SOCIAL HOUSING FINANCE CORPORATION

DATA PRIVACY POLICY

I. INTRODUCTION

The Social Housing Finance Corporation (SHFC or the "Corporation") respects and values data privacy rights, and ensures that all personal data collected from employees, clients and partners are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

SHFC's commitment to meet the standard policy provided in the Data Privacy Act of 2012 (DPA) or RA. No.10173, and its Implementing Rules and Regulations (IRR) and all relevant issuances of the National Privacy Commission (NPC) is set out in this Policy. This Policy shall inform its stakeholders and the public of SHFC's data protection and security measures, and may serve as guide in exercising the data subject's rights under the DPA.

II. DEFINITION OF TERMS

The DPA and its IRR define the following:

a. **"DATA SUBJECT"** – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of the Corporation.

b. **"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.

Examples of Personal information are: name, home, address or office address, email address, birth date, birth place, telephone number, place of work, gender, location of an individual at a particular time, IP address, country of citizenship, citizenship status, payroll and benefits information and other identifying information.

c. **"PERSONAL DATA"** - refers to both personal information and sensitive personal information.

d. **"PERSONAL DATA BREACH"** – refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

e. **"PERSONAL INFORMATION PROCESSOR"** – refers to any natural or juridical person qualified to act as such under the Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

f. **"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.

g. **"PRIVILEGED INFORMATION"** - refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

h. **"SECURITY INCIDENT"** - is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

i. **"SENSITIVE PERSONAL INFORMATION"** - refers to personal information:

(i) About an individual's race, ethnic, origin, marital status, age, color, and religious, philosophical or political affiliations;
(ii) 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(iii) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
(iv) Specifically established by an executive order or an act of Congress to be kept classified.

III. SCOPE AND LIMITATION

a. This Policy is applicable to all SHFC's management, employees, clients, mobilizers, contractors, other stakeholders or any person or entity who may receive personal data from SHFC, or who provide information to SHFC. It covers personal data collected or processed by or on behalf of SHFC including its Personal Information Processor/s (PIP/s).

b. All personnel of the Corporation, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Policy.

c. This Policy covers the treatment of personal information gathered and used by SHFC for lawful business purposes. This policy also covers the personal information shared with authorized Third Parties or that Third Parties shared with SHFC specifically other government agencies for project coordination and policy making purposes.

IV. PROCESSING OF PERSONAL DATA

SHFC, in the processing of personal information, adheres to Section 12 of the DPA which provides:

The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

a. The data subject has given his or her consent;

b. The processing of personal information is necessary and is related to the fulfilment of a contract with the data subject or in order to take steps at the request of the data prior to entering into a contract;

c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

d. The processing is necessary to protect vitally important interests of the data subject, including life and health;

e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfil functions of public authority which necessarily includes the processing of personal data for the fulfilment of its mandate; or

f. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedom of the data subject which require protection under the Philippine Constitution.

In processing of sensitive personal information, SHFC implements and observes the following applicable provisions of Section 13 of the DPA which states that:

The processing of sensitive personal information and privileged personal information shall be prohibited, except in the following cases:

a. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

b. The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing

d. The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations: Provided , that such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, that the sensitive personal information are not transferred to third parties: Provided further, that the sensitive personal information are not transferred to third parties: Provided finally, that consent of the data subject was obtained prior to processing.

e. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

f. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

A. COLLECTION

SHFC collects Personal Data by lawful means and for lawful purposes and is directly related and necessary to the nature, functions, and purposes of SHFC as a government agency which undertakes financing of social housing programs.

SHFC collects the basic contact information from the following:

1. Member-beneficiaries of community associations applying for social housing loans, including their full name, name of spouse, gender, age, residential address, socio-economic profile, credit information, email address, contact number, government issued identification card, salary, and such other information that the SHFC may require;

2. Mobilizers, Local Government Units and other partners who assist SHFC in community organizing;

3. Contractors/Developers who seek to be accredited by SHFC including their full name, name of spouse, residential/business address, address, email address, contact number, government issued identification card, salary, tax identification records, financial information and such other information that the SHFC may require;

4. SHFC shall also collect the basic contact information of individuals who transact with SHFC. The basic contact information consists of full names, addresses or email addresses, place of work, gender, and contact numbers; and

5. Likewise, SHFC also collects the Personal Data from its members of the Board of Directors, officials, and employees, regardless of the type of employment or contractual arrangement, including on-the-job trainees and applicants for vacant positions and consultants. Personal Data are collected through documents submitted or gathered in relation to job application.

