



# Customer Personal Data Protection Policy

**Piraeus Asset Management**  
Single Member Mutual Funds Management Company  
General Commercial Registry No. 6314201000  
87 Syngrou Avenue 117 45 Athens  
Tel.: +30 (210) 328 82 22 | Fax: +30 (210) 328 86 90  
E-mail: [piraeusaedak@piraeusbank.gr](mailto:piraeusaedak@piraeusbank.gr)  
[www.piraeusaedak.gr](http://www.piraeusaedak.gr)

## Content

<b>Customer Personal Data Protection Policy .....</b>	<b>3</b>
• 1. Purpose and Basic Principles .....	3
• 2. Legislative and Regulatory Framework .....	3
• 3. Definitions .....	3
• 4. Processing of customer personal data by the Company .....	4
4.1. Lawfulness of processing .....	4
4.2. Obligation of previous information .....	5
4.3. Data subject to processing .....	5
4.4. Purposes of processing .....	7
4.5. Safekeeping and maintenance period .....	7
4.6. Recipients .....	7
4.7. Security .....	8
4.8. Data Protection Impact Assessment .....	8
4.9. Transfer of personal data to third countries/international organizations .....	9
• 5. Right of customers as data subjects .....	9
• 6. Security of Personal Data .....	10
6.1. Security of processing .....	10
6.2. Personal Data Breach .....	10
• 7. Obligations of the Company .....	11
7.1. Privacy by design .....	11
7.2. Privacy by default .....	12
7.3. Records of activities .....	12
7.4. Training of personnel .....	12
7.5. Recording of telephone conversations .....	12
• 8. Delegation of processing to processors .....	13
• 9. Data Protection Officer .....	13

# Customer Personal Data Protection Policy

## ➤ 1. Purpose and Basic Principles

Piraeus Asset Management M.F.M.C. (hereinafter the “Company”) shall establish a Customer Personal Data Protection Policy (hereinafter the “Policy”) aiming to the protection of the customer personal data collected and processed by the M.F.M.C., as well as to the prevention of any form of unlawful/unfair processing, accidental/unlawful destruction, loss, alteration, prohibited dissemination or access thereto.

The Customer Personal Data Protection Policy and the personal data processing conducted by the Company, which is based thereon, rely on the following principles:

- Lawfulness, objectiveness and transparency in the processing
- Restriction of purpose of processing
- Minimization of processed data
- Accuracy and updating of processed data
- Integrity and confidentiality in the processing
- Restriction of maintenance/storage period
- Compliance with the relevant applicable legislative and regulatory framework from time to time

The Company shall be responsible and shall always be able to evidence its continuous compliance with the above principles, as specified in this Policy.

The Company shall control, review and update in regular intervals and, in any case, when considered necessary, this Policy in view of the applicable legislative and regulatory framework from time to time.

## ➤ 2. Legislative and Regulatory Framework

The Company shall adopt and apply this Policy, in its capacity as **Personal Data Controller**, in the framework of its compliance with the provisions of the General Data Protection Regulation (EU) 2016/679 (hereinafter “GDPR”) and Greek law 4624/2019, including the decisions, circulars, opinions and, in general, acts issued by the Hellenic Data Protection Authority.

## ➤ 3. Definitions

“**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.

“**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.

“**processor**”: means a natural or legal person that processes personal data on behalf of the controller.

**“processing”**: means any collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, restriction or erasure of their personal data which have come or shall come to the knowledge of PIRAEUS ASSET MANAGEMENT M.F.M.C., both in the framework of its transaction relationships with customers and in the framework of information received by the Company from third, natural or legal, persons or entities of the public sector upon the exercise of the legal rights of them or the Company.

**“profiling”**: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

**“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.

**“customer” of the Company**: any natural person who has acquired UCITS units/shares managed and/or represented by the company, as well as any natural person to whom the Company provides investment services. In case of customers – legal persons, as customers for the purposes of this Policy shall be considered the natural persons legally representing the customers – legal persons.

**“restriction of processing”**: the labelling of stored personal data with the purpose of restriction of the processing in the future.

**“consent” of the customer**: any freely given, specific, informed and unambiguous indication of the Company customer’s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

**“third party”**: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons that, under the direct authority of the controller or processor, are authorised to process personal data.

