

AIFM CAYROS CAPITAL INVESTMENT MANAGEMENT LTD



82 Acropoleos Avenue
1st Floor
2012 Akropolis,
Nicosia, Cyprus
T: +357 22 107 242

Version dated: 23/01/2026

Regulated by the Cyprus Securities & Exchange Commission (License# AIFM11/56/2013)

Contents

BEST EXECUTION POLICY.....	3
CLIENT COMPLAINT HANDLING POLICY	12
DATA PRIVACY POLICY	18
CONFLICT OF INTEREST POLICY	40
SFDR Disclosure	51

BEST EXECUTION POLICY

1. Introduction

Following the implementation of the Markets in Financial Instruments Directive 2014/65/EU ("MiFID II") and in accordance with the provisions of the Investment Services and Activities and Regulated Markets Law of 2017 (the "Law") of the Cyprus Securities and Exchange Commission ("CySEC"), AIFM Cayros Capital Investment Management Limited (the "Company") is required to establish Best Execution Policy (the "Policy") and take all reasonable steps to obtain the best possible result ("Best Execution") on behalf of its clients.

The purpose of this policy is to provide a sound, transparent and comprehensive best execution framework for AIFM Cayros Capital Investment Management Limited (the "Company"). This framework covers all material aspects of the best execution processes, procedures and controls in respect of each relevant Alternative Investment Fund (AIF) managed by the Company as the Alternative Investment Fund Manager (AIFM), as well as in respect of each client, Investment Portfolios of which managed by the Company as Portfolio Manager under Markets in Financial Instruments Directive 2014/65/EU ("MiFID II").

The Policy describes the way that the Company will achieve the best possible results for its clients by taking into consideration the provisions of the Delegated Regulation (EU) 2017/565 and onward amendments including information that must be provided to clients and potential clients in relation to the execution criteria and factors considered when trying to obtain best possible results on a consistent basis.

During management of investment portfolios of its clients, the Company will take all reasonable steps to achieve best execution. The Company applies processes which are designed to take all sufficient steps, as required under MiFID II Article 27, to obtain the best possible execution result on a consistent basis, subject to and considering the Financial Instrument subject to the order, the nature of the orders and the execution venues (on reasonable commercial terms) available for such Financial Instruments. The Company will generally give price a higher relative importance when obtaining the best possible result for orders executed. However, the Company may also take into consideration a range of different factors, including the need for timely execution, availability of price improvement, the liquidity of the market (which may make it difficult to execute an order), potential price impact, the size of the order, the nature of the financial transaction (including whether or not such transactions are executable on a regulated market, over the-counter, or via either route) and the quality and cost effectiveness of any related clearing and settlement facilities.

This policy serves the following purposes:

- act in best interests of AIFs and investors, as well as other clients through implementation of effective arrangements for ensuring that all activities of the AIFM are carried out in compliance with the legal requirements.
- act in best interests of the Company's shareholders by creating new business opportunities by satisfying current and attracting potential clients with our solid best execution framework; and
- act in best interests of the regulator by fulfilment of regulatory requirements.

2. **Scope**

The Policy applies to professional clients/investors, as well as well-informed investors, when providing the investment services of:

- a) Collective portfolio management, and
- b) Individual portfolio management.

The Company's Best Execution obligations do not extend to Eligible Counterparties, as per Article 30(1) of MiFID II.

This Policy applies to the following assets:

- Equities
- Bonds
- Money Market Instruments
- Exchange Traded Derivatives
- OTC (Over the counter) Derivatives
- Forward Foreign Exchange
- Collective Investment Schemes

3. **Best Execution Factors & Criteria**

It should be noted that the Company is authorised to provide only Portfolio management services. The Company does not perform receiving and transmitting clients' orders. All investment decisions are made by the Portfolio Managers of the Company independently.

During portfolio management the Company takes into account multiple Execution Factors, in order to obtain the best possible result for its clients, such as:

- Price
- Costs (direct or indirect)
- Speed of execution
- Likelihood of execution
- Likelihood of settlement
- Size of the trade
- Nature of the trade
- Any other considerations relevant to the execution of an order (e.g. prevailing market conditions).

The weighting of each factor depends on the specifics of the individual investment and is determined by the portfolio manager on a case-by-case basis.

When the Company executes a trade on behalf of an AIF, the Company will determine the relative importance of the aforementioned best execution factors based on the experience and judgement, per product type, with respect to available market information at the time and taking into account the following Best Execution Criteria:

- The characteristics of the fund (including its categorisation)
- The characteristics of the fund trade/order
- The characteristics of the financial instruments which are the subject of the fund trade/order
- The characteristics of the execution venues to which the fund trade/order can be directed.

In relation to Individual portfolio management, the Company determines the relative importance of the aforementioned Execution Factors by taking into account the characteristics of the following Execution Criteria:

- The client, including the categorisation of the client (as retail or professional),
- The characteristics of the trade/order against the client's Portfolio,
- The characteristics of the financial instruments that are the subject of that trade/order, and
- The characteristics of the Execution Venues to which the trade/order can be directed.

The process by which the Company performs this assessment depends on the specifics of each case. The Company's execution obligations will be discharged in a manner that considers the different circumstances associated with the execution of the order as they relate to the financial instruments involved.

Price and costs will ordinarily be of high relative importance in obtaining best possible results. However, in some circumstances, reference to the Execution Criteria may appropriately determine that other Execution Factors have greater importance in achieving the best possible result for the client.

The relative importance of the execution factors considered by the Company to obtain the best possible result for its clients are depicted in Annex 1 of the Policy.

4. Execution Venues

"Execution Venues" are the locations (with or without a physical presence) such as:

- Regulated Markets,
- Multilateral Trading Facilities,
- Organised Trading Facilities,

- Systematic Internalisers,
- Market Makers,
- Liquidity Providers or any other entity that facilitates trading of Financial Instruments.

The Company will, as a matter of principle, transmit orders to another broker or dealer for execution on trading venues (the Company will not access trading venues directly), in which case we will either determine the ultimate execution venue itself on the basis described above, and instruct the other broker or dealer accordingly, or we will satisfy ourselves that the other broker or dealer has arrangements in place to enable us to comply with our best execution obligations.

A list of the Execution Venues and intermediaries (third party brokers) used by the Company for the execution of client orders in respect to each class of financial instruments can be found below:

Approved Execution Venues:

The factors relevant to the Company for selecting Execution Venues include the following:

- Reliability of intermediary;
- Reputation, financial strength and stability;
- Access to primary and/or secondary markets;
- Ongoing reliability;
- Overall costs of a trade including commissions, mark-ups, markdowns or spreads;
- Electronic connectivity; and
- Willingness to execute difficult transactions

In addition, the following conditions must be met before Execution Venues can be approved:

- Licensed, as required, to execute the type of transaction; and
- Supervision by national authorities.

The Company reserves the right to use other Execution Venues, where deemed appropriate, in accordance with the execution policy and may add or remove any Execution Venues from this list.

5. **Selecting an Execution Venue**

Subject to proper consideration of the Execution Criteria and Execution Factors referred to above, where there is more than one competing Execution Venue to execute an order for a financial instrument, the Company shall assess and compare the results for the client that would be achieved by executing the order on each of the Execution Venues.

The Company will transmit orders to those execution venues that it deems sufficient to provide the best possible result based on comparable venue information. Subject to any specific instructions, in meeting the best execution obligation to take all sufficient steps to obtain on a consistent basis the best possible result for the execution, the Company considers the following execution venues as appropriate:

- Regulated Markets ("RM");
- Multilateral Trading Facilities ("MTF");
- Organised Trading Facilities ("OTF");
- Systematic Internalisers ("SI");
- An entity which performs a similar function in a third country to the functions performed by any of the foregoing outside the EEA which are regulated according to their local rules.

However, the decision to use any of the Execution Venues may also be influenced by other additional criteria, although this is always conditional upon obtaining the best possible result for the Company's AIFs.

These additional criteria include:

- Quality of research
- Financial screening
- Suitability of counterpart
- Liquidity concentration

Notwithstanding the above, the Company reserves the right to execute its order using a venue other than the methods or venues that are indicated, where the Company considers this to be in the best interests of its AIFs. In such cases, the Company will endeavour to execute based on the same best execution principles as summarised in this Policy.

Pursuant to MIFID II, since the transactions are executed outside of the trading venue (i.e. OTC), the Company will monitor and check the fairness of the price by collecting market data used in the estimation of the price of such products, and in cases that is possible, compare with comparable or similar products. The determination of the relevancy of any similar products or markets will be solely at the Company's discretion, when assessing and monitoring the fairness of price and may choose different markets for different products or circumstances.

6. **Broker Selection and Assessment**

The Company's policy seeks to achieve the best possible result for the Funds and clients' Portfolios managed by the Company by ensuring that brokers and other intermediaries used for trade execution take all sufficient steps to provide best execution, in accordance with Article 27 of MiFID II. The Company conducts due diligence on potential brokers, which includes an evaluation of their Best Execution Policy, operational capabilities, financial standing, and execution strategies.

Prior to selection, brokers must demonstrate that:

- Their execution practices are aligned with MiFID II standards;
- Their systems support Transaction Cost Analysis (TCA) and other execution quality monitoring tools.

Ongoing Review of Broker Execution Quality

The Company will regularly review the execution quality of its brokers and execution venues through a structured monitoring framework.

This includes:

- Transaction Cost Analysis (TCA): Comparing the execution price against market benchmarks, arrival price, and post-trade slippage.
- Execution Performance Meetings: Internal reviews and meetings with brokers to discuss past performance and improvements.

Methodology and Documentation

The methodology used to monitor execution quality includes:

- Evaluating the cost and effectiveness of execution, including spreads and commissions;
- Periodic validation of TCA assumptions and tools.

