sciens

SCIENS GROUP DATA PROTECTION AND PRIVACY POLICY

Contents Page

Introduction

This Policy relates to the Sciens Group, its affiliated group companies (together, the "Sciens Group") and all funds managed by the Sciens Group (each, a "Fund", and together, the "Funds").

The Sciens Group and the Funds are incorporated across several jurisdictions, including the United States of America, the Cayman Islands, Guernsey and the European Union (the United Kingdom and Ireland). There may be shareholders or prospective investors in the Funds and/or service providers to the Sciens Group and the Funds in countries in the European Union.

Each entity within Sciens Group and the Funds will have to comply with applicable legislation in respect of data protection.

In the Cayman Islands:

- Data protection laws having effect in the Cayman Islands; and
- The European Union's General Data Protection Regulation ("GDPR") in respect of its extra territorial application relating to third country firms holding Personal Data (as defined below) on citizens of the European Union. The Cayman Islands is not recognised as an equivalent jurisdiction under GDPR and it is not intended that the data of EU citizens will be held by any Cayman Islands entity within the Sciens Group or by a Fund.

In the European Union (Ireland and the United Kingdom):

- 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; and
- The European Union's GDPR (both in respect of its general application in the United Kingdom (prior to leaving the European Union) and 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 (as defined below) relating to citizens of the European Union.

In Guernsey:

- Data protection laws having effect in the Bailiwick of Guernsey; and
- The European Union's GDPR in respect of its extra-territorial application relating to third country firms holding Personal Data. Guernsey is recognised as an equivalent jurisdiction under GDPR.

In the United States of America:

- Data protection laws having effect in the United States of America (federally) or any specific relevant State;

- The European Union's GDPR in respect of its extra-territorial application relating to third country firms holding Personal Data. The United States of America is not recognised as an equivalent jurisdiction under GDPR and it is not intended that the data of EU citizens will be held by any United States entity within the Sciens Group and the Funds; and

- No United States entity within the Sciens Group and the Funds are registered under Privacy Shield. The EU-US Privacy Shield frameworks were designed by the US Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring Personal Data from the EU to the US in support of transatlantic Commerce.

Additionally, the Sciens Group and the Funds have contractual confidentiality obligations which are owed to investors, prospective investors, trading advisors, fund administrators, custodians, depositaries, prime broker, banks and other service providers (together, "Service Providers") and potentially others.

In the ordinary course of their business, the Sciens Group and the Funds come into possession of Personal Data (defined below) in respect of natural persons **("Individuals"),** such as:

- Prospective investors in the Funds and their directors, officers, employees, agents, representatives and personnel;

- Shareholders in the Funds and their directors, officers, employees, agents, representatives and personnel;

- Service Providers to the Sciens Group and the Funds, and their directors, officers, employees, agents, representatives and personnel; and

- Directors, officers, employees, agents, representatives and personnel of the Sciens Group and the Funds.

For the purposes of this policy, "Personal Data" means personal information, contracts and related documents between the Sciens Group and the Funds and other parties (whether or not Individuals) including the 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 the Sciens Group and the Funds have or is likely to obtain).

"Personal Data" includes 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, Service Providers and others as may be applicable, the Sciens Group or a Fund may act as a data controller (a "Data Controller") under GDPR.

The Data may be held electronically, processed via automated processes, or held in general files, and where processed on behalf of a member of the Sciens Group or a Fund 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 the policies and guidelines of the Sciens Group and the Funds with regard to the obtaining, storing, processing, use, disclosure, transfer and safeguarding of Personal Data as a Data Controller.

For the avoidance of doubt and notwithstanding anything to the contrary in this policy, nothing in this policy shall prevent the Sciens Group and the Funds 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 the Sciens Group and the Funds and their Service Providers to report under both the Foreign Account Tax Compliance Act and the Common Reporting Standard.

Obtaining and Using Personal 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, a member of the Sciens Group or a Fund is 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; and
- 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, the Sciens Group and the Funds impose confidentiality obligations on their Service Providers and are subject to confidentiality obligations with regard to shareholders (and prospective investors) in the Funds, as well as to Service Providers.

