- SCIENS GROUP RISK SERVICES LIMITED AND AFFILIATED GROUP COMPANIES BASED IN THE EU/GUERNSEY

DATA PROTECTION AND CONFIDENTIAL INFORMATION POLICY

Introduction

This Policy relates to Sciens Group Risk Services Limited and all affiliated group companies based in the EU and Guernsey (**"SGRS AND AFFILIATED COMPANIES"**) or **("SGRS")**

SGRS AND AFFILIATED COMPANIES is incorporated in England and has a passport under the Alternative Investment Fund Managers Directive to operate in Ireland. There may be shareholders or prospective investors in the funds that it manages and/or Service Providers in countries in the European Union. SGRS AND AFFILIATED COMPANIES where applicable are therefore obliged to adhere to:

- Data protection laws having effect in the Republic of Ireland
- Data protection laws having effect in the United Kingdom (as a whole) and/or England & Wales
- Equivalent Data protection laws in Guernsey (Channel Islands)
- The European Union's General Data Protection Regulation (both in respect of its general application in the United Kingdom (prior to leaving the European Union), the Republic of Ireland and (following the United Kingdom leaving the European Union) the extra-territorial application relating to third country firms holding personal data on citizens of the European Union. In addition to any equivalent data protection laws in Guernsey.

Additionally, SGRS AND AFFILIATED COMPANIES have contractual confidentiality obligations which are owed to investors, prospective investors, Service Providers and potentially others.

In the ordinary course of its business, SGRS AND AFFILIATED COMPANIES come into possession of personal and / or confidential information ("**Data**") in respect of individuals ("**Individuals**"), such as:

- Prospective investors of the funds that it manages and their directors, officers, employees, agents, representatives and personnel
- Shareholders in the funds that it manages and their directors, officers, employees, agents, representatives and personnel
- Service providers to SGRS AND AFFILIATED COMPANIES and where applicable, the funds that are managed and their directors, officers, employees, agents, representatives and personnel
- Directors, officers, employees, agents, representatives and personnel of SGRS AND AFFILIATED COMPANIES

For the purposes of this policy, Data may include personal information, contracts and related documents between SGRS AND AFFILIATED COMPANIES and other parties (whether or not Individuals) including the service providers to SGRS AND AFFILIATED COMPANIES and where applicable the funds that are managed ("**Service Providers**"), and includes any information that relates to an identified or identifiable living Individual from which that Individual can be identified (whether from that information alone, or in

conjunction with other information which SGRS AND AFFILIATED COMPANIES has or is likely to obtain) ("**Personal Data**").

Personal data is defined in the relevant legislation, including without limitation: name, address, email address, date of birth, identification documents, anti-money laundering related information, account numbers, bank account details, tax and other public or social security identifiers, and residency information, and online identifiers.

In obtaining and using Personal Data in connection with shareholders or prospective investors in the funds that it manages, Service Providers and others as may be applicable, SGRS AND AFFILIATED COMPANIES may act as a data controller.

The Data may be held electronically, processed via automated processes, or held in general files, and where processed on SGRS AND AFFILIATED COMPANIES's behalf by Service Providers, will be subject to written contracts governing that processing and setting out the security and confidentiality measures which the Service Providers have committed to implement.

This document sets out SGRS AND AFFILIATED COMPANIES's policies and guidelines with regard to the obtaining, storing, processing, use, disclosure, transfer and safeguarding of Data as data controller.

For the avoidance of doubt and notwithstanding anything to the contrary in this policy, nothing in this policy shall prevent SGRS AND AFFILIATED COMPANIES from complying with any legal or regulatory obligation to disclose Data in accordance with applicable law. Particularly, this includes (but is not limited to) the obligations of SGRS AND AFFILIATED COMPANIES and its Service Providers to report under both the Foreign Account Tax Compliance Act and the Common Reporting Standard.

