



DATA PRIVACY MANUAL

2019 Edition



 <i>Sharp Travel Service (Phils.) Inc.</i>		INITIAL ISSUE DATE January 02, 2019
TITLE OF MANUAL DATA PRIVACY MANUAL		NO. OF PAGES 22
AUTHORIZATION  President		REVISION DATE REVISION NO.

TABLE OF CONTENTS

I. INTRODUCTION	03
II. DEFINITION OF TERMS	03
III. SCOPE AND LIMITATIONS	05
IV. PRINCIPLES OF PROCESSING OF PERSONAL DATA	07
1. TRANSPARENCY	07
2. LEGITIMATE PURPOSE	07
3. PROPORTIONALITY	07
V. RIGHTS OF DATA SUBJECTS	07
1. RIGHT TO BE INFORMED	07
2. RIGHT TO OBJECT	08
3. RIGHT TO ACCESS	08
4. RIGHT TO RECTIFICATION	08
5. RIGHT TO ERASURE OR BLOCKING	09
6. RIGHT TO DAMAGES	09
7. RIGHT TO DATA PORTABILITY	09
8. RIGHT TO FILE A COMPLAINT	10
9. TRANSMISSIBILITY OF RIGHTS	10
VI. PROCESSING OF PERSONAL DATA	10
1. COLLECTION	10
2. PRIVACY NOTICE	10
3. CONSENT	10
4. USE	11
5. GOVERNMENT-MANDATED USE	12
6. RETENTION	13
7. DISPOSAL	13
8. DISCLOSURE AND SHARING	13

VII. SECURITY MEASURES	13
1. ORGANIZATIONAL MEASURE	14
2. PHYSICAL MEASURE	14
3. TECHNICAL MEASURE	15
VIII. PERSONAL DATA BREACH & SECURITY INCIDENTS	16
1. DATA PRIVACY RESPONSE TEAM	16
2. DUTIES OF THE DATA PRIVACY RESPONSE TEAM	16
3. PREVENTION OF SECURITY INCIDENTS AND PERSONAL DATA BREACH	17
4. PROCEDURE FOR RECOVERY AND RESTORATION OF PERSONAL DATA	17
5. DOCUMENTATION AND NOTIFICATION PROTOCOL	17
6. NOTIFICATION PROTOCOL TO THE COMMISSION	18
IX. DATA PROTECTION OFFICER & COMPLIANCE OFFICER FOR PRIVACY	18
1. DATA PRIVACY OFFICER (DPO)	18
2. COMPLIANCE OFFICER FOR PRIVACY (COP)	19
3. FUNCTIONS OF DPO AND/OR COP	19
X. NOTIFICATION, REQUESTS, INQUIRIES, AND COMPLAINTS	20
1. NOTIFICATION ON USE OF PERSONAL DATA FOR MARKETING & PROFILING	20
2. REQUESTS AND INQUIRIES PERTAINING TO THE DATA PRIVACY ISSUES	20
3. PROCEDURE FOR COMPLAINTS	20
XI. EFFECTIVITY	21

I. INTRODUCTION

Sharp Travel Service (Phils.), Inc. hereby adopts this Data Privacy Manual in compliance with the Republic Act No. 10173, also known as the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

With the Data Privacy Act, other pertinent laws and issuances of the Commission, the Company abides by this Manual in carrying out its principal business to ensure that personal data under its control remain safe and secured while being processed in the course of its key operations, processes and services.

This Manual aims to inform employees, clients, partners and stakeholders of the Company's data protection and security measures, and to guide them in the exercise of their rights under the Data Privacy Act and other relevant regulations and policies.

II. DEFINITION OF TERMS

Whenever used in this Manual, the following terms shall have their respective meanings as herein set forth:

Act or DPA – refers to the Republic Act No. 10173, also known as the Data Privacy Act of 2012.

Authorized Personnel – refers to employee/s or officer/s of the Company authorized to collect and/or process Personal Data either by function of their office or position, or through specific authority given in accordance with the policies of the Company.

Commission – refers to the National Privacy Commission.

Company – refers to Sharp Travel Service (Phils.), Inc.

Compliance Officer for Privacy or COP – refers to an individual or individuals who shall perform some of the functions of a DPO.

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 data. 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 Privacy Response Team – refers to the group of individuals designated to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policies of the Company.

