DATA PROTECTION POLICY

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

1 INTRODUCTION

In the course of our business, including as an employer, we need to collect and process certain data about investors, portfolio companies, Partners and employees and, in some cases, members of their families. Samarang Asset Management S.A. (hereafter "Samarang" or "**Samco**") only collects information that is necessary and appropriate.
We process personal data (defined below) during the course of our business. We are subject to legal and regulatory requirements that oblige us to have in place policies and procedures to ensure the personal data we process is adequately protected.
The type of personal data we process include: personal data regarding our employees (and their family members) and individual contract workers, visitors to our websites and premises, individual investors in funds, individual representatives of investors in funds, suppliers, transaction counterparties, other business partners and regulatory and other governmental agencies, and other individuals (referred to in this policy as "**data subjects**") in the course of our business, and for regulatory and/or legal reasons (e.g. in accordance with anti-money laundering or bribery, US Foreign Account Tax Compliance Act, other tax reporting and investor reporting obligations).

2 APPLICATION OF THIS POLICY

This policy applies to (a) all partners and employees in Samco's investment management business ("**Samco**"), (b) any contractors, temporary employees, secondees or interns working in/with Samco.
Some provisions of this policy only apply in the EU (the "European Region", pending the outcome of the Brexit).
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 living individual; 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…).
- *"**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 - and **process**, **processed** and **processable** should be read accordingly); and,
- *"**you**", "**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 we include shareholders herein).

You should be aware 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 note the Confidentiality and Privacy of data section within the Manual of Procedures together with the Data Protection Policy and the Data Protection Protocol. The specific General Data Protection Regulation – Data Protection Web Policy is also available on our Samco web site.
We have a **Data Protection Register** which sets out a detailed framework for how we deal with 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 our Transfer Agent – hereafter "TA"). This Protocol is designed to supervise those who deal with a high volume of personal data, including the HR service provider, Finance and Compliance teams at our TA.
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 you have not received training, please contact Corinne Piret (Conducing Officer in charge of Compliance function also acting as Compliance Officer).

4 COMPLIANCE WITH DATA PROTECTION LAWS AND REGULATIONS

Anyone who processes personal data for or on our 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 **Compliance Officer** ("**CO**")[1].
The CO reports to the Conducting Officer in charge of the Compliance function, which is responsible for data privacy within Samco.
If you believe that we may not have complied with this Policy, the GDPR or another applicable data privacy law, you should inform the CO as soon as practicable. If you are in doubt as to the requirements of the Policy in any particular case, you should consult the CO.

5 TRANSPARENCY AND PRIVACY STATEMENT

For employees in the European Region, in relation to each IT system or other arrangement involving the processing of personal data (a **processing system**), we will ensure you are provided with (and periodically reminded of) information about the processing of your personal data through Samco's Data Protection Notices (the **Employee Privacy Notice**). Provision of this information does not need to be repeated through separate notices and communications, but you should be provided with any information about each processing system which is not included in the Employee Privacy Notice.
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, you should assume that arrangements involving the collection or use of information regarding identifiable individuals are covered by this policy.

[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.

We may not provide an Employee Privacy Notice 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 Employee Privacy Notice 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 we have concluded that the GDPR and other applicable laws do not require the information to be provided.

As part of our transparency, we have a GDPR – Data Protection Web Policy published on our websites (www.samarang.lu). You can also request a copy of the present policy and web policy from the CO. Both policies set out information about our processing of personal data to a wide range of other individuals, including visitors to our websites and premises, suppliers, transaction counterparties, other business partners and regulatory and other governmental agencies. We take 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 where practicable you should direct attention (or, at least, the attention of the organisations that they represent) to this published policy. You should note, 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 we have collected data to satisfy anti-money laundering obligations, then we should not use that data for general marketing purposes.

Generally, you should only process personal data if:

- the processing is **necessary** for the purposes of the legitimate interests that Samco pursues (and by "**necessary**" we mean 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.

We 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, we will not process personal data unless it falls within a lawful reason for processing. Our Data Protection Protocol sets out further information on this.

7 SENSITIVE PERSONAL DATA

You 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).

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

Samco will notify you 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 your 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. Your Personal Data will only be disclosed to such service suppliers if Samco has deemed, in its reasonable opinion, that such service providers offer appropriate guarantees with regard to confidentiality, security and protection of your Personal Data.
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 your 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.
Your Personal Data will be deleted when:

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

10 INTERNATIONAL DATA TRANSFER

Where you or we are transferring personal data from inside the European Region to outside the European Region you or we should consider whether this is restricted under the GDPR.
We shall put in place an international data transfer agreement (IDTA), as and when needed, which governs transfers between Samco's offices. This means personal data can be transferred globally around our offices under the terms of the IDTA. Transfers of personal data to entities (other than Samco offices) outside the European Region 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 Region 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, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) 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).

In the context of the Brexit and given the connection of SAMCO with the United Kingdom, we anticipate the European Commission will consider UK as providing adequate protection. It is indeed foreseen UK will ensure alignment between GDPR rules and its data protection act.

If you have any questions or concerns about the transfer of personal data outside the European Region please contact the CO.

11 CONSENT

We do not generally rely on consent as the basis for processing personal data. There may be some exceptions e.g. we consider that individuals who actively sign up to receive our technical material on the fund and its performance (fact sheet) are doing so on the basis of consent. You 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**. Our Data Protection Protocol sets out further information on this.

12 KEEPING PERSONAL DATA UP TO DATE AND ACCURATE

Where we process your personal data, you 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 you should inform us if your personal information needs to be updated. You should also make sure you keep personal data you hold on other people, e.g. investor records, up to date and accurate. This applies to HR data kept with the person in charge of HR matters and processes.

13 DATA SECURITY

We are obliged to report certain breaches of security affecting personal data to competent data protection authorities. It is important you 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)

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

14 DATA SUBJECT RIGHTS

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

You (or they) may also have the right, in certain circumstances to require us, without undue delay, (a) to delete your (their) personal data; (b) to "restrict" our processing of your (their) personal data, so that it can only continue subject to very tight restrictions; and (c) to require personal data which you (they) have provided to us, and which are processed based on your (their) consent or the performance of a contract with you (them), to be "ported" to you (them) or a replacement service provider.
If you receive a communication from any data subject in which he or she seeks to exercise any of these rights, that communication should be passed to HR and the CO as soon as is reasonably practicable. You 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 the European Region, namely the CNPD (Commission Nationale pour la Protection des Données). 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 withing 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).

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. You are therefore advised to review it from time to time for any possible changes.

18 QUESTIONS

If you have any questions about this policy speak to Corinne Piret (Conducting Officer in charge of compliance also acting as Compliance Officer) and Phu-Van Luc (Conducting Officer in charge of HR matters).

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

ANNEX 1 Data Protection Protocol

ANNEX 2 Data Protection Web Policy

ANNEX 3 CNPD - Data breach notification form