Obtaining and Using Personal and Confidential Data

Personal Data may only be processed if the data subject has given his / her consent, or if the processing is necessary for the performance of a contract to which the data subject is party, for the taking of other pre-contractual measures at his / her request, where processing is otherwise necessary for compliance with legal obligations, to protect the vital interests of the data subject; or is otherwise necessary for legitimate interests or on public interest grounds.

As a Data Controller, SGRS AND AFFILIATED COMPANIES are responsible for, and must be able to demonstrate, compliance with the Data Protection Principles:

- Personal Data must be processed fairly, lawfully and in a transparent manner
- Personal Data must be collected for specified, explicit and legitimate purposes, and not further processed in a manner which is incompatible with those purposes
- Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected
- Personal Data must be accurate and, where necessary, kept up to date, and reasonable steps must be taken to ensure that Personal Data that is inaccurate is erased or corrected without delay
- Personal Data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which it is processed

- Personal Data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures

In addition, SGRS AND AFFILIATED COMPANIES imposes confidentiality obligations on its Service Providers, and is subject to confidentiality obligations with regard to shareholders (and prospective investors) in the funds that it manages and Service Providers.

Accordingly:

- Only Data, which is strictly necessary for the purpose of a subscription into the funds managed by SGRS AND AFFILIATED COMPANIES and / or the contract between SGRS AND AFFILIATED COMPANIES and a shareholder or prospective investor in the funds that it manages or a Service Provider, should be requested or obtained from the relevant party

- Through the application forms of the funds, privacy statement(s) and prospectus of the funds managed by SGRS AND AFFILIATED COMPANIES makes shareholders and prospective investors of the funds, Service Providers and relevant Individuals aware of;

    - the identity of SGRS AND AFFILIATED COMPANIES;

    - the purposes for which the Data relating to that relevant Individual will be stored and used;

    - the legal basis for that processing and

        - where that legal basis is a legitimate interest of SGRS AND AFFILIATED COMPANIES or a third party, a description of those legitimate interests and the right to object to the processing; and

        - where the legal basis is consent, the right to withdraw consent;

    - the recipients or categories of recipients (if any) of the Data;

    - where applicable, details of international data transfers;

    - details of storage and retention periods;

    - details of any automated decision-making, including any profiling;

    - the right of Individuals to get access to their Personal Data, to rectify any such Personal Data, and their other rights applicable to data protection laws;

    - the right to lodge a complaint with the Information Commissioner (in the United Kingdom) by telephone on 0303 123 113 and/or the Data Protection Commissioner (the "**DPC**") (in the Republic of Ireland) by telephone on 00353 57 8684800 or by email on info@dataprotection.ie. For individuals living or working in Guernsey, or where the alleged infringement has occurred in Guernsey, the relevant supervisory authority will be the Office of the Data Protection Commissioner. Their contact telephone number is 01481 742074 and they can also be contacted by email on enquiries@dataci.org

- SGRS AND AFFILIATED COMPANIES will not use Data other than for the purposes which have been brought to the attention of the relevant Individual and, if consent is required, to which the relevant Individual has consented.

- Where Service Providers process Data for SGRS AND AFFILIATED COMPANIES pursuant to contracts between SGRS AND AFFILIATED COMPANIES and the Service Providers, the Service Providers act as data processors of SGRS AND AFFILIATED COMPANIES. SGRS AND AFFILIATED COMPANIES will therefore ensure that:

    - appropriate due diligence is undertaken on such Service Providers to confirm that the Service Providers provide sufficient guarantees to implement appropriate technical and organisational security measures so as to meet the requirements of applicable law and to ensure the protection of the rights of the Individuals with regard to their Personal Data; and

    - any contracts with such Service Providers impose obligations on the Service Providers which are required under applicable law and which assist SGRS AND AFFILIATED COMPANIES in complying with its own obligations under applicable law.

- Where Service Providers are dealing with existing shareholders, the Service Providers have confirmed that they have procedures in place to verify on behalf of SGRS AND AFFILIATED COMPANIES that all existing Data held relating to those existing shareholders is accurate and up to date.

