AML/ KYC POLICY
and
CLIENT DUE DILIGENCE

Responsibility & Approval

Version:	1.0
Overall responsibility:	CEO
Approved by the Board of Directors in its meeting of:	01.09.2025

Document management

Document owner

Name	Function	Date
Louiza Savchenko	Compliance	01.09.2025

Versions

Version	Date	Status	Author/editor
1.0	01.07.2025	approved	Thomas Heinig

Revisioning history:

Version	Description
1.0	Implementation of the AML/KYC Compliance Policy

MK Global Kapital

TABLE OF CONTENTS

I. OVERVIEW

1. INTRODUCTION

The purpose of this anti-money laundering and know your customer (AML/KYC Policy, the "Policy") is to implement best practices and various legal provisions defined in the Luxembourg and international legal framework aiming at combatting Money Laundering and Financing of Terrorism, in particular, Law of 12 November 2004 "On the fight against money laundering and terrorist financing" (as amended) to MK Global Kapital (" MKG") and the securitization funds and companies represented and managed by MKG , in particular, ALTERNATIVE ("ALT"), and Mikro Kapital Investment S.A. ("MKISA"), (together – the "Entities").

This Policy applies to all Entities and to all employees, officers, directors and independent directors, if any, and contractors of the Entities. It is particularly relevant to those who are engaged in business development, relations with current and potential investors ("Investors") and those involved in the acceptance or processing of new investments. Non-compliance with the Policy is a serious matter which could result in disciplinary action, including dismissal in the case of an employee, termination of engagement in the case of contractors, or withdrawal of a mandate from an officer or director. Financial organizations that receive investment proceeds from the securitization funds are required to develop and implement an AML/KYC Policy in accordance with their domestic laws and regulations, while also taking this Policy into account ("Other Companies").

2. PURPOSE OF THIS POLICY

The purpose of this Policy is to establish rules in relation to the anti-money laundering and combatting the terrorist financing, in particular, in view of the risk assessment, the minimum requirements know your customer standards ("KYC"), in particular, customer due diligence ("CDD") and on-going due diligence standards to be applied across the Entities and Other Companies to ensure they know their customers and counterparties and play their respective part in combatting money laundering and financing of terrorism. This policy also sets forth the rules relating to know your assets standards ("KYA"). Furthermore, this policy stipulates the rules governing internal controls, reporting and cooperation and record keeping.

II. SCOPE OF THE POLICY

The Policy applies across the Entities and covers all business relationships and relationship with investors, both new and existing.

Wherever such services are being provided, the standards set out in this Policy must be applied.

The standards are to be applied at both the start of relationships with customer and counterparties, and on an on-going basis throughout the duration of the relationship with customer.

CDD is not only related to obtaining identification documents of persons and companies, and for the purposes it encompasses all the activities involved in:

- KYC; and
- Understanding the activities of the customer and counterparties.

Risk Management together with Legal and Compliance officers are responsible for developing and implementing, as necessary, supplementary policies, procedures and processes to ensure continuing compliance with this Policy as well as other applicable regulatory requirements.

The collection of information and documents for the performance of the initial and on-going CDD is performed at MKG by middle office supported by the sales team ("Counterparty Manager").

The Policy does not cover detailed process or procedures in relation to CDD, or other more general aspects of the Anti-Money Laundering and Counter Terrorist Financing (the "AML/CTF") regulatory framework including the reporting knowledge or suspicions of money laundering or terrorist financing or record keeping requirements.

III. DEFINITION OF THE COUNTERPARTY

For the purposes of this Policy the term "Counterparty" should be interpreted in its broadest sense. It relates to:

1. The persons or companies investing in debt or equity securities of the Entities ("Investors").
2. Any other business counterparties of the Entities, including services and goods providers, clients, as well as sponsorship and donations subjects.
3. Other Companies granting micro loans/microfinance products (including car sharing and leasing) to their clients.