Accordingly:

- Only Personal Data, which is strictly necessary for the purpose of a subscription into the Funds and / or a contract between Sciens Group or a Fund and a third party, should be requested or obtained from the relevant party;

- The application forms / subscription agreements of the Funds, privacy statement(s) and offering documents of the Fund make shareholders and prospective investors of the Funds, Service Providers and third-party individuals aware of;

  - the identity of the Sciens Group and the relevant Fund;

  - the purposes for which the Personal 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 the Sciens Group, a Fund 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 Personal Data;

  - where applicable, details of international Personal Data transfers;

  - details of storage and retention periods;

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

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

  - the right to lodge a complaint with the relevant data protection regulator:

Jurisdiction	**Regulator**	**Contact Details**
Cayman Islands	The Information Commissioner	+1 345 747 5402 info@infocomm.ky
Guernsey	Office of the Data Protection Commissioner	01481 742074 enquiries@dataci.org
Ireland	The Information Commissioner	+353 57 8684800 info@dataprotection.ie

United Kingdom	The Data Protection Commissioner	0303 123 113
United States of America	Federal Trade Commission	ftc.gov/complaint

- The Sciens Group and the Funds will not use Personal 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 a Service Provider processes Personal Data for the Sciens Group or a Fund to contracts between the Sciens Group or a Fund and such Service Provider, the Service Provider acts as a Data Processor for the Sciens Group or the Funds, the Sciens Group and the Funds will therefore ensure that:

- appropriate due diligence is undertaken on the Service Provider to confirm that the Service Provider provides sufficient guarantees to implement appropriate technical and organisational security measures to meet the requirements of applicable law and to ensure the protection of the rights of any individuals regarding their Personal Data; and

- any contracts with a Service Providers imposes obligations on the Service Provider which are required under applicable law and which assist Sciens Group and the Funds in complying with their 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 the Sciens Group and the Funds that all existing Personal Data held relating to those existing shareholders is accurate and up to date.

Storage and Security of Personal Data

Each of the Sciens Group, the Funds 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.

Generally, the Sciens Group and the Funds shall, and where they appoint a Service Provider, shall ensure that such Service Provider 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:

- pseudonymisation 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; and

- 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; and

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

Retention Periods

The Sciens Group and the Funds are 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 the Sciens Group and the Funds or as required or permitted for legal, regulatory, fraud prevention and legitimate business purposes. In general, the Sciens Group and the Funds (or their Service Providers) will hold this information for a period of seven years from the termination of the relevant business relationship, unless obliged to hold it for a longer period under applicable law or regulations. Certain Personal Data of directors may be held indefinitely where it forms part of the statutory books and records of the Sciens Group or a Fund.

The Sciens Group and relevant Funds (or their Service Providers) may retain records of telephone calls and other electronic communications for a certain period of time, in accordance with other applicable legislation. For the purposes of GDPR, records of telephone calls and other electronic means are used in accordance with the third principle of GDPR ensuring that records are adequate, relevant and held for a limited time to what is necessary in relation to the purposes for which they are processed.

Breach Notifications

In accordance with applicable data protection laws, the Sciens Group and the Funds may be obliged to notify the relevant regulator of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data within a prescribed period e.g.72 hours in [the European Union] of becoming aware of same, unless the Personal Data Breach is unlikely to result in risks to any individuals. Furthermore, the Sciens Group and the Funds will 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:

- The Sciens Group or a Fund 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 Personal Data Breach, the period of the Personal Data 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 relevant regulator within the prescribed period of time e.g. 72 hours for [the European Union] of the Sciens Group or a Fund becoming aware of the incident. Where a report is made to a regulator, the Sciens Group and the Funds will provide such information and detail as is required under applicable data protection laws and / or as the regulator 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; and

    - a description of measures to mitigate possible adverse effects;

- reporting to the relevant regulator may be conducted in phases where the full extent of the Personal Data Breach is not known within the prescribed period of time from the Sciens Group or –Fund becoming aware of the same. Any such phased reporting will be conducted in consultation with the regulator;

- 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 the Sciens Group or the relevant Fund;

- Where, having considered the matter, the Sciens Group or a Fund comes to a determination that no notification need or will be made to a regulator and / or the affected data subjects, the Sciens Group or such Fund 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 the Sciens Group or the Fund did not consider it necessary to inform the regulator.