Storage and Security of Data

Each of SGRS AND AFFILIATED COMPANIES and the Service Providers is obliged to implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access. This applies particularly where such Personal Data will be transmitted over a network. Similar security measures should also apply to the other Data.

Generally, SGRS AND AFFILIATED COMPANIES shall, and where it appoints the Service Providers, shall ensure that the Service Providers shall:

- taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, which shall include, as appropriate:

    - psuedonymisation and encryption;

    - the ability to ensure ongoing confidentiality, integrity, availability and resilience;

    - the ability to restore availability and access in a timely manner in the event of a technical incident;

    - a process for regular testing, assessing and evaluating the effectiveness of those measures;

- take all reasonable steps to ensure that employees and other agents are aware of and comply with the security measures which have been implemented, including training of their respective relevant employees and agents;

- ensure that technical security controls are implemented to limit access to the Data on a "need to know" basis;

- ensure that all hard copies of Data are securely stored and are only accessed on a "need to know" basis.

Retention Periods

SGRS AND AFFILIATED COMPANIES is obliged to retain certain information to ensure accuracy, to help maintain quality of service and for legal, regulatory, fraud prevention and legitimate business purposes.

It is obliged by law to retain AML related identification and transaction records for six years from the end of the relevant investor relationship or the date of the transaction respectively. Other information, including personal data of the directors and business contact information, will be retained for no longer than is necessary for the purpose for which it was obtained by SGRS AND AFFILIATED COMPANIES or as required or permitted for legal, regulatory, fraud prevention and legitimate business purposes. In general, SGRS AND AFFILIATED COMPANIES (or its service providers on its behalf) will hold this information for a period of seven years from the termination of the relevant business relationship, unless it is obliged to hold it for a longer period under law or applicable regulations. Certain director information may be held indefinitely where it forms part of the statutory books and records of SGRS AND AFFILIATED COMPANIES.

[SGRS AND AFFILIATED COMPANIES (or its service providers on its behalf) will also retain records of telephone calls and any electronic communications for a period of five years and, where requested by the Central Bank, for a period of up to seven years from the date of such call or communication.]

Breach Notifications

In accordance with applicable data protection laws, SGRS AND AFFILIATED COMPANIES will be obliged to notify the DPC of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data (each a "**personal data breach**") within 72 hours of becoming aware of same, unless the personal data breach is unlikely to result in risks to Individuals. Furthermore, SGRS AND AFFILIATED COMPANIES will need to notify any impacted Individuals without undue delay where a personal data breach is likely to result in a high risk to those Individuals.

In the event of a personal data breach:

- SGRS AND AFFILIATED COMPANIES shall give immediate consideration to the likely risks arising from the Personal Data breach, taking into account the nature and scope of the personal data in question, the extent of the breach, the period of the breach, and any security measures which may militate against risk, such as encryption. In doing so, the potential consequences for the affected Individuals will be considered;

- any incident in which Personal Data has been put at risk will be reported to the DPC within 72 hours of SGRS AND AFFILIATED COMPANIES becoming aware of the incident. Where a report is made to the DPC, SGRS AND AFFILIATED COMPANIES will provide such information and

detail as is required under applicable data protection laws and / or as the DPC may request, which shall include:

- a description of the nature of the personal data breach, including where possible, the categories and approximate numbers of impacted Individuals, and the categories and approximate number of personal data records concerned;
- a description of the likely impact of the personal data breach;
- a description of measures to mitigate possible adverse effects;

