Personal Data Protection Policy

As of 24/02/2020

1. Personal Data Protection Policy

1.1 Scope of application

This data protection policy ("**Policy"**) describes how the Company treats the information collected or provided during the course of the Company's activities, how it is stored, processed, secured and what are the rights of Data Subjects (as defined below) in relation to these data.

This Policy is issued by the Company, identified as personal data controller ("**Data Controller**") and applies to individuals with whom the Company interacts ("**Data Subjects**").

Personal Data may be collected, recorded, stored in digital form or otherwise, adapted, transferred or otherwise processed and used in accordance with the Luxembourg law of 2 August 2002 on the protection of persons with regard to the processing of Personal Data (as amended), the European Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data and any other European Union or national legislation which implements or supplements the foregoing ("**General Data Protection Rules**" or "**GDPR**").

This Policy applies to any Data Subject whose Personal Data is provided to the Company directly by the Data Subject or indirectly through another natural or legal person, public authority, agency or another body in connection with the Company's relationship with the Data Subject where the

This Policy may be amended from time to time to reflect changes in our practice with respect to the processing of Personal Data, or changes in applicable law.

Data Protection Officer

The principal contact person at the level of the Companyfor Personal Data protection matters ("**Data Protection Officer**") is the Compliance Officer.

The Data Protection Officer is responsible for acting as the first point of contact at the level of the Company, for data breaches escalated to it by any of its stakeholders.

Types of Personal Data Collected or Provided to the Company

The main categories of **Personal Data** processed which can be used to identify natural persons are (inter alia):

- With respect to the employees and resources provided work to the Company;
- With respect to persons to whom is required or have a legitimate interest to perform Know-Your-Client or other due diligence checks;
- With respect to persons to whom the Company contractually required or otherwise have a legitimate interest to provide information to;

- With respect to persons to whom the Company is obliged to make payments or reimbursements according to the Company's obligations, in addition to the Know-Your-Client information mentioned above;
- With respect to website users only.

For the avoidance of doubt, the Company does not collect and service providers of the Company are not authorized to process any special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health related data or data related to sexual orientation, except for medical certificates provided by the Employee in case of sickness.

1.2 Protection of Personal Data: purposes and legitimate basis of processing

Any Personal Data provided to the Company is processed based on the legal grounds enumerated in Art. 6, Par. 1 of the GDPR. The Company does not use Personal Data for marketing purpose without consent of the relevant Data Subject.

Most of the Company's data processing arises from regulatory or contractual requirements, without which the Company would not be able to operate or be in compliance with applicable laws.

Regarding website users, their data is processed for statistics purposes, to communicate with the user and to answer any request.

In accordance with Art. 30 of the GDPR, each service provider of the Company which is processing Personal Data on behalf of the Company, shall maintain a record of its data processing, which shall be made available to the Controller for inspection upon request.

Certain personal data, such as business cards and photographs that the Company may have of Data Subjects further to events, or IP address (for website users), may be processed based on consent or to pursue legitimate interest, such as internal communication and business administration.

For the processing of data that are based on Data Subject's consent, Data Subjects have the right to withdraw their consent and request that the Company stops processing and to delete such data at any time.

1.3 Security Systems

The Company ensures the highest level of security regarding all communication systems in use. All material client's Personal Data is encrypted and sufficiently protected.

Emails are associated to certain risks that are only partly limited by technical measures. Thus, for confidentiality and privacy reason, employees of the Company shall always consider whether informing by writing is the most secured and efficient mean. When deciding to communicate in writing, employees should consider whether using emails is the most appropriate channel for sending information including Personal Data.

The Company has established an IT and Infrastructure Policy including systems and procedures to safeguard the security, integrity and confidentiality of information.

1.4 Duration of storing

Any and all Personal Data will not be retained for longer than the duration required by applicable law or contractual obligations, taking into account any required retention period to meet any legal procedural requirements in case of any need to provide information with integrity to competent authorities.