It further relates to parties associated with the above-mentioned counterparties including, but not limited to, those who are:

- The ultimate beneficial owner(s) or UBOs of the counterparties, i.e. the natural person(s) who ultimately owns or controls the entity or on whose behalf the legal arrangement has been established;
- The controller(s) of the counterparties, being those individuals or entities who ultimately control or exercise control over the entity or arrangement (whether alone or with any other person or persons), e.g. persons to whom powers of attorney have been granted, bank account signatories or persons in equivalent roles, co-trustees, external trustees, protectors, enforcers, etc.;
- Persons who could make a request to trustees, e.g. beneficiaries;
- Providers of initial and on-going wealth or funds into the investors where different from those above e.g. settlor or dedicator.

For the purposes of this Policy, the above parties are also collectively or individually referred to as "Verification Subjects".

IV. DOCUMENTED DUE DILIGENCE

Documented Due Diligence shall be performed for every new counterparty. For onboarding new counterparties and ongoing KYC/AML monitoring, the Entities and Other Companies shall use an appropriate and market standard KYC/AML software.

The passport verification and face authentication of new counterparties can be done either in a physical meeting with the Counterparty Manager or virtually (natural persons only). If it is done virtual, the counterparty receives a link to verify his/her identity (passport + face screening) via the KYC/AML software. No further certified copies would be needed.

V. RISK-BASED APPROACH

MKG applies a risk-based approach to identifying and managing potential risks of money laundering and terrorist financing. This means that MKG focuses its attention and controls on the areas of greatest relevance to its business, in particular its customers, investors and counterparties.

MKG considers the nature of its relationships and transactions to determine whether any present a heightened risk and, where appropriate, applies proportionate measures to address and mitigate such risks. This approach ensures that MKG's efforts are practical, consistent with the scale and nature of its activities, and directed toward areas where risk exposure is most significant.

The following table sets out the key risk factors that must, at minimum, be taken into account for the purposes of assessing counterparty risk:

Risk factors	Factors to consider
Counterparty specific risk	- Source of Wealth / Source of Funds (SoW/SoF) considerations - Politically Exposed Person (PEP) profile/status - Reputationally Exposed Person (REP) profile/status (i.e. individuals who are high profile or are in the public domain) - Regulatory profile/status - Whether the counterparty or connected parties are engaged in higher risk or sensitive activities, as set out in the Responsible Investment Policy - Other identified or potential risk indicators (transparency, behaviour of customer) - Counterparties on a sanction list as described in the Sanctions Compliance Policy - Negative press or social media release / Adverse media screening - Criminal prosecution - Insolvency / bankruptcy
Country risk	- Whether the counterparty or connected parties have a material relevant exposure to prescribed higher risk jurisdiction, as set out in the Responsible Investment Policy.
Product/Service risk	- Complexity of structure or associated planning advice - Use of excessively complex or opaque structures (e.g. bearer share companies, intensive cash payments, untransparent corporate structures) - Nature of services being provided - Nature and value of assets under administration
Delivery risk	- Frequency & nature of contact with customer - Whether services are delivered exclusively by post, telephone, internet etc. where there is no physical contact with the customer (non-face to face relationships)

When considering an onboarding of an investor for an Entity, it is important that MKG obtains sufficient reliable information on how the counterparty has amassed its wealth. This relates especially to the source of the money, or other assets being put into the structure SoF/SoW information and explanations may be obtained directly from the counterparty, from their advisors and/or other reliable (including open) sources. The extent to which such information needs to be independently corroborated will depend upon the particular counterparty's circumstances but the overriding requirement is that MKG should take reasonable measures to be satisfied as to the legitimacy of the origin of the wealth and have a clear and documented understanding of those activities that generated the counterparty's funds and property. Whilst not mandatory, a counterparty-signed Declaration of Source of Wealth / Source of Funds – supported on higher risk relationships by suitable corroborating evidence - should be obtained where appropriate.

Information and documents gathered as part of the CDD process need to be assessed and evaluated as part of a documented counterparty risk assessment. This risk assessment will typically be performed via two-step verification and documented at the serviced entity level (or, in the case of funds, as part of an investor risk assessment process), but should also take into account, and clearly evidence consideration of, any relevant risk factors that apply at the ultimate counterparty level.

- In cases where the level of AML/CTF risk is assessed to be **low**, it may be possible and appropriate to apply **simplified CDD measures**;
- In all cases where the AML/CTF risk is assessed to be standard or medium, the Group's Standard or medium CDD measures must be applied;
- In cases where the level of AML/CTF risk is assessed to be **high**, it will also be necessary to undertake **Enhanced Due Diligence (EDD) measures**.