- reporting to the DPC may be conducted in phases where the full extent of the personal data breach is not known within 72 hours of SGRS AND AFFILIATED COMPANIES becoming aware of same. Any such phased reporting will be conducted in consultation with the DPC;
- any incidents which are likely to result in high risk to Individuals will be notified to the impacted Individuals without undue delay unless this would involve disproportionate effort. In this latter case, a public communication or similar equally effective notification measure shall be implemented by SGRS AND AFFILIATED COMPANIES;
- Where, having considered the matter, SGRS AND AFFILIATED COMPANIES comes to a determination that no notification need or will be made to the DPC and / or the affected data subjects, SGRS AND AFFILIATED COMPANIES shall in any event keep a summary record of each incident which has given rise to the risk of unauthorised disclosure, loss or alteration of personal data, which will include an explanation as to why SGRS AND AFFILIATED COMPANIES did not consider it necessary to inform the DPC.
- Records of security incidents will be made available to the DPC on request.

SGRS AND AFFILIATED COMPANIES shall ensure that the Service Providers notify SGRS AND AFFILIATED COMPANIES without delay of any security incident and provide all reasonable assistance to SGRS AND AFFILIATED COMPANIES to enable it to comply with its obligations under applicable data protection laws with regard to notification of personal data breaches.

Privacy Impact Assessments

SGRS AND AFFILIATED COMPANIES may be required to undertake privacy impact assessments in relation to the processing of Personal Data in certain circumstances and will undertake an impact assessment where the processing in question, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to Individuals.

Without limitation, the following may be indicative of high risk processing:

- a significant change to the processing operations relating to the Personal Data, including where implemented by one of the Service Providers;
- processing involving evaluation, scoring, monitoring or profiling of Individuals;
- Combining of two or more data sets arising from separate processing operations conducted for different purposes;

- Innovative use of technologies or of organisational measures to protect Personal Data;
- Data transfers across borders outside the European Economic Area (the "**EEA**").

Any privacy impact assessment shall include:

- a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate purposes pursued by SGRS AND AFFILIATED COMPANIES;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to Individuals; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure protection of personal data and to demonstrate compliance with applicable data protection laws taking into account the rights and legitimate interests of Individuals.

SGRS AND AFFILIATED COMPANIES shall consult with the DPC where necessary in accordance with applicable data protection laws, and where appropriate shall seek the views of Individuals or their representatives.

SGRS AND AFFILIATED COMPANIES shall ensure that the Service Providers notify SGRS AND AFFILIATED COMPANIES without delay of any new processing or change in processing arrangements (including implementation of any new technology) to facilitate SGRS AND AFFILIATED COMPANIES in determining whether the processing is likely to result in high risk to Individuals and shall provide all reasonable assistance to SGRS AND AFFILIATED COMPANIES to enable it to comply with its obligations under applicable data protection laws with regard to undertaking a privacy impact assessment.

Transfers of Data

The transfer and distribution of Personal Data, whether to an entity related to SGRS AND AFFILIATED COMPANIES or any of the Service Providers, or to a third party, is restricted, and is only permitted in limited circumstances. Particular restrictions and limitations apply to the transfer of Personal Data to countries outside of the EEA, where such countries do not have equivalent levels of data protection to that afforded to Personal Data under Irish law.

In the event that SGRS AND AFFILIATED COMPANIES or a Service Provider wishes to transfer Personal Data to a country outside the EEA, it will in general be necessary for SGRS AND AFFILIATED COMPANIES (as data controller) to have in place a written agreement with the third party to whom the Personal Data is transferred (the "**Importer**") which will:

- limit the scope of use of that Personal Data to specified and permitted purposes,
- prohibit further distribution without the express consent of SGRS AND AFFILIATED COMPANIES and / or the relevant Individual or entity to whom the Data relates,
- contain an undertaking from the Importer to comply with policies and guidelines similar to those to which SGRS AND AFFILIATED COMPANIES is subject; and

- contain an undertaking from the Importer that it will impose adequate technical and organisational safeguards to protect the Personal Data.

It may be possible for SGRS AND AFFILIATED COMPANIES to transfer Personal Data outside the EEA where such transfer is necessary for the performance of a contract between SGRS AND AFFILIATED COMPANIES and an Individual, or where the Individual has explicitly consented to the transfer.