Data Processing Systems – refer to the structures and procedures by which personal data is collected and further processed by the Company in its information and communications system/s and/or relevant filing system/s including the purpose and intended output of the processing.

Data Protection Officer or DPO - refers to an individual designated to monitor and ensure the implementation of the Data Privacy policies of the Company.

Data Sharing – refers to the disclosure or transfer to a third party of Personal Data under the control or custody of the Company.

Data Sharing Agreement – refers to any written contract or agreement that contains the terms and conditions of a Data Sharing arrangement entered into by the Company.

Data Subject – refers to an individual whose Personal Data is processed by the Company or its authorized personnel.

Filing System – refers to any set of information relating to a natural or juridical person 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 person is readily accessible.

Manual – refers to this Data Privacy Manual.

Outsourcing – refers to the disclosure or transfer of Personal Data by the Company to a Personal Information Processor (PIP) for the latter's processing, which shall be done strictly in accordance with the instructions of the Company.

Outsourcing Agreement – refers to any written contract entered into by the Company with a PIP, including its service providers.

Personal Data – refers to all types of personal information, including privileged 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 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 Controller or PIC – 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 his behalf.

Personal Information Processor or PIP – refers to a 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.

Privacy Impact Assessment – refers to a process undertaken and used to evaluate and manage the impact on privacy of a particular program, project, process, measure, system, or technology product of the Company or its PIP/s. It takes into account the nature of the Personal Data to be protected, the Personal Data flow, the risks to privacy and security posed by the Processing, current data privacy best practices, and the cost of security implementation.

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.

Security Incident – refers to 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 safeguards that have been put in place.

Sensitive Personal Information – refers to personal information:

- a) about an individual's race, ethnic, origin, marital status, age, color, and religious and philosophical or political affiliations;
- b) about an individual's health, education, genetic or sexual life or 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;
- c) 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 return; and
- d) specifically established by an Executive Order or an act of Congress to be kept classified.

III. SCOPE AND LIMITATIONS

This Manual applies to all processed personal data contemplated under the DPA by the Company and third party service providers (sub-cons) whom the Company has outsourcing agreements to process data in line with its nature of business and services.

This Manual applies to all departments of the Company – its managers, staff and employees. The data covered by this Manual are personal data of data subjects depending on the kind of

transactions involved which includes, but not limited to the following:

1. **Clients/Customers:**

- a) **Client/User Information:** e.g. first and last name, passport details, telephone and mobile number, postal and email addresses, company name and position and other related information.
- b) **Billing Information:** e.g. credit card information (such as credit card number, cardholder name, credit card expiry date and billing address).
- c) **Travel Itinerary:**
 - Travel Details (e.g. origin, destination, departure, arrival dates and times, class of travel, and frequent flyer program);
 - Documentation assistance (e.g. Passport, Immigration and Visa);
 - Accommodation Details (e.g. duration of stay, number of guests and room preferences);
 - Tour Packages (e.g. tour operator, land transfers, car rentals and cruises);
 - Travel Companion (e.g. identity and basic information about the person who is included in the travel itinerary);
 - Other Ancillary Services (e.g. Travel Insurance, seat and meal preferences, wheelchair assistance).

2. **Vendor/Supplier or Prospective Vendor/Supplier:** Portfolio and contact information, which may include, for example, some or all of your name, business address, email address, phone number, social media links; invoices sent by suppliers or generated by the Company for clients; printed materials supplied for the purposes of fulfilling a contract; materials supplied for the purposes of marketing; contractual information agreed between both parties; payment details and the likes.

3. **Employee or Prospective Employee:** Photo, present address, birth date, birth place, citizenship, civil status, educational record, government exams taken and corresponding rating, employment history, references and other related information necessary for purposes of evaluating the applicant for eligibility for employment and/or necessary while being employed with the Company.

4. **Company Stockholder:** Personal data relating as a stockholder (e.g. name; personal identity number and contact details, information regarding shareholding such as number of shares and any notes/information to be linked to that shareholding according to law; data from any communication between the Company and stockholder including data in minutes of board meetings and general meetings; and other personal data necessary to fulfill the Company's obligation under law, including securities and tax legislations and the Company's legitimate interest of convening general meetings and administering other matters relating to the shareholders of the Company.

5. **Visitor:** e.g. name, home or office address, contact details and signature.