1. LOW RISK RELATIONSHIPS – SIMPLIFIED CDD MEASURES

A common feature of many AML/CTF regulatory regimes is that regulated firms may in certain prescribed circumstances apply simplified CDD measures – for example, not having to perform full identity verification procedures where the counterparty itself (or its parent) is listed on a recognised public stock exchange and/or regulated by an appropriate authority in an equivalent jurisdiction. Taking advantage of such exemptions allows firms to remain competitive and to focus their AML/CTF resources and efforts on higher risk counterparties and relationships.

The Policy is therefore to apply simplified CDD measures where these are available under applicable local AML/CTF regulation. In common with most regulatory requirements, however, such measures should not be applied in cases where the level of AML/CTF risk has been assessed to be other than Low in accordance with section 5 above.

The application of the simplified CDD measures shall be discussed and agreed upon between the Counterparty Manager and the Chief Compliance Officer subject to any specific regulatory constraints –to determine and document the extent to which it needs to obtain CDD on employees of the relevant counterparty institution. For example, where a large, regulated institution has 20 authorised signatories or directors, the Counterparty Manager may decide to obtain CDD only on those individuals that have signed our letter of engagement and/or with whom it will deal with most often. For the avoidance of doubt, a copy authorised signatory list must be obtained.

Where permitted by local law/regulation and where the AML/CFT Risk Rating is "Low", CDD may also be obtained after the relationship has started subject to adequate controls being in place to ensure CDD is received and that transactions for the counterparty are limited and closely monitored until the required CDD is received/obtained in full.

2. STANDARD OR MEDIUM RISK RATED RELATIONSHIPS – MINIMUM CDD MEASURES

The Group's minimum CDD measures should be completed in all cases with a new or existing Counterparty.

MKG shall apply CDD measures in the following cases:

(a) when establishing a business relationship;
(b) when monitoring an existing business relationship, if circumstances indicate a need to update or refresh CDD information;
(c) when there is knowledge or suspicion of money laundering or terrorist financing, regardless of the amount involved;
(d) when there are doubts about the accuracy, adequacy or completeness of previously obtained identification data.

MKG shall apply CDD measures that include:

Customer identification and verification

Identifying the customer and verifying identity using reliable and independent documents, data or information (including electronic means where appropriate).

Beneficial ownership

Identifying and taking reasonable measures to verify the beneficial owner(s).

For legal entities, understanding the ownership and control structure and identifying senior managing officials where no natural person is identifiable as controlling owner.

For trusts or similar legal arrangements, identifying the settlor, trustee(s), protector (if any), beneficiaries (or class of beneficiaries), and any other person exercising ultimate control.

Purpose and nature of the relationship

Assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship.

Ongoing monitoring

Conducting ongoing monitoring of the relationship, including scrutiny of transactions to ensure consistency with MKG's knowledge of the customer, their business and risk profile, including source of funds where necessary.

Ensuring records are kept up to date and relevant.

Record-keeping

Retaining CDD documents and transaction records for at least five years after the end of the relationship or the date of the transaction.

Enhanced vigilance

Paying special attention to complex, unusually large or otherwise unusual transactions that have no apparent economic or lawful purpose.

In case MKG is unable to complete CDD, it shall not enter into or shall terminate the relationship and shall consider filing a suspicious transaction report with the competent authority.

The following table sets out the identity information that MKM's is required to gather for individuals (natural persons), companies/entities and express trusts, as well as acceptable verification documents for each type of person or arrangement. Guidance for other forms of entity (foundations, Anstalten, LPs Partnerships, pension funds, etc.) should be developed by MKM's Legal / Compliance as required.

