Del Monte Group of Companies

Data Privacy Manual

Approved as of 29 January 2018

Table of Contents

I. Background

It is the policy of the Philippine government to safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development.

Philippine Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, (the "**DPA**"), and its Implementing Rules and Regulations (the "**IRR**") are aimed at protecting personal data in information and communication systems both in the government and private sector. The DPA and the IRR apply to the processing of all types of personal information and to any natural or juridical person involved in personal information processing.

II. Introduction

Consistent with the policy behind the DPA, Del Monte Pacific Limited and its subsidiaries and affiliates (each, an "**Organization**" and, together, the "**Group**") believe that their interest to ensure the free flow of information to promote innovation and growth and for the proper management of their businesses must be balanced with data subjects' fundamental right to privacy. Towards this end, to ensure that all personal data collected by the Group are processed in accordance with the provisions of the DPA, the IRR, and other relevant policies, including issuances of the Philippine National Privacy Commission (the "**NPC**") (the DPA, the IRR, and such other relevant policies are hereinafter collectively referred to as the "**Rules**") and the general principles of transparency, legitimate purpose, and proportionality, the Group hereby promulgates this Data Privacy Manual (the "**Manual**").

Accordingly, when acting as PICs and/or PIPs (as these terms are defined below) and to the extent that this Manual applies pursuant to Article IV below, each Organization shall adhere to the Rules and this Manual.

This Manual serves as a guide or a handbook to ensure compliance by the concerned Organizations with the Rules, as well as to provide information to internal data subjects of the measures employed by such Organizations to guarantee that personal information is processed lawfully and that protocols are in place to make certain that mechanisms are available for internal data subjects to exercise their rights under the Rules.

It is the responsibility of every employee of the concerned Organizations who has knowledge of any infringement of any of the policies contained in this Manual to immediately notify his Organization's DPO or COP (as these terms are defined below) of the violation.

III. Definition of Terms

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

a. "**Collector**" refers to an individual involved in the collection of Personal Data from Data Subjects.

b. "**Compliance Officer for Privacy**" or "**COP**" refers to an individual who shall perform some of the functions of the DPO, as provided in this Manual.

c. "**Conflict of Interest**" refers to a scenario wherein the DPO is charged with performing tasks, duties, and responsibilities that may be opposed to, or could affect, his performance as DPO. This includes, inter alia, holding a position in the Group or its PIP that leads him to determine the purposes and the means of the Processing of Personal Data. The term shall be liberally construed relative to the provisions of this Manual.

d. "**Consent**" refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and processing of his 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.

e. "**Data Custodian**" refers to the Organization, group/department, or individual who has custody of Personal Data in any form.

f. "**Data Owner**" refers to the Organization, group/department, or individual who has the primary responsibility and decision making authority over the information throughout its life cycle, including as to its creation, classification, editing, modification, sharing, restriction, regulation, and administration.

g. "**Data Protection Officer**" or "**DOP**" refers to an individual appointed by the Group or Organization, who shall have the qualifications, and who shall perform the functions, of a data protection officer as provided in this Manual.

h. "**Data Sharing**" is the disclosure or transfer to a third party of Personal Data under the custody of an Organization, acting as a PIC or PIP. In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes outsourcing or the disclosure or transfer of Personal Data by a PIC to a PIP.

i. "**Data Sharing Agreement**" refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a Data Sharing arrangement between two or more parties; provided, that only PICs shall be made parties to a Data Sharing Agreement.

j. "**Data Storage Area**" refers to a secured location capable of being locked such as a data center, storage room, or space holding filing cabinets or drawers.

k. "**Data Subject**" refers to an individual whose Personal, Sensitive Personal, or Privileged Information is Processed.

l. "**Mobile Devices**" refer to portable self-contained electronic devices, including laptops, tablets, smart phones, cellular phones, digital cameras, and the like.

m. "**Personal Data**" refers to all types of Personal Information.

n. "**Personal Data Breach**" refers to a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

o. "**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.

p. "**Personal information controller**" or "**PIC**" refers to any individual or entity, including any Organization, who controls the Processing of Personal Data, or who instructs another to Process Personal Data on his/its behalf. The term excludes:

   i. an individual or entity who performs such functions as instructed by another individual or entity; or
   ii. an individual who Processes Personal Data in connection with his personal, family, or household affairs.

