DATA PRIVACY	
Date:	**January 18, 2018**
Version No.	**1_01182018**
Page No.	**Page 1 of 8**

BACKGROUND

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.
It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each personal information controller or personal information processor is expected to produce a Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates 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 fulfilment and realization of the rights of data subjects.

INTRODUCTION

National Confederation of Cooperatives Mutual Benefits Association, Inc. (NATCCO MBAI) is a duly licensed provider of micro-insurance coverage for various risks involving life, accident, sickness and other contingencies. NATCCO MBAI was established in 2009 to further support the NATCCO Network in its needs to provide micro-insurance products to its members. Since then, it has been extending financial assistance to members and their dependents, in the form of death benefits, sickness benefits, provident savings, and loan redemption assistance.

NATCCO MBAI is an institution covered by Insurance Commission (IC). IC, with its Circular Letter 2017-29, dated May 2, 2017, has instructed all Covered Institutions (CIs), including MBAs, to create Related Party Transactions Committee and establish policies and procedures for transactions between related parties. These policies shall be made to ensure that such transactions are only undertaken on an arm's length basis for financial, commercial, and economic benefit of NATCCO MBAI, and the entire group where it belongs.

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values data privacy rights, and makes sure that all personal data collected from members/policyholders, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

DEFINITION OF TERMS

Act - refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

Commission - refers to the National Privacy Commission;

Consent of the data subject - refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

Data subject - refers to an individual whose personal, sensitive personal, or privileged information is processed;

Data processing systems - refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

Data sharing - is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

Direct marketing - refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals;

Filing system - refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

Information and communications system - refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;

Personal data - refers to all types of personal information;

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;
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 controller - refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

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 data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

Profiling - refers to 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, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

Privileged information - refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

Public authority - refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

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;
.
Sensitive personal information - refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. 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;
3. 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
4. Specifically established by an executive order or an act of Congress to be kept classified.

SCOPE AND LIMITATIONS

1. This manual covers all customers/members of NMBAI, including their insured dependents.

2. All staff of NMBAI, regardless of employment status and tenure, must comply with the terms and conditions set in the Data Privacy Manual.

PROCESSING OF PERSONAL DATA

This section lays out the various processing systems within NMBAI:

A. Collection – Partner cooperatives collect the customer information and send it to NMBA via email. Data are encoded to excel file, using the templates created by NMBAI for data collection purposes. Collected customer information are as follows:
   a. Coop affiliated with
   b. Member's full name
   c. Gender
   d. Birthdate
   e. Age
   f. Civil Status
   g. Birthplace
   h. Nationality
   i. Address
   j. Telephone number
   k. Email address
   l. Employment status
   m. ID's – SSS / GSIS / TIN / Others
   n. Source of funds
   o. Company/business Name
   p. Company/business address
   q. Type of business
   r. Name of spouse
   s. Spouse's birthdate
   t. Spouse's age
   u. Dependent's full name
   v. Dependent's relationship to member
   w. Dependent's full name

B. Use - Personal data collected are used by the company for underwriting and documentation purposes.

C. Storage, Retention and Destruction – Data are stored in NMBAI Customer Data Portal, and can only be accessed by MIS Personnel and Manager. The association will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The company will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All electronic information gathered is retained while hard copies are retained for at least ten (10) years.

D. Access – only authorized staff of MIS Unit, Claims Unit, and NMBAI Manager have access to the collected and processed data. Staff concern will be limited to data directly related and needed in their function.

E. Disclosure and Sharing - All employees of the association shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the association shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

SECURITY MEASURES

As a personal information controller or personal information processor, an organization must implement reasonable and appropriate physical, technical and organizational measures for the

protection of personal data. Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. This section gives a general description of those measures.

A. **Organization Security Measures**

Every personal information controller and personal information processor must also consider the human aspect of data protection. The provisions under this section shall include the following:

1. Data Protection Officer (DPO), or Compliance Officer for Privacy (COP)
    - The designated Data Protection Officer is Ms. Ma. Cherish G. Solsona, who is concurrently serving as the Database Associate of the Association.

2. Functions of the DPO, COP and/or any other responsible personnel with similar functions
    - The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

3. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security
    - The organization 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, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

4. Conduct of Privacy Impact Assessment (PIA)
    - The organization shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data.

5. Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.
    - The organization 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, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.
6. Duty of Confidentiality
    - All employees will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.
7. Review of Privacy Manual
    - This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. **Physical Security Measures**

This portion shall feature the procedures intended to monitor and limit access to the facility containing the personal data, including the activities therein. It shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others. To ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats, provisions like the following must be included in the Manual:

1. Format of data to be collected
   - Personal data in the custody of the organization may be in digital/electronic format and paper-based/physical format.

2. Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/separate room or part of an existing room)
   - All personal data being processed by the organization shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the association
   .
3. Access procedure of agency personnel
   - Only authorized personnel shall be allowed to access the data.

4. Design of office space/work station
   - The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

5. Persons involved in processing, and their duties and responsibilities
   - Staff involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to copy to their personal gadgets or storage device any form of information.

6. 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.

7. Retention and disposal procedure
   - The organization shall retain the personal data of a client for at least ten (10) years from the data of purchase. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. **Technical Security Measures**

Each personal information controller and personal information processor must 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
   - The organization shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used
   - The organization shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

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

- The organization shall review security policies, conduct vulnerability assessments and perform penetration testing within the company 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
    - Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

BREACH AND SECURITY INCIDENTS

Every personal information controller or personal information processor must develop and implement policies and procedures for the management of a personal data breach, including security incidents. This section must adequately describe or outline such policies and procedures, including the following:

1. Creation of a Data Breach Response Person
    - A Data Breach Response Person shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. He/she 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
    - NATCCO MBAI 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
    - The organization 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 Data Breach Response Person shall inform the Board of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law..

5. Documentation and reporting procedure of security incidents or a personal data breach
    - The Data Breach Response Person shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

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. This section shall feature such procedure.

- Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization at inquiry@company.com and briefly discuss the inquiry, together with their contact details for reference.

  Complaints shall be filed in three (3) printed copies, or sent to natccombai2010@hotmail.com. The concerned staff shall confirm with the complainant its receipt of the complaint.

EFFECTIVITY

The provisions of this Manual are effective this __ day of _____, 2018, until revoked or amended by this association, through a Board Resolution.