COLUMNA CAPITAL

Data Protection Policy

INTRODUCTION

This data protection policy is for each of the investment funds and investment vehicles (and, where such fund is a limited partnership, its general partner) managed or advised by Columna Capital LLP (**"Columna"**) or any of its affiliates as may decide to adopt this policy from time to time (each, a **"Fund" and one or more together "Funds"**). This policy sets out the Funds' compliance with the European Union's General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**).

Scope

The GDPR applies to the collection, Processing and storage of Personal Data undertaken by organisations within the European Economic Area ("**EEA**") as well as to organisations outside the EEA that handle Personal Data relating to the offering of goods or services to individuals in the EEA. This policy applies to the Funds' Processing of Personal Data and all such Personal Data processed on behalf of the Funds by any service provider.

Responsibility

The board of directors of each Fund (each, a "**Board**") are responsible for this policy and can be contacted in relation to this policy at GDPR@columnacapital.com.

Reliance on service providers

Where a Fund does not have any employees or its own IT infrastructure, or where otherwise deemed necessary, that Fund has engaged various service providers to perform certain services on its behalf. As such, each Fund has delegated many of its compliance obligations under the GDPR to one or more service providers. Due diligence is performed on those service providers and reasonable steps taken to ensure their ability to comply with the relevant GDPR and other regulatory and/or legal obligations. Each Fund requires such service providers, by contract, to meet such obligations.

Technical terms

A number of terms applied in this policy are defined in the applicable legislation and their definitions are set out at the end of the policy.

Obligations as a Controller

As a data Controller under GDPR, each Fund must:

(a) be able to demonstrate compliance with the six principles relating to Processing of Personal Data set out in the GDPR (the **Data Protection Principles**) (see further below);
(b) implement appropriate technical and organisational measures to ensure and to demonstrate that its Processing activities are compliant with the GDPR;
(c) ensure that the data protection principles and appropriate safeguards are addressed and implemented in the planning phase of Processing activities and in the implementation phase of any new product or service (**Privacy by Design**);

(d) appoint a representative in one of the Member States in which the Controller offers goods or services to or monitors EU data subjects and does not process data in a way that is occasional and small scale;
(e) only appoint a Processor that will comply with GDPR and that will enter into an agreement in writing to that effect;
(f) keep records of its Processing activities;
(g) cooperate, on request, with the relevant data protection supervisory authorities ("**DPAs"**);
(h) implement appropriate technical and organisational securities measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access; and
(i) notify Personal Data breaches to the relevant DPA within the requisite timeframe and to data subjects when required.

Responsibility for Data Protection

The relevant Board should be contacted in relation to any data protection issues and will also consider such issues periodically. In particular, the relevant Board should be contacted immediately if:

- a Fund is not complying or may not be complying with any part of this policy;
- a Fund is engaging in a new Processing activity or there has been a change to existing Processing activities;
- there is an actual or suspected Personal Data Breach (in which case see the section on Data Breach Notification below); or
- a subject access request or other request to enforce rights available to data subjects under data protection legislation is received by a Fund.

Accountability

Each Fund is responsible for ensuring compliance with the data protection principles (which are set out below) and must also be able to demonstrate that they are compliant. It aims to do so by:

- drafting, maintaining and implementing various policies and procedures relating to Personal Data Processing;
- ensuring due diligence and periodic reviews are conducted on service providers who process Personal Data on the Funds' behalf, taking reasonable steps to ensure those providers are capable of complying with the data protection principles, any data subject requests that the Funds may receive and any GDPR compliance obligations that the Funds may delegate to such service providers;
- maintaining records of its Processing activities; and
- implementing measures, or taking reasonable steps to ensure that its service providers take measures that meet the principles of data protection by design and default.

The Data Protection Principles

The Data Protection Principles underpin the lawful Processing of Personal Data, and each Fund is required to comply with these principles. The six principles are as follows. Personal Data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness and transparency**);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**);

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);
4. accurate and, where necessary, kept up to date (**accuracy**);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data is processed (**storage limitation**);
6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage using appropriate technical or organisational measures (**integrity and confidentiality**).

The steps adopted by each Fund that are designed to achieve compliance with each of the data protection principles are set out below.

