Firm Privacy Policy & Notice

(Effective date: *25 May 2018)*

This privacy policy and notice ("Policy") is issued on behalf of Finisterre Capital LLP, Finisterre Malta Limited and Finisterre USA Inc, together "Finisterre" and is meant to help you understand the type of personal information we collect and use, why we use the information, who we may need to share the information with, how we protect your information and your privacy rights.

Your personal information is important to us. That's why we do so much to protect your information, while continually providing service you can count on. While no one can guarantee absolute information security, we protect your information in many ways—from using safe and secure information security practices, working to ensure that our buildings are secure, to proactively preparing for disasters and business interruptions. We continually review and make enhancements to how we safeguard and protect your information.

References to "you" or "your" include, as applicable, references to individuals within, or associated with, your organization.

About this Policy

This Policy applies to personal information which we receive from or relate to our: (a) clients, investors and potential investors; (b) business partners and associates; (c) business contacts; (d) contractual counterparties; and (e) others from whom we collect and use information. Where the personal information relates to your employees, contractors, workers, directors, representatives, agents and other relevant third parties, you should bring the Policy to their attention.

Finisterre is a data controller for purposes of applicable data protection law, including the European Union's General Data Protection Regulation. We are responsible for ensuring that we use your data in compliance with applicable data protection law.

This Policy explains the type of personal information we collect and use, why we use the information, who we may need to share the information with, how we protect your information, and your rights under data protection law.

Depending on the nature of our relationship with you, other privacy policies may also apply. For example, if you use our website or other digital technologies, the personal information we collect will be governed by our separate Online Privacy Policy, which can be accessed via our website at www.finisterrecapital.com.

References to 'personal data' and/or 'personal information' mean any information that identifies, or can be used to identify, an individual. References to 'process' or 'processing' of your personal information mean the use of that information as set forth in data protection law.

Information we process

The personal information we process varies depending upon the nature of our relationship with you.

In many instances, the personal information we process is limited to:

1. **Contact information** – e.g., email address, physical address, telephone/fax number;
2. **Identity information** – your name, date of birth, nationality, gender, photograph, identification number (e.g., passport number, tax number, national id number, social security number) or other information contained in identity-related documentation (e.g., passport, driver's license);

Depending on the nature of our business relationship, we may also process the following:

3. **Professional information** – your occupational history, job title, or other professional information regarding the nature of our business relationship;
4. **Financial information** – your income, assets, liabilities, tax residency, bank details, and other financial information, both current and historical;
5. **Transactional information** – details about your accounts that you have with us and other details of services you have engaged us to perform;
6. **Contractual information** – details about the contractual services we provide to you;
7. **Technical information** – details on the devices and technology you use;
8. **Communications information** – information we obtain through letters, emails, telephone calls, conversations, social media interactions, or any other correspondence between you and us;
9. **Open Data and Public Records information** – details about you that are available in public records or that are openly available on the internet;
10. **Usage information** – information about how you use the services we provide to you; and

The personal information described above may be collected from you in a variety of ways, such as:

- When you engage us for services;
- By telephone or in person;
- Through email or letter correspondence;
- Via our website;
- In Requests for Proposals, due diligence reviews, and interviews;
- National/Tax identity requests;
- When we enter into an agreement for the exchange of services; and
- In client surveys.

Information received from third parties

In addition to information you provide to us, we may also collect or receive personal information about you from third parties such as:

- Companies that introduce you to us;
- Funds that we provide investment management services to;
- A client that you are associated with (e.g., your employer, a trust, corporate entity, institutional client);
- A counterparty that you are associated with (e.g., trading partners, distribution partners);
- A business partner that you are associated with (e.g., vendors, suppliers)
- Financial advisors;
- Credit reference agencies;
- Social networks;
- Fraud prevention agencies;
- Public information, such as information available for public registries;
- Agents working on our behalf;
- Market researchers;
- Government and law enforcement agencies.

