

FILIPINO FUND, INC.

**DATA PRIVACY POLICY**

Filipino Fund, Inc. (the "Corporation") recognizes the value of ensuring that all personal information and data of its stakeholders is protected against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

In compliance with the general data privacy principles embodied in Republic Act No. 10173 or the Philippine Data Privacy Act of 2012 ("Data Privacy Act"), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission ("NPC") (the "Data Privacy Laws"), the Corporation issues this Policy to serve as guidelines and to show its commitment to the protection of personal information and data. This Data Privacy Policy (the "Policy") shall also encapsulate the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

The Corporation shall exercise its responsibility with the due diligence expected from the nature of the industry, and ensure that its directors, officers, and employees perform their duties with a strict and faithful compliance with these guidelines on personal information and data security and confidentiality.

**1. Definition of Terms**

**"Data Subject"** refers to an individual whose personal, sensitive, or privileged information is processed;

**"Personal Data"** refers to all types of personal information;

**"Personal Information"** refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

**"Personal Information Processor"** refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

**"Processing"** refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data; and

**"Sensitive Personal Information"** refers to personal data:



- a. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- b. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
- c. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- d. Specifically established by an executive order or an act of Congress to be kept classified.

## 2. Scope and Limitations

All personnel of the Corporation including but not limited to its directors, officers, and employees, regardless of their type of employment or contractual arrangement, must comply with this Policy.

## 3. Processing of Personal Data

### A. Collection

The Corporation as a closed-end investment company collects the Personal Information of its shareholders and customers which include basic contact information such as their full name, address, e-mail address, and contact number. In addition, The Corporation also processes the Sensitive Personal Information of its shareholders and customers which include, among others, the tax identification numbers.

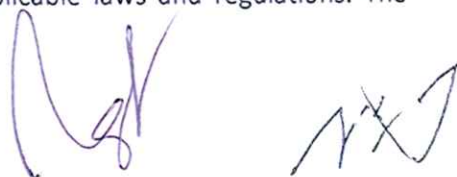
### B. Use

Personal Information and Sensitive Personal Information is collected by the Corporation for the following major reasons:

- To allow the Corporation to comply with its duties and responsibilities with the relevant government regulators or legal authorities; and
- To allow the Corporation to carry out its business as a closed-end investment company and for internal business and administrative purposes; and
- For any other purpose that the Corporation's shareholders and customers will be given prior notice to and for which their consent shall be obtained.

### C. Storage, Retention and Destruction

Any Personal Information and Sensitive Personal Information provided to the Corporation is retained only for such duration that is necessary to fulfill whatever purpose for which it is collected subject to compliance with applicable laws and regulations. The



Corporation will exercise reasonable security measures to prevent unauthorized, accidental, or unlawful access, processing, deletion, loss or use, including providing standard restrictions to physical access to data within the Corporation's systems, and encryption of sensitive data when transmitting such data. Such reasonable measures will also be taken to remove information when no longer necessary.

#### **D. Access**

Due to the sensitive and confidential nature of the personal data under the custody of the Corporation, only the data subjects and the authorized representative of the Corporation shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

#### **E. Disclosure and Sharing**

Where permitted by law and where such disclosure is necessary to satisfy the purpose or a directly related purpose for which the Personal Information and Sensitive Personal Information was collected, the Corporation may share personal data to the Corporation's affiliates or similar relationships and government regulators after having obtained the consent of the Data Subjects and provided that the provisions and conditions of the Data Privacy Act have been complied with.

### **4. Security Measures**

The Corporation will take appropriate organizational, physical, and technical measures which are consistent with the Data Privacy Laws. The Corporation will use security procedures and technology to protect the information it holds.

#### **A. Organizational Security Measures**

A Data Protection Officer ("DPO") shall be appointed by the Corporation. The DPO is responsible for ensuring the Corporation's compliance with the Data Privacy Laws.

##### **I. General Qualifications**

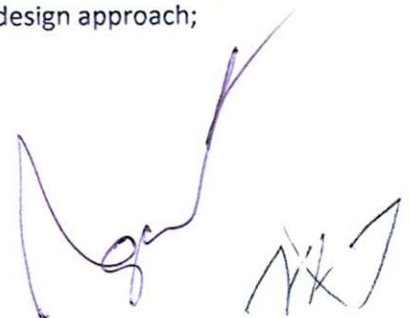
- The DPO shall possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the Corporation, including the latter's information systems, data security and/or data protection needs.
- As far as practicable, the DPO shall be a full-time or organic employee of the Corporation. Where the employment of the DPO is based on a contract, the term or duration thereof shall be at least be two (2) years to ensure stability.



