Personal Data.
Policy	this Data Protection Policy.
Processing	any use of Personal Data. For example: storage in databases, input onto systems and sharing with third parties.

Processor	the organisation(s) processing Personal Data on behalf of the Controller (for example, the Administrator).
Relevant Legislation	the Data Protection Act 1988, as modified by the Data Protection (Amendment) Act 2003 and the General Data Protection Regulation when it comes into force on 25 May 2018.
Special Categories of Personal Data	more sensitive Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data, data concerning health or data concerning an individual's sex life or sexual orientation.

3. IMPLEMENTATION AND ENFORCEMENT OF POLICY

3.1 The Firm will ensure that adequate steps are taken to maintain compliance with this Policy. This includes:

- designating Partner to act as a Data Privacy Manager (see section 4 below);
- conducting an annual review of the Policy to ensure that it provides an accurate description of the Firm's data protection framework;
- conducting an annual review on the data protection policies and procedures of key Processors to ensure compliance with service standards; and
- ensuring that the Board and all relevant staff receive data protection training and are informed of the Firm's responsibilities in respect of this Policy.

3.2 Where any material non-compliance with the Policy is identified, remediation measures will be implemented.

4. DATA PRIVACY MANAGER

4.1 The Firm has determined that it is not required to designate a data protection officer for the purposes of compliance with Article 37 of the GDPR on the basis that the Firm's core activities do not consist of:

- processing operations which require regular and systematic monitoring of data subjects on a large scale; or
- processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

4.2 However, in recognition of the key GDPR principle of "accountability", the Firm has appointed Matthew Wrigley to fulfil the role of Data Privacy Manager. The Data Privacy Manager is responsible for:

- co-operating, as necessary, with the Office of the Information Commissioner's Office ("ICO") in respect of the Firm's compliance with the Relevant Legislation;

- with the assistance of the Firm's legal advisers and / or consultants (where relevant), conducting an annual review of the Policy to ensure that it is line with Relevant Legislation and provides an accurate

- description of the Firm's data protection framework;

- ensuring that key Processors provide an annual report to ensure compliance with service standards;

- monitoring compliance with Relevant Legislation;

- acting as a point of contact for individuals whose Personal Data is processed by the Firm (e.g. directors and investors);

- reporting directly to the Board on data protection related matters; and

- ensuring that the Firm maintains a record of all the Firm's Personal Data processing activities.

5. DATA PROTECTION STATEMENT

5.1 The Firm is committed to privacy and respecting the rights of those whose Personal Data we collect and use in accordance with applicable law.

5.2 Data Protection is about providing individuals with protection as to how information about them is used by organisations. This protection is enshrined in the Relevant Legislation.

5.3 To provide this protection, data protection law establishes good data handling and data management principles. It also grants specific rights to individuals regarding their Personal Data which is processed by the Firm. The Firm is committed to respecting and supporting the right to data protection, including the rights of individuals under applicable law to control the dissemination and use of the Personal Data that relates to them.

6. DATA PROCESSING BY THE FIRM

6.1 In the course of its daily organisational activities, the Firm acquires, processes and stores Personal Data in relation to:

- Clients and / or potential clients;

- Investors and / or potential investors to the Firm’s products;

- Business contacts;

- its directors and staff;

- third-party services providers;

- portfolio investments;

- Other

6.2 The categories of Personal Data that may be held can be summarised as follows:

- Personal Data: name, contact details, bank details, tax details, investment details, transaction details, identification and verification documents; criminal record checks, education and qualification details, negative screening list matches, prior employment details, professional body memberships,.