1.5 Transfer of Personal Data

In order to fulfil the Company's obligations arising from contract or applicable laws, certain Personal Data may be transmitted to other service providers.

To the extent practicable, the Company avoids transferring Personal Data to non-EU countries or to countries without EU equivalent data protection. In the event Personal Data is transferred outside of the EU, prior due diligence is performed to ensure that the data processor or service providers only transfer data to their affiliates that are compliant with GDPR, the IT cloud solutions chosen have implemented GDPR compliant security measures, and that the data is transferred in a secure way.

The data systems shall be maintained and backed-up by an external IT service provider located within the EU, in jurisdictions deemed to have an EU-equivalent level of protection, or are otherwise bound contractually to comply with GDPR requirements, based on standard contractual clauses.

1.6 Rights of Data Subjects

Requests from Data Subjects related to their exercise of the rights below shall in general be referred to as "Data Requests" and shall be handled in accordance with the section below "Handling of Data Requests".

The Company's Data Subjects have the following rights:

- Right to access and rectification
- Right to transfer
- Right to withdraw your consent
- Right of erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Right to complain

Data Subjects have the right at all time to lodge a complaint regarding the processing of their data. This can be done with the contact form on the website or directly to a national data protection authority of a European Union Member State.

1.7 Handling of Data Requests

Processors shall assist the Controller within the scope of its abilities and the information reasonably available to it, to respond to requests from Data Subjects regarding the Personal Data mentioned hereabove.

For data requests received by a specific service provider, the same service provider shall be responsible for providing a first response to the data subject within two weeks.

For data requests addressed to the Company, the Company shall be responsible for obtaining and coordinating the necessary information from the relevant service providers as well as responding to the relevant data subject.

1.8 Handling of Data Breaches

In the event of a data breach likely to result in harm to Data Subjects, the Company in its capacity as controller has the responsibility to notify the *Commission Nationale de Protection des Données* ("**CNPD**") in accordance with Art. 33 of the GDPR.

Taking into account the delegated processing and storage of the Company's data, a data breach of the requires detection by the relevant service provider, which will in turn will immediately notify the Company (addressing the Data Protection Officer) without undue delay.

The service provider experiencing data breach is the primary party responsible for performing assessment regarding the nature of the breach and the likelihood of risk to the rights of natural persons. The service provider will need to notify the Company no later than 36 hours after becoming aware of such breach.

The Board of the Company will determine the likelihood of risk to the rights of natural persons (with the continuous information from the service provider) and whether there is a need to further notify the CNPD and the Data Subjects (as required).

The abovementioned notifications shall include the following information:
a) Describe the nature of the Personal Data breach;
b) Communicate the name and contact details of the Data Protection Officer or contact point where 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 controller to address the Personal Data breach.

1.9 Reporting from Service Providers

Each Service Provider shall provide information to the Company on how GDPR compliance is ensured. The Company can request additional information from each Service Provider to asses and verify status of GDPR compliance for its due diligence processes.

For each calendar year, each Service Provider, acting as data processor, shall provide the following reporting to the Board relating to the protection of Personal Data:

- In case of no data breach during a calendar year, confirmation shall be provided to the Data Protection Officer and the Data Protection Coordinator ahead of the first quarterly board meeting of the following calendar year;
- In case of data breach during a calendar year, above-mentioned notifications will be required and a summary of incident(s) with relevant resolution, remedial measures and time taken will be reported to the Data Protection Officer before the next Board meeting in the following calendar quarter;
- In case of Data Requests, above-mentioned required notifications will be required and a summary with the number and nature of data requests, as well as relevant resolutions will need to be provided to the Data Protection Officer before the next Board meeting in the following calendar quarter;

1.10 Data Contact PointsRights of data subjects

All notices and communications between the relevant service providers shall be sent in writing by e-mail and addressed as follows:

For the Company
complaints@innpactfundmanagement.com
Subject line: ToA Data Protection Officer