

PRIVACY STATEMENT

VERSION CONTROL

Policy Owner: Athlos Capital Investment Services Ltd

Created on: January 2018

Date of approval by the Board of Directors: 21st of November 2022

Review date	Reviewed by	Comments and suggestions for amendments	Date of approval
29/03/2019 (V.01/2019/03)	Compliance Function	Policy has been amended to include versioning	02/05/2019
04/09/2022 (V.01/2020/09)	Compliance Function	Policy has been amended as part of the annual review	03/01/2021
05/08/2022 (V.01/2022/08)	Compliance Function	Annual review of the Policy	23/08/2022
16/11/2022 (V.02/2022/11)	Compliance Function	Updated to include the new address details of the Company	21/11/2022

TABLE OF CONTENTS

1	Introduction.....	4
2	GDPR references.....	6
3	Rights of Clients.....	9
4	Data Protection.....	12
5	Other requirements.....	13

1 Introduction

1.1 Scope of the Privacy Statement

- 1.1.1 The Privacy Statement applies to natural persons who are either existing or prospective Clients of the Company or are authorised representatives/agents or beneficial owners of legal entities or of natural persons who are existing or prospective Clients of the Company.

1.2 Purpose

- 1.2.1 The Privacy Statement provides an overview of how the Company aims to collect and process its Clients' personal data and information of the Clients' rights under the Data Protection Law and the GDPR.

1.3 Definitions

- 1.3.1 The following words or phrases shall have the meaning set out herein, as defined by the Applicable Laws and Regulations:

"AML Law" means Law 188(I)/2007 which provides for the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007 as amended from time to time.

"Applicable Laws and Regulations" Means any laws, regulations and directives which regulate the provision of investment services by a CIF, including any circulars and guidelines issued by competent authorities that are addressed to CIFs and any laws, regulations and directives which regulate the protection and processing of personal data.

"Client" means any natural or legal person who wishes to enter into a business relationship with the Company for the provision of one or more of the investment services and activities that the Company is authorised to provide under its license and who has been accepted by the Company as its Client.

"Company" means Athlos Capital Investment Services Ltd.

"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.

"CySEC" means the Cyprus Securities and Exchange Commission.

"Data Protection Law" is the Processing of Personal Data (Protection of Individuals) Law 138(I)/2001 as amended from time to time.

"EEA" means the European Economic Area.

"ESMA" means the European Securities and Markets Authority.

"GDPR" is Regulation (EU) 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.

"International Organisation" shall have the meaning set out in the GDPR.

"Law" is Law 87(I)/2017 which provides for the provision of investment services, the exercise of investment activities, the operation of regulated markets and other related matters.

"Member State" means a country which is a member of the European Union or the EEA.

"MiFID II" is Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

"personal data" shall have the meaning set out in paragraph 2.1 of the Privacy Statement.

- "Processing"** shall have the meaning set out in paragraph 2.2 of the Privacy Statement.
- "Processor"** means a natural or legal person, public authority, agency or other body which process personal data on behalf of the controller. It is noted that the Company is considered as a processor under the GDPR.
- "Republic"** means the Republic of Cyprus.
- "Third party"** shall have the meaning set out in the GDPR.
- "Union"** means the European Union.
- "4th AML Directive"** means Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

1.4 Legal framework

1.4.1 The Policy has been developed taking into consideration the Applicable Laws and Regulations as follows:

- Law 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets and other related markets as amended from time to time ("**Law**").
- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU ("**MiFID II**").
- Law 188(I)/2007 regarding the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007 as amended from time to time ("**AML Law**").
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ("**4th AML Directive**").
- Law 138(I)/2001 regarding the Processing of Personal Data (Protection of Individuals) amended from time to time (the "**Data Protection Law**").
- Regulation (EU) 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**").

2 GDPR references

2.1 Personal Data

- 2.1.1 Under GDPR, *personal data* has been defined as any information relating to an identified or identifiable natural person i.e. that it 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.
- 2.1.2 During the course of the business relationship with the Clients, the Company may collect any of the following types of personal data which are necessary for the provision of investment services and as required by the Applicable Laws and Regulations:
- (a) personal details
 - (b) family and lifestyle details
 - (c) financial details
 - (d) education/employment details
 - (e) medical details and
 - (f) online identifiers such as I.P. addresses, cookie identifiers and RFID tags.