Verification subject	Identify information to be obtained	Acceptable identity verification documents
Company	• Name of company / legal entity. • Any trading names. • Date and country of incorporation/registration. • Official identification number. • Registered office address. • Mailing address (if different). • Principal place of business/operations (if different). • Identity information for all directors. • Identity information for all UBO(s) and controllers with an interest of 25% or more in the capital of the company. • If the entity has no beneficial owners (i.e. Fund), or UBO cannot be identified, then ID (Identification Document/Passport etc.) for directors/ managing company shall be requested.	• Copy of an identification document such as a valid national identity card ("ID") or passport for applicable UBOs and directors • Certified copy of the Certificate of incorporation (or other appropriate certificate of registration or licensing) • Certified copy of the Memorandum and Articles of Association (or equivalent) • Printed on Customer's or Shareholder's letterhead or copy of share register. and Register of Directors & Officers • Latest audited financial statements or copy of such statements by a suitable certifier. • Subscription form, filled in and signed by the Counterparty (investor or its legal representative).
Private Individuals	• counterparty picture • counterparty signature • surname and first name • place and date of birth • nationality • residence • identification number (if any)	• A copy of current original passport taken by Counterparty Manager, or certified copy of passport (photograph valid for KYC software verification) • A copy of current national identity card taken by Counterparty Manager or certified copy of national identity card (photograph valid for KYC software verification) • A copy driving licence. To validate the residence:

		• A copy of a recent bank statement or utility or telecom bill or similar (within the last three months). • If needed, a letter of introduction confirming the individual's residential address from a regulated financial institution operating in a well-regulated country or territory. • Reliable electronic / online data sources (where permitted under applicable local regulation) • Documented record of visit to client's residence (where permitted under applicable local regulation) • Subscription form filled in and signed by the UBO or its legal representative (director).
Express Trust	• Name of trust. • Date of establishment. • Official identification number (e.g. tax identification number or registered charity or non-profit organisation number). • Correspondence address of trustee(s). • Identity of each trustee • Identity of settlor(s) • Identity of each beneficiary with a vested right • Identity of any other power holders (Protector, Enforcer etc)	• Identity verification documents for associated individuals in line with verification requirements for individuals, as above • Certified copies of the trust constitutive documents (or relevant extracts therefrom) confirming the name and date of establishment of the trust, the appointment of the trustee and nature of the trustee's duties

3. ENHANCED DUE DILIGENCE – HIGHER RISK RELATIONSHIPS

EDD measures must be performed in addition to the minimum CDD measures described at Section V above, in all cases where a high level of AML/CTF risk is assessed. EDD consists of more rigorous enquiries, information gathering and analysis to enable us to better understand the potential risks attached to counterparty relationships and take action accordingly. There are a number of reasons why a business relationship or one-off transaction might be assessed as higher risk, and accordingly a "one size fits all" approach to EDD will rarely be appropriate.

The nature and scope of EDD measures performed should be commensurate to the assessed level of risk and may include, for example:

- where the customer, or the customer's beneficial owner, is a PEP
- with a respondent institution from a non-EEA state;
- where the natural persons or legal entities is established in high-risk third countries[1]; and
- all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.
- Obtaining reliable information from other Counterparty Managers with which the counterparty has an existing relationship.
- Obtaining reliable information directly from the counterparty concerned, for instance by obtaining certified copies of corroborating SoW/SoF documentation such as contracts of sale, property deeds, salary slips, etc.
- Mandatory obtaining reliable information from the investor about the source of funds involved and counterparty's source of wealth.
- Where information is publicly available or available through subscription databases, obtaining reliable information from a public or private source about the source of funds involved and/or counterparty's source of wealth.
- Obtaining reliable information through financial statements that have been audited in accordance with generally accepted auditing standards.

Where counterparties have an AML/CFT Risk Rating of "Very High" or "High" Risk (or the equivalent risk rating for individual investors in funds administered) the relationship should not commence – nor should MKG hold itself out to be acting on behalf of the prospective counterparty with advisors, bankers etc - until all CDD and EDD measures have been satisfactorily completed, and all necessary internal approvals obtained. The related communication and received documentation are to be saved in an electronic folder.

VI. RELIANCE ON THIRD PARTIES AND OUTSOURCING CDD FUNCTIONS

4.1 Reliance on Third Parties

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R1675-20240207

In certain prescribed circumstances, the MKG may be entitled to rely on the CDD measures performed by third parties - e.g. where the counterparty is being introduced or intermediated by a third party which is regulated in an "equivalent" jurisdiction for AML/CTF purposes.