   There is control if the individual or entity, including any Organization, decides on what information is collected, or the purpose or extent of its Processing.

q. "**Personal information processor**" or "**PIP**" refers to any individual or entity, including any Organization, to whom a PIC may outsource or instruct the Processing of Personal Data pertaining to a Data Subject.

r. "**Privacy by Design Approach**" is an approach to the development and implementation of projects, programs, and processes that integrates into the latter's design or structure, safeguards that are necessary to protect and promote privacy, such as appropriate organizational, technical, and policy measures.

s. "**Privacy Impact Assessment**" is a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process, or measure.

t. "**Privileged Information**" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication.

u. "**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. Cognate expressions shall be construed similarly.

v. "**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.

w. "**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 is 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.

x. "**User**" refers to an individual involved in the Processing of Personal Data.

IV. Scope and Limitations

This Manual shall apply to and should be strictly complied with by any Organization that:

a. is found or established in the Philippines;

b. has links to the Philippines such as but not limited to:

i. uses equipment located in the Philippines, or maintains an office, branch, or agency in the Philippines for Processing of Personal Data;

ii. enters into a contract in the Philippines;

iii. unincorporated in the Philippines but has central management and control in the Philippines;

iv. has a branch, agency, office, or subsidiary in the Philippines and has access to Personal Data;

v. carries on business in the Philippines; or

vi. collects or holds Personal Data in the Philippines;

c. processes Personal Data about a Philippine citizen or Philippine resident; or

d. processes Personal Data in the Philippines.

All directors, officers, and employees (regardless of type of employment or contractual arrangement) of any Organization who falls under any of (a) to (d) above must similarly comply with the provisions of this Manual. The concerned Organization who falls under any of (a) to (d) above shall advise its directors, officers and employees that the Rules and the Manual apply to them.

Where an Organization Processes in the Philippines Personal Information originally collected from residents of foreign jurisdictions according to the laws of those foreign jurisdictions, including any applicable data privacy laws, it has the burden of proving the law of the foreign jurisdiction. Otherwise, the applicable law shall be deemed to be the DPA. At any rate, such Organizations must still comply with the requirements of implementing security measures for Personal Data protection.

V. Processing of Personal Data

A. Collection

1. *Type of Data Collected*

The Group collects the Personal Data described in the attached Schedule 1.

2. *Mode of Collection*

Personal data are collected directly from Data Subjects or indirectly from third parties.

Collection, whether directly or indirectly, is done through the following means, among others:

a. verbal request for information;

b. written request for information;

c. Data Subject provides information verbally, which information is then recorded in writing;

d. Data Subject provides information in writing such as by submitting hard copies of documents, sending information or soft copies of documents through email, facsimile, mobile messaging, web-based messaging, or the like; and

e. Data Subject accomplishes online forms.

3. *Person collecting the information*

Personal Data may be collected by employees of an Organization or by third parties engaged for the purpose of Processing Personal Data.

4. *Obligations of Person collecting the information*

When collecting Personal Data directly, the Collectors shall ensure that Personal Data are collected for a declared, specified, and legitimate purpose and that only Personal Data that are necessary and compatible with such purpose shall be collected. Before collecting any Personal Data, the Collectors must:

a. Inform the Data Subject in clear and plain language of the following matters:

   i. description of the Personal Data to be entered into the processing system. If there will be Data Sharing, the categories of Personal Data concerned;

   ii. specific purpose of the Processing of his Personal Data including Processing for direct marketing, profiling, or historical, statistical, or scientific purpose. If there will be Data Sharing, the purpose of the same;

   iii. specific extent of the Processing of his Personal Data, including, where applicable, the automated Processing of Personal Data for profiling, or Processing for direct marketing, and Data Sharing;

iv. basis of Processing, when Processing is not based on the Consent of the Data Subject;

v. nature and method of the Processing;

vi. the recipients or classes of recipients to whom Personal data will be disclosed;

vii. methods utilized for automated access, if the same is allowed by the Data Subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;

viii. identity and contact details of the PIC or its representative, and identify of the PIP, if any;

ix. period during which the information will be stored;

x. existence of the rights of Data Subjects, including the right to access, correction, and object to the Processing, as well as the right to lodge a complaint before the NPC; and

xi. Consent given can be withdrawn; and

b. Obtain the Consent of the Data Subject prior to the collection of Personal Data. If Consent cannot be obtained prior to collection, Consent must be obtained as soon as practicable and reasonable. However, in the event the Personal Data to be collected include Sensitive Personal Information, Consent must always be obtained prior to the Processing unless the Data Subject is not legally or physically able to express his Consent prior to the Processing and Processing of such Personal Data is necessary to protect the life and health of the Data Subject or another person.

