DATA PROTECTION POLICY

This Policy is issued by Samarang Asset Management S.A.: 11a, Avenue Monterey, L-2163 Luxembourg.

1) INTRODUCTION

This policy explains how personal data are collected and processed by Samarang Asset Management (hereafter "Samarang" or "Samco") as well as the measures taken to preserve their confidentiality and security.

Samco collects and processes personal data (further defined below) about investors and their representatives, target companies, visitors on the website, business partners, regulatory and other governmental agencies, directors and employees and, in some cases, members of their families (hereafter together referred as "data subjects" in this policy).

In this context, Samarang complies with the following legal and regulatory framework:

- the EU regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter referred to as "GDPR").
- The law dated August 1, 2018 organizing the "Commission nationale pour la protection des données" (hereafter "CNPD") and implementing specific provisions linked to the EU regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- The law dated August, 1 2018 on the protection of natural persons with regard to the processing of personal data in criminal matters and in the context of national security.

2) APPLICATION OF THIS POLICY

This policy applies to (a) all partners and employees in Samco's business activities, (b) any contractors, temporary employees, secondees or interns working within/with Samco.

Some provisions of this policy only apply in the European Union and in the United Kingdom.

In this policy, any reference to

- "***Samarang Funds***" refers to any fund, sub-funds managed by Samco;
- "***Personal Data***" means information that (a) relates to an identified or identifiable natural person; and (b) is held either (i) on computer or in other electronic or automatically **processable** form; or (ii) in a paper filing system arranged to be accessible according to specified criteria; Personal Data does not include any information or data related to legal entities (e.g. investment funds, securities issuers…).
- "***Identifiable natural person***" or ***"data subject"*** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- *"**Processing**" any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means (e.g. collection, recording, organization, storage, consultation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) - and **process**, **processed** and **processable** should be read accordingly); and,
- "***Data Controller***": natural or legal person who determines the purposes and means of the processing of personal data;
- "***Data Processor***": natural or legal person who process natural data on behalf of Samco;
- "***Samco employees***" or "***employees***" include partners, members and employees of Samco, as well as contractors, temporary employees, secondees and interns (given the governance of Samco, shareholders are included herein).

Employees should be aware that failure to comply with this Policy is a serious matter that could give rise to disciplinary sanctions, up to and including dismissal.

3) OTHER POLICIES

Other policies will also be relevant. In particular, please refer to the section "rules of confidentiality" in the Code of Conduct and to the Inducement policy together with the IT security policy and the Data Protection Protocol. The GDPR policy is also available on Samco's website.

A **Data Protection Register** has been put in place and sets out a detailed framework for how Samco deals with personal data, including data collected and used in the Human Resources ("**HR**") process and process of completing anti-money laundering checks (the latter being delegated to a Transfer Agent – hereafter "TA"). This Protocol is designed to supervise those who deal with a high volume of personal data and who are processors, including the HR service provider, the accounting and tax service providers and the transfer agent.

Employees should have received training on data protection and be aware of the standards set out in the EU General Data Protection Regulation (**GDPR**). If an employee has not received any training, please contact the Compliance Officer of Samco.

4) COMPLIANCE WITH DATA PROTECTION LAWS AND REGULATIONS

Anyone who processes personal data for or on Samco's behalf, including contract workers as well as employees, must comply with this Policy. Exceptions to this Policy can be made only with the written approval of the Conducting Officer in charge of the Compliance function ("CO")1. The CO is responsible for data privacy within Samco.

[1] Given the volume and nature of personal data dealt with by Samco, it has been decided not to appoint a data compliance officer within Samco.

If an employee believes that Samco may not have complied with this Policy, the GDPR or another applicable data privacy law, he or she should inform the CO as soon as practicable. If there is any doubt as to the requirements of the Policy in any particular case, please consult the CO.

5) TRANSPARENCY AND PRIVACY STATEMENT

For employees and directors in the European Union and United Kingdom, Samco will ensure they are provided with (and periodically reminded of) information about the processing of personal data through Samco's Personal Data Protection Agreement (the **Personal Data Protection Agreement**) in relation to each IT system or other arrangement involving the processing of personal data (a **processing system**). Provision of this information does not need to be repeated through separate notices and communications, but information about each processing system which is not included in the Employee Personal Data Protection Agreement should be provided.

The term “processing system” has a broad scope and is not limited to software applications. It includes other arrangements, practices and procedures that involve the processing of personal data, including those that do not involve any use of software and/or are or manual handling of personal data. As a general rule, data subjects should assume that arrangements involving the collection or use of information regarding identifiable individuals are covered by this policy.

Samco may not update the Personal Data Protection Agreement in certain circumstances, including when, (a) subject to applicable law, processing occurs to investigate an alleged or actual crime, regulatory breach or disciplinary issue, and an update to the Personal Data Protection Agreement would prejudice the investigation; (b) subject to applicable law, the relevant personal data are not obtained by us directly from the data subject but from a third party, and the effort expended to inform the data subject would be disproportionate to the benefit provided to the data subject; or (c) otherwise, if Samco has concluded that the GDPR and other applicable laws do not require the information to be provided.

