

This Privacy Notice sets out how your personal data is collected, processed and disclosed in connection with Spartan Investment Management Limited (the “Licensee”).

We take privacy and security of your information seriously and will only use such personal information as set out in this Privacy Notice.

Privacy Notice – Users of the Spartan Investment Management Limited website

The following section of this notice sets out how the Company may process personal data (as a controller) about visitors to its website.

We may collect, use, store and transfer different kinds of personal data about you which you provide to us through our website: name, date of birth, address, email address, telephone numbers, technical data (including internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website, usage data (including information about how you use our website, products and services, and marketing and communications preferences (including your preferences in receiving marketing from us and your communication preferences).

We do not collect any sensitive personal data or special categories of personal data about you through our website (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

Privacy Notice – Directors and personnel of service providers

As a result of you acting as a director, employee or consultant of the Licensee or one of the Licensee's service providers (a “**Relevant Person**”), your personal information may be provided to the Licensee, which will act as a data controller in respect of such personal data. The Licensee may process your personal information. If you are a director, employee or consultant of an entity that provides us with personal data on individuals connected to you for any reason in relation to your involvement with us, this will affect those individuals and you should transmit this document to those individuals or otherwise advise them of its content.

Your personal data may also be collected and processed by us as a result of your professional or family connection with a Relevant Person.

As the Licensee is incorporated in Guernsey, the Licensee is obliged to comply with the provisions of the Guernsey data protection laws.

1 Where we obtain your personal data:

1.1 Your personal data comprises the following categories:

- 1.1.1 information related to identification (including name, signature, nationality, place and date of birth, passport number, residential address, email address and other contact details);
- 1.1.2 information required for payroll, benefits and expenses purposes;

- 1.1.3 bank account details;
- 1.1.4 correspondence records;
- 1.1.5 professional qualifications, employment history, references and other details regarding your career history such as training records;
- 1.1.6 tax status and tax identification numbers; and
- 1.1.7 where necessary, information regarding your investment activity or health.

1.2 We primarily collect your personal data from the following sources:

1.2.1 from information which you or your authorised representative gives to us, including but not limited to:

- (a) information set out in any application to act or by virtue of you acting as a Relevant Person;
- (b) such other forms and documents as we may request that are completed in relation to the you acting as a Relevant Person;
- (c) any documentation that we may obtain as part of our regulatory requirements; and
- (d) any personal data provided by you by way of correspondence with us by phone, e-mail or otherwise;

1.2.2 personal data we receive from you or any third party sources which may include:

- (a) entities in which you or someone connected to you has an interest;
- (b) your legal and/or financial advisors;
- (c) your relatives, trustees, personal representatives or shareholders;
- (d) other financial institutions who hold and process your personal data to satisfy their own regulatory requirements; and
- (e) credit reference agencies and financial crime databases for the purposes of complying with our regulatory requirements.

1.3 We may also collect and process your personal data in the course of dealing with advisors, regulators, official authorities and service providers by whom you are employed or engaged or for whom you act.

2 Why we collect your Personal data:

Lawful grounds for processing:

2.1 We are entitled to hold and process your personal data on the following lawful grounds:

- 2.1.1 the processing is necessary for our legitimate interests, provided your interests and fundamental rights do not override those interests;
- 2.1.2 the processing is necessary for us to comply with our contractual duties to you under the terms of any contract which we have with you;
- 2.1.3 to comply with our legal and regulatory obligations;
- 2.1.4 (on exceptional occasions) where we have obtained your consent; and
- 2.1.5 (on rare occasions) where it is needed in the public interest.

Some of the grounds for processing described above will overlap and there may be several grounds which justify our use of your personal data.

Inaccurate or Amended Information

- 2.2 Please let us know if any of your personal data (including correspondence details) changes as soon as possible. Failure to provide accurate information or to update changed information may have a detrimental impact upon your directorship, employment or consultancy, including the processing of any payment due to you. Failure to provide information where the same is required for anti-money laundering, pursuant to automatic exchange of information agreements, or other legal requirements may mean that any payment due to you cannot be processed.

Purposes of processing

- 2.3 Pursuant to paragraph 2.1, we may process, store and use your personal data for the purposes set out below ("**Purposes**"). Those based wholly or partly on our legitimate interests are set out in paragraphs 2.3.1 to 2.3.7:
- 2.3.1 to reflect your directorship, employment or consultancy relationship with the Licensee or with one of its service providers;
 - 2.3.2 to communicate with you as necessary in connection with your affairs and generally in connection with your directorship, employment or consultancy relationship with the Licensee or with one of its service providers;
 - 2.3.3 to operate the Licensee's IT systems, software and business applications;
 - 2.3.4 to support our IT and business applications support teams, accounting, legal, reporting, internal audit and risk management, administrative, transfer, document storage, record keeping and other related functions, including but not limited to processing personal data in connection with the Licensee;
 - 2.3.5 for service, training and related purposes;
 - 2.3.6 to monitor and record telephone and electronic communications and transactions:
 - (a) for quality, business analysis, training and related purposes in order to improve service delivery;
 - (b) for investigation and fraud prevention purposes, for crime detection, prevention, investigation and prosecution of any unlawful act (or omission to act); and
 - (c) to enforce or defend the Licensee's rights, or through third parties to whom we may delegate such responsibilities or rights in order to comply with a legal or regulatory obligations imposed on us;
 - 2.3.7 disclosing your personal data to any bank, financial institution or other third party lender providing any form of facility, loan, finance or other form of credit or guarantee to the Licensee;
 - 2.3.8 to carry out our obligations to you in connection with your directorship, employment or consultancy with the Licensee or with one of its service providers;
 - 2.3.9 to discharge our anti-money laundering obligations to verify the identity of our directors, employees or consultants (or those of our service providers) or for prevention of fraud or for legal, regulatory or tax reporting purposes or in response to legal requests or requests from regulatory authorities (i.e. where it is