**“controller”**: the legal person which determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company shall be considered as the Controller.

**“data protection officer”**: the natural or legal person appointed by the controller in order to participate in all matters related to personal data protection, according to this Policy and the applicable legislative and regulatory framework from time to time, that undertakes to exercise the duties described in Article 9 hereof.

**“data subject”**: any identified or identifiable natural person to whom the person data under processing are related. For the purposes of this Policy, the customers of the Company shall be considered as data subjects.

## ➡ 4. Processing of customer personal data by the Company

### 4.1. Lawfulness of processing

The Company shall process the personal data of its customers in the following cases, according to those specifically defined in the applicable legislation and the terms and conditions set out therein:

1. if processing is necessary for the service, support and monitoring of its transaction relationships with its customers, as well as for the correct and lawful performance of the contracts between them. The processing considered necessary to take the necessary steps upon request of the customer prior to entering into a contract (pre-contractual stage) is included in this case,
2. if processing is necessary for the compliance of the Company with a legal obligation or for the pursue of its legitimate interests arising from its transaction relationships with the customers or other rights arising from the applicable legislation,
3. if processing is necessary for the performance of a task carried out in the public interest, according to the applicable legislative and regulatory framework from time to time\*,
4. if processing is necessary for the establishment, exercise or defence of legal claims.
5. if the customer has given consent to the processing of their personal data for one or more specific purposes and under the condition that the processing is not based on one of the above-mentioned legitimate bases under 1 – 4. In this case, the customer has the right to withdraw their consent and the relevant withdrawal shall not affect the lawfulness of the processing based on the consent prior to its withdrawal. Withdrawal shall be conducted by a relevant document submitted, in writing or electronically, to the Company (addressed to the Data Protection Officer) and shall enter into force from the date of its submission and onwards.

\*It is noted that personal data are processed by M.F.M.C. also according to the provisions of Law 4557/2018 with the purpose of preventing and combating money laundering and terrorist financing. In this context, personal data may be transferred to the competent authorities, which supervise the implementation of the above provisions, as well as to other public authorities entrusted with tasks for combating money laundering and terrorist financing. The processing of personal data for the aforementioned purpose is considered as a matter of public interest.

#### **4.2 Obligation of previous information**

In case the processing of personal data by the Company is based on a relevant consent of the customer, the Company, prior to the acquisition of the required specific, explicit and written consent, according to the above, shall inform the customer, as a minimum, of the following:

- i. its capacity as Data Controller,
- ii. the contact details of the Data Protection Officer,
- iii. the type of personal data processed,
- iv. the purpose/purposes of processing,
- v. the legal basis of processing,
- vi. the categories of possible data recipients,
- vii. the storage period of data,
- viii. the rights of the customer as regards to its processed data.

#### **4.3. Data subject to processing**

4.3.1. The Company processes customer personal data which:

- I. have been submitted or will be submitted by the customers themselves or by their legal representatives, which are necessary for the initiation, maintenance and performance of their transaction relationships with the Company, existing or future ones,
- II. acquires or come to its knowledge by third, natural or legal persons or by public entities, if they are necessary for the achievement of the legitimate interests of the Company or a third person, or for the performance of its tasks carried out in the public interest
- III. come from sources and/or records accessible to the public and to the extent that they are necessary for the purposes of processing.

Personal data coming from customers must be complete and accurate and they must be updated with the care of the customers themselves, promptly in each case of change thereof or whenever it is considered necessary or appropriate by the Company for the maintenance of the transaction relationships between them or the compliance of the Company with its obligations arising from the applicable legislative and regulatory framework from time to time.

For the initiation and maintenance of its transaction relationship with its customers, PIRAEUS ASSET MANAGEMENT M.F.M.C., in compliance with the applicable legislative and regulatory framework governing the mutual fund management companies which, at the same time, provide investment services (M.F.M.C. of extended purpose), shall collect, maintain and process the following personal data of its customers, which are necessary pursuant to the applicable legislation, restricted to the minimum required for the purposes for which they are processed:

- name and surname,
- father's name,
- details of identity card/passport or another official document,
- date of birth,
- nationality,
- permanent place of residence, residence address and correspondence address,
- profession and professional address,
- tax residence, tax identification number (TIN) and competent Tax Office,
- phone number (fixed and mobile),
- Utilities bills (electricity, telephony or water supply),
- E-mail address,
- Financial/investment profile, knowledge and experience in investment and
- Signature sample (physical or electronic).