For transparency purpose, Samco has published a GDPR Policy on the website www.samarang.lu. Data subjects can also request a copy free of charge of the present policy from Samco. The policy sets out information about Samco’s processing of personal data of data subjects such as employees, directors, investors, visitors on the website, business partners and regulatory and other governmental agencies. Samco takes the view that it is not necessary to provide each of these individuals directly with those policies or specific notice, in relation to routine processing of their personal data for business purposes, but reference will be made to this published policy. Samco is aware, however, that processing of *sensitive* personal data, or of personal data (other than names) relating to individuals in their *personal* rather than their *business or professional* capacity, is not to be regarded as routine for these purposes.

6) FAIRNESS, LEGITIMACY AND PROPORTIONALITY

A key principle of good data protection, and a requirement of the GDPR, is that personal data should be processed *fairly* and for specified and explicit purposes. For example, if Samco has collected data to satisfy anti-money laundering obligations, then we should not use that data for general marketing purposes.

Personal data are processed by Samco for the following purposes:

- the management of the commercial relationship to provide clients with the products and services contracted;
- Legal grounds: processing is necessary for the performance of a contract to which the data subject is a party or for the performance of pre-contractual measures taken at the request of the data subject.
- for direct marketing purposes to inform clients about products as well as invitations to events.
- Based on consent: the data subject has consented to the processing of his/her personal data for one or more specific purposes.

Generally, Samco should only process personal data if:

- the processing is **necessary** for the purposes of the legitimate interests that Samco pursues (and by "**necessary**" it is meant that those purposes could not reasonably be achieved without the relevant processing); and
- either the processing does not prejudice the privacy of the affected data subjects or, if it does, it is sufficiently trivial or minor that it does not override the need to pursue those legitimate interests.

Samco will only process personal data on this basis (this is referred to as the **legitimate interests condition**) if the specified tests set out above are met.
Where the legitimate interests condition does not apply, Samco will not process personal data unless it falls within a lawful reason for processing. A Data Protection Protocol sets out further information on this.

The personal data processed are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data will not be processed at a later stage in a manner incompatible with the purposes described above.

7) SENSITIVE PERSONAL DATA

Employees should take particular care in relation to the processing of personal data in the following, sensitive categories (**sensitive personal data**):

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- genetic data and biometric data processed for the purpose of uniquely identifying a living individual;
- personal data concerning a living individual's health, sex life or sexual orientation; and
- personal data relating to criminal convictions and offences or related security measures.

Samco commits in his oversight function towards its transfer agent to ensure his delegate does ensure the above sensitive personal data are properly dealt with (either kept confidential in accordance with GDPR and AML/KYC rules or not accepted).

Employees should only process sensitive personal data where, subject to applicable law:

- the data subject has given his or her explicit consent;
- the processing is necessary for the purposes of performing contractual obligations or exercising specific rights under employment and social security and social protection law; or
- the sensitive personal data has been deliberately made public by the data subject.

8) STORAGE

Samco takes reasonable and appropriate technical and organizational security measures in order to:

- Store Personal Data in secure databases or systems with restricted access,
- Protect Personal Data against loss, accidental or intentional misuse, alteration, destruction and access by unauthorized persons.

Samco will notify the data subjects without undue delay in the event Samco becomes aware of any unauthorized or improper use, access or disclosure of the Personal Data, which is likely to result in a high risk to their rights and freedoms.

Please kindly note that some of the databases or systems used by Samco for mailing services and storage systems may be hosted and/or maintained by third party service providers located inside or outside of the European Union. Personal Data will only be disclosed to such service providers if Samco has deemed, in its reasonable opinion, that such service providers offer appropriate guarantees with regard to the implementation of technical and organizational measures to ensure confidentiality, security and protection of Personal Data in accordance with the GDPR requirements and the instructions given by Samco and exclusively for the purposes described in this Policy.
Samco also reserves the right to disclose Personal Data to any court, judicial or administrative authority when required or legally compelled to do so.

9) RETENTION PERIOD

Samco will retain Personal Data in accordance with the legal retention periods applicable in Luxembourg or where required for Samco to assert or defend against legal claims until the end of the relevant retention period or until the claims in question have been settled.

Personal Data will be deleted when:

- It is no longer reasonably required for the purpose the Personal Data were initially collected for,
- the data subject withdraws his or her consent (where applicable); or
- Samco is not legally required or otherwise permitted to continue storing the Personal Data.

10) INTERNATIONAL DATA TRANSFER

Where Samco is transferring personal data from inside the European Union to outside the European Union, it will consider whether this is restricted under the GDPR.
Samco shall put in place an international data transfer agreement (IDTA) and/or specific Standard Contractual Clauses (SCCs), as and when needed, which governs transfers between Samco's offices. This means personal data can be transferred globally around Samco's offices under the terms of the IDTA or SCCs. Transfers of personal data to entities (other than Samco offices) outside the European Union should be carefully considered. There may be solutions which allow the personal data to be transferred subject to some safeguards e.g. specific contractual protections or gaining explicit consent from data subjects. Without such safeguards, some transfers may be unlawful.
Transfers of personal data outside the European Union are permitted to countries/territories considered by the European Commission to have equivalent protections to the EU.