Lawfulness, fairness and transparency Processing

For Personal Data to be processed lawfully, there must be a lawful basis for Processing it. Each Fund processes Personal Data because it is necessary:

- for the performance of a contract with the data subject; or
- for compliance with EU legal obligations to which it is subject; or
- for the purposes of the legitimate interests pursued by the Fund, or any Third Party, including but not limited to any service provider or other Processor except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of the data subject.

The Funds do not rely on consent to process any Personal Data.

Purpose limitation

Each Fund aims to only process Personal Data for the legitimate purposes for which such data was collected, such purposes being specified in the Funds' privacy notice. Should it no longer be necessary for a Fund to process Personal Data for the purpose (or purposes) for which it was originally collected, it may be necessary to delete it in accordance with the section of this policy entitled **Records Retention**. Alternatively, if the purpose for which the Personal Data is being processed has changed but Processing is still legitimate, data subjects must be informed as soon as possible via an updated privacy notice.

Data minimisation

Each Fund aims to limit its Processing of Personal Data to circumstances where such Processing is adequate, relevant and necessary for the purposes for which such data is being processed. This includes avoiding Processing or disseminating Personal Data unnecessarily.

Accuracy

Each Fund takes steps designed to ensure that the Personal Data which it processes is kept accurate and up-to-date. Investors are told in the Funds' privacy notice to advise the relevant Fund if their Personal Data changes during their relationship with the Fund. Each Fund aims to ensure that such Personal Data is accurate at the point of collection, and that it is reviewed on a regular and systematic basis to ensure that it remains up-to-date.

If a Fund becomes aware that Personal Data is inaccurate, the Board should be informed and take reasonable steps to ensure that it is corrected or erased.

Storage limitation

Each Funds' policy on data retention is set out below in the section of this policy entitled **Records Retention**. After the relevant retention period has expired, Personal Data should be permanently deleted in accordance with this policy.

Integrity and confidentiality

Each Fund has put in place contractual obligations on its service providers to have in place appropriate security to protect against data breaches.

Transfers of Personal Data outside the EEA

There are restrictions on a Funds ability to transfer Personal Data outside the EEA to ensure that the level of protection afforded by EU data protection legislation is not undermined.

As each Fund is domiciled in an EU member state, Personal Data that a Fund collects may be processed outside of the EEA. Each Fund may also transfer Personal Data outside the EEA through its service providers based, or with affiliates based, outside of the EEA. Where this is the case, a Fund will, or will ensure that its service providers, put in place appropriate safeguards such as the EU Commission approved standard contractual clauses.

Sharing Personal Data

A Fund is generally not permitted to share Personal Data with a Processor, service provider or any other Third Party unless certain safeguards and contractual arrangements are in place so that it can be satisfied that third parties are Processing Personal Data in compliance with data protection legislation. The ways in which a Fund shares Personal Data are set out in the Funds' privacy notice. The Funds have entered into data Processing agreements with third parties that process Personal Data on their behalf.

Data Subjects' Rights

Data Subjects have various rights under the applicable data protection legislation and these are set out in the Funds' Privacy Notice. Further information is available from the website of the relevant data protection authority.

Timing for response to data subject requests

A Fund, as Controller, must, within one month of receiving a request made by a data subject to exercise one of the rights referred to above, provide information on action taken in relation to a request to exercise any of the rights of data subjects. If it fails to meet this deadline, the data subject may complain to the relevant data protection authority and may seek a judicial remedy. Where a Fund receives a large number of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.

A Fund must not charge for the rights of access, rectification, erasure and the right to object, but may request a "reasonable fee" from a data subject where requests are manifestly unfounded or excessive.

Responsibility

Each Fund has processes in place to respond to data subject requests to the extent the Fund receives those requests directly. In addition, pursuant to the data Processing agreements a Fund has entered into with its service providers, a Fund relies upon those service providers to assist with responses to such data subject requests in a proper and timely manner.

DATA BREACH NOTIFICATION

A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by a Fund or by any Processor. Examples of a Personal Data Breach may include but are not limited to:

(a) Personal Data that is processed by a Fund being lost, or left in an insecure location e.g. on an unattended desk, or on public transport;
(b) unauthorised access to a service provider's systems which affects Personal Data processed by a Fund;
(c) a letter containing Personal Data processed by a Fund that is sent to the wrong address;
(d) an email containing Personal Data processed by a Fund sent to the wrong recipients, such as where an email is sent "cc all" to people who should not have been copied; and
(e) loss or theft of a mobile device or other ICT equipment containing Personal Data processed by a Fund.