2.2 Processing

- 2.2.1 Under GDPR, *processing* of personal data has been defined as 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.
- 2.2.2 It is noted that the Company does not intend to collect and/or process any personal data which reveals either racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, processing of genetic data, biometric data, health data or data concerning sex life or sexual orientation.
- 2.2.3 It is further noted that the Company does not intend to process personal data collected in any way other than in accordance with the provisions of the Data Protection Law and the GDPR. The Company is committed at protecting the privacy of its Clients and processing data in an open and transparent manner.
- 2.2.4 The Company shall be processing personal data of its Clients for one or more of the following reasons and in accordance with the provisions of the Data Protection Law and GDPR:
- (a) **For the performance of a contract:** the Company shall process personal data in order to perform its obligations under a contract for the provision of investment services and activities to its Clients and in order to satisfy the onboarding procedure as established by the Company for the purposes of entering into a business relationship with its Clients.
 - (b) **Compliance with legal obligations:** As an investment firm, the Company has several legal obligations arising from several national and EU laws i.e. MiFID II and the AML Law, as well as national and EU supervisory authorities i.e. the Cyprus Securities and Exchange Commission ('**CySEC**') and European Securities and Markets Authority ('**ESMA**'). In order for the Company to be in compliance with such laws and regulations, the Company is required to process personal data due to its reporting obligations, its obligations for verification of identity and other anti-money laundering controls.
 - (c) **For the performance of a task carried out in the public interest:** the processing of personal data on the basis of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (herein the "**4th AML Directive**") shall be considered to be a matter of public interest. Under the 4th AML Directive, the Company is obliged to conduct due diligence prior to the establishment of a business relationship or carrying out an occasional transaction with a Client. The Company is required to keep

appropriate records for a period of 5 (five) years after the end of the business relationship and/or the carrying out of an occasional transaction with the Client.

- (d) **Consent:** Provided that a Client has given his specific consent for processing of personal data other than for the reasons set out in paragraphs (a) to (c) above then the lawfulness of such processing is based on such consent. A Client has the right to revoke his consent at any time prior to the processing of personal data.

2.3 Collection

- 2.3.1 The Company collects information about prospective or existing Clients from various sources i.e. from the Client himself and/or through an appointed representative of the Client and/or through alternative channels of communication such as the Company's website and/or Bloomberg, in the context of the business relationship.
- 2.3.2 The Company may also collect personal data from publicly available sources i.e. the Department of Registrar of Companies and Official Receiver, the Bankruptcy Archive, commercial registers, the press, media and the internet). Such information is lawfully obtained and the Company is permitted to process.

2.4 Recipients of Personal Data

- 2.4.1 For the purposes of the establishment and continuation of a business relationship between the Company and its Clients, for the purposes of providing to its Clients, the investment services and activities under its authorization, the Company may share and/or transfer its Clients' personal data to the following recipients:
- (a) Any relevant person in relation to the Company i.e. members of the board of directors, partners or equivalent, manager or a tied agent, employees of the Company or of a tied agent of the Company or of a branch of the Company or of a service provider with whom the Company has an outsourcing arrangement;
 - (b) Supervisory and other regulatory and public authorities located in the Republic and/or within or outside the Union (examples include but are not limited to CySEC and ESMA);
 - (c) The tax authorities established in the Republic of Cyprus and/or any other tax authorities located within or outside the Union;
 - (d) Credit institutions with whom the Company has entered into arrangements for the safekeeping of Clients' assets (i.e. Clients' funds and financial instruments) and/or the settlement of transactions;
 - (e) Auditors (Internal and External) and Accountants;
 - (f) Legal advisors/consultants;
 - (g) Financial and business advisors;
 - (h) Fraud prevention agencies located in the Republic and/or within or outside the Union;
 - (i) Unit for combating money laundering and terrorist financing established in the Republic and/or within or outside the Union;
 - (j) Rating Agencies;
 - (k) The Investor Compensation Fund and the Financial Ombudsman;
 - (l) Regulated and unregulated markets, Multilateral Trading Facilities or Organised Trading Facilities;
 - (m) Stock Exchanges;
 - (n) Marketing companies and other market research companies;
 - (o) File storage companies, archiving and/or records management companies and/or cloud storage companies;
 - (p) Issuer of financial securities;
 - (q) Any other entities to whom the Company might have a statutory duty to transfer and/or share personal data, from time to time.

2.5 Duration of processing/Storage

- 2.5.1 Under the Applicable Laws and Regulations the Company is required to keep records of personal data of its Clients throughout the business relationship and for 5 (five) years after the end of the business relationship. It is noted that the same applies where the Client and the Company have entered into an occasional transaction.
- 2.5.2 For prospective Clients who have provided to the Company any personal data for the purposes of entering into a business relationship with the Company and who have been notified of the Company's decision not to proceed

with the establishment of the business relationship, the Company may keep such personal data for a period no longer than 6 (six) months from the date that the Company has communicated its decision to the prospective Client.