IV. PRINCIPLES OF PROCESSING PERSONAL DATA

In the processing of personal data, the Company, its employees and PIP/s shall abide by the following principles espoused by the DPA:

1. **TRANSPARENCY.** The Data Subject shall be informed of the nature, purpose, and extent of the processing of his/her personal data, including the risks and safeguards involved, the identity of the Company, his/her rights as a data subject, and how these rights may be exercised.
2. **LEGITIMATE PURPOSE.** The processing of personal data shall only be for the purpose declared and specified to the data subject. No further processing of personal data shall be done without the consent of the data subject.
3. **PROPORTIONALITY.** The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data will be processed by the Company only if the purpose of the processing could not be reasonably fulfilled by other means, and if required by the Company's business operations and services.

V. RIGHTS OF DATA SUBJECTS

1. RIGHT TO BE INFORMED

The data subject has the right to be informed whether personal data pertaining to him/her shall be, are being, or have been processed, including the existence of automated decision-making and profiling. He/she shall be notified and furnished with information indicated hereunder before the entry of such personal data into the processing system and/or filing system of the Company, or at the next practical opportunity:

- a) Description of personal data to be entered into the processing system or filing system;
- b) Purpose/s for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
- c) Basis of processing, when processing is not based on the consent of the data subject;
- d) Scope and method of personal data processing;
- e) The recipient or classes of recipients to whom the personal data are or may be disclosed;
- f) Methods utilized for automation access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about logic involved, as well as the significance and envisaged consequences of such processing for the data subject;
- g) The identity and contact details of the personal data controller or its representative;
- h) The period for which the information will be stored; and
- i) The existence of their rights as data subjects, including the right to access, correction, and object to processing, as well as the right to lodge a complaint.

2. RIGHT TO OBJECT

The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. He/she shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the Personal Information Controller (PIC) shall no longer process the personal data, unless:

- a) The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
- b) The information is being collected and processed as a result of a legal obligation.

3. RIGHT TO ACCESS

The data subject has the right to reasonable access, upon demand or request, to the following:

- a) Contents of his or her personal data that were processed;
- b) Sources from which personal data were obtained;
- c) Names and addresses of recipients of the personal data;
- d) Manner by which such data were processed;
- e) Reasons for the disclosure of the personal data to recipients, if any;
- f) Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
- g) Date when his or her personal data concerning the data subject were last accessed and modified; and
- h) The designation, name or identity, and address of the Personal Information Controller (PIC).

4. RIGHT TO RECTIFICATION

The data subject has the right to dispute the inaccuracy or error in the personal data and have the Personal Information Controller (PIC) correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the Personal Information Controller (PIC) shall ensure the accessibility of both new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, that recipients or third parties who have previously received such processed personal data shall be

informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

5. RIGHT TO ERASURE OR BLOCKING

The data subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal data from the Personal Information Controller's filing system.

This right may be exercised upon discovery and substantial proof of any of the following:

- a) The personal data is incomplete, outdated, false, or unlawfully obtained;
- b) The personal data is being used for purposes not authorized by the data subject;
- c) The personal data is no longer necessary for the purposes for which they were collected;
- d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
- e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
- f) The processing is unlawful;
- g) The Personal Information Controller or Personal Information Processor violated the rights of the data subject;
- h) The Personal Information Controller or Personal Information Processor violated the rights of the data subject.

6. RIGHT TO DAMAGES

The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

7. RIGHT TO DATA PROTABILITY

Where personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the Personal Information Controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of the data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means.

8. RIGHT TO FILE A COMPLAINT

The Data Subject shall have the right to file a complaint before the Commission for any data privacy violation committed by the Company, if any.

9. TRANSMISSIBILITY OF RIGHTS

The lawful heirs and assigns of the Data Subject may invoke the rights of the data subject, to which he or she is an heir or an assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding numbers.

VI. PROCESSING OF PERSONAL DATA

Whenever necessary, the Company may modify any of its Data processing Systems but, under all circumstances, must respect the rights of the Data Subjects and observe compliance with this Manual, requirements of the Data Privacy Act, its Implementing Rules and Regulations (IRR), and relevant issuances by the Commission.

1. COLLECTION

The collection of personal data is done by lawful means and for a lawful purpose and is directly related and necessary in the achievement of the Company's business operations and services.

2. PRIVACY NOTICE

Information on collection and processing of personal data of the data subject shall be relayed to the data subject through a Privacy Notice, which shall be posted in the Company's website and conspicuous areas in the Company's premises.