Notification of a Personal Data Breach to the Board

If a service provider or a member of the Board is notified that there has been an actual or suspected Personal Data Breach, details of the breach must be recorded. The Board will document the breach, the facts relating to it, its effects and the remedial action taken.

All investigations, notifications, etc. would be conducted by the Board or on the Board's behalf by a service provider.

Notification of a Personal Data Breach to the relevant DPA

If the Board determines that a data breach is likely to result in a risk to the rights and freedoms of the data subject(s) affected by the data breach, the Fund is required to report the Personal Data Breach to the relevant DPA without undue delay, and where feasible, not later than 72 hours after becoming aware of the Personal Data Breach. The 72 hours will begin to run when the Fund has a reasonable degree of certainty that a Personal Data Breach has occurred (or where a Processor has notified the Fund of a potential breach). Where the notification to the DPA is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification to the DPA shall:

(a) describe the nature of the Personal Data Breach including where, possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
(b) communicate the name and contact details of the Board from whom more information can be obtained;
(c) describe the likely consequences of the Personal Data Breach;
(d) describe the measures taken or proposed to be taken by the Fund to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Communication of a Personal Data Breach to the data subject

If the Board determines that a Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Fund is required to report the Personal Data Breach to the affected data subject(s) without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the Personal Data Breach and contain at least the information and measures referred to in points (b), (c) and (d) above.

A communication to the data subject will not be required if:

(a) the Fund has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;
(b) each Fund has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject(s) affected is no longer likely to materialise; or
(c) it would involve disproportionate effort. In such a case, the Fund would be required to make a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

RECORDS RETENTION

This section of the policy sets out the Funds' guidelines and procedures for the storage, archiving, retention and destruction of records. Having a retention policy is important because:-

- data protection legislation requires that Personal Data which is processed by the Funds' should be retained for no longer than is required for the purpose for which it is processed;
- the Fund has legal and regulatory obligations to retain certain documents for prescribed periods; and
- it seeks to ensure that confidential information and Personal Data is stored and destroyed securely.

In this policy the term **"records"** includes but is not limited to: paper documents, paper files, Word, PowerPoint, Excel and PDF documents, emails, text messages, instant messages, CCTV footage, recordings of telephone conversations. Records may be stored using the following media: paper files, hard drives, computer disks; memory sticks; web-based storage (e.g. cloud storage); backup tapes; mobile phone and blackberry SIMs but this is not an exhaustive list.

Responsibility

Each Fund does not itself maintain any records (except insofar as the relevant Board processes any records in performing its role as the board of directors), so contractually obliges its service providers to return or destroy Personal Data on termination of their provision of services to the Fund except to the extent that European Union or Member State law requires otherwise.

Storage

Each Funds' records must be stored securely to avoid potential misuse, inappropriate access or loss. This is particularly important for documents which contain Personal Data or confidential information.

Retention

Records should only be kept for as long as necessary. This is particularly important for any records which contain Personal Data which must be retained for no longer than is necessary for the purpose(s) for which the data was being processed. Nevertheless, data protection legislation does not override any statutory requirement to keep records for a certain period (for example certain tax or other regulatory records).

Records relevant to disputes/investigations

If a Fund is advised by external counsel that any Fund records are relevant to litigation, contemplated litigation (i.e. a dispute that could result in litigation), arbitration or, any government or regulatory investigation, any such records must be preserved and not deleted, destroyed, or modified in any way, until external counsel advises otherwise. This is referred to as a litigation hold or legal hold and will override any retention schedule for all relevant records.

RECORDS OF PROCESSING ACTIVITIES

Each Fund shall (or shall delegate responsibility to its service providers as appropriate to) keep records of its Processing activities, including:

- contact details of the Controller and Data Protection Officer equivalent where appointed;
- the purposes for which it processes Personal Data;
- the categories of data subjects and Personal Data it processes;
- the categories of recipients with whom the data may be shared;
- information regarding Cross-Border Data Transfers;
- the applicable data retention periods; and
- a description of the security measures implemented in respect of the processed data.

Upon request, these records must be disclosed to the DPAs.

DEFINED TERMS

Controller: the entity which alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this policy, the Controller is a Fund.

Personal Data: any information relating to an identified or identifiable natural person ("**Data Subject"**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Processing: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. A service provider is a Processor.

Special Category Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third Party: a natural or legal person, public authority, agency or body other than the data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.