- 2.5.3 The Company undertakes to erase any personal data received when it is no longer required to be recorded pursuant to the Applicable Laws and Regulations.

3 Rights of Clients

3.1 Right of Access

- 3.1.1 The Client shall have the right to obtain from the Company confirmation whether or not personal data concerning him are being processed, and where that is the case, access to the personal data and the following information:
- (a) The purposes of the processing;
 - (b) The categories of personal data concerned;
 - (c) The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (d) The envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period;
 - (e) The existence of the right to request for the rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;
 - (f) The right to lodge a complaint;
 - (g) Where the personal data are not collected from the Company, any available information as to their source;
 - (h) The existence of automated decision-making, including profiling and the consequences of such processing.
- 3.1.2 The Client shall have right to be informed of appropriate safeguards where his personal data are transferred to a third country or to an international organisation.
- 3.1.3 The Client shall have the right to obtain a copy of the personal data undergoing processing.

3.2 Right to Rectification

- 3.2.1 The Client has the right to request from the Company to rectify inaccurate personal data concerning his person and complete any incomplete personal data held by the Company.

3.3 Right to Erasure

- 3.3.1 The Client shall have the right to obtain from the Company the erasure of personal data concerning him without undue delay and the Company shall have the obligation to erase personal data without undue delay where one of the following grounds apply:
- (a) The personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
 - (b) The Client withdraws his consent on which the processing is based and there are no other legal grounds for the processing;
 - (c) The Client objects to the processing and there are no overriding legitimate grounds for the processing;
 - (d) The personal data have been unlawfully processed;
 - (e) The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject;
 - (f) The personal data have been collected in relation to the offer of information society services.
- 3.3.2 The Client acknowledges and understands that the right for erasure does not apply to the extent that processing is necessary either:
- (a) For exercising the right of freedom of expression and information;
 - (b) For compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company;
 - (c) For reasons of public interest in the area of public health;
 - (d) For achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right of erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - (e) For the establishment, exercise or defence of legal claims.

3.3.3 The Client acknowledges, agrees and understands that the Company shall not proceed with the erasure of any personal data unless the personal data are no longer necessary for the purposes for which it was collected and/or unless the Company is no longer required to comply with its legal obligations as a CIF under the Applicable Laws and Regulations.

3.4 Right to Restriction of Processing

3.4.1 The Client shall have the right to obtain from the Company restriction of processing where one of the following applies:

- (a) The accuracy of the personal data is contested by the Client, for a period enabling the Company to verify the accuracy of the personal data;
- (b) The processing is unlawful and the Client opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) The Company no longer needs the personal data for the purposes of processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) The Client has objected to the processing pending the verification whether the legitimate grounds of the Company override those of the Client.

3.4.2 Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Client's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3.4.3 The Company shall notify each recipient to whom personal data has been disclosed of the rectification or erasure of personal data or restriction of processing of such personal data, unless this proves impossible or involves disproportionate effort.

3.4.4 The Client has the right to request from the Company to be informed of those recipients.

3.5 Right to Data Portability

3.5.1 The Client shall have the right to receive the personal data concerning him, which he has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, where:

- (a) The processing is based on consent or on a contract;
- (b) The processing is carried out by automated means;

3.5.2 The Client has the right to request from the Company to have his personal data transmitted directly from the Company to another controller, where technically feasible.

3.6 Right to Object

3.6.1 Where the Company has declared to the Client that the processing of his personal data is lawful based on the following reasons, the Client shall have the right to object, on grounds relating to his particular situation, at any time to the processing of his personal data:

- (a) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company; or
- (b) The processing is necessary for the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Client which require protection of personal data.

3.6.2 In order for the Company to continue the processing of the Client's personal data, the Company has to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Client or for the establishment, exercise or defense of legal claims.

3.6.3 Where the Client's personal data are to be processed for direct marketing purposes, the Client shall have the right to object at any time to the processing of his personal data for such marketing, including profiling to the extent that it is related to such direct marketing.

- 3.6.4 The Company undertakes to no longer process the Client's personal data for direct marketing purposes where it has received an objection from the Client.
- 3.6.5 The Company shall inform the Client of his right to object to direct marketing at the first time of communication with the Client.