The Company's authorized personnel shall inform the data subject of the purpose/s for the collection and processing of personal data, extent of processing of personal data, and the rights of the data subject with regard to privacy and data protection.

3. CONSENT

The consent of the data subject shall be evidenced by written, electronic, or recorded means.

Consent may also be given on behalf of a data subject by a lawful representative or an agent authorized by the data subject to do so.

4. USE

- a) The use of the personal data shall only be for the purpose/s specified and declared to the data subject, and with the consent of the data subject.
- b) The Company's use of the personal data shall only be for the purpose of carrying out the business operation of the Company. The processing of personal data shall be for the following general purpose, among others:
 - to document and manage the Company records;
 - to conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract thereafter;
 - to respond to queries, complaints, and requests;
 - to provide information about the Company services;
 - to conduct research and analysis to improve customer experience;
 - to maintain security; and
 - comply with legal, regulatory, and contractual requirements or obligations.
- c) The use and processing of personal data also depends on the Company transactions involved.
- d) If a data subject asks about, or avails him/herself of the Company services, the Company may collect, use, or process the data subject's personal data to:
 - prepare and execute the necessary contract to cover the transaction;
 - update the Company records and keep its contact details and billing address up-to-date; and
 - communicate any advisories, changes, and other information relevant to the data subject's contract with the Company.
- e) If a data subject is a vendor/supplier, a potential vendor/supplier, or a contractor, the Company may collect, use, or process the data subject's personal data to:
 - conduct the appropriate due diligence checks;
 - evaluate the data subject's proposal, including his/her technical, financial, and operational capacity;
 - assess the viability of the data subject's proposal and process his/her accreditation;
 - communicate any decision on such proposal; and
 - perform any other action as may be necessary to implement the terms and conditions of the contract with the data subject, if any.

- f) If the data subject is a prospective employee, the Company may collect, use, or process the data subject's personal data to:
- evaluate his/her suitability for employment and, with written or expressed consent, retain his/her personal data for a maximum of one (1) year for future job opportunities that may be of interest to the data subject;
 - communicate with the data subject about his/her employment application;
 - if hired, process his/her personal data as may be necessary for purposes such as, but not limited to, payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand or require processing of his/her personal data.
 - while employed, evaluate his/her performance and career development;
 - upon separation, process his/her personal data for the exit interview and to prepare his/her final pay;
 - provide assistance to, and account for, employees in case of emergency; and
 - perform such other processing or disclosure that may be required in the course of the Company's business or under law or regulations.
- g) If the data subject is a Company stockholder, the Company may use, collect, or process the data subject's personal data to:
- maintain and update the data subject's record with the Company;
 - administer his/her stock transactions; and
 - comply with legal, regulatory, and contractual requirements or obligations.
- h) If the data subject is a visitor of the Company premises, the Company may use, collect, or process the data subject's personal data to:
- grant access to the premises; and
 - maintain the security within the premises.
 - In the course of client-data subject's dealings with the products and services, the Company shall request for personal data for availment and completion of such products and services.

5. GOVERNMENT-MANDATED USE

- a) The Company may use and process the personal data of data subjects for government regulatory compliance, company disclosures, and reportorial requirements, and pursuant to a lawful order of any court or tribunal.

6. RETENTION

- a) Personal Data should only be stored for as long as necessary to carry out an aspect of the business operation or contractual obligations of the Company relative to its products and services.
- b) The purpose/s for which personal data were collected and processed, as well as the applicable periods prescribed by law, if any, shall be considered in the retention.

7. DISPOSAL

- a) Upon the expiration of the retention period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure means that would render the personal data unreadable and irretrievable and prevent the occurrence of any personal data breach and other security incidents.

8. DISCLOSURE AND SHARING

- a) **Data Sharing Agreement.** Whenever the Company discloses, or transfers personal data under its control to another PIC, it shall execute a Data Sharing Agreement, substantially containing the relevant terms and conditions as prescribed by the Data Privacy Act, its IRR and related issuances by the Commission.
- b) **Outsourcing Agreement.** The Company may subcontract or outsource the processing of personal data, as well as the functions of the DPO and/or COP/s, provided that such arrangement, if any is covered by an Outsourcing Agreement. The PIP/s must have the competence and qualification to ensure personal data captured through its engagement with the Company is kept secured, and adequate protective measures has been in place. Regular inspections shall be conducted by the Company to third party entities to validate compliance with privacy laws.