How and why we use personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you;
- Where it is necessary for our legitimate interests (i.e. we have a business or commercial reason for using your information) and your interests and your fundamental rights do not override those interests, such as:
    - Complying with regulations that apply to us.
    - Administering and managing contracts with our business partners and counterparties.
    - Being efficient about how we fulfill our legal and contractual duties.
    - Providing high quality customer service.
    - Developing services, and what we charge for them.
    - Defining types of customers for new services.
    - Seeking your consent when we need it to contact you.
    - Developing and improving the network security, efficiency and technical specification of our IT systems and infrastructure.
    - Developing and improving how we deal with and manage financial crime.
    - Providing our customers with high quality services and online features.
    - Keeping our services and online features updated and relevant.
- Where we need to comply with a legal or regulatory obligation; or
- Where you consent.

We use your personal information for the following reasons:

- To comply with our legal and regulatory obligations (including verifying your identity and conducting identity and background checks for things such as anti-money laundering, fraud, sanctions, credit, and security purposes) and to exercise our legal rights.
- To run our business in an efficient and proper way, including in respect of our financial position, business capability, corporate governance, audit, risk management, compliance, product development, strategic planning, marketing, and communications.
- To process transactions and carry out obligations arising from any contract entered into between you (or your organization) and us.
- To exercise our rights in agreements and contracts to which we are a party.
- To administer auditing, billing and reconciliation activities and other internal and asset management related functions.
- To deliver services you receive from us.
- To detect, investigate, report, and seek to prevent financial crime and to manage risk for us and our customers.
- To communicate with you and respond to your inquiries, including responding to complaints and attempting to resolve them.
- To send you promotional and marketing materials, newsletters or other related communications (including making suggestions and recommendations to you about services that may be of interest to you).
- To conduct research and analysis to improve the quality of our marketing and the experience of and relationships with our customers.
- To provide and manage our services and digital technologies (including any online account with us).
- To administer and protect our business and our digital technologies (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).
- To develop, manage and improve our services and digital technologies (including conducting research and analysis) and to test new services, and features of our digital technologies.

Failure to provide personal information

Where we need to collect personal information by law or under the terms of a contract we have with you, and you fail to provide that information when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

Change of purpose

We will only use your personal information for the uses and purposes set out above, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original uses and purposes. If we need to use your personal information for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

Information shared

We share your personal information with the following categories of recipient:

- **With group companies and affiliates.** Finisterre is part of the Principal Financial Group ("Principal"). We may share the information we collect about you with other member companies of Principal, including Principal Life Insurance Company, Principal National Life Insurance Company, Principal Global Investors and their affiliates for a variety of purposes.
- **With our service providers.** We may disclose information to third party service providers that perform services for us in the processing or servicing of your account or transaction.
- **With third parties as permitted or required by law.** This includes disclosing your information to regulators, law enforcement authorities, tax authorities and credit bureaus. This information is only disclosed as required or permitted by law, and in accordance with established company procedures. We may transfer and disclose the information we collect about you to comply with a legal obligation, including responding to a subpoena or court order, to prevent fraud, to comply with an inquiry by a government agency or other regulator, to address security or technical issues, to respond to an emergency, or as necessary for other legal purposes.
- **As part of business transitions.** In relation to an ongoing or proposed business transaction or relationship, your information may be transferred to a successor organization.

- **Other –**

    - Fraud prevention agencies;
    - Any party linked with you or your business's product or service;
    - Organizations that introduce you to us;
    - Investment brokers;
    - Proxy voting servicers;
    - Custodial banks;
    - Companies you ask us to share your data with, such as, but not limited to financial administrators and audit firms.

In addition, we may share non-personal (anonymized) information, such as aggregate data and usage information with other third parties.

Except as described above, or as set forth in a separate privacy policy (e.g., Online Privacy Policy), we will not provide your personal information to other third parties without your specific consent.

How we protect your information

We understand the importance of appropriately safeguarding information you provide to us. It is our practice to protect the confidentiality of this information, limit access to this

information to those with a business need, and not disclose this information unless required or permitted by law.