necessary for compliance with a legal obligation to which we are subject). In discharging our anti-money laundering obligations we may, in certain circumstances, collect, store and process special categories of data such as information regarding criminal convictions;

- 2.3.10 facilitating the internal administration of the Licensee;
- 2.3.11 communicating with our professional advisers for the purposes of obtaining professional advice; and
- 2.3.12 conducting business analytics and diagnostics.

We will only use your personal information for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where these are required or permitted by law.

- 2.4 To the extent that such personal data contains special category data such as, for example: data relating to racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership or criminal data then the processing of such data shall solely be for the purpose of complying with any duty imposed on the Licensee by an enactment including, but not limited to, legislation and regulatory obligations relating to Anti-Money Laundering and Combatting the Financing of Terrorism and all other related legislation.
- 2.5 The Licensee will not make decisions about you based on automated processing of your personal data.

3 Sharing personal data

- 3.1 The Licensee may share your personal data with group companies and third parties (including bank, financial institution or other third party lenders, IT service providers, auditors and legal professionals) under the terms of any appropriate delegation or contractual arrangement. Those authorized third parties may, in turn, process your personal data abroad and may have to disclose it to foreign authorities to help them in their fight against crime and terrorism.
- 3.2 Data processing (as described above) may be undertaken by any entity in the Bailiwick of Guernsey or the European Economic Area.
- 3.3 This means that the country or countries to which we transfer your data are deemed to provide an adequate level of protection for your personal information. However, if we do transfer your data to a third party located in a country outside the Bailiwick of Guernsey and the European Economic Area, we will ensure that your personal data receives an adequate level of protection and will put in place appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU laws and the laws of the Bailiwick of Guernsey on data protection, including the use of model contractual safeguards. If you require further information about these protective measures, you can request it from the Licensee using the contact details in the "How to Contact Us" section below.

4 Retention of personal data

- 4.1 Your personal data will be retained for the longest of the following periods:
- 4.1.1 for the Licensee and/or any authorised third parties to carry out the Purposes for which the data was collected or as long as is set out in any relevant agreement you enter into with us;
 - 4.1.2 in order to establish or defend legal rights or obligations or to satisfy any reporting or accounting obligations; and/or
 - 4.1.3 any retention period that is required by data protection laws and any applicable laws or regulatory requirements.
- 4.2 We endeavour to store your personal data securely on the computer systems of Praxis Fund Services Limited and/or manually in accordance with accepted market standards.
- 4.3 Whilst we have taken every reasonable care to ensure the implementation of appropriate technical and security measures, we cannot guarantee the security of your personal data over the internet, via email or via our websites nor do we accept, to the fullest extent permitted by law, any liability for any errors in data transmission, machine, software or operating error or any other cause.

5 Your rights

- 5.1 You have, under certain circumstances, the following rights in respect of personal data:
- 5.1.1 the right to access and port personal data;
 - 5.1.2 the right to rectify personal data;
 - 5.1.3 the right to restrict the use of personal data;
 - 5.1.4 the right to request that personal data is erased;
 - 5.1.5 the right to object to processing of personal data; and
 - 5.1.6 where the Licensee has relied on consent to process the personal data, the right to withdraw consent at any time by contacting us via the contact details below.
- 5.2 You also have the right to lodge a complaint with the Guernsey Data Protection Authority or a supervisory authority in the EU member state of your usual residence or place of work or of the place of the alleged breach if you consider that the processing of your personal data carried out by the Licensee of any other service provider to the Licensee, has breached data protection laws. You may also appeal to certain courts against (i) any failure of the Guernsey Data Protection Authority to give written notice of whether the complaint is either being investigated or not being investigated and where applicable, the progress and the outcome of the investigation and (ii) a determination of the Guernsey Data Protection Authority not to investigate the complaint or a determination that a controller or processor has not breached or is not likely to breach an operative provision in connection with the complaint.
- 5.3 In limited circumstances we may approach you for your written consent to allow us to process certain particularly sensitive data or to use data for another purpose. Where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Manager via email Compliance-GG@apexgroup.com. Once we have received

notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

6 How to contact us:

If you have any questions about our use of your personal data, our retention procedures or our security processes, please contact the Data Protection Manager at Compliance-GG@apexgroup.com.

7 Changes to this Policy

This Privacy Notice is dated 27 February 2024.

We reserve the right to amend this Privacy Notice at any time without notice, in which case the date of the policy will be revised.