VII. SECURITY MEASURES

The Company shall establish and implement reasonable and appropriate organizational, physical and technical measures to ensure privacy and data protection. These security measures are designed 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 and alteration.

The DPO, with the assistance of the COP/s, if any, and the Data Privacy Response Team, shall monitor the Company's compliance with these security measures.

1. Organizational Measure

- a) **Key Personnel.** The Company shall appointment a Data Privacy Officer (DPO) and/or Compliance Officers on Privacy (COP/s), and constitute a Data Privacy Response Team.
- b) **Continuing Education on Data Privacy.** All employees of the Company shall be required to read this Manual upon employment, and/or upon the effectivity of this Manual, whichever is applicable. All new employees shall be oriented of their obligations under the Data Privacy Act. The Company shall also conduct trainings and seminars to keep employees updated on the developments of data privacy and security.
- c) **Conduct of Privacy Impact Assessment (PIA).** The Company shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects, and systems involving the processing of personal data. It may choose to outsource the conduct of PIA to a third party.
- d) **Non-Disclosure Agreement (NDA).** All employees shall be required to sign a Non-Disclosure Agreement to ensure strict confidentiality of all confidential information and personal data.
- e) **Review of Privacy Manual.** The Company shall review and evaluate this manual annually. Privacy and security policies and practices shall be updated to remain consistent with current data privacy best practices.
- f) **Recording and Documentation.** There shall be a detailed and accurate documentation of all activities, projects, and processing systems of the Company to ensure compliance with the requirements of applicable laws.

2. Physical Measure

The Company shall implement measures to monitor, limit and/or prevent access to the facility containing the personal data, including the activities therein.

- a) **Format of data to be collected.** Personal data in the custody of the Company may be in digital/electronic format and paper-based/physical format.
- b) **Storage type and location.** All personal data being processed by the Company shall be stored in a secure facility, whether virtual or physical. Paper-based or physical documents shall be stored in locked filing cabinets, access keys to which shall be entrusted only to authorized personnel. Digital/electronic files are stored in computers provided and installed by the Company and protected by passwords or passcodes. Computers, portable disks, and other devices used by the Company and its PIP/s in processing personal data shall be encrypted with the most appropriate encryption standard.

- c) **Access Procedure of Personnel.** Only authorized personnel shall be allowed inside the data room. They shall each be given a duplicate of the key of the room. Other personnel may be granted access to the room upon filing of an access request form with the DPO or COPs and their approval thereof.
- d) **Monitoring and limitation of access to room or facility.** All personnel authorized to enter and access the data room or facility must fill out the log sheet or logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access. There shall be appropriate surveillance and alarms systems such as CCTV cameras that can store files up to one (1) year.
- e) **Design of office space and work station.** Computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.
- f) **Personnel involved in processing, and their duties and responsibilities.** Personnel involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage devices of any form when entering the data storage room.
- g) **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.
- h) **Retention and disposal procedure.** Personal data shall only be stored for as long as necessary to carry out the business operations and services of the Company. After the legitimate purpose of the data has been completed or when processing relevant to the purpose has been terminated, the Company shall ensure the personal data collected is timely deleted. The Company shall ensure to evaluate captured personal data to determine if the same has served its purpose and thus can be deleted. All physical and electronic copies of the personal data shall be destroyed and disposed of through shredding and/or other secure technology.

3. Technical Measure

The COMPANY shall implement technical security measures appropriate and sufficient 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:

- a) **Monitoring for security breaches.** The Company shall use an intrusion detection system to monitor security breaches and alert the Company of any attempt to interrupt or disturb the system.

- b) ***Security features of the software/s and application/s used.*** The Company shall first review and evaluate software applications before the installation thereof in computers and devices of the Company to ensure compatibility of security features with overall operations.
- c) ***Regular testing, assessment and evaluation of effectiveness of security measures.*** The Company shall review security policies, conduct vulnerability assessments and perform penetration testing on regular schedule to be prescribed by the appropriate department or unit.
- d) ***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. There will be an individual and role-based user account assignment; deactivation of user account after few failed log-in attempts; automatic log-off in case of inactivity, anti-virus and anti-spam management.
- e) ***Data Accuracy and Timeliness.*** The Company shall ensure that personal data collected and kept on file is up to date, correct and complete. Inaccurate, incomplete data shall be timely corrected, deleted, supplemented or updated.
- f) ***Security and Confidentiality.*** The Company shall maintain the highest level of confidentiality and security over the personal data collected. Suitable organizational and technical security above or on par with industry standards must be provided to prevent or immediately recover from data breaches.