6.3 Personal Data is processed and transferred for the following core purposes:

- to facilitate the opening of client accounts;

- to update and maintain client records and fee calculation;

- to circulate periodic reports relating to the Firm or its products;

- to carry out anti-money laundering checks and related actions to meet any legal obligations imposed on the Firm relating to the prevention of fraud, money laundering, terrorist financing, bribery, corruption, tax evasion and to prevent the provision of financial and other services to persons who may be subject to economic or trade sanctions, on an on-going basis;

- to report tax related information to tax authorities in order to comply with a legal obligation;

- to carry out statistical analysis and market research;

- to record, maintain, store and use recordings of telephone calls and to monitor and record calls for quality, business analysis, training and related purposes in order to pursue the legitimate interests of the Firm to improve its service delivery;

- to disclose information to other third parties such as service providers of the Firm, auditors, regulatory authorities and technology providers;

- to retain AML and other records of clients to assist with the subsequent screening of them by the Administrator including;

- to send client, potential clients, investors and potential investors information about other products and services offered by the Firm and/or its delegates;

- maintenance of records relating to directors and staff.

7. DATA PROTECTION PRINCIPLES

7.1 The Data Protection Principles stipulated below set out the main responsibilities which apply to the Firm when processing Personal Data. Whenever the Firm processes Personal Data, it should comply with these Data Protection Principles.

7.2 Fairness/Transparency: the Firm should only use Personal Data in a fair, lawful and transparent manner:

- Personal Data should only be processed where an individual has been presented with access to a privacy notice;
- the privacy notice should set out clearly and in plain language the categories of Personal Data being collected and the way in which the Firm will process this Data. The contents of privacy notices must meet the requirements of Relevant Legislation; and
- any new data processing initiatives which are likely to result in a high risk to individuals' interests must be subject to a privacy impact assessment and new approved initiatives may require the adoption of a new privacy notice which outlines the way in which the Firm will process Personal Data (if current privacy notices are not adequate).

7.3 Purpose Limitation: the Firm should only process Personal Data for specific stated purposes:

- Personal Data should only be processed in line with the purposes set out in the privacy notice;
- if sharing Personal Data, the Firm should ensure it is only shared with those who require access to achieve the stated purposes;
- processing Personal Data for purposes other than those set out in the relevant privacy notice is subject to approval and sign-off from the Board.

7.4 Data Minimisation: the Firm should only collect and process necessary Personal Data:

- The Firm should only collect Personal Data which is necessary for achieving the purposes set out in the privacy notice. If a specific category of Personal Data does not serve a purpose, it should not be collected.

7.5 Accuracy: the Firm should ensure Personal Data is accurate and up-to-date:

- it is essential that the Personal Data the Firm holds remains up-to-date and accurate;
- when Personal Data is inaccurate, it should be corrected (particularly if an individual makes a request to correct their Personal Data); and
- Personal Data which is out of date should be updated or deleted.

7.6 Storage Limitation: the Firm should only retain Personal Data for as long as is necessary:

- Personal Data should be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data is collected and processed; and
-
  if there is value in retaining Personal Data in some form for prolonged periods of time, it should be considered whether it is possible to derive a benefit from the data without the Personal Data. If the Personal Data can be anonymised or pseudonymised, this should be done.

7.7 Integrity and Confidentiality: the Firm shall keep Personal Data secure:

- Personal Data must be stored and processed in a secure manner;
- in practice, Personal Data should not be shared with anyone who does not require access to the Personal Data;
- where possible and appropriate, Personal Data should be password protected and/or encrypted before sharing it with anyone (internally or externally), particularly if the sharing is via email. Good security practices should be adopted, such as using robust passwords and encrypting hardware; and
- if it is possible, Personal Data should be stored in a pseudonymised / de-identified form.

7.8 Data Transfers: International transfers of Personal Data:

- all transfers of personal data outside of the EEA shall only be permitted where they are in accordance with the privacy notice or are otherwise permitted by Relevant Legislation; and
- the Firm will ensure that a suitable transfer solution is in place to safeguard the Personal Data being transferred (for example, by using model contract clauses).