7. **Broker Selection and Assessment**

The Company's policy seeks to achieve the best possible result for the Funds and clients' Portfolios managed by the Company considering the execution policy of the broker. The Company monitors the execution quality of entities used and examine the execution approaches of these entities prior to selection. Therefore, the execution policy provided by the Broker must be consistent with the Company's Execution Policy. The Execution Policy of the broker must enable the Company to satisfy its obligations on Best Execution.

The Company will ensure by requesting a copy of the brokers Best Execution Policy that the selected brokers have appropriate arrangements in place to enable the Company's requirement of best execution to be accomplished. This review is carried out by Compliance Department.

For new counterparties / brokers through whom the Company wishes to execute security transactions on behalf of the Company's Funds under management the broker on-boarding process (KYC) applies.

8. Client Order

It should be noted that the Company does not execute a client order. All investment decisions are made by Portfolio Managers of the Company.

9. Order Aggregation

The Company is required to execute(transmit) orders in an expeditious and fair manner for all AIFs. Orders will be aggregated with other orders, if:

- the characteristics of the order make them suitable for aggregation and
- in the Company's opinion the aggregation of orders will not work to the disadvantage of any AIF and
- it complies with its order allocation procedures.

Where the Company aggregates an order with one or more other client orders and the aggregated order is partially executed, it shall allocate the related trades in accordance with its order allocation policy.

It should be noted that orders from the Collective portfolio management and orders from Individual portfolio management are not subject to aggregation. They are strictly segregated. The strict rule of the Chinese Walls applies here.

10. Bundling of Orders

The Company can bundle buy or sell orders for several investment Funds and submit them for execution as a block order if the order volume, type of security, market segment, current market liquidity and price sensitivity of the securities to be traded make this appear advisable in the respective client's interest.

Orders will be bundled only if it is improbable that individual clients/investors will be disadvantaged. All managed portfolios must be treated in a non-preferential manner such that no single portfolio may be systematically favoured over another. The allocation of orders cannot be based upon the client's account size, identity, performance and / or fee structure. In determining the suitability of each investment opportunity to a portfolio, consideration will be given to several factors, the most important being the client's investment objectives and strategies, investment guidelines, existing portfolio composition and cash levels. Having considered these factors and prior to executing any transactions, the Company will determine the allocation of an order for each portfolio.

11. Publication obligations

The Company will summarize on an annual basis, for each class of financial instruments, the top five execution venues in terms of trading volumes where they execute orders in the preceding year and information on the quantity of execution obtained. The summary must be in line with the provisions of the Delegated Regulation (EU) 2017/576 and includes among others:

- a) Information on the class of financial instrument;
- b) Venue name and identifier; and
- c) Volume of client orders executed on that execution venue expressed as a percentage of total executed volume.

12. Request to demonstrate best execution

Upon reasonable request from a client, and provided that the order was subject to the requirements of this Policy, the Company will demonstrate to the client that it has been executed its order in accordance with this Policy.

In the absence of evidence, the records of the Company will constitute conclusive evidence to the actions taken by the Company to obtain best execution on behalf of its clients. The Company keeps records in relation to the best execution requirements, including records of its trading activities and versions of this Policy, for a period of five years in accordance with record-keeping requirements under MiFID II.

13. Monitor and Review

The Company will monitor on a regular basis and the effectiveness of this Policy, and the execution quality of the procedures explained in this Policy, making any changes where appropriate.

In addition, the Company will review and assess this Policy at least once a year.

Annex 1: Relative importance of best execution factors

Complex instruments			
Retail clients**		Professional clients	
Execution factors*	Importance*	Execution factors*	Importance*
Price	1	Price	1
Likelihood of execution and settlement	5	Likelihood of execution and settlement	5
Size of order	4	Size of order	4
Costs	2	Costs	2
Speed of execution	3	Speed of execution	3
Nature of order	6	Nature of order	6
Any other consideration relevant to the execution	7	Any other consideration relevant to the execution	7

* 1 is the most important factor and 7 the least important one

** Not applicable for this moment due to the fact that the Company does not work with Retail clients

CLIENT COMPLAINT HANDLING POLICY

1. Introduction

AIFM CAYROS Capital Investment Management Ltd (hereinafter called the "Company") established, implements, and maintains effective and transparent procedures for the reasonable and prompt handling of complaints received from clients or potential clients, and to keep a record of each complaint and the measures taken for the complaint's resolution.

According to the Complaint Handling Rules, the Company must deal with any expression of dissatisfaction about any financial services activity provided or withheld by the Company.

The Company is committed to providing the highest quality of service to all its clients. If a client is not satisfied with the quality of service provided, they have the right to complain. The Company will respond to all complaints promptly in a fair and confidential manner. The Company will keep a record of the complaints received and the measures taken for their resolution.

The Company will monitor complaints and the outcomes in order to improve the quality of service provision. The Compliance Department will monitor the operations of the complaints-handling process and consider complaints as a source of relevant information in the context of its general monitoring responsibilities. The Compliance Department will analyse complaints and complaints-handling data to ensure that they identify and address any risks or issues.

The Company will ensure that no client will in any way be disadvantaged as a result of making a complaint. Clients and potential clients can submit complaints free of charge. The Company employees shall communicate with clients or potential clients clearly, in plain language that is easy to understand and reply to the complaint without undue delay.

To allow the Company to fully and fairly investigate a complaint, it would expect the client to make the Company aware of the cause of the complaint as soon as possible of the issue arising.

The Company is part of an efficient and effective complaints and redress procedures for the out-of-court settlement of consumer disputes regarding investment and ancillary services.

2. Procedure

This Client Complaint Procedure (the "Procedure") has been approved by the Board of Directors of the Company. The ownership and maintenance of this Procedure are the responsibilities of the Board of Directors of the Company, which shall ensure that it is

communicated to all of the Company's personnel on the purpose of its provisions to be followed literally during the provision of its services and activities. The Board of Directors shall also be responsible for updating the Procedure whenever deemed necessary.

The clients' complaints obligations fall under the Managing Director and the Compliance Officer responsibility, who examine any complaints received from clients.

Special file is dedicated to complaints and the Compliance Officer is responsible for recording on it of the customer complaint (the Complaints Register). Once the complaint is recorded, it shall never be deleted and hence the resolution of the issue needs to be followed through and documented.

The following details are documented

- The details of the identity of the customer who filed the complaint.
- The service to which the complaint refers to.
- The details of the employee that undertook to provide the service to the customer.
- The department or organisational unit to which the employee relates to.
- The date of receipt of the complaint.
- Details of employees that undertook to provide the service to the client.
- Department to which the relevant employee relates to.
- The details of the complaint – full description, including dates, figures, amounts, etc.
- The extent in financial terms of the potential loss that the customer claims he/she has suffered or as it is derived from the content of the complaint.
- The date and in summary, the content of the reply of the company to the said complaint.

It should be noted that a complaint cannot be accepted if it does not meet the above requirements. In such cases, the Company will contact the client and request that he/she corrects the complaint before it can be accepted.

The Compliance Officer and, if necessary, the Managing Director, will liaise with the appropriate department to resolve the issue. The Compliance Officer and, if necessary the Managing Director, should do their best in order to ensure that complaints are investigated fairly and possible conflicts of interest are identified and mitigated

The Compliance Officer and, if necessary the Managing Director, should register the complaints they receive on an internal register, as quickly as possible, and in an appropriate manner.

As soon as the Compliance Officer receives a complaint, the Compliance Officer should acknowledge the Complainant regarding the receipt of a complaint and provide written information regarding the Company's complaints-handling process.

Complaints may be submitted in writing, orally, by fax or by email at the contact details provided below:

1. Postal Address: 82 Akropoleos Avenue, 1st floor, Akropoli, Nicosia, CY-2012, Cyprus
2. By telephone: (+357) 22 107242
3. By Facsimile: (+357) 22 450775
4. By email: complaints@cayros.eu

All complaints shall be dealt by the Company's Complaint Handling Officer in accordance with the procedures set below:

- A. The Complainant provides the Company with the Complaint.
- B. The employee, who receives the Complaint, ensures that all the required details are provided. In case not all the details have been submitted, the receiver of the Complaint requests the Complainant to provide the missing data.

The following information should be provided:

- The details of the identity of the customer who filed the complaint.
 - The service to which the complaint refers to.
 - The details of the employee that undertook to provide the service to the customer.
 - The department or organisational unit to which the employee relates to.
 - The date of receipt of the complaint.
 - Details of employees that undertook to provide the service to the client.
 - Department to which the relevant employee relates to.
 - The details of the complaint – full description, including dates, figures, amounts, etc.
 - The extent in financial terms of the potential loss that the customer claims he/she has suffered or as it is derived from the content of the complaint.
 - The date and in summary, the content of the reply of the company to the said complaint.
- C. As soon as the Complaint is submitted, the employee immediately notifies the Compliance Officer and forwards the initial Complaint.
 - D. The Compliance Officer registers the Complaint in the Complaints Register and notifies the Complainant regarding the receipt of the Complaint and provides the Complainant with the Complaints' Handling Process of the Company. The Complainant should be also informed of the unique registration number of his Complaint.
 - E. The Company confirms, within five days, the receiving of the complaint to the complainant.

- F. The Compliance Officer gathers and investigates all relevant evidence and information regarding the complaint.
- G. Within 4 weeks from the date a complaint is received, the Company will send to the client a Final Response about the outcome/decision. During the investigation of the complaint, the Company informs the complainant of the handling process of his/her complaint.

