



**LEON**  
MFO Investments

---

# **DATA PRIVACY POLICY**

*in relation to the provision of  
investment services*

---

**VERSION 1**

**10 April 2020**

**TABLE OF CONTENTS**

<b>1. INTRODUCTION.....</b>	<b>3</b>
<b>2. LEGAL FRAMEWORK .....</b>	<b>3</b>
<b>3. DATA PROTECTION OFFICER.....</b>	<b>4</b>
<b>4. PURPOSE AND SCOPE .....</b>	<b>4</b>
<b>5. COLLECTION OF PERSONAL DATA .....</b>	<b>4</b>
<b>6. LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA.....</b>	<b>5</b>
<b>7. CLIENTS' OBLIGATION TO PROVIDE THE COMPANY WITH PERSONAL DATA .....</b>	<b>6</b>
<b>8. SHARING AND DISCLOSURE OF PERSONAL DATA .....</b>	<b>6</b>
<b>9. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA.....</b>	<b>7</b>
<b>10. PERSONAL DATA RETENTION PERIOD.....</b>	<b>7</b>
<b>11. DATA SUBJECTS RIGHTS.....</b>	<b>7</b>
<b>12. INTERNATIONAL TRANSFER OF PERSONAL DATA .....</b>	<b>8</b>
<b>13. AUTOMATED DECISION-MAKING AND PROFILING .....</b>	<b>9</b>
<b>14. DIRECT MARKETING.....</b>	<b>9</b>
<b>15. CHANGES OF THE POLICY .....</b>	<b>9</b>

## 1. Introduction

Leon MFO Investments Limited (hereinafter the “**Company**” or “**LEON MFO**”) is registered and incorporated under the Laws of Cyprus with registration number HE 326316 and authorised as an Alternative Investment Fund Manager (hereinafter the “**AIFM**”) by the Cyprus Securities and Exchange Commission (hereinafter the “**CySEC**”) in accordance with the provisions of the Alternative Investment Fund Managers Law of 2013, as amended from time to time (hereinafter the “**AIFM Law**”), with authorisation number AIFM 37/56/2013.

In addition to the collective management of Alternative Investment Funds, the Company under its capacity as an AIFM is also authorised by CySEC to provide the following services:

- i. the management of portfolios of investments, including those owned by pension funds and institutions for occupational retirement provision in accordance with paragraph 1 of Article 19 of Directive 2003/41/EC, in accordance with mandates given by investors on a discretionary, client-by-client basis under section 6(6)(a) of the AIFM Law (hereinafter the “**Portfolio Management Service**”); and
- ii. the non-core service of investment advice under section 6(6)(b)(i) of the AIFM Law.

[services (i) and (ii) above shall be collectively referred to as the “**Investment Services**”].

In accordance with section 6(8) of the AIFM Law, whenever the Company provides any of the Investment Services, a number of provisions of the Investment Services and Activities and Regulated Markets Law of 2017, as amended from time to time, (hereinafter the “**Law 87(I)/2017**” or the “**Law**”) will apply to the Company, irrespective of the Company being an authorised AIFM under the AIFM Law. This is because the Company, will be providing services that fall under the definition of investment services of Law 87(I)/2017.

This Data Privacy Policy (hereinafter the “**Policy**”) of the Company sets out the rules on collecting, maintaining, using, disclosing and safeguarding personal data (hereinafter the “**Personal Data**”) in relation to the Investment Services. The Policy is the internal document approved by the board of directors of the Company and the provisions of the Policy are mandatory for each director, officer and employee of the Company involved with the provision of Investment Services. This Policy applies to natural persons who are existing or prospective clients or who act as authorized representatives of legal entities or natural persons who are current or prospective clients of the Company or are the directors or beneficial owners of legal entities who are existing or prospective clients of the Company (hereinafter jointly referred to as the “**Clients**” or “**Data Subjects**”). This Policy also applies to natural persons who had such business relationship with the Company in the past.

## 2. Legal Framework

The Company is committed to protecting the privacy of all Clients’ Personal Data, which it processes in accordance with the provisions of the European General Data Protection Regulation (EU) 2016/679 (hereinafter the “**GDPR**”) and any laws or regulations in the Republic of Cyprus, which implement or supplement the GDPR (hereinafter referred to collectively as the “**Data Protection Legislation**”).

For the purposes of this Policy, references to “Personal Data” shall mean data, which identifies or may identify Clients, directly or indirectly, and which may include, for example, a Client’s name, address, identification number, telephone number and date of birth. The Company acts as a controller of the Personal Data under GDPR, which means that it determines solely or jointly with others, the purposes and means of the processing of the Personal Data. ‘Processing’ means any operation or set of operations, which is performed on Personal Data, such as collection, recording, storage, use, disclosure, erasure or destruction.

### **3. Data protection officer**

The GDPR requires appointment of a data protection officer. The data protection officer of the Company is its compliance officer. The data protection officer is responsible for educating the Company and its employees about compliance, training staff involved in data processing, and conducting regular security audits. The data protection officer also serves as the point of contact between the Company and any supervisory authorities that oversee activities related to Personal Data. In addition, the data protection officer maintains comprehensive records of all data processing activities conducted by the Company and interfaces with Data Subjects to inform them about how their data is being used, their right to have their Personal Data erased, and what measures the Company has put in place to protect their Personal Data.