7.9 Vendor Control: Engaging with third parties:

- Third parties involved in the processing of Personal Data on behalf of the Firm must be subject to a contract which contains the required Personal Data protection terms; and
- all agreements with third parties processing Personal Data on behalf of the Firm shall be subject to the approval of the Board.

8. LEGAL BASIS FOR PROCESSING

8.1 When the Firm processes Personal Data, it shall do so on the basis of one of the lawful grounds set out in the GDPR. The legal basis for each Personal Data processing activity carried out by the Firm must be detailed in privacy notices. Legal bases include: consent, performance of a contract, compliance with legal obligations and legitimate interests.

8.2 Whenever the Firm processes Personal Data it shall be clear which legal basis is being relied on. The Firm's current practices have been assessed and the relevant legal bases are set out in the privacy notices.

8.3 In practice, for all new material Personal Data processing activities, the Firm should take the following steps:

- identify the categories of Personal Data to be collected;
- identify the purposes of processing this Personal Data;
- assess whether the current privacy notices are adequate;
- if the current privacy notices are not adequate, new / updated privacy notices shall be prepared prior to collection of the Personal Data; and
- where necessary, implement new technical solutions. For example, if relying on consent, implementing a consent mechanism.

9. INDIVIDUAL RIGHTS

9.1 Relevant Legislation provides a number of rights for individuals regarding their Personal Data which is being processed by data controllers such as the Firm. The Firm shall respond to requests as soon as possible and subject to the deadlines set out under the Relevant Legislation.

9.2 Individuals have the right to make the following types of request regarding the Personal Data the Firm holds about them:

- **Right of access (subject access requests)** – the right to request a copy of the Personal Data the Firm holds concerning an individual and supporting information explaining how the Personal Data is used.
- **Right of rectification** – the right to request the Firm to rectify inaccurate Personal Data concerning an individual.
- **Right of erasure (right to be forgotten)** – the right to request the Firm erase all Personal Data concerning an individual.
- **Right to restrict processing** – the right to, in some situations, request the Firm not to use an individual's Personal Data they have provided (e.g. if they believe it to be inaccurate).
- **Right to object** – the right to object to certain processing of his/her Personal Data (unless the Firm has an overriding compelling legitimate grounds to continue processing) and the right to object to direct marketing.
- **Rights relating to automated decision making** – the right to object/opt-out of automated decision making that significantly affects an individual.
- **Right to data portability** – the right to, in some situations, request the Firm to port an individual's Personal Data to the individual or a new provider in machine readable format.

9.3 In certain circumstances, the Firm will be exempted from responding to certain requests. The Firm may use these exemptions to the extent appropriate.

9.4 A request which does, or which may, concern Personal Data, should be notified to the Data Privacy Manager.

10. SECURITY

10.1 Relevant Legislation requires that the Firm implements appropriate technical and organisational measures to ensure Personal Data is subject to a level of security appropriate to the risk associated with the processing. The Firm shall ensure that its delegates and service providers take appropriate technical and organisational measures with a view to protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing (including taking reasonable steps to ensure the reliability of employees who have access to the Personal Data).

11. INCIDENT RESPONSE

11.1 The response to any breach of Personal Data can have a serious impact on the Firm's reputation and the extent to which the public perceives the Firm as trustworthy. The consequential impact can be immeasurable.

11.2 Not all Personal Data protection incidents result in data breaches, and not all data breaches require notification. Therefore, exceptional care must be taken when responding to data breach incidents.

11.3 A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to Personal Data in usable form, whether manual or automated. This could mean:

- loss of a laptop, memory stick or mobile device that contains Personal Data;
- lack of a secure password on computers and applications;
- emailing Personal Data to someone in error;
- giving a system login to an unauthorised person; or
- failure of a door lock or some other weakness in physical security which compromises Personal Data.

11.4 Actual, suspected, or potential breaches should be reported immediately to the Data Privacy Manager.

11.5 All data breaches will be recorded by the Data Privacy Manager in an incident log. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of Personal Data. The record will include a brief description of the nature of the incident and (if applicable) an explanation of why the relevant regulatory authority was not informed.