Within 5 business days of the completion of an investigation a written report must be sent to the complainant explaining clearly:

- i. The outcome of the investigation.
 - ii. The nature and terms of any offer of settlement which the Company is prepared to make in satisfaction of the complaint.
 - iii. The reasons for declining to offer a settlement.
 - iv. A statement of the fact that the Company will treat the complaint as settled if the complainant does not indicate dissatisfaction within one month of receiving the report.
- H. If it is NOT possible to resolve the complaint within this period, a letter of acknowledgement should state that the complaint is under investigation and the reasons for the delay and when the Company expects to be able to contact the customer again and send a final letter with the outcomes of the investigation.
 - I. In case the investigation is not concluded within two (2) months following the submission of the complaint, the complainant will be informed in writing of the reasons for the delay and when he should expect completion of the investigation process (this period will not exceed three (3) months from the submission of the complaint).
 - J. When a final decision does not fully satisfy the complainant's demands, the Company should notify in writing the complainant using a thorough explanation of its position on the complaint and set out the complainant's option to maintain the complaint e.g. through the Cyprus Securities and Exchange Commission, the Financial Ombudsman, ADR Mechanism, or the relevant Courts.

The details of the Financial Ombudsman of the Republic of Cyprus are:

Address: 13 Lord Byron Avenue, 1096 Nicosia

Phone: +357 22848900

Facsimile (Fax): +357 22660584, +357 22660118

E-mail:

- Complaints: complaints@financialombudsman.gov.cy
- Financial Ombudsman: fin.ombudsman@financialombudsman.gov.cy
- Website: <http://www.mcit.gov.cy/ccps>

The details of the Cyprus Securities & Exchange Commission are:

Address: 27 Diagorou Street, 1097 Nicosia

Telephone: +357 22506600

Fax: +357 22506700

E-mail: info@cysec.gov.cy

<https://www.cysec.gov.cy/en-GB/complaints/how-to-complain/>

<https://www.cysec.gov.cy/en-GB/investor-protection/how-to-complain/ref/>

Note: The Company shall cooperate with the Cyprus Securities and Exchange Commission and/or the Financial Ombudsman in case they carry out their own investigation in relation to a client's complaint.

- K. Once the issue has been resolved the Compliance Officer documents the resolution of the complaint, inputs in to the system/register a closed status for the complaint, indicating description of taken actions.
- L. The Compliance Officer shall on an on-going basis analyse complaints-handling data, to ensure that the Company's employee identify and address any recurring or systemic problems, and potential legal and operational risks.

3. Internal Complains Register

As soon as the Company receives the complaints, the Compliance Officer must register it in an internal register with an appropriate manner, as well as for easy reference and retrieval, the Company should apply the following:

Upon receiving the complaint, the Compliance Officer must register the complaint directly to an internal register, giving it a unique reference number.

The unique reference number must be consisted of ten digits:

- The first two digits are the code of the Company regarding the Transaction Reporting System - TRS (click here for the TRS code),
- The following four digits define the year, and
- The last four digits denote the number of each complaint serial number (e.g. for 2022 - AI20220001, AI20220002, for 2023 - AI20230001, AI20230002).
- The unique reference number is communicated to the complainant.
- The Company informs the complainant that he should use the said reference number in all future contact with the Company, the Financial Ombudsman and/or the CySEC regarding the specific complaint.

4. **Documentation**

The Company will maintain all resolved complaints with notes for a minimum period of 5 years after the termination of the business relationship. The electronic form of the client's complaint once the complaint is recorded will also be saved.

The compliance's function risk-based monitoring programme shall take into consideration all areas of the firm's investment services, activities and any relevant ancillary services, including relevant information gathered in relation to the monitoring of complaints handling.

The Compliance Officer shall report to the management body, on at least an annual basis, on the implementation and effectiveness of the overall control environment for investment services and activities, on the risks that have been identified and on the complaints-handling reporting as well as remedies undertaken or to be undertaken.

DATA PRIVACY POLICY

DEFINITIONS

Regulation/Law/Applicable Regulations/ GDPR (EU) 2016/679 is a legal framework in the European Union (EU) addressing data protection and privacy for individuals within the EU and the European Economic Area (EEA). It became effective on May 25, 2018. In conjunction with other regulations pertaining to the recording of personal data, the GDPR is complemented by Cyprus Law, specifically Law 125(I)/2018, which is designed to safeguard the rights of natural persons in the processing of their personal data and facilitate the unrestricted movement of such data.

Personal data - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person 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 - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Restriction of processing - means the marking of stored personal data with the aim of limiting their processing in the future;

Controller - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data controller - means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor/ Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient - means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the

processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Personal data breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

INTRODUCTION

The General Data Protection Regulation ("GDPR") (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA), it came in force as from 25/05/2018.

On 31 July 2018 Cyprus Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), was published in the official gazette of the Cyprus Republic. The law was adopted for the effective implementation of certain provisions of the Regulation (EE) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (GDPR), which applies as of 25 May 2018.

Data protection as a fundamental right, Respect of the fundamental rights and freedoms, Directive 95/46/EC harmonisation, Data protection in balance with other fundamental rights, Cooperation between Member States to exchange personal data, Ensuring a high level of data protection despite the increased exchange of data, The framework is based on control and certainty, Adoption into national law, Different standards of protection by the Directive 95/46/EC, Harmonised level of data protection despite national scope, Harmonisation of the powers and sanctions, Authorization of the European Parliament and the Council.

While GDPR preserves many aspects of the Directive 95/46/EC, it imposes changes designed to address the realities of evolving, digital world while increasing the level of accountability for organizations processing personal data.

AIFM CAYROS CAPITAL INVESTMENT MANAGEMENT LTD (“Company”) is committed to ensuring compliance with GDPR across all products and services and in how Company manages the client relationships. Company knows, that the clients are focused on matters of data privacy and security, and this overview is designed to give insight and visibility into the GDPR program.

Company hereby notifies the Client, that: AIFM CAYROS CAPITAL INVESTMENT MANAGEMENT LTD, acting as data controller, may process information about the Client, the Client’s directors, officers, employees, affiliates, agents, which may constitute personal data under the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing personal data and on the free movement of such data (“Personal Data”).

This Policy has been approved by the Board of Directors of the Company. The ownership and maintenance of this Policy are the responsibilities of the Board of Directors of the Company, which shall ensure that it is communicated to all of the Company’s personnel on the purpose of its provisions to be followed literally during the provision of its services and activities. The Board of Directors shall also be responsible for updating the Policy whenever deemed necessary.

What is personal data and what constitutes personal data?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

The GDPR applies to ‘personal data’, meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law.

Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible.

The law protects personal data regardless of the technology used for processing that data – it’s technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria (for example alphabetical order). It also doesn’t matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data

- a name and surname;

- a home address;
- an email address such as name.surname@Company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- the advertising identifier of your phone;
- other data, which could be a symbol that uniquely identifies a person.

Examples of data not considered personal data

- a Company registration number;
- an email address such as info@Company.com;
- anonymized data.

THE COMPANY'S GDPR POLICY SETS OUT RELEVANT INFORMATION REGARDING:

- collection and creation of Personal Data by the Company
- the categories of Personal Data Processed
- the lawful basis for such processing
- the purposes of such processing
- the disclosure of Personal Data to third parties
- the international transfer of Personal Data
- the data security measures applied by the Company
- the Company's compliance with the principles of data accuracy, data retention and data minimisation
- the rights of Data Subjects
- the contact details for enquiries and the exercise of data protection rights.

THE OBJECTIVES OF GDPR POLICY:

- Explain the GDPR Requirements.
- Provide affected individuals with detailed information about the categories of personal data collected and processed by the Company, along with the purpose of processing (e.g., providing services to the Client, complying with applicable law, etc.).
- Offer information about third parties to whom the Company may disclose personal data (e.g., other members of the group, service providers, law enforcement agencies).
- Clarify the principles that the Company adheres to in its processing activities, including data security, data accuracy, and data minimization.
- Provide affected individuals with information about their rights (e.g., the right of access to data, the right to object to processing, and the right to deletion), along with an explanation of how these rights can be exercised. The key aim behind these objectives is

to offer individuals a detailed, clear, and transparent explanation of what the Company does with their personal data and why it does so.

PROCESSING PERSONAL DATA

What constitutes data processing?

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

Examples of processing that is used in the Company

- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data (for ex.: World Check);
- shredding documents containing personal data;
- storing IP addresses or MAC addresses;
- phone recording;
- disclosure of personal data to third parties.
-

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions, and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Personal Data collection

Company collects Personal Data about the clients/counterparties and its employees from a variety of sources as follows:

- Company obtains the Client's/counterparty's Personal Data, when the Client/counterparty provides it to Company (e.g. via email, telephone, or by any other mean)
- Company obtains the Client's/counterparty's Personal Data in the ordinary course of the relationship with the Client/counterparty (I the course of managing transactions)
- Company obtains the Client's/counterparty's Personal Data, that the Client/counterparty manifestly chooses to make public, including via social media

- Company obtains the Client's/counterparty's Personal Data from third parties who provide this to Company (e.g. the client's customers, credit reference agencies, law enforcement authorities, etc.)
- Company obtains the Client's/counterparty's Personal Data when the Client/counterparty visit any of the Company's sites or uses any feature or resources available on or through the Company's site. When the Client/counterparty visits a site, the device and browser may automatically disclose certain information (such as device type, operating system browser type, browser settings, IP address, language settings, dates and times of connecting to a Site and other technical communications information (some of which may constitute Personal Data.
- Company obtains the employees' Personal Data in the process of hiring and during work relationship.

Creation of Personal Data

Company creates a Personal Data about the Client, such as records of the client's interaction with Company, details of the accounts, subject to applicable law.