Counterparty Manager is entitled to rely on such third party arrangements where considered appropriate, providing always that any specific local regulatory or legislative requirements are met (for example, under many regimes, a condition of placing reliance upon third parties is that they are subject to a documented risk assessment by the person placing reliance, including regular ongoing testing for compliance with applicable AML/CTF requirements, and that the person upon whom reliance is placed provides a written undertaking that they hold, and will make available upon request, the underlying CDD records). In any event, any Counterparty Manager proposing to place reliance upon a third party in the performance of CDD measures must take reasonable steps to satisfy itself as to the adequacy of the third party's AML/CTF arrangements.

Reliance should not be placed upon third parties for counterparties that are assessed to present a High or Very High level of AML/CTF risk (or the equivalent risk rating for individual investors in funds administered), or in any situation where money laundering or terrorist financing is suspected. In addition, Counterparty Managers must remind staff that such exemptions only relate to obtaining certain documents, they do not exempt MKM from its other CDD obligations.

For investors subscribing to tokenised bonds issued by an Entity, MKG does not have a direct relationship with the investor. In such cases, CDD is performed by the relevant digital asset intermediary or cryptocurrency exchange through which the subscription is made.

4.2 Outsourcing of AML/KYC Functions

MKG has engaged Fundamentals S.A. ("Fundamentals"), a Commission de Surveillance du Secteur Financier (CSSF)-regulated *Professionnel du Secteur Financier (PSF)*, to perform CDD and related AML/CTF services on its behalf. Fundamentals is duly authorised by the CSSF and operates in compliance with the Luxembourg Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended, together with applicable EU regulations and guidance.

By outsourcing investor onboarding and monitoring functions to Fundamentals, MKG ensures that CDD, KYC and ongoing monitoring activities are conducted in accordance with Luxembourg regulatory requirements and international best practices. MKG remains ultimately responsible for compliance with AML/CTF obligations and exercises appropriate oversight over the outsourced functions.

VII. KEEPING CDD FILES UP-TO-DATE

This Policy applies to both new and existing counterparties. MKG shall have processes in place to ensure that the information and documents required from new counterparties are also obtained for the parties with an existing relationship. MKG must ensure that it understands the business of its customers.

CDD documentation that is held for existing counterparties and associated Verification Subjects should be subject to periodic review and, where necessary, update. As a minimum, existing CDD documentation should be reviewed and updated where at any time:

- There is reasonable ground to suspect money laundering; and/or
- There are doubts about the veracity or adequacy of documents, data or information previously obtained under applicable CDD measures.

Existing CDD documentation should otherwise be periodically reviewed as part of a regular, structured periodic review process and/or upon the occurrence of a relevant "trigger event". The frequency of periodic reviews should be determined under a risk-based approach and will typically be:

Risk profile	**Frequency of review**
Very High / High	Annual
Medium/Standard	Every two years
Low	Every three years

Counterparty Managers must also provide guidance as to what constitutes a "trigger event", i.e. circumstances where CDD held will be revisited to ensure that MKG continues to know its counterparties and understand their activities. Such triggers could also be used to update CDD (e.g. where CDD may not have been obtained historically to the standards required in this Policy).

The mere fact that an existing document has become out of date does not automatically means that updated documentation should be obtained. Provided that there have been no material changes in the Counterparty's identity information and/or their relationship with MKG, the Entities or Other Companies, then it will generally be acceptable to continue to rely on CDD documentation gathered at the inception of the relationship without needing to refresh (provided of course that such documentation meets current AML/CTF standards – for example, in terms of suitable certification requirements, quality/legibility of copy documents etc).

As a matter of best practice, however, Counterparty Managers need to request and obtain current valid passport copies (or equivalent) for each Verification Subject as and when these expire, as such documentation is in any event likely to be required to support the ongoing servicing or extension of the relationship with MKG or third-party financial services providers. Documentation must also be refreshed where expressly required in order to satisfy applicable local regulatory requirements.

Counterparty Managers must have processes in place to monitor transactions (both financial and non-financial) on an on-going basis. The objective of such monitoring processes is to allow for the timely and accurate identification of notable transactions or activity, i.e. those that:

- Are inconsistent with our knowledge of the counterparty (i.e. unusual transactions or activity);
- Are complex or unusually large;
- Form part of an unusual pattern; or
- Present a higher risk of money laundering or financing of terrorism.