B. USE

The Personal Data collected by the Corporation shall be used for the following purposes:

(i) processing of loan application;

(ii) processing of insurance claim application;

(iii) research/statistical data collection purposes;

(iv.) estate management;

(v.) securitization;

(vi.) processing of the application for accreditation of mobilizers and contractors/developers;

(vii.) sharing of information with government agencies for legitimate purpose; and

(viii.) for other documentation purposes.

C. STORAGE, RETENTION AND DESTRUCTION

SHFC shall ensure that Personal Data under its custody, whether in paper or electronic format, are protected against any accidental or unlawful destruction, alteration, and disclosure, including against any other unlawful processing.

SHFC implements appropriate security measures in storing collected Personal Data, depending on the nature of the information. Personal Data whether in paper or electronic format will be safely destroyed through secure means, after the lapse of the retention period provided by law, rules or regulations or as determined by SHFC. More importantly, Personal data records, as well as incoming and outgoing emails, of enduring value may be archived pursuant to Republic Act No. 9470 also known as the National Archives of the Philippines Act of 2007.

D. ACCESS

Due to the sensitive and confidential nature of the Personal Data under the custody of SHFC, only the authorized representatives of the Corporation shall be allowed to access such Personal Data for any purpose, except:

(i) for those contrary to law, public policy, public order or morals, or

(ii) when access by others is required or allowed by law or rules and regulations of the Rules of Court or ordered by a competent Authority,

(iii) when required by exigency of the business and operation of SHFC.

E. DISCLOSURE AND SHARING

All employees, officers, and directors of SHFC shall maintain the confidentiality and secrecy of all Personal Data that come to their knowledge and possession, even after resignation or termination of contract or other contractual relations, unless otherwise required to be disclosed by law, its rules and regulations, or with the consent of the Data Subject.

Personal data under the custody of SHFC shall be disclosed only pursuant to a lawful/legitimate purpose, and as authorized by Data Privacy Act of 2012 to authorized recipients of such data.

V. SECURITY MEASURES

A. ORGANIZATION SECURITY MEASURES

1. DATA PROTECTION OFFICER

SHFC designated Atty. Maria Remedios L. Bello-Camata as its Data Protection Officer (DPO) who is concurrently serving as Attorney IV of the Legal Affairs Division of this Corporation.

2. FUNCTIONS OF THE DPO:

The following are the functions of the DPO pursuant to NPC Advisory 2017- 01:

a. Monitor SHFC's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

(i) collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
(ii) analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
(iii) inform, advise, and issue recommendations to the PIC or PIP;
(iv) ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
(v) advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
c. advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
d. ensure proper data breach and security incident management by the PIC or PIP, 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;
e. inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
f. advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
g. serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
h. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
i. perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

3. Conduct of trainings, recording and documentations of compliance

SHFC shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of Personal Data, the management, through the DPO, shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

SHFC will keep a recording and documentation of activities carried out by the DPO, or SHFC itself, to ensure compliance with the DPA, its IRR and other relevant policies or issuances of the NPC.

4. Conduct of Privacy Impact Assessment

SHFC shall conduct a PIA relative to all activities, projects and systems involving the processing of Personal Data. The PIA may be conducted on a specific project or system when deemed to be necessary. SHFC may outsource the conduct of the PIA to a third party.

5. Duty of Confidentiality

All employees and officers of SHFC shall be required to sign confidentiality and nondisclosure agreement. All SHFC employees and officers with access to Personal Data shall operate and hold Personal Data under strict confidentiality if the same is not intended for public disclosure or unless such disclosure is required under the law, or with the consent of the Data Subject.

6. Review of Privacy Manual

This Privacy Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within SHFC shall be updated to remain consistent with current data privacy best practices.

B. PHYSICAL SECURITY MEASURES

1. Format of Personal Data

Personal data in the custody of SHFC are in digital or electronic format and paper based or physical format.

2. Storage type and location

All Personal Data in paper-based documents being processed by SHFC are stored in designated storage areas or kept in locked filing cabinets while the digital or electronic files are safely stored in computers provided and installed by SHFC with appropriate passwords which are changed on a regular basis. This includes the paper-based documents under the custody of the Documents Control and Custodian Department and SHFC branches, and other electronic documents stored in the Zeus Program.