The Categories of Personal Data about the Client that Company processes, subject to applicable law:

Personal Details:

- given name(s),
- preferred name(s),
- nickname(s),
- gender,
- date of birth/age,
- place of birth,
- marital status,
- Social Security number,
- passport number(s),
- other government issued number(s),
- tax identification number(s),
- Green card number(s),
- driving license number(s),
- nationality,
- lifestyle and social circumstances,
- images of passports,
- signature,
- authentication data (responses to questions),
- photographs,

- visual images,
- personal appearance,
- behaviour
- CV information and other.

Family Details:

- family members,
- dependents,
- where applicable contact details

Contact Details:

- address,
- telephone number,
- email address,
- social media
- profile details

Employment Details:

- industry,
- role,
- business activities,
- names of current and former employer,
- work address,
- work telephone number,
- work email address,
- work-related
- social media profile details.

Education History:

- details of the education and qualification,
- the client's knowledge and experience in specific financial instruments, products, investment and ancillary services.

Financial Details:

- bank account details,
- instruction records,

- transaction details,
- source of funds,
- source of wealth,
- overall financial situation

Electronic Identifying Data:

- IP Addresses,
- activity logs,
- online identifiers,
- unique device identifiers and geolocation data.

Sensitive Personal Data

Personal data which is, by its nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.

Processing Sensitive Personal Data

The Company does not collect or otherwise process the sensitive personal data, except where:

- the processing is necessary for compliance with a legal obligation (e.g. to comply with the diversity reporting obligations)
- the processing is necessary for the detection and prevention of crime (including the prevention of fraud) to the extent permitted by applicable Law)
- the Client has manifestly made the Sensitive Personal Data public
- the processing is necessary for the establishment, exercise or defence of legal rights
- Company in accordance with applicable law, obtained the explicit consent prior to Processing the sensitive personal data (as above, this legal basis is only used to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way); or
- Processing is necessary for reasons of substantial public interest and occurs on the basis of an applicable law that is proportionate to the aim pursued and provides for suitable and specific measures to safeguard the fundamental rights and interests.

The processing of personal data will be done for the following purposes:

- for compliance with a legal obligation;
- for the performance of a contract the individual is a party to;
- to ensure the vital interests of the individual;
- for the legitimate interests pursued by the controller or the third party, under the condition that such interests override the rights of the individual, interests and fundamental freedoms;

- the examination of an application(s) for opening an account and assessing what instruments and/or services are appropriate/suitable to the client;
- the maintenance and development of your relations with Company and the exercise of Company's rights which arise from the relations between us, as well as the protection of the legal interests of Company in the context of its transactions with you or with persons connected with you;
- the performance of Company's legal duties and obligations;
- the control and the prevention of offences, including but not limited to, offences entailing fraud and money laundering offences

Also, the purposes for which Company may process personal data, subject to applicable law and legal basis on which Company may perform such processing:

- Client on-boarding: on-boarding new clients, compliance with internal requirements, policies and procedures.
- Conclusion contracts/agreements with new Counterparties (KYC of counterparties)
- AML/KYC: fulfilling regulatory requirement obligations, checks, identification and verification of identity, screening against government, supranational bodies, agency sanction lists, legal restrictions and publicly available news and systems.
- Provision of products and services to the Client: administering relationships and related services, performance of tasks necessary for the provision of services, communicating in relation to such services, assessment of appropriate products
- Establishing working relationships with employees.
- IT operations – management of the communication systems, IT security, IT security audits
- Investigations – detecting investigating and preventing breaches of policy, criminal offences, in accordance with the applicable law
- Legal compliance – compliance with legal and regulatory obligations under applicable law, establishing, exercising, defending legal rights
- Risk management – audit, compliance, controls, other risk management exercises
- Fraud prevention – detecting, preventing, investigating fraud

The Processing is necessary for compliance with legal obligation, is necessary in connection with any contract that the Client may enter into with Company, to take steps prior to entering into a contract, legitimate interest, prior consent is obtained (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way)

CONSENT

The Company requires that the request for consent will be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent, meaning it must be unambiguous. The Form of Consent prepared by the Company is clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. This form include an information about withdrawal of consent in easily way as it is to give it.

The Company require the parental consent in case to process the personal data of children under the age of 16.

The Company developed the Processing Personal Data Form (PPD Form) with such consent for a client/counterparty and employee. It is the responsibility of the Company to request this PPD Form (with consent) from the client/counterparty and employee and store them.

DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

Company may disclose Personal Data to:

- the Client, and where appropriate client's family, associates, representatives (in case of proper authorisation provided by the Client)
- anti-fraud services
- the third party processors
- the law enforcement agency or court
- any relevant party for the purposes of prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security in accordance with applicable law
- the accountants, auditors, financial advisors, lawyers, other outside professional advisors, subject to binding contractual obligations of confidentiality
- Governmental, legal, regulatory or similar authorities, ombudsmen, central/local government agencies, upon request and where required, including for the purposes of reporting any actual or suspected breach of applicable law or regulation.
- The regulatory authorities with regards to reporting obligations
- The brokers/custody in case of prior written consent from the Client
- The third parties, for the fulfilment of the terms of the contract/agreement with the Client/ counterparty in case of prior written consent from the Client/counterparty.

If Company will engage a third-party processor to process client's personal data, the processor will be subject to binding contractual obligations to:

- only process personal data in accordance with the prior written instructions; and
- use measures to protect the confidentiality and security of the Personal Data;
- together with any additional requirements under applicable law.

The Company will notify the Clients/counterparties of the transfer of Personal Data to third parties and the risks associated with this.

INTERNATIONAL TRANSFER OF PERSONAL DATA

Because of the international nature of the business, Company may need to transfer Clients Personal Data to third parties as noted above, in connection with the purposes set out in this Policy.

For this reason, Company may transfer the Personal Data to other countries that may have different laws and data protection compliance requirements, including data protection laws of lower standard to those that apply in the country in which the Client is located.

Where Company will transfer the Client's Personal Data to other countries, Company will do so on the basis of:

- adequacy decisions
- binding corporate rules
- suitable Standard Contractual Clauses
- other valid transfer mechanisms

DATA SECURITY

Company implemented appropriate technical and organisational security measures designed to protect the Client's Personal Data against accidental and unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, other unlawful or unauthorised forms of Processing, in accordance with applicable law.

The Company implemented the good security system. All computers in the Company are equipped with the latest data protection systems and constant change of password. All documents in hard copies and originals containing personal data are stored in special cabinets, access to which is available only to those employees who work with personal data.

ACCURACY

The Company takes all reasonable steps designed to ensure that: Personal Data of the Client is accurate and where necessary kept up to date, as well as that any of the Personal Data that Company process that is inaccurate (having regards to the purposes for which they are processed) are erased or rectified without delay.

From time to time Company may ask the Client to confirm the accuracy of the Personal Data.

DATA MINIMISATION

The Company takes all reasonable steps designed to ensure that Personal Data that Company process is limited to the personal data reasonably required in connection with the purposes set out in this Policy.

DATA RETENTION

Client's Personal Data is necessary in connection with the lawful purposes set out in the Policy, for which Company has already had a valid legal basis Company takes all reasonable steps designed to ensure that Personal Data of Clients that Company process is only processed for the minimum period necessary for the purposes set out in this Policy.

Company will retain copies of the Personal Data in a form that permits identification only for as long as: For at least 5 years from the date of the termination business relationship for all information, with the except of tax information, that will be held for 7 years.

In accordance with the decision and relevant request from the Cyprus Securities and Exchange Commission and/or MOKAS, this period may be extended.

LEGAL RIGHTS

Hereby, the Company informs the Clients/counterparties and/or employees that they have the following rights:

- right to request access to, or copies of, the Personal Data that the Company processes or control, together with information regarding the nature, processing and disclosure of those personal data
- right to request rectification of any inaccuracies in the personal data that the Company processes or controls
- right to request on legitimate grounds a) erasure of the personal data that the Company processes or controls, or b) restriction of Processing of Personal Data that the Company processes or controls
- right to have the Personal Data that the Company processes or controls transferred to another controller, to the extent applicable
- right to withdraw the consent, where the Company processes or controls Personal Data on the basis of the consent
- right to loge complaint with a Data Protection Authority regarding the Processing of Personal Data by Company or on behalf of Company
- right to object on grounds relating to the particular situation, to the processing of the personal data by Company or on behalf of Company

CONFIDENTIALITY

The Company will, except only in so far as is:

- i. Established by Law or applicable regulation; or
- ii. Necessary for effecting settlement; or
- iii. Permitted in writing by the Client, ensure that all non-public matters relating to the Portfolio will be kept strictly confidential within the Company and its Affiliates.

Notwithstanding the foregoing, the Company's composite performance record may include the results of the Portfolio's trading without naming the Client.

The Parties will at all times keep confidential and shall not disclose to a third party any information of a confidential nature acquired in connection with the Agreement or Portfolio, except for information which is bound to disclose under compulsion of law or by request of regulatory agencies or to respective professional advisers or where disclosure to a third party such as an intermediary or clearing house is necessary in order to facilitate the proper performance under the Agreement.

All information which Company and/or Company's brokers receive from the Client concerning Client's business or affairs and any information or work product generated from such information, which is not in the public domain, or is not available to Company on a non-confidential basis, or has not been independently developed by us and which we and/or our brokers are not required to disclose by

any applicable regulation or as authorised or required to be disclosed by a court of law or by any Competent Authority including without limitation the Courts or authorities in order to fulfil any requirements under the relevant legislation will be held in confidence by Company and/or Company's brokers, as applicable, unless and until such time as the Client specifically consent to the disclosure of that Confidential Information.

For the avoidance of doubt, nothing in this rules will prevent Company from disclosing information to the extent required to perform the Services.