- Records of Data Protection Breaches will be made available to any relevant regulator on request.

The Sciens Group and the Funds shall ensure that all Service Providers notify the Sciens Group or the relevant Fund without delay of any Data Protection Breach and provide all reasonable assistance to the Sciens Group and the relevant Fund to enable it to comply with its obligations under applicable data protection laws regarding notification of Personal Data Breaches.

Privacy Impact Assessments

The Sciens Group and the Funds 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; and
- 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 Sciens Group or the relevant Fund;
- 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.

The Sciens Group and the Funds shall consult with any relevant regulator where necessary in accordance with applicable data protection laws, and where appropriate shall seek the views of individuals or their representatives.

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

Transfers of Data from the EU or an equivalent jurisdiction

The transfer and distribution of Personal Data, whether to an entity related to the Sciens Group, the Funds 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 relating to EU data subjects to countries outside of the EEA, where such countries do not have equivalent levels of data protection to that afforded to Personal Data under GDPR.

If the Sciens Group, a Fund or a Service Provider wishes to transfer Personal Data to a country outside the EEA, it will in general be necessary for the Sciens Group, the Fund (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 the Sciens Group or the Fund and / or the relevant individual or entity to whom the Personal Data relates;
- contain an undertaking from the Importer to comply with policies and guidelines similar to those to which the Sciens Group or the Fund 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 the Sciens Group or a Fund to transfer Personal Data outside the EEA where such transfer is necessary for the performance of a contract between the Sciens Group or a Fund and an individual, or where the individual has explicitly consented to the transfer.

The Sciens Group or a Fund 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 Personal Data be transferred outside the EU without the consent of the Sciens Group or the relevant Fund except within the Sciens Group. No transfer of data outside of the EU/EEA or recognised equivalent territories (including Guernsey) will be permitted unless the Sciens Group or the board of directors or alternative investment fund manager of the relevant Fund 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 the Data Controller to provide certain information to the data subject.

Accordingly, on receipt of any data subject access request, the Sciens Group or the relevant Fund shall within 30 days:

- inform the Individual as to whether the data processed by or on behalf of the Sciens Group or the Fund 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 the Personal Data is being or is to be processed;
- the recipients or categories of recipients to whom the Personal Data are or may be disclosed;
- information as to source of the Personal Data, 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 relevant regulator;
- details of any automated decision making or profiling; and
- the appropriate safeguards with regard to international data transfers.
- provide the individual with a copy of the Personal Data of the individual; and
- 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 the Sciens Group or a Fund does not intend taking action at the request of the data subject, the Sciens Group or such Fund shall inform the individual without delay and provide the reasons for not taking action, as well as the right of the individual to complain to the relevant regulator. In the event of a complex query, the Sciens Group may require more time, though the data subject will be kept informed in this instance.

The Sciens Group and each Fund shall ensure that its Service Providers notify the Sciens Group and such Fund without delay of any data subject access request and provide all reasonable assistance to the Sciens Group and such Fund 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; and
- the right to data portability.

The Sciens Group and the Funds shall comply with applicable data protection laws in honouring the rights of Individuals as set out above. However, if the Sciens Group or a Fund determines not to take action at

the request of the data subject, the Sciens Group or such Fund 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 relevant regulator.

The Sciens Group and the Funds shall ensure that any Service Providers notify the Sciens Group or the Relevant Fund without delay if any data subject requests to enforce the above rights and provide all reasonable assistance to the Sciens Group or the relevant Fund 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. If you have any further questions or concerns about the processing of your personal data, please contact the DPO on the below details:

Melissa Bradford – Data Protection Officer, Direct telephone number – (01481) 735519
Sigma Asset Management (Guernsey) Limited and Sciens Group Fund Services Limited
Suite 5/6, Pollet House, Lower Pollet, St Peter Port, Guernsey, GY1 1WF

Updates to this Policy - Any changes we make to this Data Protection and Privacy Policy in the future will be posted on the Sciens Group's website – www.sciensam.com - please check back frequently to view any updates.