Such transactions and activity should be subject to a heightened level of scrutiny or examination. For inwards fund flows, the Management Company will aim at ascertain the remitting bank account details (name and number of account) for any funds coming into the Entities. The Management Company must ensure that the money is coming from the anticipated source. Otherwise, additional inquiries are to be performed and potentially consider additional CDD requirements on this new Investor. If the result is unclear, the funds will not be accepted and returned to the remitter.

Monitoring processes should as much as possible be automated and remind staff to be vigilant for unexpected changes in relationships, third parties and transactions. Staff need to be mindful of receipts from and payments to parties who are third parties to the transaction and ensure that they understand the reason for such receipts and payments and record proper explanations in these circumstances.

In addition, Counterparty Managers, together with Compliance must remind staff of the distinctions between money laundering and terrorist financing in terms of money flows. Money

laundering involves the proceeds of crimes which have already taken place. Terrorist financing may also involve the proceeds of crime, but equally it may involve completely clean funds. In terrorist financing situations, it is the destination of the funds which is of primary importance as they may be used to finance future terrorist acts, organisations, resources and support networks.

Also, Counterparty Managers must remind staff that the value of funds involved in terrorist financing is different from money laundering. To undertake a terrorist act, does not necessarily involve large sums of money. Enhanced CDD and monitoring processes should not therefore be limited to higher value transactions.

Counterparty Managers are required to have processes in place for tracking counterparties with outstanding CDD and for considering the action to be taken where CDD is found to be deficient and not forthcoming. Such processes must include recording how long the CDD has been outstanding, what the related AML/CFT Risk Rating is and what is being done to obtain the CDD. Such records must be reviewed frequently by the Counterparty manager's senior management. Where CDD is outstanding for an individual who is associated with more than one serviced entity the highest AML/CFT Risk Rating should be shown.

If CDD has been long outstanding despite MKG's repeated efforts to obtain it especially for serviced entities with a "Very High" or "High" AML/CFT rating (or the equivalent risk rating for individual investors in funds administered), Counterparty Managers must report to the MKG and the latter shall consider what action needs to be taken, which may include suspending non- essential services to the counterparties, making a report to the appropriate authorities and ultimately termination of the relationship.

VIII. COOPERATION WITH AUTHORITIES AND REPORTING OF SUSPICIOUS ACTIVITY

MKG is committed to cooperating with competent Luxembourg authorities responsible for the prevention of money laundering and terrorist financing.

All officers and employees must promptly escalate to the Chief Compliance Officer any knowledge, suspicion or reasonable grounds for suspicion that a counterparty, investor, or transaction may be connected to money laundering or terrorist financing. Such internal reports should be accompanied by any supporting information or documentation available.

The CCO is responsible for reviewing such reports and shall escalate substantiated suspicions to the Management Board. Where relevant to MKG's securitisation fund or other regulated structures, the Management Board will ensure that appropriate reports are made to the Financial Intelligence Unit (FIU) through the responsible regulated entity or service provider (e.g., Fundamentals S.A.).

MKG prohibits "tipping off," i.e. disclosing to a customer or third party that an internal report has been made or that an investigation may be underway. No adverse action shall be taken against staff who, in good faith, report suspicions internally.

IX. TRAINING

MKG has a continuing responsibility to ensure that all persons subject to this Policy shall comply at all times with all applicable AML/CTF legislation and regulation as well as with this Policy.

Compliance must ensure that all relevant staff receive regular training, on their CDD procedures, processes and controls. Records of this training must be retained which must contain as a minimum detail:

- Date of training;
- Name of person who participated in the training;
- Provider of the training; and
- Overview of content.

X. GOVERNANCE

MKG shall maintain this Policy and related procedures to mitigate and manage effectively the risks of money laundering and terrorist financing, in a manner proportionate to the nature, complexity and size of its activities.

The Chief Compliance Officer shall have access to all necessary identification data, due diligence information, transaction records and other relevant information, and shall report directly to the CEO.

MKG shall establish procedures allowing employees to raise concerns regarding potential breaches of AML/CTF obligations, with appropriate safeguards for confidentiality and protection against retaliation.

This Policy shall be reviewed annually by Compliance and approved by CLO, before submission to the MKG´s Board of Directors.