In addition to any other right or obligation by virtue of which Company or any of Company's brokers may be entitled or bound by law to disclose information, Company or any of Company's brokers will be entitled, if requested or required, at our discretion, to disclose any information (including Confidential Information) known to Company or any of Company's brokers, and/or to produce any documents relating to the Client's business or affairs to any governmental or regulatory agency or authority (whether in Cyprus or elsewhere), to any exchange, clearing house, credit reference agencies, auditors, professional advisers, dealers, custodians, agents, bankers and any of the Company's affiliate and any relevant self-regulatory organisation. In addition, Company will, where reasonably practicable, seek to impose a confidentiality requirement in any case where the information is not subject to statutory restrictions on disclosure by the recipient.

Neither Company nor any of Company's brokers will have any duty to disclose to the Client any information that comes to Company or one of Company's brokers, in the course of carrying on any other business or as a result of or in connection with the provision of services to other persons.

The Client Accepts that Company and any of Company's brokers may be prohibited from disclosing or having regard to, or it may be inappropriate for Company and any of Company's brokers to disclose to the Client or have regard to, such information even if it relates to the Client or to the Services.

All information, documents and communications in Company's possession or control relating to the Services or the subject matter of the Services shall be Company's sole property, save for original contracts, share certificates and other original documents held on the Client's behalf. Company shall be permitted to retain a copy of all information, documents and communications between Company or sent or received by Company in connection with the Services for regulatory and risk management purposes.

Any information which: was already in Company's possession prior to delivery by the Client,

- i. was or becomes available in the public domain other than as a result of disclosure by Company,
- ii. becomes available to Company from a third party who Company does not know may be under an obligation of confidentiality to the Client, or
- iii. was or is independently developed by Company,

shall not be Confidential Information for the purposes of this subject.

DATA PROTECTION OFFICER (DPO)

The Data Protection Officer:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provide
- Contact details must be provided to the relevant Data Protection Authority
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

The Regulation emphasises the independence of the DPO, which prevents him from receiving instructions regarding the exercise of their tasks. No DPO should suffer any prejudice in the workplace because of their function. The appointment of the DPO for a fixed term is also an important factor in ensuring their independence.

The Company took advantage of the recommendation of the Data Protection Authority and appointed DPO for three years. DPO is allowed to have other functions, but depending on each case, the instances where conflict of interests could arise should be carefully considered. The evaluation of the performance of the DPO for his function should be clearly separated from the evaluation of other tasks.

The DPO is assigned with the tasks of informing data controllers of their obligations and data subjects of their rights, advising on data protection related issues, cooperating with the Data Protection Authority, ensuring internal application of the Regulation and handling queries and complaints.

Expertise and skills of the DPO:

The Company will designated the DPO on the basis of professional qualities, in particular, expert knowledge of data protection law and practices, and the abilities to fulfil their tasks.

Ability to fulfil the tasks incumbent on the DPO interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities include integrity and high professional ethics.

As the DPO function requires a high level of confidentiality the Company results that the best maintained of confidentiality is an in-house DPO, as the DPO function is attributed to a designated physical person that would serve as lead contact be in charge for the Company.

The Company controls that the DPO's contact details will be included in the information to be given to data subjects when their data are collected.

By recommendation of European Data Protection Supervisory the Company set up a functional mailbox for the DPO, which is indicated in data protection notices, on the internet and other public communications. This mailbox is DPO@cayros.eu.

Involvement of the DPO

The Company as a controller ensures that the DPO is involved, properly and in a timely manner, in all issues which relate to data protection. Involving the DPO early and systematically whenever decisions with data protection implications are taken has become a standard procedure within the Company. The Company believe that this will help ensuring compliance with the principles of data protection.

In addition, the DPO is a part of the relevant working groups, steering committees of the Company, etc., dealing with data processing activities.

The DPO is invited to participate regularly in Board of Directors Meetings of the Company on issues where personal data is affected and that he opinion always be given due weight.

The information on DPO in a timely manner is visible within the organisation to allow him to provide adequate advice. Information on DPO is reflected on the Company's internal informational portal.

The Company as a controller (in accordance with Article 39(2)) seeks advice of the DPO when carrying out a data protection impact assessment, and in accordance with Article 34(5), the Company as a controller always informs the DPO about personal data breaches.

The Company will consult the DPO in the planning phase of an IT systems before it is launched. The Company consider that involving the DPO early can help identifying and evaluating issues, such as whether personal information will be processed, the exact categories of data that will be collected, the purpose of the processing operation, etc.

The Company will support the DPO in performing their tasks by providing resources necessary to carry out those tasks. This implies that the DPO will be provided not only with adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate, but also that the senior management actively supports the DPO function. Such support includes that the designation of the DPO is communicated officially to all staff to ensure that their existence and function are known within the Company. If needed, DPOs will be given support from other services, such as the legal service or the communication team. The necessary resources also include giving access to personal data, processing operations and premises.

The training on new requirements under data protection rules will be assigned by the Company on an ongoing basis for both DPO, and for employees. DPO will be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim of this should be to constantly increase the level of expertise of DPO and he will be encouraged to participate in training courses on data protection, meetings of the DPO network, and other forms of professional development, such as participation in privacy fora, workshops, etc.

The Company establishes a percentage of time for the DPO function (part-time DPO) as it is not performed on a full-time basis because of small size of the Company and its business.

For part-time DPO the most important element is to have sufficient time to fulfil their duties (as conflicting priorities could result in the DPO duties being neglected).

For the calculation of this percentage, the working days, including travel time and preparation, for the DPO meetings will be taken into consideration.

The Company proceeds from the fact that there are 200 working days per year, 10% for the DPO function means that the DPO should work 20 days/year on data protection issues. The Company as a Controller should evaluate whether this allocation of time for the DPO function is proportionate to the workload in order to ensure application of the revised Regulation.

Independence of the DPO

The Company takes into account that the DPO is placed in a dual position: he is a part of the Company and yet must remain independent from it in the performance of his duties. As part of the Company he is ideally placed to monitor compliance from the inside and to advise or to intervene at an early stage, thereby avoiding possible intervention from the European Data Protection Supervisory. A number of guarantees, which aim at ensuring that the DPO fulfil his duties in an independent manner, have been provided by the Company:

The Company ensures that the DPO does not receive any instructions regarding the exercise of their tasks (It refers not only to direct instructions from a superior, but also implies that a DPO must not be in a position to be inclined to accept certain compromises when dealing with controllers in high positions).

The Company ensures that in order to guarantee independence, the DPO will not be dismissed or penalised by the Company for performing their tasks (such penalties could include: denial of benefits that other employees receive, delay of promotion, and any other type of discriminatory measures imposed on the DPO solely for performing their duties).

The Company ensures that the DPO and Company's staff will be bound by secrecy or confidentiality concerning the performance of their tasks.

The DPO will develop his own common principles of good supervision (requirements, annual work programme, annual report, etc.), which will serve to measure the performance of his work.

Conflict of interests

According to Article 44(6), the DPO may fulfil other tasks and duties. The Company allows the combination of positions in the absence of a conflict of interest.

The Company as a controller ensures that any DPO's tasks and duties do not result in a conflict of interests. The absence of conflict of interests is closely linked to the requirement to act in an independent manner.

DPO can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests.

The DPO cannot hold a position within the Company that leads them to determine the purposes and the means of the processing of personal data, i.e. the part-time DPO should not act as a controller in his initial activity.

In some cases, functions lower down in the organisational structure can be concerned if such positions lead to the determination of purposes and means of processing.

Functions that would in principle be incompatible with the DPO function include high level positions within management, human resources, IT services, security services, internal audit, etc. A conflict of interests may typically also arise (even for lower level positions), when a DPO who is also part of the compliance team must assess compliance checks and related data processing that they have designed. The Company provides monitoring and control of conflict of interests on the ongoing basis. As well as the Company acting as a controller identifies the positions which would be incompatible with the function of DPO, draws up internal rules to this effect in order to avoid conflicts of interests, and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests (depending on the activities, size and structure of the Company).

The Company created a separate functional mailbox for DPO matters (so that the rest of the organisation can see whether the advice comes from the DPO function or legal advisory function).

Evaluation of a DPO in the performance of their duties as DPO must not be related in any way to the performance of other tasks. Furthermore, the DPO should not be prevented from exercising his duties due to lack of time as a result of other official duties.

Term of appointment

The Company appoints its DPO on three years in accordance with article 42.8. DPO may be eligible for reappointment.

DPO may only be dismissed from the post if two cumulative conditions are met:

- if he no longer fulfil the conditions required to perform their duties, and
- with the consent of the European Data Protection Supervisory.

The fact that the European Data Protection Supervisory must consent to the dismissal of the DPO if he no longer fulfil the conditions required for the performance of his duties also contributes to ensuring independence.

European Data Protection Supervisory take part in the evaluation the work of the DPO on a regular basis (see Article 45(3)).

Tasks of the DPO

The DPO has a central role within the Company:

- DPO is familiar with problems of the organisation and, given their status,
- have a crucial role to play in giving advice and
- helping solve data protection issues.

The DPO will simultaneously act as advisor, educator and point of contact for competent authorities and data subjects. The Company involves the DPO properly and in a timely manner, in all issues, which relate to the protection of personal data.

The DPO of the Company has a number of tasks, duties and powers:

Information and awareness-raising function

This implies both informing data controllers and processors of their obligations and responsibilities, and ensuring that data subjects are informed of their rights and obligations pursuant to the Regulation. Awareness-raising can take the form of staff information notes, training sessions, setting up of a web site, data protection notices, etc.

Advisory function

DPO shall ensure in an independent manner the internal application of the Regulation and advise data controllers on fulfilling their obligations.