B. Use

1. *Uses of Personal Data*

The Group uses the Personal Data collected for the following matters, among others:

a. Where the Personal Data relate to an employee of an Organization –

- Administering compensation and benefits, including government mandated benefits
- Complying with applicable laws, rules, and regulations or requirements of lawful authorities
- Organizational planning, including forecasting and predictive modelling
- Data Sharing with parent company, subsidiaries, and affiliates, for the same or similar purposes listed above
- Internal audits
- Internal investigations
- Employee disciplinary proceedings
- Documentation purposes

b. For other Data Subjects

- Monitoring and verifying compliance with contractual undertakings (*i.e.* independent contractor agreements, distributor agreements, service agreements, and other similar agreements)
- Providing services and to approve, manage, administer, or effect any transactions that may be requested or authorized
- Collecting any amounts due and outstanding
- Conducting credit checks and obtaining or providing credit references
- Enforcing or defending the Group's or any Organization's rights
- Internal operational requirements (including credit and risk management, system or product development and planning, insurance, audit, and administrative purposes)
- Maintaining overall relationship
- Documentation for purposes of account sign-up, providing feedback or sending relevant communication such as notifications regarding changes to Terms and Conditions and Privacy Policy, responding to customer complaints, website visits, facilitating communication when the Data Subject is referred by a current customer, and similar internal business purposes
- Database for sending promotional mail (direct or electronic), newsletters, marketing offers, and the like. Personal Data submitted may also be used in targeting and geolocation in order to determine which specific products or services would be most relevant to the customer. This shall be applicable only to individuals who have specifically requested these services or have opted-in for these services. Personal Data submitted may also be used for advertising that uses Personal Data as inspiration or basis for purposes of determining the appropriate demographic and characteristics for effective advertisements. In the event the actual details of a single customer will be used for this purpose, a specific Consent therefor will be requested from the customer.
- Conduct of activities related to marketing and promotions such as customization of user experience through the websites and Social Media accounts
- Market research including determining the target market demographics, data mining, statistical analysis, and big data analysis which uses a combination of demographic indicators and metadata
- Data Sharing with parent company, subsidiaries, and affiliates, for the same purposes listed above
- Complying with applicable laws, rules, and regulations or requirements of lawful authorities
- Documentation purposes

2. *General obligations of Users of Personal Data*

The "Users" shall ensure that the Personal Data collected are:

a. used only for the declared, specified, and legitimate purpose made known to the Data Subject at the time of collection;

b. used or Processed only to the extent made known to the Data Subject at the time of collection;

c. used only for such as time as may be necessary to accomplish the declared, specified, and legitimate purpose made known to the Data Subject at the time of collection; and

d. not used once the Data Subject has withdrawn his Consent.

Without prejudice to the generality of the foregoing, employees of an Organization are prohibited from using the Organization's computer systems for the transmission of unsolicited bulk email advertisements or commercial messages which are likely to trigger complaints from the recipients. Colloquially known as "spam", these prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches.

C. Storage, Retention, and Destruction

1. *Storage and Retention*

The storage facility, including but not limited to Data Storage Areas, and all equipment where Personal Data are stored and retained shall, at all times, be compliant with the applicable physical, technical, and organizational data security measures provided in this Manual.

Moreover, unless the storage of the Personal Information is required for the Organization to comply with statutory requirements, Personal Data shall be stored and retained only for as long as necessary –

a. for the fulfilment of the declared, specified, and legitimate purpose made known to the Data Subject at the time of collection, or when the Processing relevant to the purpose has been terminated;

b. for the establishment, exercise, or defense of legal claims; or

c. for legitimate business purposes, which must be consistent with the standards followed by the applicable industry or approved by appropriate government agency, including compliance with legal requirements on retention of relevant files including tax returns and other documents on statutory benefits.

References or details from Personal Data which are aggregated or kept in a form which does not permit identification of Data Subjects may be kept longer than necessary for the declared, specified, and legitimate purpose. However, no Personal Data may be retained in perpetuity in contemplation of a possible future use that has yet to be determined.

2. *Destruction*

Personal Data shall be disposed of or discarded in a secure manner that would prevent further Processing, unauthorized access, or disclosure to any other party or the public, or that would prejudice the interests of the Data Subjects.

Destruction is defined as any action which prevents the recovery of information from the storage medium on which it is recorded, including encryption with unknown keys, erasure, reformatting, or disposal of the hardware needed to recover the information.

Unless otherwise permitted under this Manual, employees should not destroy or dispose of potentially important records or information of the Organization without the approval of the Group Head of the Data Owner.