#### 4.3.2. Children's data

The processing of personal data related to minors shall be performed under the strict condition of previous approval of the parents or persons exercising parental responsibility, according to those especially set out by the applicable legislation from time to time.

#### 4.3.3. Special categories of data

PIRAEUS ASSET MANAGEMENT M.C.M.F. shall not process its customers' personal data which reveal race or national origin, political opinions, religious or philosophical beliefs or the participation in a trade union, or genetic or biometric data with the purpose of identification of the customer or data related to the health or sexual life of the customer or the sexual orientation thereof.

#### 4.4. Purposes of processing

Purposes of processing of the personal data of the Company's customers are:

- a) the service, support and monitoring of the interest of the unitholders in the UCITS managed and/or represented by PIRAEUS ASSET MANAGEMENT M.F.M.C., based on the applications of entry, redemption and redemption-reinvestment to UCITS managed/represented by the Company,
- b) the service, support and monitoring of the transaction relationships of PIRAEUS ASSET MANAGEMENT M.F.M.C. with customers to whom it provides portfolio management and/or investment consultancy services, as well as the correct and lawful performance of the contracts between them,
- c) the registration, recording and archiving of all kinds of orders, application and requests of the customers to the Company given in writing, electronically or by phone, in the framework of their participation in UCITS managed and/or represented by PIRAEUS ASSET MANAGEMENT M.F.M.C. or the provision thereto of investment services by the M.F.M.C.,
- d) the fulfilment of the obligations of PIRAEUS ASSET MANAGEMENT M.F.M.C. arising from the applicable legislative and regulatory framework from time to time in the framework of UCITS management and/or representation and provision of investment services, as well as its compliance with the decisions of the competent supervisory, administrative, public and judicial/prosecutorial Authorities and Services,
- e) the satisfaction of all kinds of requests of the customers addressed to the Company and the examination of complaints of the customers, and
- f) the sending of print and electronic messages to customers for advertisement/promotional reasons, if they have previously given specific consent to the Company.

#### 4.5. Safekeeping and maintenance period

The personal data of the Customers of the Company are processed, maintained and kept by PIRAEUS ASSET MANAGEMENT M.F.M.C. in a safe environment, exclusively and solely for the intended purposes and only for as long as it is necessary for the achievement of such purposes, subject to those specifically provided for by the applicable legislation. In any case, the personal data of customers shall be maintained for a period of twenty (20) year from the termination in any way of the contractual relationship between the Company and the customer or from the full redemption by the customer of all UCITS units under management and/or representation, as the case may be. The above time limits shall not apply in case of judicial disputes, in which case the provided time of maintenance of data is extended until the adoption of irrevocable judgement.

#### 4.6. Recipients

Recipients of the personal data of the Company's customers may be the following:

- i) any credit institution acting as a depositary/sub-depositary of the UCITS under the management and/or representation of the Company, the brokers/sub-brokers appointed from time to time for the disposal of UCITS units under the management and/or representation of the Company, as well as

third persons – providers, to whom PIRAEUS ASSET MANAGEMENT M.F.M.C. has delegated its operations in the framework of UCITS management/representation and investment services provision, pursuant to a relevant contract,

ii) third persons, to whom PIRAEUS ASSET MANAGEMENT M.F.M.C. has delegated, in whole or in part, the exercise of operations of personal data processing, for the best service of UCITS management and representation and investment services provision to customers, as well as of its compliance with the applicable legislative and regulatory framework from time to time,

iii) third persons, with whom PIRAEUS ASSET MANAGEMENT M.F.M.C. A.E.Δ.A.K. cooperates in exercising its activities, with the purpose of fulfillment of its obligations in the framework of UCITS management and representation and investment services provision to customers,

iv) the UCITS management companies that PIRAEUS ASSET MANAGEMENT M.F.M.C. represents, their depositaries, as well as any person, to whom the management companies and depositaries of UCITS represented by the Company have delegated the exercise of their operations in the framework of such UCITS management/representation, including the processing of the personal data of customers on their behalf, pursuant to a relevant contract,

v) all businesses of Piraeus Bank Group, to the extent that the relevant transfer serves the interest of unitholders in UCITS managed and/or represented by the Company or the provision of investment services by the Company to its Customers,

vi) any person to whom the transfer must be made, pursuant to the applicable legislative and regulatory framework or based on a judicial judgment, and

vi) the supervisory authorities competent for the audit and operation of the UCITS managed and/or represented by PIRAEUS ASSET MANAGEMENT M.F.M.C. and of the Company, as well as any public, administrative, supervisory, judicial, prosecutorial or other Authority and/or Service upon the exercise of its lawful duties.