VIII. PERSONAL DATA BREACH AND SECURITY INCIDENTS

1. Data Privacy Response Team

A Data Privacy Response Team, consisting seven (7) officers, including the DPO shall be constituted, which shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The Company may also designate other key personnel to form part of the Data Privacy Response Team.

2. Duties of the Data Privacy Response Team

The Data Privacy Response Team shall, among others:

- a) ensure the implementation of this Manual;
- b) ensure the management of security incidents and personal data breaches, if any;

- c) ensure the Company's compliance with relevant provisions of the Data Privacy Act, its IRR, and all related issuances by the Commission;
- d) assess and evaluate the occurrence of a security incident or personal data breach, if any;
- e) execute measures to mitigate the adverse effects of any security incident or personal data breach, if any; and
- f) comply with reportorial and notification requirements.

3. Prevention of Security Incidents and Personal Data Breach

The Data Privacy Response Team shall periodically conduct a Privacy Impact Assessment (PIA) to identify risks in the data processing systems. The team shall likewise periodically review the existing policies and procedures of the Company with regard to data privacy, including this Manual and its implementation.

4. Procedure for Recovery and Restoration of Personal Data

The Company shall always maintain a backup file for all personal data under its custody. In the event of a security incident or personal 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.

5. Documentation and Notification Protocol

- a) In the event that there is a security incident or personal data breach, the Company employees, its agents and/or sub-contractors are obligated to report the same within twenty-four (24) hours of its discovery to the Data Privacy Response Team.
- b) All security incidents or personal data breach shall be recorded and accordingly reported containing the following:
 - Description of the nature of the security incident or personal data breach, its root cause, chronology of events, estimate of the number of data subjects affected, and circumstances regarding its discovery.
 - Measures undertaken to address the breach and reduce the harm or its negative consequences;
 - Outcome of the breach or incident management, and difficulties encountered.
 - Assistance provided or to be provided to the affected data subject.
 - Name of the Company, including contact details, from whom the data subject may obtain additional information about the security incident or personal data breach.
- c) The head of the Data Privacy Response Team shall inform the Management of the Company of the need to notify the Commission and the data subjects affected by the incident or breach within the period prescribed by law.

6. Notification Protocol to the Commission

- a) The Commission and affected data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the Company or PIC or PIP that a security breach requiring notification has occurred.
- b) Notification of security breach to the Commission shall be required when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud, are reasonably believed to have been acquired by an unauthorized person, and the Company or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.
- c) If there is doubt as to whether the Commission has to be notified, the Data Privacy Response Team shall consider the following: (i) the likelihood of harm or negative consequences on the affected data subjects; (ii) how notification, particularly of the data subjects, could reduce the risks arising from the incident or breach reasonably believed to have occurred; and (iii) if the personal data involved information that would likely affect national security, public safety, public order, or public health; at least one hundred (100) individuals; information required by all applicable laws or rules to be confidential; or personal data of vulnerable groups.
- d) The Annual Security Incident Report that must be submitted to the Commission shall be prepared by the Data Privacy Response Team.

IX. DATA PROTECTION OFFICER AND COMPLIANCE OFFICER FOR PRIVACY

1. Data Privacy Officer (DPO)

The Company shall designate a Data Privacy Officer (DPO) who shall be responsible for ensuring the Company's compliance with applicable laws and regulations on data privacy/protection.

The name and contact details of the DPO shall be made available to all data subjects.

The DPO, being internally independent shall perform the following functions:

- a) Monitors the Company's compliance with this Manual, the Data Privacy Act, its IRR, issuances of the Commission, and other applicable local and internal laws on data privacy and protection.
- b) Acts as liaison between the Company and other regulatory institutions, and is in charge of the applicable registration, notification, and reportorial requirements mandated by laws on data privacy/protection based on local and international laws as applicable.
- c) Develops, establishes, and reviews procedures and policies for the exercise by data

subjects of their rights in data privacy.