We have security practices and procedures in place to protect data entrusted to us. These procedures and related standards include limiting access to data and regularly testing and auditing our security practices and technologies.

All employees are required to complete privacy, security, ethics and compliance training. We also offer a wide variety of other training to all employees and temporary workers to help us achieve our goal of protecting your information.

Ultimately, no website, mobile application, database or system is completely secure or "hacker proof." While no one can guarantee that your personal information will not be disclosed, misused or lost by accident or by the unauthorized acts of others, we continuously review and make enhancements to how we protect personal information.

Retaining your information

We will retain your information for as long as your information is necessary for the purposes for which it was collected. The amount of time we hold your information will vary depending on the nature of our business relationship, the purpose for which we are using your information, the type of information, and the applicable legal obligations.

For example, we may retain your personal data if it is necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this Policy and prevent fraud and abuse. If requested by a law enforcement authority, we may also retain your personal data for a period of time. It may not always be possible to completely remove or delete all of your information from our databases without some residual data remaining because of backups and other reasons.

To determine the appropriate retention period for the information we collect from you, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorised use or disclosure of the data, the purposes for which we process the data, whether we can achieve those purposes through other means, and the applicable legal requirements.

Children's privacy

We do not knowingly collect or use personal information from children under the age of 13. If we determine that we have collected the information of an individual under this age, we will not use or maintain his or her personal information without parent or guardian consent. If we become aware that we have unknowingly collected personal information from a child under the age of 13, we will make reasonable efforts to delete such information from our records.

Data Privacy Rights

Under certain circumstances, you have rights under data protection laws in relation to your personal information:

- **Right to withdraw consent at any time**: This applies where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

- **Request access to your personal data**: This enables you to request a copy of the personal data we hold about you and to check that it is accurate and that we are processing it lawfully. This is not, however, an absolute right, and the interests of other individuals may restrict your right of access.

- **Object to processing of your personal data**: This enables you to object to processing of your personal data where we are relying on a legitimate interest and there is an impact on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms. You also have the right to object in cases where we are processing your personal data for direct marketing purposes. We will provide you with appropriate choices to opt-in or opt-out as set out above in our Policy.

- **Request correction of your personal data**: This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- **Request erasure of your personal data**: This enables you to ask us to delete or remove personal data where there is no lawful basis for us continuing to process it. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- **Request transfer of your personal data**: This enables you to request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use, or where we used the information to perform a contract with you.

- **Request restriction of processing**: This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal

claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- **Right not to be subject to a decision based on automated profiling**: This applies where the automated processing produces legal effects on you or similarly significantly affects you. Note, it does not apply if the decision: (a) is necessary for the performance of a contract between you and us; (b) is authorized by applicable law; or (c) is based on your explicit consent. However, where (a) or (c) applies, you have the right to obtain human intervention. You also have the right to be informed of the logic involved in such processes.

- **Make a complaint**: You have the right to make a complaint at any time to the relevant data protection supervisory authority. We would, however, appreciate the chance to deal with your concerns before you approach your supervisory authority so please contact us using the information provided below.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We require that your request be in writing. In addition, we may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within 30 days. Occasionally it may take us longer than 30 days if your request is particularly complex or you have made a number of requests. In this case, we will notify you of a 60-day extension.

Data Transfers

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA").

We share your personal data within the Principal Financial Group which will involve transferring your data outside the EEA. Furthermore, many of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Where we transfer personal data to a destination outside the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.

- We will use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield Framework which requires them to provide similar protection to personal data shared between Europe and the US.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

Effective date and changes to this Policy

The effective date of this Policy is posted above. We reserve the right to update or modify this Policy at any time by providing any notice required under applicable law and by providing you with the revised version in hardcopy, electronically or by otherwise making the revised version available on our website.

Contact us

If you have any questions about this Policy or if you would like to exercise any rights you may have in relation to your personal information, please contact us by email using **both** the following email addresses:

1. FINISTERRE-GDPR-WG@finisterrecapital.com; and
2. CorpPrivacy@exchange.principal.com