#### **4.7. Security**

PIRAEUS ASSET MANAGEMENT M.F.M.C. has taken the appropriate technical and organizational measures to ensure privacy and for the lawful maintenance, processing, protection and safekeeping of the personal data of its customers from any illegal or unlawful processing, accidental or unlawful destruction, loss, alteration, prohibited dissemination or access, according to those specifically set out in the applicable legislation. Such measures shall be reviewed and updated, whenever it is considered necessary.

#### **4.8. Data Protection Impact Assessment**

In case the Company, taking into account the nature, scope, framework and purposes of processing, considers that it may result in a high risk to the rights and freedoms of its customers, it shall carry out, prior to the processing and with the assistance of the Data Protection Office, an assessment of the impact of the envisaged processing operations on the protection of personal data, which shall include all details provided for by Article 35 of the GDPR. The above impact assessment shall be considered necessary in case of systematic and extensive evaluation of personal aspects relating to



customers, which is based on automated processing, including profiling, and on which decisions are based, that produce legal effects concerning the customers or similarly significantly affect the customers.

An impact assessment, according to the above, shall be carried out in any case of use of new technologies or adoption/conduct of data processing operations which may result in a high risk to the rights and freedoms of the customers as personal data subjects.

If it is considered necessary and, mainly, if the risk raised by the processing operations changes, the Company shall proceed to the review, in order to assess if the processing of personal data is carried out according to the data protection impact assessment.

#### **4.9. Transfer of personal data to third countries/international organizations**

The transfer of personal data to a third country or international organization may be carried out only if an adequate level of protection is ensured by the third country or international organization. Otherwise, the Company may transfer personal data to a third country or international organization, only under the strict conditions provided for in the GDPR.

### **➤ 5. Right of customers as data subjects**

The customers of PIRAEUS ASSET MANAGEMENT M.F.M.C., as data subjects, have the following rights:

- a) Right of information and access to personal data related to them and receiving information on them, as well as on their origin, the purposes of their processing, the recipients or the categories of recipients and the period of storage thereof\*.
- b) Right to rectification of inaccurate data and completion of incomplete kept data.
- c) Right to erasure of data, subject, however, to the obligations and legal rights of the Company to maintain them for a minimum specified period, pursuant to the applicable legislative and regulatory framework from time to time.
- d) Right to restriction of data processing, if either their accuracy is contested, or their processing is unlawful, or the purpose of their processing no longer exists and under the condition that there is no lawful reason for their maintenance.
- e) Right to data portability to another controller under the condition that the processing is based on the consent of the customer and it is carried out by automated means. The satisfaction of such right is subject to the legal rights and obligations of the Company to maintain the data and perform its task in the public interest.
- f) Right to object the processing of data related to them on grounds related to their particular situation, in cases where the data are processed for the performance of a task in the public interest or for the purposes of the legitimate interests pursued by the Company or a third party.

The requests of the customers of the M.F.M.C. regarding their personal data and the exercise of their rights shall be submitted to the Data Protection Officer of the Company, at the e-mail address

[DPO\\_aedak@piraeusbank.gr](mailto:DPO_aedak@piraeusbank.gr) or in writing at the offices of the M.F.M.C. (87 Syngrou Avenue, Athens), to the attention of the Data Protection Officer. To this end, the special form of the Company under the title “REQUEST OF CUSTOMER FOR EXERCISING RIGHTS IN THE FRAMEWORK OF THE GENERAL DATA PROTECTION REGULATION (GDPR)” shall be filled in.

In addition, the data subject has the right to lodge a complaint before the Hellenic Data Protection Authority (1-3 Kifissias Avenue, Athens/[contact@dpa.gr](mailto:contact@dpa.gr)) for any issue related to its personal data.