11.6 Requirement to Notify

- Relevant Legislation imposes strict requirements to notify the ICO in the event of a data breach.

- If a notifiable data breach occurs, the Firm shall notify:
  - the ICO without delay and not later than within 72 hours of becoming aware of the data breach; and
  - affected individuals, unless any of the following applies:

- the Firm has implemented security measures to ensure the Personal Data is unintelligible to anyone not authorised to access it (e.g. the Personal Data is encrypted);

11.7 Incident Response Objectives

- In the event of a data / cyber breach incident the Firm's primary objectives are to:
  - stop the incident and limit the damage caused;
  - prevent the spread/loss of data;
  - recover data and/or systems that have been lost/stolen/damaged or otherwise compromised;
  - minimise the impact of the incident on our business and get 'up and running' again as soon as possible;
  - identify risks arising from the incident;
  - notify appropriate parties or authorities of the incident;
  - learn from the incident; and
  - take steps to prevent future incidents.

12. DATA RETENTION

12.1 The Firm should only retain Personal Data for so long as is necessary in connection with the purposes for which it was collected.

13. DATA SHARING

13.1 The Firm may share Personal Data with third parties. These third parties can be categorised broadly as follows:

- Service providers: Administrator, Depositary, Auditors, Legal Advisors, Secretary, Investment Advisers, Investment Manager, Consultants and Distributor;

- Non-contractual parties: Revenue Commissioners, Government agencies and law enforcement agencies; and

- Other third parties as authorised by the individual

13.2 Certain Service Providers will act as Controllers in respect of Personal Data shared by the Firm whereas other Service Providers will act as Processors. The Firm will ensure that a formal written contract is in place with each Processor containing all of the mandatory contractual requirements under the Relevant Legislation.

14. PRIVACY NOTICES AND CONSENT

14.1 Whenever the Firm collects Personal Data from individuals we shall provide information regarding the following as part of a privacy notice:

14.2

- what Personal Data is being collected;
- why it is being collected;
- how it will be used;
- who will have access to it; and
- the rights individuals have in relation to their Personal Data.

14.3 If the DPA considers it necessary to obtain the consent of individuals to collect and process their Personal Data, a consent mechanism must be implemented.

15. DATA PROTECTION BY DESIGN AND BY DEFAULT

15.1 Relevant Legislation requires the Firm to conduct a privacy impact assessment before carrying out processing of Personal Data in particular circumstances. A privacy impact assessment is an assessment of the risks and mitigations involved in processing Personal Data.

15.2 Relevant Legislation also requires the Firm to have in place measures and processes which demonstrate that privacy has been factored into all new business processes, vendors, projects, products or services where relevant. This is known as "privacy by design" and "privacy by default".

15.3 In practice this means the Firm shall conduct a privacy impact assessment in circumstances where any new data processing initiatives are likely to result in a high risk to individuals' interests. This may include the collection of Personal Data through a new channel or the sharing of Personal Data with a new third party.

16. MARKETING

16.1 The Firm shall not use Personal Data to send marketing information to any individual unless the individual has given consent to receive such marketing information or unless the marketing is otherwise permitted under Relevant Legislation i.e. based on the legitimate interests of the Firm to conduct marketing.

16.2 If an individual requests the Firm to stop processing their Personal Data for direct marketing purposes, the Firm shall stop processing the Personal Data for those purposes in accordance with the deadlines specified by Relevant Legislation.

17. DATA PROTECTION TRAINING

17.1 Data protection training will be made available for the Board and or members of staff as relevant. The Firm maintains a record of the data protection training which has been delivered and who has received this.

18. CHANGES TO THIS POLICY

18.1 The Firm reserves the right to change this Policy at any time. Material changes will be notified to affected parties as appropriate.