As of the date of this Policy, the European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under GDPR and the Law Enforcement Directive and Uruguay as providing adequate protection.
Please be aware this list can change. An up-to-date list can be found on the European Commission website (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en).

If there is any questions or concern about the transfer of personal data outside the European Union please contact the CO.

11) CONSENT

Samco does not generally rely on consent as the basis for processing personal data. There may be some exceptions e.g. Samco considers that individuals who actively sign up to receive the technical material on the fund and its performance (factsheet) are doing so on the basis of consent. Employees should be aware that the standards for gaining consent to process data are very high and specific conditions apply if consent is needed to process **sensitive data**. A Data Protection Protocol sets out further information on this.

12) KEEPING PERSONAL DATA UP TO DATE AND ACCURATE

Where Samco processes personal data, employees must take every reasonable step to ensure that those personal data are accurate and, where relevant, up to date, and to correct inaccurate personal data without delay. This means data subjects should inform us if personal information needs to be updated. Employees should also make sure to keep personal data held on other people, e.g. investor records, up to date and accurate. This also applies to HR data kept with the person in charge of HR matters and processes.

13) DATA SECURITY

Samco is required to report certain breaches of security affecting personal data to competent data protection authorities. It is important that employees immediately report any incidents which may put personal data at risk to the CO.
Examples of incidents affecting personal data are:

- Loss/theft of a device (e.g. phone, laptop)
- Loss/theft of any electronic files (e.g. on a USB stick)
- Loss/theft of paper files (e.g. hard copies of candidates' CVs, event invitation lists)
- Unauthorised access or compromising of electronic or paper files (e.g. a hacking incident)

Employees should also immediately inform the conducting officers of Samco and the CO where they receive any communication from a third-party which indicates they have been subject to a data breach. If employees are unsure whether an event or report may amount to an incident that should be reported, they should escalate the matter to the CO.

14) DATA SUBJECT RIGHTS

Where Samco in the European Union and United Kingdom processes personal data of employees (e.g. in its role as employer) or the personal data of other individuals (e.g. suppliers, investors), they have the right to:
(a) be provided with a copy of any personal data that Samco holds about them, with certain related information;
(b) require Samco, without undue delay, to update or correct any inaccurate personal data, or complete any incomplete personal data, concerning them;
(c) require Samco to stop processing their personal data for direct marketing purposes; and
(d) object to the processing of their personal data more generally.

They may also have the right, in certain circumstances to require Samco, without undue delay to:
(a) delete their personal data;
(b) "restrict" processing of their personal data, so that it can only continue subject to very tight restrictions; and
(c) require that personal data provided to Samco and which are processed based on their consent or the performance of a contract with them, to be "ported" to them or a replacing service provider.

To exercise their rights, Data Subjects can contact Samco at the email address info@samarang.lu or at the following mailing address:

Samarang Asset Management S.A.
Data Controller
11a Avenue Monterey
L-2163 Luxembourg

www.samarang.lu

In addition, Data subjects have the right to file a complaint with the Lead Supervisory Authority which is the National Commission for Data Protection in Luxembourg (Commission Nationale pour la Protection des Données – CNPD) using the contact details below:

Commission nationale pour la protection des données
15 Boulevard du Jazz
L-4370 Belvaux

www.cnpd.lu

If employees receive a communication from any data subject in which he or she seeks to exercise any of these rights, that communication should be escalated to HR and the CO as soon

as reasonably practicable. Employees must comply with the instructions from the CO in relation to the exercise of these rights.

15) CO-OPERATION WITH DATA PROTECTION AUTHORITIES

Each Samco entity/member is obliged to co-operate with the competent data protection authorities in Luxembourg, namely the CNPD. Any communication received from a competent data protection authority should be passed to the CO.

Data controllers shall notify personal data breaches to the CNPD within 72 hours after having become aware of them, if the violation in question is likely to result in a high risk to the rights and freedoms of natural persons (see Annex 3).

Samco will also ensure that agreements concluded with data processors foresee escalation of any personal data breaches to Samco without delay as soon as they are aware of them.

16) COLLABORATION WITH INTERNAL/EXTERNAL CONTROL FUNCTIONS

To comply with relevant regulations and provided these entities/bodies are to abide by similar rules and requirements, Samco is entitled to share personal data with its external auditor, its internal auditor (delegated function) and its regulator (CSSF) which all commit to comply with GDPR provisions.

17) AMENDMENT TO THE POLICY

The Policy may be amended, replaced or supplemented at any time and without prior or further notice by Samco. Data subjects are therefore advised to review it from time to time for any possible changes.

18) QUESTIONS

If data subjects have any questions about this policy, do not hesitate to contact the Compliance Officer.

Alternatively, please feel free to send any queries or requests related to the processing of Personal Data by Samco, in the context described above, to info@samarang.lu.

ANNEX 1 Data Protection Protocol

ANNEX 2 CNPD - Data breach notification form