### **4. Purpose and Scope**

This Policy provides, inter alia, information on the following key areas:

- (a) the categories of Personal Data that is collected and processed by the Company and the purposes of that processing;
- (b) the legal basis for the processing of Personal Data;
- (c) the recipients or categories of recipients of Personal Data;
- (d) the principles relating to the processing of Personal Data;
- (e) Clients’ rights under applicable legislation and an explanation of how those rights can be exercised.

### **5. Collection of Personal Data**

The Company collects different types of Personal Data from Clients. The provision of certain Personal Data is required for establishing a contractual relationship with the Company. The Company will not be able to render its investment services to Clients, if they are not wishing to provide Personal Data to the Company.

Clients have a responsibility to ensure that the Personal Data they provide to the Company and recorded in their personal files remain accurate and up to date throughout the period of their contractual relationship with the Company.

In addition to the information provided by Clients, the Company also lawfully collects and processes Personal Data from publicly available sources (including, inter alia, the press, social media and the Internet) and third-party risk management software solutions in order to meet its regulatory obligations (including background checks on information in relation to criminal convictions, offences and sanctions lists) and for confirming the validity of the provided information.

In order to establishing a contractual relationship with the Company, the following Personal Data is required from Clients:

- (a) Personal information such as name, gender, age, date and place of birth, citizenship, nationality, home address, passport/ ID number, FATCA/ CRS information (tax residency, tax identification number), contact details (telephone, email), bank account details, education, occupation and information on whether a Client holds/held a prominent public function (for PEPs);
- (b) Financial information such as income, source of wealth and source of funds, experience in investments and investment objectives;
- (c) Documents that verify your identity and residency such as an international passport or national ID and utility bills or bank statements.

## 6. Legal basis for the processing of Personal Data

The protection of Personal Data is of great importance to the Company. Personal Data is processed lawfully, fairly and in a transparent manner on the following basis:

- (a) ***For the performance of a contract.*** The processing of Personal Data is necessary for the performance of a contract, namely the investment services agreement, or in order to take steps at Clients' request prior to entering into a contract. In order to be able to render investment services to a Client and administer the relationship between the Company and a Client, the Company needs to collect certain information about a Client's identity, financial background and investment objectives. Processing is necessary for the Company in order to provide the Client with its products and services, and more specifically in order:
  - To verify the Client's identity and carry out any required background checks;
  - To ensure that the Client meets the suitability requirements to use the Company's services;
  - To process the Client's transactions; and
  - To send to the Client any information about transactions/post-transactions services.
- (b) ***For compliance with a legal obligation.*** The processing of Personal Data is necessary for compliance with the legal obligations emanating from a number of laws, to which the Company is subject, e.g. the European Markets in Financial Instruments Directive (hereinafter the "**MiFID II**") and the corresponding Investment Services and Activities and Regulated Markets Law of the Republic of Cyprus, the European and Cyprus legislation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the Common Reporting Standard (hereinafter the "**CRS**"), the Market Abuse Regulation (hereinafter the "**MAR**"), the European Market Infrastructure

Regulation (hereinafter the “**EMIR**”), the Foreign Account Tax Compliance Act (hereinafter the “**FATCA**”), sanctions or restrictive measures of the EU, the UN and the US (hereinafter the “**Sanctions**”). Compliance with these legal obligations requires, inter alia, identity verification procedures and processes, anti-money laundering controls, the retention of Personal Data for a certain period of time, the disclosure of Personal Data to the supervisory and other regulatory and public authorities, etc.

- (c) ***For the purposes of the legitimate interests pursued by the Company.*** The processing of Personal Data is necessary for the purposes of the legitimate interests pursued by the Company, where those interests do not infringe Clients’ interests, fundamental rights and freedoms. These legitimate interests include business interests and examples of relevant processing activities include: preparing the Company’s defense in litigation procedures; preventing fraud and money laundering activities; managing business and further developing and marketing of products and services.

## **7. Clients’ obligation to provide the Company with Personal Data**

The provision of Personal Data is a requirement necessary to enter into a contract with the Company. Clients have statutory and contractual obligation to provide and keep up to date and accurate Personal Data they provide to the Company. Failure to provide such data will not allow the Company to commence or continue business relationship, as compliance with the Company’s legal obligations will be deemed impossible.

## **8. Sharing and disclosure of Personal Data**

In the course of the performance of contractual and statutory obligations and for legitimate business purposes, Personal Data may be disclosed by the Company to:

- (a) Supervisory and other regulatory and public authorities, upon request or where required. Some examples are the CySEC, the Unit for Combating Money Laundering (MOKAS), criminal prosecution authorities;
- (b) Bankers, auditors, lawyers, tax consultants and other external professional advisors of the Company for the purposes of their internal anti-money laundering controls;
- (c) Data reporting service providers;
- (d) Affiliates of the Company;
- (e) Third party processors such as services providers who assist the Company with the effective provision of investment services to Clients by offering technological expertise, solutions and support, file storage and records management companies. All data processors appointed by the Company to process Personal Data on behalf of the Company are bound by contract to comply with the GDPR provisions.