Documents or materials in hardcopy form (paper, microfilm, microfiche, and the like) should be either shredded or incinerated by the Data Owner, or the Data Custodian upon instruction of the Data Owner, except where they contain Sensitive Personal Information in which case they should be delivered to the relevant DPO or COP for secure destruction. The shredders to be used for this purpose should create confetti or other similar small particles; strip cut shredders may not be used for this purpose because they allow unauthorized parties to readily reconstruct shredded hard copy documents or materials.

For magnetic media such as but not limited to hard disks, floppy disks, and magnetic recording tape, erasing or reformatting is not an acceptable data destruction method because the data previously stored therein can still be recovered. For destruction of electronic storage devices, assistance must be secured from the Group's Information Technology (IT) Department.

All materials used in the Processing of Personal Information including materials used in the handling thereof such as, but not limited to, typewriter ribbons, carbon paper sheets, mimeograph stencil masters, photographic negatives, aborted computer hardcopy output, unacceptable photocopies, and the like should also be destroyed as provided above as may be appropriate.

All waste copies of documents containing Personal Information that are generated in the course of copying, printing, or other methods of reproduction or handling should be destroyed in accordance with the guidelines under this Manual. If a copy machine jams or malfunctions when employees are making copies of documents containing Personal Information, the concerned employees should not leave the machine until all copies of the document containing Personal Information are removed from the machine or destroyed beyond recognition as provided in this Manual.

D. Access

All individuals subject to this Manual must operate and hold Personal Data under strict confidentiality. This obligation shall continue even after such individual transfers to another position in an Organization or is terminated or terminates his employment or contractual relations with an Organization. The employee's obligation to maintain secrecy and confidentiality shall be provided in the Employee Confidentiality Agreement which all employees are required to sign as a condition for employment or continued employment.

On the other hand, the duty of confidentiality for contractors, providers, and other individuals who have access to Personal Data shall be as provided in their respective Non-Disclosure and Confidentiality Agreements and/or Confidentiality undertakings in their respective contracts.

Even within a particular Organization, only select individuals or employees specifically authorized to access a particular type of Personal Data should view or access the same.

1. *Access by Data Subjects*

Data Subjects have the right to reasonable access, upon demand, to the following matters:

a. Contents of his Personal Data that were Processed;
b. Sources from which his Personal Data were obtained;
c. Names and addresses of the recipients of his Personal Data;
d. Manner by which his Personal Data was Processed;
e. Reasons for the disclosure of his Personal Data to recipients, if any;
f. Information on automated processes where his Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect him;
g. Date when his Personal Data was last accessed and modified, including copies of the new and retracted information; and
h. The designation, name or identity, and address of the PIC.

For this purpose, the Organization shall ensure that the application system which handles Personal Data must generate logs that show every addition, modification, and deletion of data.

Where Personal Data are Processed by electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain from the PIC a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Data Subject.

E. Disclosure and Sharing

1. *Outsourcing and Subcontracting*

An Organization may subcontract or outsource the Processing of Personal Data provided it shall use contractual or other reasonable means to:

a. ensure that proper safeguards are in place;
b. ensure the confidentiality, integrity, and availability of the Personal Data Processed;
c. prevent the use of Personal Data Processed for unauthorized purposes; and
d. comply with the requirements of the Rules and other applicable laws for Processing of Personal Data.

An Organization that subcontracts or outsources the Processing of Personal Data must ensure that its agreements with PIPs contain the following provisions:

a. subject-matter of the Processing;
b. duration of the Processing;
c. nature of the Processing;
d. purpose of the Processing;
e. type of Personal Data;
f. categories of Data Subjects;
g. obligations and rights of the Organization as PIC;
h. geographic location of the Processing;
i obligations of the PIP including but not limited to:

i. to Process the Personal Data only upon the documented instructions of the Organization, including transfers of Personal Data to another country or an international organization, unless such transfer is authorized by law;

ii. to ensure that an obligation of confidentiality is imposed on persons authorized to Process the Personal Data;

iii. to implement appropriate security measures and comply with the Rules;

iv. not to engage another processor without prior instruction from the Organization; provided that where such engagement is allowed by the Organization, the PIP shall ensure that the same obligations for data protection under the contract are implemented by the other processor, taking into account the nature of the Processing;

v. to assist the Organization, by appropriate technical and organizational measures and to the extent possible, to fulfil the obligation to respond to requests by Data Subjects relative to the exercise of their rights;

vi. to assist the Organization in ensuring compliance with the Rules and other relevant laws, taking into account the nature of Processing and the information available to the Organization;

vii. at the option of the Organization, to delete or return all Personal Data to the Organization after the end of the provision of services relating to the Processing; provided, that this includes deleting existing copies unless storage is authorized by the DPA or another law;

viii. to make available to the Organization all information necessary to demonstrate compliance with the obligations laid down in the DPA, and to allow for and contribute to audits, including inspections, conducted by the Organization or another auditor mandated by the latter; and

ix. to immediately inform the Organization if, in its opinion, an instruction infringes the Rules.