- A DPO must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the Corporation. In his or her capacity as DPO, an individual may perform (or be assigned to perform) other tasks or assume other functions that do not give rise to any conflict of interest.

## II. Duties and Responsibilities

- Monitor the the Corporation's compliance with the Data Privacy Laws. For this purpose, he or she may:
  - Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the Corporation, and maintain a record thereof;
  - Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
  - Inform, advise, and issue recommendations to the Corporation;
  - Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
  - Advise the Corporation as regards the necessity of executing a data sharing agreement with third parties, and ensure its compliance with the law;
- Ensure the conduct of privacy impact assessments relative to activities, measures, projects, programs, or systems of the Corporation;
- Advise the Corporation regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- Ensure proper data breach and security incident management by the Corporation, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- Inform and cultivate awareness on privacy and data protection within the organization of the Corporation, including all relevant laws, rules and regulations and issuances of the NPC;
- Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the Corporation relating to privacy and data protection, by adopting a privacy by design approach;

Handwritten signature and initials in blue ink, located at the bottom right of the page. The signature is a cursive name, and the initials are 'AKJ'.

- Serve as the contact person of the Corporation vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the Corporation;
- Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- Perform other duties and tasks that may be assigned by the Corporation that will further the interest of data privacy and security and uphold the rights of the data subjects.

#### **B. Physical Security and Technical Security Measures**

The Corporation shall ensure that physical security measures are in place, which shall, include, among others, monitoring and limiting access to, and activities in the departments and offices of the Corporation where personal data is processed, including guidelines that specify the proper use of and access to electronic media. In addition, the Corporation shall implement technical security measures to ensure that, among others, the Corporation's processing systems are not vulnerable to data breach. The Corporation shall faithfully comply with the standards and guidelines in the Data Privacy Act on physical security and technical security measures.

### **5. Breach and Security Incidents**

#### **A. Data Breach Notification**

All employees and agents of the Corporation involved in the processing of personal data are tasked with regularly monitoring for signs of a possible data breach or security incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or security incident.

The DPO shall notify the NPC and affected Data Subjects of any incident of data breach pursuant to requirements and procedures prescribed by the Data Privacy Act.

The notification to the NPC and affected Data Subjects shall describe, among others, the nature of the breach, the personal data possibly involved, and the measures taken by the Corporation to address the breach.

#### **B. Breach Reports**

The Corporation shall ensure that all security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by



the personal information controller as defined under the Data Privacy Act. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted by the DPO to the NPC annually.

#### 6. Rights of Data Subjects, Inquiries and Complaints

The Corporation shall ensure that the rights of Data Subjects are protected and recognized. Towards this purpose, the Corporation shall ensure that all Data Subjects shall be given the (i) right to be informed, (ii) right to object, (iii) right to access, (iv) right to rectification, (v) right to erasure or blocking, and (vi) right to damages as these are provided for in the Data Privacy Act.

Data Subjects may inquire or request for information regarding any matter relating to the processing of their personal data with the Corporation's DPO.

#### 7. Personal Information Processor

The Corporation may engage a Personal Information Processor such as a stock transfer agent to process the Personal Information and Sensitive Personal Information of the Corporation's Data Subjects. Such engagement shall comply with the requirements of the Data Privacy Act and shall at all times be covered by the appropriate contractual agreements. The Corporation shall ensure that such Personal Information Processor shall also, where applicable, implement the security measures of the Data Privacy Act. At all times the Personal Information Processor must ensure the confidentiality, integrity and availability of the personal data processed, and prevent its use for unauthorized purposes.

Approved on \_\_\_\_\_ 2017 in Makati City.

**BERNARDO M. VILLEGAS**  
Chairman

**FRANK S. GAISANO**  
Director

**JOHN G. TAN**  
Director

**MARGARET G. ANG**  
President

**EDWARDS S. GO**  
Director

**ALJIM C. JAMANDRE**  
Director

**VINCENT E. TOMANENG**  
Director