SGRS AND AFFILIATED COMPANIES may, as data controller, appoint a Service Provider as its agent for the purposes of executing the European Commissioner's approved model clauses. In no case will Data be transferred outside Ireland without SGRS AND AFFILIATED COMPANIES's consent except within the group of companies of which SGRS AND AFFILIATED COMPANIES is part. No transfer of data outside of the EU/EEA or recognised equivalent territories (including Guernsey) will be permitted unless the board of SGRS AND AFFILIATED COMPANIES has approved both the transfer itself and that appropriate measures have been implemented at the appropriate company.

Data Access Requests

Where an Individual makes a data subject access request in writing, there is an obligation on a data controller to provide certain information to the data subject.

Accordingly, on receipt of any data subject access request, SGRS AND AFFILIATED COMPANIES shall within 30 days:

- inform the Individual as to whether the data processed by or on behalf of SGRS AND AFFILIATED COMPANIES includes Personal Data relating to the Individual, and where it does, to provide a description of:
    - the categories of the Personal Data;
    - the Personal Data constituting the data;
    - the purposes for which they are being or are to be processed;
    - the recipients or categories of recipients to whom they are or may be disclosed;
    - information as to source, where not obtained directly from the Individual;
    - where possible, the envisaged storage period, or alternatively the criteria used to determine that period;
    - the right to lodge a complaint to the DPC;
    - details of any automated decision making or profiling;
    - the appropriate safeguards with regard to international data transfers.
- provide the Individual with a copy of the information Personal Data of the Individual;
- provide the relevant information to the Individual free of charge, in an easily visible, intelligible and clearly legible manner within one month of a proper request from the data subject, unless an exception applies under applicable data protection laws.

If SGRS AND AFFILIATED COMPANIES does not intend taking action at the request of the data subject, SGRS AND AFFILIATED COMPANIES shall inform the Individual without delay and the reasons for not taking action, as well as the right of the Individual to complain to the DPC.

SGRS AND AFFILIATED COMPANIES shall ensure that the Service Providers notify SGRS AND AFFILIATED COMPANIES without delay of any data subject access request and provide all reasonable assistance to SGRS AND AFFILIATED COMPANIES to enable it to comply with its obligations under applicable data protection laws in relation to any data subject access requests.

Other Data Subject Rights

Individuals have the following rights, in certain circumstances:

- the right to rectify Personal Data
- the right to restrict processing
- the right to object to processing
- the right to be forgotten
- the right to data portability.

SGRS AND AFFILIATED COMPANIES shall comply with applicable data protection laws in honouring Individual rights as set out above. However, if SGRS AND AFFILIATED COMPANIES does not intend taking action at the request of the data subject, SGRS AND AFFILIATED COMPANIES shall inform the Individual without delay and the reasons for not taking action, as well as the right of the Individual to complain to the DPC.

SGRS AND AFFILIATED COMPANIES shall ensure that the Service Providers notify SGRS AND AFFILIATED COMPANIES without delay of any data subject requests to enforce the above rights and provide all reasonable assistance to SGRS AND AFFILIATED COMPANIES to enable it to comply with its obligations under applicable data protection laws in relation to any such data subject requests.

Appointment of a Data Protection Officer ("DPO")

Melissa Bradford assumes the role of Data Protection Officer for the Sciens Group. In the event that you have any further questions or concerns about the processing of your personal data, please contact the DPO on the below details:

Melissa Bradford -Compliance Manager, Europe. Direct telephone number – (01481) 735519

Sigma Asset Management (Guernsey) Limited and

Sciens Group Fund Services Limited

a member of the Sciens Capital Management Group

Suite 5/6, Pollet House, Lower Pollet

St Peter Port, Guernsey, GY1 1WF

Updates to this Policy

Any changes we make to our Data protection and Privacy Policy in the future will be posted on our website, please check back frequently to see any updates or changes to our policy.