- d) Acts as primary contact for data subjects to coordinate and consult with all concerns relating to their personal data.
- e) Formulates capacity building, orientation and training programs for employees, agents or representatives of the company regarding personal data privacy and security.
- f) Prepares and file reports as mandated by applicable laws on data privacy and protection.

2. Compliance Officer for Privacy (COP)

Each Department or Business Unit of the Company shall, likewise, appoint among its ranks a Compliance Officer for Privacy (COP), who shall assist the DPO in ensuring that the Department or Business Unit assigned to him/her complies with this Manual, the Data Privacy Act, its IRR, other pertinent laws and issuances on data privacy and protection.

The name and contact details of the COP/s shall be made available to all employees, process owners and data subjects.

3. Functions of DPO and COP

The functions of the DPO and/or COP include:

- a) Monitor the PIC's/PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For such purpose, the DPO and/or COP may:
 - Collect information to identify the processing operations, activities, measures, projects, or systems of the Company, and maintain or cause the maintenance of records thereof;
 - Analyze and check the compliance of processing activities, including the issuance of security clearances to, and compliance of service providers, with the applicable laws and contracts in data privacy;
 - Inform, advise, and issue recommendations to the Company;
 - Advise the Company on the necessity of executing Data Sharing Agreement/s and/or Outsourcing Agreement/s with third parties;
 - Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing.
- b) Ensure the conduct of Privacy Impact Assessment relative to activities, measures, projects, programs, or systems of the Company.
- c) Advise the Company regarding complaints and/or the exercise by subjects of their rights.
- d) Ensure proper data breach and security incident management by the Company, including the latter's preparation and submission to the Commission of reports and other documentation concerning security incidents or data breaches within prescribed period.

- e) Inform and cultivate awareness on privacy and data protection within the Company, including all relevant laws, rules and regulations and issuance of the Commission.
- f) Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the Company relating to privacy and data protection, by adopting a privacy by design approach.
- g) Serve as the contact person of the Company vis-à-vis data subjects, the Commission and other authorities in all matters concerning data privacy or security issues or concerns and the Company.
- h) Cooperate, coordinate and seek advice of the Commission on matters concerning data privacy and security.
- i) Perform other duties and tasks that may be assigned by the Company that will further the interest of data privacy and security and uphold the rights of the data subjects.

X. NOTIFICATION, REQUESTS, INQUIRIES, AND COMPLAINTS

1. Notification on Use of Personal Data for Marketing and Profiling

A Data Subject must be notified within forty-eight (48) hours before entry of his/her personal data into the system of the Company, whether such personal data shall be used for direct marketing, profiling, or historical or scientific purpose/s. Notification shall be made to electronic mail to the address of data subject found in the Company Records.

2. Requests and Inquiries Pertaining to the Data Privacy Issues

A Data Subject may access and recommend corrections to his/her personal data being processed by the Company by accomplishing the form for this purpose which shall be devised by the Company.

Any person, including an employee who is required by his/her functions within the Company to access the personal data of data subjects, may request access thereto through a prescribed request form.

3. Procedure for Complaints

The Company shall implement the following procedure in cases of complaints for data privacy violations:

- a) Any suspected or actual violations of this Manual, the Data Privacy Act, and/or related issuances on data privacy, or any breach, loss, or unauthorized access or disclosure of personal data in the possession or under the custody of the Company must be reported immediately to the DPO, COP or any member of the Data Privacy Response Team who shall reply within twenty-four (24) hours to acknowledge receipt of the complaint.

- b) In case of a complaint for violations of this Manual, the Data Privacy Act, and other related issuances, or any breach, loss, or unauthorized access, disclosure of personal data in the possession or under the custody of the Company, the DPO, the COP, if any, or any two (2) members of the Data Privacy Response Team shall:
 - (i) verify the allegations of the complaint;
 - (ii) if warranted, conduct an official investigation in case of serious security breach as provided under the Data Privacy Act and its IRR; and
 - (iii) report the security incident or personal data breach to the Commission following the procedure laid down in this Manual.

The Data Privacy Response Team may also convene as an investigation committee to recommend actions, particularly when the violation is serious, or causes or has the potential to cause material damage to the Company or any of its data subjects. Such recommendation shall be submitted to the management of the Company for approval.

XI. EFFECTIVITY

The provisions of this Manual are effective this 2nd day of January, 2019, until validly revoked or amended by this Company.

XII. ANNEXES