3. Access procedure of SHFC personnel

Only authorized personnel shall be allowed inside the document vault or cabinets in the SHFC main office or in its branches. For this purpose, they shall each be given a duplicate of the key to the room.

4. Monitoring and limitations of access

Physical access is restricted to authorized personnel and any visitor is escorted by an authorized individual while in the office or secure area. All authorized personnel who seek to access the stored Personal Data must fill out and register access details in a logbook. They shall indicate the date, time, duration and purpose of each access.

5. Design of office space/work station

For purposes of ensuring privacy of Personal Data, the computers used by SHFC personnel are positioned with considerable spaces between them to maintain privacy and protect the processing of Personal Data. A nightly closing protocol requires employees and officials of the SHFC to log out of all computers.

6. Person involved in processing, and their duties and responsibilities

Persons involved in processing shall always maintain confidentiality and integrity of Personal Data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room. Moreover, all employees and officers of the SHFC with access to Personal Data shall operate and hold Personal Data under strict confidentiality if the same is not intended for public disclosure or unless such disclosure is required under the law or its rules and regulations.

7. Modes of transfer of personal data within the organization, or to third parties

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data, unless with the consent of the data subjects.

8. Retention and disposal procedure

SHFC shall retain the Personal Data for a period allowed by law, rules and regulations and until within the period the Personal Data collected is used by SHFC. Upon expiration of such period, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure technology pursuant to the rules and regulations set by Republic Act 9740 or the National Archives of the Philippines Act of 2007.

C. TECHNICAL SECURITY MEASURES

SHFC shall implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of Personal Data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

1. Monitoring for security breaches

SHFC may use an intrusion detection system to monitor security breaches and alert SHFC of any attempt to interrupt or disturb the system. SHFC installs anti-virus software to computers and laptops that regularly access the internet and uses firewalls and antivirus/anti-spyware software to protect systems that are accessible from the internet. The systems that are exposed to the Internet such as the web servers and their software or servers supporting sensitive applications are removed or disabled of unnecessary services and applications and with properly configured user authentication. SHFC regularly reads the firewall logs to monitor security breaches or any unauthorized attempt to access the network of SHFC.

2. Security features of the software/s and applications/s used

SHFC reviews and evaluates software applications before the installation thereof in computers and devices of SHFC to ensure the compatibility of security features with overall operations and to ensure privacy protection of Personal Data stored in said computers.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

SHFC reviews security policies, conduct vulnerability assessments, and perform penetration testing within SHFC on regular schedule to be prescribed by the appropriate department or unit.

4. Encryption, authentication process, and other technical security measures that control and limit access to personal data

SHFC personnel with access to Personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

VI. BREACH AND SECURITY INCIDENTS

1. Creation of a Data Breach Response Team

A Data Breach Response Team comprising of {five (5) officers – NAME OF THE TEAM} shall be responsible for ensuring immediate action in the event of a security incident or Personal Data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to prevent and minimize occurrence of breach and security incidents

SHFC shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of Personal Data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

3. Procedure for recovery and restoration of personal data

SHFC shall always maintain a backup file for all Personal Data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

4. Notification protocol

The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team. Such notification shall be done within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by SHFC that a Personal Data breach requiring notification has occurred. A breach shall be subject to notification requirements under the following conditions.

a. The compromised data involves sensitive personal information or other information that may be used to enable identity fraud;
b. There is reason to believe that the information may have been acquired by an unauthorized person; and
c. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The report shall contain the following:

a. Description of the nature of the breach;

b. Sensitive personal information possibly involved;
c. Measures taken by the entity to address the breach;
d. Measures taken to reduce the harm or negative consequences of the breach; and e. Name of the DPO or representatives of SHFC, including their contact details, from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.

5. Documentation and reporting procedure of security incidents or a Personal Data breach

The Data Breach Response Team shall prepare a detailed documentation of all security incidents and Personal Data breaches, 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 SHFC. 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 to the NPC annually.

VII. INQUIRIES AND COMPLAINTS

Every data subject has the right to reasonable access to his or her Personal Data being processed by the personal information controller or personal information processor. Other available rights include:

(1) right to dispute the inaccuracy or error in the Personal Data;
(2) right to request the suspension, withdrawal, blocking, removal or destruction of Personal Data; and
(3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data.
Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. The data subject may write to the DPO SHFC to discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies or sent to dpo@shfcph.com. The concerned department or unit of SHFC shall confirm with complainant its receipt of the complaint.