*\*It is noted that the satisfaction of such right is subject to the legal obligation of M.F.M.C. for prohibition of notification of details and information, if there is a case of Article 27 of Law 4557/2018 in the context of prevention, investigation and detection of any money laundering and terrorist financing.*

## ➤ 6. Security of Personal Data

### 6.1. Security of processing

The Company shall apply appropriate technical and organizational measures in order to ensure, on a consistent basis, the required level of security towards the customers related to the personal data and the risks of their processing. In this framework, the Company:

- i. has adopted and applies on a permanent basis Policy and procedures for observing privacy and ensuring the integrity, availability and reliability of the processing systems and services,
- ii. has adopted a Business Continuity Plan, ensuring that in case of a natural or technical incident there is an ability of prompt restoration of availability and access to personal data, without delay,
- iii. carries out regularly trial, assessment and evaluation of the effectiveness of technical and organization measures for ensuring the security of processing, considering mainly risks coming from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transferred, stored or otherwise processed,
- iv. ensures that any natural person acting under its supervision and having access to personal data, processes them only within the limits of the relevant order given to them by the Company and under the terms and conditions set out by the Company,
- v. has adopted encryption procedures of the personal data, where considered necessary.

### 6.2. Personal Data Breach

Any breach of this Policy, as well as of the applicable legislative and regulatory framework on personal data and their protection from time to time, and, in general, any breach of security resulting to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transferred, stored or otherwise processed, constitutes a personal data breach.

In order to handle possible cases of data breach, the Company has adopted and applies a Policy of response and management of personal data breaches.

In case of a personal data breach, the Company shall notify without delay, and, if possible, within 72 hours from the moment it took notice of the incident, the personal data breach to the Hellenic Data Protection Authority, unless the breach may not raise risk to the rights and freedoms of the customers.

In addition, in case of data breach, the Company shall immediately inform the Data Protection Officer, who shall take, in consultation with the Company, all necessary measures and carry out all necessary actions for the limitation, non-extension of the breach and for its restoration. The Data Protection Officer shall record the data breaches occurring, evaluate their causes and document each breach, indicating the true facts connected to it, its consequences and the measures taken for its restoration.

Where the personal data breach may raise high risk to the rights and freedoms of the customers, the Company shall announce without delay the personal data breach to them, according to those specifically set out in the GDPR.

## ➤ 7. Obligations of the Company

### 7.1. Privacy by design

The Company shall effectively implement, both at the time of determination of means for data processing and at the time of processing, appropriate technical and organizational measures, which are designed to implement data protection principles, which shall ensure that they comply, on a permanent basis, with the requirements of the GDPR and protect the rights of its customers as personal data subjects. In this framework, in the collection, maintenance and processing of data, the following principles shall apply:

- Minimization of processed data – the Company shall collect and process only the personal data necessary for the purposes of processing,
- Lawfulness, objectivity and transparency,
- Accuracy and updating of processed data,
- Restriction of access to data only to the persons which need them for the correct and lawful execution of the obligations/duties appointed to them and only to the extent that access is necessary,
- Tests and controls on a continuous basis regarding the adequacy of personal data processing procedures and the organizational and technical measures implemented,
- Adoption of simple, easy and effective procedures for the exercise by customers of their rights connected to their data,
- Pseudonymization – if not required for the service of the purposes of processing, the data shall be kept in a manner, so that they cannot be attributed to a specific customer, without the use of supplementary information, provided that such supplementary information are kept separately and are subject to technical and organizational measures, in order to ensure that they cannot be attributed to an identified or identifiable natural person.

## 7.2. Privacy by default

The Company shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for the relevant purpose of the processing are processed. The above obligation applies to all personal data collected, to the extent of their processing, to the period of their storage/maintenance and their accessibility. The extension of processing shall be possible only after a special, explicit and written relevant consent of the customer, according to those set out under 4. 2.

## 7.3. Records of activities

The Company, as the Controller, shall maintain a record of processing activities under its responsibility, which shall include the following information:

- a) the name and contact details of the Company, its representatives and the Data Protection Officer,
- b) the purposes of the processing,
- c) description of the categories of data subjects and 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/international organisations,
- e) where applicable, transfers of personal data to a third country/international organisation, including the identification of that third country or international organisation,
- f) where possible, the envisaged time limits for erasure of the different categories of data, g) where possible, a general description of the technical and organisational security measures it has adopted and applies.