In addition to this general advisory role, the DPO should provide advice in a number of specific situations:

- the DPO should advise, where requested, on the necessity for a notification or a communication of a personal data breach pursuant to Article 34 and 35 of the Regulation.
- the DPO should provide advice, where requested, on data protection impact assessments ('DPIAs') and monitor their performance pursuant to Article 39 of the Regulation (It is the responsibility and task of the data controller, not of the DPO, to carry out DPIAs).
- the DPO should provide advice, where requested, on the need for prior consultation of the European Data Protection Supervisory in accordance with Article 40 of the Regulation.

The Company developed and implemented a secure channel for communication with the DPO. This entails the use of an encrypted email address: DPO@cayros.eu.

The DPO is free to choose which communication options he would like to provide, the DPO encouraged to be as open as possible to any inquiries and whistleblowing efforts. Also, the DPO should demonstrate his commitment to protect the identity of complainants vis-à-vis the Company if needed, to encourage data subjects to exercise their rights without fear of repercussions.

The Company should be borne in mind that the responsibility of carrying out all processing operations in compliance with the revised Regulation remains with the controllers. In accordance to Article 31 of the Regulation, the Company as a data controller and/or the processor, is required to maintain a record of processing operations under its responsibility and maintain a record of all categories of processing activities carried out on behalf of a controller (not the DPO).

The DPO creates inventories and hold a register of processing operations based on information provided to them by the entities responsible for the processing of personal data. Keeping such a register is the responsibility of the DPO and it enabled him to have an

overview of all processing operations carried out within the Company. Also, this allows to the European Data Protection Supervisory, upon request, to have an overview of all the personal data processing activities carried out by the Company.

The Company takes into account that it is the Company's task to keep appropriate records, and that accountability for generating records and for their content remains with the controller. The DPO can help generating the records and supporting documentation, but this is the duty of the controller.

Monitoring compliance

The DPO is to ensure in an independent manner the internal application of the Regulation and to monitor compliance with the Regulation, with other applicable EU law containing data protection provisions, and with the policies of the data controller or processor in relation to data protection, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits.

In order to monitor compliance, DPO can:

- prepare templates for the Company as a data controllers to fill in, on the basis of which they can monitor compliance with the Regulation and make recommendations.
- assist the Company by developing internal policies and FAQs on thematic topics to provide guidance to data controllers.
- on their own initiative or at the request of the Company, the staff committee, or any individual, investigate matters and occurrences directly relating to their tasks and which come to their notice, and report back to the person who commissioned the investigation, or to the Company.

It is the Company's responsibility to insure that the staff committee and all services of the Company cooperate closely with the DPO in cases of an alleged breach of data protection rules and ensure that they are duly informed and consulted.

Handling queries or complaints

The DPO is granted with investigatory powers as laid out above and can as a result handle queries or complaints submitted by members of staff or the public.

No one shall suffer prejudice on account of a matter brought to the attention of the competent DPO alleging that a breach of the Regulation has occurred.

The DPO prepares the investigation and handling of complaints and, as a general rule, all applicants of complainants should at first contact the DPO.

The DPO has the possibility to bring to the attention of the European Data Protection Supervisory any failure to comply with the obligations under the Regulation.

Publication of contact details of DPO

The Company published the contact details of the DPO on the Internal Portal of the Company and communicate him to the Data Protection Authority (according to the Art. 43(5)).

The communication of the name of the DPO to the Data Protection Authority is naturally essential in order for the DPO to serve as contact point between the Company and the Data Protection Authority.

The Company informs all staff members of the name and contact details of the DPO, by publishing them internally on the Company's intranet portal.

Appointment

DPOs must be appointed in the case of:

- public authorities,
- organizations that engage in large scale systematic monitoring, or
- organizations that engage in large scale processing of sensitive personal data (Art. 37).

Our Company doesn't fall into one of these categories, therefore the Company do not need to appoint a full time DPO. But due to the importance of the issue of protection of personal data and the need to transfer personal data to third parties from countries that may not have relevant personal data protection rules, the Company decided to appoint a part time DPO.

For all questions regarding personal data and its processing, the employees and clients/counterparties can contact Company's DPO.

DATA BREACHES

Data breaches which may pose a risk to individuals must be:

- notified to the Data Protection Authority within 72 hours and
- notified to affected individuals without undue delay.

PENALTIES

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient client consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a Company can be fined 2% for not having their records

in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

CONTACTS

Data Protection Officer: Mrs. Maryna Chernenko

Address:

82 Akropoleos Avenue, 1st Floor,
2012 Akropolis, Nicosia, Cyprus

E-mail: DPO@cayros.eu

Tel.: Tel.: +357 22 107 242

Fax: +357 22 450 775

If the Client/counterparty and/or the employee have any comments, questions, concerns about any of the information in this Policy or any other issues relating to Processing of Personal Data by the Company, the Client/counterparty and/or the employee may contact/submit request via above mentioned contacts.

Also, for more information all Clients/counterparties and/or the employees could contact with their Data Protection Authorities.

WHAT ARE DATA PROTECTION AUTHORITIES (DPAS) OR DATA PROTECTION SUPERVISORY?

DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.

To find your DPA please follow the link:

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

COMMISSION FOR PERSONAL DATA PROTECTION IN CYPRUS

Ms. Irene LOIZIDOU NIKOLAIDOU

Commissioner for Personal Data Protection

Contact details:

Address: 1 Iasonos Street, 1082 Nicosia P.O. Box 23378, CY-1682 Nicosia

Tel. +357 22 818 456

Fax +357 22 304 565

e-mail: commissioner@dataprotection.gov.cy

Website: <http://www.dataprotection.gov.cy/>

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/cvs/cy_nikolaidou.pdf

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page6a_en/page6a_en?opendocument

Art 29 WP Alternative Member: Mr. Constantinos Georgiades

UPDATING THE POLICY

The Company will update this Policy periodically to take into account changes as and when appropriate.

The updated policy will be immediately communicated to all employees, Clients/counterparties and service providers and will be published on the internal portal of the Company.

This Policy will be provided to the Client or counterparty up

CONFLICT OF INTEREST POLICY

1. **Aim of the Policy**

The Policy aims to identify and prevent or manage conflicts of interest between the Company, including its managers, employees and tied agents, or any person directly or indirectly linked to them by control, and its clients or between one client and another, or combinations thereof, including those caused by the receipt of inducements from third parties or by the investment firm's own remuneration and other incentive structures.

Specifically, the Policy:

- a) identifies, with reference to the specific investment services and activities and ancillary services carried out by or on behalf of the Company, the circumstances which constitute or may give rise to a conflict of interest entailing a risk of damage to the interests of one or more clients; and
- b) specifies the procedures to be followed and the measures to be adopted to prevent or manage such conflicts.

Conflicts of interest should be regulated only where an investment service or ancillary service is provided by the Company. The Company provides discretionary portfolio management and investment advice, therefore, the conflict of interest policy should be strictly followed. The status of the client to whom the service is provided — as either retail, professional or eligible counterparty — is irrelevant for this purpose.

2. **Identification of conflicts of interest**

For the purpose of identifying the types of conflicts of interest that may arise, the Company shall take into account whether itself or a relevant person or a person directly or indirectly linked by control to the Company, may in the course of providing Investment and Ancillary Services or a combination thereof:

- a) is likely to make a financial gain or avoid a financial loss at the expense of the client;
- b) has an interest in the outcome of a service provided to the client or of a transaction carried out on behalf of the client, which is distinct from the client's interest in that outcome;
- c) has a financial or other incentive to favor the interests of another client or group of clients over the interests of the client;
- d) carries on the same business as the client;
- e) receives or will receive, from a person other than the client, an inducement in relation to a service provided to the client, in the form of monetary or non-monetary benefits or services.

Specifically, given the Company's current business model, the following conflicts of interest have been identified:

- Personal Account Dealing
- Inside and Proprietary Information
- Inducements
- Cross Holdings
- Selection of Service Providers
- Outside Affiliations
- Remuneration of Staff
- Valuations
- Expenses charged to the AIFs
- Risk management of client portfolios
- Liquidity management of funds
- Access to electronic data
- Supervision and segregation of departments

In respect of these conflicts, the Company maintains and operates procedures with a view to taking all appropriate steps to prevent conflicts of interest from constituting or giving rise to material risk of damage to the interests of the Company's clients.

3. Management and Prevention of conflicts of interest

Senior management is responsible for ensuring that the Company identifies, prevents and manages its conflicts of interest. In managing the Company's conflicts of interest, senior management will:

- a) ensure that all staff are aware of the critical importance of the Policy in carrying out the Company's business, and the need to report any perceived conflict of interest promptly;
- b) review any actual or potential conflict of interest as soon as it is identified and identify appropriate steps to manage the conflict as necessary; these steps shall have the aim of preventing the risks of damage to the interests of a client;
- c) communicate to all relevant staff the procedures to be followed in order to manage the conflict of interest; and
- d) document the conflict of interest and the measures undertaken in the Policy.

Moreover, the Company ensures that relevant persons engaged in different business activities involving a conflict of interest carry on those activities at a level of independence. The procedures to be followed and measures to be adopted that are necessary for the firm to ensure the requisite degree of independence include the following:

- a) an effective security policy with various access levels to prevent or control the exchange of information between relevant persons engaged in activities involving a risk of a conflict of interest where the exchange of that information may harm the interests of one or more clients;

- b) the separate supervision of relevant persons whose principal functions involve carrying out activities on behalf of, or providing services to, clients whose interests may conflict, or who otherwise represent different interests that may conflict, including those of the firm;
- c) the removal of any direct link between the remuneration of relevant persons principally engaged in one activity and the remuneration of, or revenues generated by, different relevant persons principally engaged in another activity, where a conflict of interest may arise in relation to those activities;
- d) measures to prevent or limit any person from exercising inappropriate influence over the way in which a relevant person carries out investment or ancillary services or activities; and
- e) measures to prevent or control the simultaneous or sequential involvement of a relevant person in separate investment or ancillary services or activities where such involvement may impair the proper management of conflicts of interest.