## **9. Principles relating to the processing of Personal Data**

The Company implements appropriate technical and organizational measures to ensure appropriate security of Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

The Company takes reasonable steps to ensure that Personal data that the Company processes is accurate and, where necessary, is kept up to date. From time to time the Company may request from Clients to confirm the accuracy of Personal Data. The Company takes every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purposes, for which it is processed, is erased or rectified without delay.

The Company also makes sure that all Personal data that is collected is adequate, relevant and limited to what is necessary in relation to the purposes, for which it is processed.

## **10. Personal Data retention period**

The Company retains Personal Data for the duration of business relationship with a Client and for five (5) years after the termination of the business relationship, unless otherwise requested by a competent authority, in line with the provisions of the applicable legislation.

The Company may keep Personal Data for longer, if it cannot delete the data for legal or regulatory reasons. In particular, the retention of data is not limited in time in the case of pending legal proceedings or an investigation initiated by a public authority, provided that in each case the Company has been informed of the pending legal proceedings or the investigation initiated by a public authority within the retention period described hereinabove.

## **11. Data Subjects rights**

Clients have the following rights regarding their Personal Data that the Company controls and processes:

- (a) **Right of access.** The Client has the right to be informed whether the Company is processing his/her Personal Data, and if so, to provide the Client with a copy of that Personal Data.
- (b) **Right to rectification.** The Client is entitled to request that the Company corrects or completes his/her Personal Data, if it is inaccurate or incomplete.
- (c) **Right to erasure.** The right to request, on legitimate grounds and where there is no good reason for the Company continuing to process it, erasure of the Client's Personal data.
- (f) **Right to object.** The Client may ask the Company at any time to stop processing his/her Personal Data, and the Company will do so:

- If the Company is relying on a legitimate interest to process the Client's Personal Data and the Company cannot demonstrate compelling legitimate grounds for the processing, or
  - If the Company is processing Client's Personal Data for direct marketing.
- (g) **Right to restrict processing.** This enables the Client to ask the Company to restrict the processing of the Client's Personal Data if:
- it is not accurate;
  - it has been used unlawfully, but the Client doesn't want it to be deleted;
  - it is not relevant any more, but the Client wants the Company to keep it for use in possible legal claims;
  - the Client has already asked the Company to stop using his/her Personal Data, but he/she is waiting for the Company to confirm, if it has legitimate grounds to use such Personal Data.
- (h) **Right to data portability.** The right to have Personal Data transferred to another controller, to the extent applicable.
- (i) **Rights in relation to automated decision-making and profiling.** The Client has the right to be free from decisions based solely on automated processing of his/her Personal Data, including profiling, that affect him/her, unless such profiling is necessary for entering into or the performance of a contract between Client and the Company or the Client provides explicit consent.
- (j) **Right to withdraw consent.** If the Company relies on the Client's consent to process his/her Personal Data, the Client has the right to withdraw that consent at any time. This will not affect the lawfulness of the processing that took place on the basis of the Client's prior consent.
- (k) **Right to lodge a complaint with the data protection authority.** The Client has the right to lodge a complaint regarding the processing of Personal Data by the Company. The Client can lodge his/her complaint at [compliance@leonmfo.com](mailto:compliance@leonmfo.com). If a Client believes that his/her concerns have not been adequately addressed by the Company, the Client has the right to lodge a complaint with the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus. Information about submitting a complaint could be found on the following website - <http://www.dataprotection.gov.cy>.

## **12. International transfer of Personal Data**

Personal Data may be transferred to third countries (i.e. countries outside the European Economic Area), to recipients mentioned in paragraph above, in connection with the purposes set out in this Policy.

The Company may transfer Personal Data to countries that may have different laws and data protection compliance requirements; however processors in third countries are obliged to comply with the European data protection standards, when processing Personal Data.



### **13. Automated decision-making and profiling**

The decision to establish a business relationship with a Client is not based on automated processing of Personal Data. The Company may process some of Personal Data automatically, in order to comply with regulatory requirements the Company is subject to. Data assessments, including transaction monitoring, are carried out in the context of combating money laundering and fraud.

### **14. Direct marketing**

The Company may process Personal Data to contact Clients, primarily by email, in order to provide them with information concerning services that may be of interest to the Clients. It should be noted that in accordance with the applicable law, the processing of Personal Data for direct marketing purposes may be regarded as carried out for a legitimate interest pursued by the Company. However, if a Client does not wish to receive marketing communications from the Company, such Client can opt out at any time by contacting the Company. After a Client unsubscribes, the Company will not send further promotional emails, but the Company will continue to contact a Client to the extent necessary for the purposes of any services that such a Client has requested.

### **15. Changes of the Policy**

The board of directors of the Company may amend this Policy at any time. Clients will be notified about material changes, however they are encouraged to review this Policy periodically, so as to be always informed about how the Company is processing and protecting Personal Data.