3.7 Automated individual decision-making

- 3.7.1 The Client shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him.
- 3.7.2 This right shall not apply where such a decision:
- (a) Is necessary for entering into, or performance of, a contract between the Company and the Client;
 - (b) Is authorised by Union or Member State law to which the Company is subject and which also lays down suitable measures to safeguard the Client's rights and freedoms and legitimate interests; or
 - (c) Is based on the Client's explicit consent.

3.8 Right to lodge a complaint, remedies and liabilities

- 3.8.1 The Client shall have the right to lodge a complaint with a supervisory authority, in particular, in the Member State of his habitual residence, the place of work or the place of the alleged infringement and if successful, the Client shall have the right to an effective judicial remedy against the legally binding decision of the supervisory authority.
- 3.8.2 The Client shall have the right to an effective judicial remedy where the competent supervisory authority fails to handle his complaint and/or does not inform the Client on the progress/outcome of his complaint within 3 (three) months. Such proceedings can be brought before the courts of the Member State where the supervisory authority is established.
- 3.8.3 Without prejudice to any available administrative or non-judicial remedy, the Client shall have the right to an effective judicial remedy where he considers that his rights have been infringed. Proceedings against a controller or a processor may be brought before the courts of the Member State where the controller or processor is established.
- 3.8.4 If the Client has suffered a material or non-material damage as a result of an infringement of his rights under the GDPR, he shall have the right to receive compensation, provided that the damage was caused by the processing of personal data which infringes the provisions of the GDPR.
- 3.8.5 It is noted that court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State where the controller/processor are established.

4 Data Protection

4.1 Data Protection Measures

- 4.1.1 The Company has been registered with the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus. The Company ensures that all Clients' personal data is kept in accordance with the Applicable Laws and Regulations.
- 4.1.2 The Company has implemented appropriate technical and organisational measures to ensure that data protection principles are implemented in an effective manner and has integrated necessary safeguards into the processing of personal data to protect the rights of its Clients and to comply with the requirements of the Data Protection Law and GDPR.
- 4.1.3 The Company has implemented appropriate technical and organisational measures to ensure that only personal data which are necessary for each specific purpose of the processing are processed. To that effect, the Company shall:
- (a) Collect only the necessary personal data which are required to be collected by virtue of its legal obligations to comply with Applicable Laws and Regulations;
 - (b) Process personal data to the extent Applicable Laws and Regulations;
 - (c) Store personal data for the period specified by the Applicable Laws and Regulations;
 - (d) Ensure that personal data is accessible only to individuals who are permitted to have access to such personal data as required by Applicable Laws and Regulations.

4.2 Security of Processing

- 4.2.1 In order to comply with its legal obligations under the Data Protection Law and the GDPR, the Company shall apply the following security measures:
- (a) Pseudonymisation and encryption of personal data;
 - (b) The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident by establishing a disaster recovery plan;
 - (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.3 Notification of Personal Data Breach

- 4.3.1 Where the Company has identified a personal data breach, it shall inform the supervisory authority without undue delay and not later than 72 (seventy-two) hours after having become aware of the breach.
- 4.3.2 The Company shall maintain records and documentation of any personal data breaches identified, comprising the facts relating to the personal data breach, its effects and the remedial action taken.
- 4.3.3 Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall communicate the personal data breach to the Client without undue delay, describing in a clear and plain language the nature of the breach and measures to be taken.

4.4 Administrative Fines

- 4.4.1 The supervisory authority shall have the right to impose administrative fines in respect of infringements of the GDPR which are effective, proportionate and dissuasive in each individual case.

5 Other requirements

5.1 Record keeping

- 5.1.1 The Company shall maintain a record, in writing or in electronic form, of the processing activities conducted by it, which shall contain the following information:
- (a) The name and contact details of the Company (or where applicable the joint controller, the Company's representative) and the data protection officer;
 - (b) The purposes of the processing;
 - (c) A description of the categories of data subjects and of the categories of personal data;
 - (d) The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
 - (e) Where applicable, transfers of personal data to a third country or an international organisation and documentation of suitable safeguards;
 - (f) Where possible, the envisaged time limits for erasure of the different categories of data;
 - (g) Where possible, a general description of the security measure adopted by the Company.
- 5.1.2 The Company shall make such records available to the supervisory authority on request.

5.2 Review and Amendments

- 5.2.1 The Privacy Statement shall be reviewed by the Company at least on an annual basis or sooner in response to any change in the legal and regulatory framework affecting data protection.
- 5.2.2 The Company shall keep its Clients informed of any amendments to this Privacy Statement as appropriate.