The Company pays special attention to the activities of collective portfolio management, risk management, investment advice and individual portfolio management. In particular, such special attention is appropriate where the Company or a person directly or indirectly linked by control to the Company performs a combination of two or more of these activities.

All Conflicts of interest are reflected in the Register of conflicts of interest. The Compliance Officer maintains this registry.

Based on the conflicts identified in Section 3 of this Policy, the Company applies the following measures to prevent such conflicts from arising.

3.1. Personal account dealing

The Company has implemented a personal account dealing policy, with which staff, and related persons under their control, must comply. At the commencement of their functions, members of staff are required to commit to comply with this policy.

All new employees are required to provide information on the availability of their personal accounts. In addition, at least once a year, all employees of the Company must either provide an information about the absence of personal account deals during a year, or timely inform about the desire to make transactions on their personal accounts.

If an employee intends to complete a transaction on his personal account, he must notify the Compliance in advance about this by sending a notification (no later than 2 days before the date of the proposed transaction). As well as, the employee must send an appropriate confirmation of the transaction to the Compliance Officer within 2 days after the transaction made.

All transactions in financial instruments by staff and relevant persons must be reported to the Compliance Officer promptly. These transactions must include precise dates and timings and any authorization or prohibition in connection with such a transaction.

All the information on the availability of personal accounts, as well as on transactions carried out on personal accounts (Personal Account Dealing), is reflected in the Register of personal accounts and transactions. The Compliance Officer maintains this registry.

3.2. Inside and proprietary information

Staff members, who, in pursuit of the Company's business activities, possess inside or proprietary information must preserve its confidentiality and disclose it only to other staff who have a valid business reason for receiving it. Members of staff who believe they have received inside information from any source must immediately contact the Compliance Officer. The Company and its staff members cannot use or further disclose the information where it has been received.

Additionally, the Company has established "Chinese walls" to prevent or control the exchange of information between relevant persons engaged in activities involving a risk of a conflict of interest where the exchange of that information may harm the interests of one or more clients. Specifically, the Chinese walls have been established between the following departments/functions:

- Collective portfolio management
- Risk Management
- Investment Advice
- Individual Portfolio Management
- Commodities management

The Company recognises the following AIFM-specific scenarios as potential sources of conflict:

- Fund Structuring: Choosing fund structures that disproportionately benefit certain investor classes (e.g., preferred redemptions or fee schedules).
- Side Letters and Preferential Treatment: Offering specific terms to certain investors (e.g., reduced fees, greater liquidity access) that are not offered to others.
- Allocation of Trade Opportunities: Allocating illiquid or high-yielding assets unevenly across funds.
- Cross Transactions: Purchasing or selling assets between funds under Company management.
- Rebates or retrocessions from service providers: Receiving kickbacks or revenue-sharing arrangements that are not transparently disclosed or justified.

These situations are reviewed by Compliance and the Risk function and subject to formal escalation procedures and internal oversight mechanisms.

3.3. Inducements

Personal gifts

The Company operates a personal gifts policy, which is applicable to benefits or inducements to staff which might be seen as conflicting with their duties to the Company or to any of the Company's clients. To address conflicts of interest that may arise when a member of staff accepts a gift, the Company applies a general rule that always any such gifts cannot exceed the amount of EUR100.

The Company is dedicated to providing honest, fair and professional investment services and/or ancillary services to clients. For this reason, the Company would not accept inducements (monetary and non-monetary benefits) in relation to the investment service and/or ancillary service, unless these qualify as a minor non-monetary benefit.

The following gifts may be considered acceptable provided it is reasonable, proportionate, declared in company records, not a Restricted Practice (see below) and received/given in the furtherance of a normal business relationship:

- Gifts of an incidental nature such as bottles of wine or spirits, limited to a total market value of EUR100 total gifts in any one year/season per person from any one supplier.
- Free attendance for employee and companions on standard excursions offered by a supplier.

The following gifts/inducements are specifically prohibited (Restricted Practices) and if they are offered to or requested from you, you should inform your immediate line manager without delay.

- Cash, cash equivalent or vouchers, gift certificates and the like redeemable against goods or services;
- Gifts where it has been made clear that the recipient's independence will be compromised by taking the gift. Gifts from a supplier, the receipt of which changes the relationship with the supplier.
- Any gifts which the giver or recipient requests is kept "off book" or confidential from your or their employers;
- Gifts to a public official outside of public holidays or in order to facilitate "smooth" or "speed up" any official process they are engaged in;
- Gifts to or from a business associate when they are engaged in a competitive tender process.
- Free tickets which are able to be sold on to members of the public (all such free ticket arrangements should be agreed on a formal basis with the Company's management).

Receipt of fees and commission

The Company is not paying or is being paid any fee or commission or providing or being provided with any non-monetary benefit in connection with the provision of an investment service or ancillary service to the client, unless the fee, commission or non-monetary benefit is designed to enhance the quality of the relevant service to the client.

A fee, commission or non-monetary benefit shall be considered to be designed to enhance the quality of the relevant service to the client

if all of the following conditions are met:

- I. it is justified by the provision of an additional or higher-level service to the relevant client, proportional to the level of inducements received, such as:
 - a) the provision of non-independent investment advice on and access to a wide range of suitable financial instruments including an appropriate number of instruments from third party product providers having no close links with the investment firm;
 - b) the provision of non-independent investment advice combined with either: an offer to the client, at least on an annual basis, to assess the continuing suitability of the financial instruments in which the client has invested; or with another on-going service that is likely to be of value to the client such as advice about the suggested optimal asset allocation of the client; or
 - c) the provision of access, at a competitive price, to a wide range of financial instruments that are likely to meet the needs of the client, including an appropriate number of instruments from third party product providers having no close links with the investment firm, together with either the provision of added-value tools, such as objective information tools helping the relevant client to take investment decisions or enabling the relevant client to monitor, model and adjust the range of financial instruments in which they have invested, or providing periodic reports of the performance and costs and charges associated with the financial instruments.
- II. it does not directly benefit the recipient firm, its shareholders or employees without tangible benefit to the relevant client;
- III. it is justified by the provision of an on-going benefit to the relevant client in relation to an ongoing inducement.

In relation to any payment or benefit received from or paid to third parties, the Company shall disclose to the client the information required by the relevant Law.

3.4. Cross holdings

Where the Company or the funds it manages has holdings in other funds which in their turn invest in the Company's funds, any such cross holdings are noted at the time of investment and are reviewed periodically by the compliance officer. In addition, the Company neither grants nor receives any preferential terms.

3.5. Selection of service providers

The selection of service providers is made on an arm's length basis. In the event of any personal relationship between the Company and the third party, or a person connected to them, the Company takes this into account and considers potential conflicts or the appearance of conflicts in making its selection. As far as possible, the connected party should refrain from being involved in the actual decision-making process.

The Company prevents conflicts arising regarding the selection of a service provider by not accepting or providing fees, commissions and non-monetary benefits which do not directly enhance the service offered.

3.6. Outside affiliations

No member of staff may serve as an officer or director for any business operation other than the Company or its affiliates without prior approval from an executive director. In providing this approval, the executive director will take into account any actual or potential conflict.

3.7. Remuneration of staff

Staff remuneration is carefully considered to ensure that conflicts do not inadvertently arise through targets that inappropriately incentivise staff members to behave in a manner that disadvantages the interests of clients in favour of the Company.

As a policy, none of the Company's employees and/or Directors can be remunerated based on the successful promotion of certain products or financial instruments over others. The remuneration of the personnel is not dependent solely on quantitative criteria but also takes into account compliance with regulations, the fair treatment to the clients and the quality of the services provided. Please refer to the Remuneration policy for more details

Inducements and Soft Commission Arrangements

In accordance with MiFID II Articles 23 and 24 and CySEC Directive DI87-, the Company shall not accept or pay any inducement in relation to the provision of investment services unless the following conditions are met:

- a. The inducement is designed to enhance the quality of the relevant service to the client;
- b. The inducement does not impair the Company's duty to act honestly, fairly, and professionally in accordance with the best interests of the client;
- c. Full, prior disclosure is made to the client in a durable medium regarding the nature and amount of the inducement (or the method of calculating it, if not possible to determine the exact amount in advance).

Examples of inducements that may be received or paid include:

- Monetary commissions or fees from third-party brokers or distributors;
- Non-monetary benefits such as training, research, or access to investment tools or conferences;
- Soft commissions tied to fund execution, custody or research, provided they benefit the client.

The Company maintains a dedicated Inducements Register as a separate part of the Conflict of Interest Register, recording:

- The type and value of each inducement received or paid;
- The identity of the third party involved;
- The justification for how the inducement enhances the service to the client;
- Any identified conflicts of interest.

This Register is maintained by Compliance and reviewed on a yearly basis. A summary of inducements received or paid is reviewed annually by the Board of Directors to ensure continued compliance.

The Company does not enter into soft commission arrangements unless:

- They are disclosed to clients;
- The services received are used directly to enhance client outcomes;
- They do not result in excessive trading or higher client costs.

3.8. Valuations

Where the Company is involved in the valuation of client portfolios, potential for conflicts of interest arise as the Company is also remunerated by reference to the net asset value of its clients' portfolios. This potential conflict is mitigated by the Company's fee being based on the valuation of the assets.

3.9. Expenses charged to the AIFs

The Company has a fiduciary duty to ensure that the AIFs it manages and therefore the investors in these AIFs are not charged undue costs. A conflict of interest arises where the Company could charge to the AIFs certain fees and expenses arising in relation to it that do not directly benefit the AIF and/or its investors. The Company's policy is:

1. to make adequate disclosure in the offering documents of the AIFs in relation to the nature of fees and expenses charged to the AIFs; and
2. not to charge the AIFs any fees and expenses that do not directly benefit the AIFs and their investors and to pay for such costs itself. Expenses charged to the AIFs are authorised by the board of each AIF.