## 7.4. Training of personnel

The Company shall ensure full information and training of its entire personnel (employees and executives) regarding all matters related to the protection of the personal data of its customers and the compliance of the personnel with the relevant obligations arising from the GDPR, the applicable legislative and regulatory framework from time to time, as well as from policies/procedures from which the Company has adopted obligations. The initial information – training shall take place upon the hiring of the employee or the initiation, in any way, of the employment relationship/cooperation between them and the Company, while throughout the employment relationship/cooperation, the Company shall ensure the regular further training/retraining of the entire personnel.

## 7.5 Recording of telephone conversations

The Company uses technical means for the recording of telephone conversations with customers, for the service and security of the transactions they carry out and of their trading relationships with the Company, in continuous compliance with the applicable legislative and regulatory conditions from time to time and the respective procedures of the Group of Piraeus Bank SA. The departments, the telephone conversations with clients of which are recorded, are: the Investment Directory, the

Operation Directorate (Unitholder Service Department) and the Institutional Mandates & Distribution Directorate.

## ➤ 8. Delegation of processing to processors

In cases where the Company wishes to delegate the execution of processing of customer personal data to third parties, on its behalf, it shall only use processors which provide adequate assurances on the implementation of appropriate technical and organizational measures, in a manner that processing complies with all requirements of the GDPR and the applicable legislative and regulatory framework from time to time and the protection of the rights of customers is ensured.

The above delegation is made, pursuant to a written agreement signed between the Company and the processor, which binds the latter towards the Company and determines, as a minimum, among others, the subject and the duration of the processing, the nature and the purpose of the processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the Company as Controller.

## ➤ 9. Data Protection Officer

PIRAEUS ASSET MANAGEMENT M.F.M.C. has appointed a Data Protection Officer, who duly and timely participates in all matters related to the personal data protection. In particular, the Data Protection Officer undertakes the following duties:

- a) informs and advises the Company and its employees/executives processing data in any manner, on their obligation arising from GDPR, the applicable legislative and regulatory framework from time to time, as well as the policies/procedures adopted by the Company regarding the protection of personal data,
- b) monitors the compliance of the Company and its employees/executives processing data in any manner with their obligations arising from GDPR, the applicable legislative and regulatory framework from time to time, as well as the policies/procedures adopted by the Company regarding the protection of personal data, including the delegation of responsibilities, the awareness and training of employees participating in processing operations and the relevant controls,
- c) provides advices, when requested, regarding the personal data impact assessment and monitors its implementation,
- d) cooperates with the Hellenic Data Protection Authority,
- e) acts as a contact point for customers on any issue related to the processing of the personal data and the exercise of their rights, and
- f) acts as a contact point for the Hellenic Data Protection Authority on issues related to the processing of personal data by the Company.

During the performance of its duties, the Data Protection Officer shall consider the risk connected to processing operations, taking into consideration the nature, scope, framework and purposes of processing.

The contact details of the Data Protection Officer appointed by the Company are:

[DPO\\_aedak@piraeusbank.gr](mailto:DPO_aedak@piraeusbank.gr)

**REQUEST TO EXERCISE RIGHT<sup>1</sup>****Under GENERAL DATA PROTECTION REGULATION (GDPR)**

PERSONAL DETAILS	
Last name :	
First name :	
Father's name :	
ID :	
TIN :	
Address:	
E-mail:	
Contact phone number::	

A. In the context of the General Data Protection Regulation (GDPR), I state hereby that I wish to exercise my following right in relation to my personal data processed by Piraeus Asset Management M.F.M.C.:

- ☐ Access to my data
- ☐ Rectification of my inaccurate/completion of my incomplete data
- ☐ Erasure of my data
- ☐ Restriction to the processing of my data
- ☐ Portability of my data
- ☐ Objection to the processing of my data

B. In particular, I request that:

---



---



---



---



---



---



---



---

<sup>1</sup> The exercise of more than one rights through the same form is possible.

[illegible]

Γ. I wish the company Piraeus Asset Management M.F.M.C. to communicate with me in relation to the progress of my request as follows:

- ☐ By phone ☐ By e-mail
- ☐ By SMS ☐ By mail

Date: \_\_\_\_\_ Signature \_\_\_\_\_