3.10. Risk management of client portfolios

There is a risk that in seeking to maximize achieved investment returns for the client accounts which they manage, portfolio managers may exceed the risk tolerance levels or stated objectives of the client (such as those set out in the prospectus of the AIFs that the Company manages), resulting in overconcentration in a single issuer or sector, or in illiquid assets, or the excessive use of leverage.

The Company has implemented a strong, documented and clear risk management framework. Decisions taken by the risk management function are based on reliable data, generated by means other than the portfolio management function. The CEO is responsible for ensuring the integrity of this data and of the risk management framework, which is subject to supervision by the Company's Board independently from the portfolio management function.

3.11. Liquidity management of funds

In relation to any AIFs that the Company manages, a conflict of interest might arise between the Company's incentive to seek returns through investment in illiquid or potentially illiquid assets and the need to maintain adequate levels of liquidity in relation to the redemption policy of the Funds that it manages. A conflict of interest may result in relation to those investors wishing to redeem their investments and those investors remaining in the fund, where there is a risk that the Company has to sell a greater proportion of the fund's liquid assets in order to meet redeeming investors' requirements than it would otherwise sell in the exercise of prudent investment management, with the result that remaining investors will hold a higher proportion of illiquid or relatively illiquid assets; or that the Company will execute sales of illiquid assets at discounted prices, thereby reducing returns for all investors.

The policy of the Company is to ensure that for each fund that it manages, the liquidity profile of the fund remains consistent with its redemption policy. The Company maintains a permanent risk management function that is independent from its investment management function and monitors the liquidity of each fund on a monthly basis against their redemption policy. The Company's Board is notified in a timely manner, whenever a liquidity mismatch arises that could result in damage to the interests of the fund or its investors.

3.12. Access to electronic data

The Company has a security policy in place, which governs the access to electronic data so that the persons engaged in each department do not have a direct physical access to records and information concerning the subject matter of another department and which are not considered necessary for the execution of specific work. Specifically, separate permissions and access rights are provided for the various departments.

3.13. Supervision and segregation of departments

The Company maintains separate supervision and segregation of departments / functions which provide services to clients, whose interests may conflict with those of other clients or with the interests of the Company.

- Collective Portfolio management (AIFs) department
- Individual portfolio management department
- Commodities management department
- Investment advice department

4. Disclosures

In the case where the Company's organisational arrangements to prevent conflicts of interest are not sufficient to ensure, with reasonable confidence, that risks of damage to client interests will be prevented, the Company a measure of last resort shall clearly disclose to the client the general nature and/or sources of conflicts of interest and the steps taken to mitigate those risks before undertaking business on its behalf. Such disclosure shall:

- a) be made in a durable medium; and
- b) include sufficient detail, taking into account the nature of the client, to enable that client to take an informed decision with respect to the service in the context of which the conflict of interest arises.

The disclosure shall clearly state that the organisational and administrative arrangements established by the investment firm to prevent or manage that conflict are not sufficient to ensure, with reasonable confidence, that the risks of damage to the interests of the client will be prevented.

The disclosure must also include specific description of the conflicts of interest that arise in the provision of investment and/or ancillary services, taking into account the nature of the client to whom the disclosure is being made. The description shall explain the general nature and sources of conflicts of interest, as well as the risks to the client that arise as a result of the conflicts of interest and the steps undertaken to mitigate these risks, in sufficient detail to enable that client to take an informed decision with respect to the investment or ancillary service in the context of which the conflicts of interest arise.

5. Record keeping

The Company shall maintain and regularly update a record of the kinds of investment or ancillary service or investment activity carried out by or on behalf of the Company in which a conflict of interest entailing a material risk of damage to the interests of one or more clients has arisen or, in the case of an ongoing service or activity, may arise.

The record will be kept by the Compliance Officer for a period of at least five (5) years. Any actions must be recorded and reported to the Board of Directors without any delay.

The Board shall receive on a frequent basis, and at least annually, written reports on cases of services or activities giving rise to detrimental conflict of interest.

6. Updating and review of the Policy

At least on an annual basis, the Company shall assess and review its Policy, and shall take all appropriate measures to address any deficiencies. The Company should avoid over-reliance on disclosure of conflicts of interest since it is considered a deficiency in the Company's overall conflicts of interest policy.

7. Internal Follow-Up of Complaints-Handling (Guideline 5 of the ESMA/EBA Guidelines)

In line with the Guidelines on complaints-handling for the securities (ESMA) and banking (EBA) sectors, and in particular Guideline 5: Internal follow-up of complaints-handling, the Company ensures that it not only responds appropriately to complaints but also uses them as a tool to identify, prevent, and manage potential or existing conflicts of interest.

Specifically, the Company shall:

- a) Analyze the Root Causes of individual complaints in order to identify any underlying issues, including those related to conflicts of interest, compliance failures, or deficiencies in internal controls.
- b) Identify Common Themes that may arise across multiple complaints, with the aim of spotting patterns or recurring issues indicative of systemic problems.
- c) Assess Whether Issues Identified May Also Affect Other Clients who have not complained but who may have been exposed to the same risks or issues.
- d) Take Corrective and Preventive Action when necessary to address any identified conflicts of interest, operational weaknesses, or non-compliance with regulatory or internal policies.
- e) Update Relevant Internal Policies and Procedures, including this Conflicts of Interest Policy, based on the findings and outcomes of the complaint analysis.
- f) Report Significant Findings to the Board of Directors, alongside the annual or ad hoc reporting obligations related to conflicts of interest under Section 6 of this Policy.

This proactive and structured approach ensures the effective use of complaint data as a means of improving service quality, enhancing compliance with regulatory obligations, and reducing the risk of damage to clients' interests stemming from unmanaged or undisclosed conflicts of interest.

SFDR Disclosure

AIFM Cayros Capital Investment Management Ltd (the "AIFM") is subject to the requirements set forth by the European Union's Sustainable Finance Disclosure Regulation (SFDR) (EU 2019/2088). As a financial market participant under the SFDR, the AIFM is required to provide transparency regarding how sustainability risks are considered in its investment decision-making processes and disclose whether principal adverse impacts (PAIs) are taken into account.

At present, the AIFM does not integrate sustainability risks into its investment decision-making process. The AIFM manages funds that do not promote environmental, social, or governance (ESG) characteristics, nor do they have sustainable investment objectives, as defined under Articles 8 and 9 of the SFDR. The investment strategies employed are based on traditional financial metrics and do not incorporate ESG factors when evaluating individual investments. The AIFM believes that sustainability risks are not material to the current investment strategies and do not significantly impact the returns of the funds under management.

The AIFM acknowledges the growing importance of ESG factors and intends to gradually integrate sustainability considerations into the investment assessment, decision-making process, and risk evaluation for each fund under management, unless otherwise stated in the relevant fund documentation.

1. Integration of Sustainability Risks (Article 3 SFDR)

The AIFM does not integrate sustainability risks into its investment decision-making processes.

This approach reflects the nature of the investment strategies pursued by the funds under management, which are based on traditional financial analysis and do not incorporate environmental, social or governance ("ESG") considerations. Following an internal assessment, the AIFM has determined that sustainability risks are not material to the investment strategies currently employed and are therefore not expected to have a material negative impact on the returns of the funds.

In accordance with Article 6 SFDR, the AIFM discloses in its pre-contractual documentation that sustainability risks are not considered relevant and provides a clear explanation of the reasons for such determination.

The AIFM maintains procedures to periodically reassess the relevance and materiality of sustainability risks, taking into account regulatory developments, market practices and the nature of the investment strategies of the funds under management.

2. Principal Adverse Impacts (PAI) (Article 4 SFDR)

The AIFM does not consider the principal adverse impacts of its investment decisions on sustainability factors.

This position has been determined taking into account the nature, scale and complexity of the AIFM's activities, the investment strategies of the funds under management, and the absence of ESG considerations within the current investment decision-making process.

Accordingly, the AIFM does not perform due diligence on principal adverse impact indicators nor collect or report on such indicators as defined under the applicable regulatory technical standards.

The AIFM will periodically review this position and may revise its approach where regulatory requirements, market practices or the characteristics of the funds under management change.

3. Remuneration Policy (Article 5 SFDR)

The AIFM's remuneration policy is designed to be consistent with sound and effective risk management and does not encourage excessive risk-taking.

Given that sustainability risks are not currently integrated into the investment decision-making process, the remuneration policy does not include specific provisions linking remuneration to the integration of sustainability risks. Nevertheless, the remuneration framework remains aligned with the overall risk profile of the AIFM and the funds under management.

4. Product Classification

The AIFM manages funds that do not promote environmental or social characteristics and do not have sustainable investment objectives within the meaning of Articles 8 or 9 of SFDR. Accordingly, all funds under management are classified as Article 6 products.

5. Future Plans

The AIFM is aware of the increasing global emphasis on sustainability and responsible investment. Although ESG factors are not currently part of the investment decision-making process, the AIFM is committed to continuously monitoring regulatory developments and best practices in sustainability. As the regulatory environment evolves and ESG factors become more relevant to the funds under management, the AIFM will assess the potential integration of sustainability risks into its investment strategies and risk management processes.

6. Update and Review of Disclosure

This disclosure reflects the AIFM's current position under SFDR and is reviewed on a periodic basis to ensure continued alignment with applicable regulatory requirements, market developments and the AIFM's activities.

Any material changes to the AIFM's approach will be reflected in this disclosure and in the relevant investor documentation.