2. *Data Sharing*

In the event the Personal Data will be shared by an Organization to individuals or entities outside the Organization, including affiliates, subsidiaries, and parent company, but excluding its PIPs, the Organization sharing the Personal Data must also ensure that the following matters are complied with:

a. The Data Subjects' Consent for the Data Sharing was obtained at the time the Personal Data was collected; and

b. If Data Sharing is for a commercial purpose (*e.g.* direct marketing to be undertaken by the recipient for its own purpose), ensure that the Data Sharing is covered by a Data Sharing Agreement. The execution of the Data Sharing Agreement is without prejudice to any additional requirements that may be necessary to allow a third party to be given access to the Group's systems.

VI. Security Measures

A. Organizational Security Measures

1. *Data Protection Officer (DPO) and Compliance Officer for Privacy (COP)*

a. DPO

The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his duties and responsibilities. As such, the DPO should have and continuously develop expertise in relevant privacy or data protection policies and practices. He should have sufficient understanding of any and all data processing operations being carried out by the Group, including the latter's information systems, data security, and/or data protection needs.

The DPO should familiarize himself with the sector or field of the Group and its internal structures, policies, and processes.

Subject to the NPC's approval, the Group may appoint a single DPO to be primarily accountable for ensuring the compliance of the entire Group with all data protection policies. Unless the Group decides in writing otherwise, the DPO of the Group shall be the Group's Chief Compliance Officer or his designee.

b. *COP*

Where a common DPO is allowed by the NPC as discussed above, the Organizations acting as PICs or PIPs must each have a COP.

Where an Organization has branches, sub-offices, or any other component units, it may also decide to appoint or designate a COP for each component unit.

The minimum qualifications for a COP shall be proportionate to his functions, as provided in this Manual.

c. *Position of the DPO or COP*

The DPO and COPs should be full-time employees of the Group. Where the employment of the DPO or COP is based on an independent contract, the term or duration thereof should at least be two (2) years to ensure stability.

In case the position of DPO or COP is left vacant, the Group or relevant Organization should arrange for the appointment, reappointment, or hiring of his replacement within a reasonable period of time. The Group or relevant Organization may also require the incumbent DPO or COP to occupy such position in a holdover capacity until the appointment or hiring of a new DPO or COP, in accordance with its internal policies or the provisions of the appropriate contract.

d. *Functions of the DPO and the COP*

A DPO shall, among other things:

i. monitor the Group's compliance with the Rules. For this purpose, he may:

   (1) collect information to identify the Processing operations, activities, measures, projects, programs, or systems of the Group, and maintain a record thereof;

   (2) analyze and check the compliance of Processing activities, including the issuance of security clearances to and compliance by third-party service providers;

   (3) inform, advise, and issue recommendations to the Group;

   (4) ascertain renewal of accreditations or certifications necessary to maintain the required standards in Personal Data Processing; and

   (5) advice the Group as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with law;

ii. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the Group;

iii. advice the Group regarding complaints and/or the exercise by Data Subjects of their rights (*e.g.*, requests for information, clarifications, rectification or deletion of Personal Data);

iv. ensure proper Personal Data Breach and Security Incident management by the Group, including the latter's preparation and submission to the NPC of reports and other documentation concerning Security Incidents or Personal Data Breaches within the prescribed period;

v. inform and cultivate awareness on privacy and data protection within the Group, including all relevant laws, rules and regulations, and issuances of the NPC;

vi. advocate for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the Group relating to privacy and data protection by adopting a Privacy by Design approach;

vii. serve as the contact person of the Group vis-à-vis the Data Subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns;

viii. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

ix. perform other duties and tasks that may be assigned by the Group that will further the interest of data privacy and security and uphold the rights of the Data Subjects.

Except for items (i) to (iii), a COP shall perform all other functions of a DPO for his Organization. Where appropriate, he shall also assist the DPO in the performance of the latter's functions.

The DPO or COP must have due regard for the risks associated with the Processing operations of the Group or the relevant Organization, taking into account the nature, scope, context, and purposes of Processing. Accordingly, he must prioritize his activities and focus his efforts on issues that present higher data protection risks.

The Group or Organization may outsource or subcontract the functions of its DPO or COP. However, to the extent possible, the DPO or COP must oversee the performance of his functions by the third-party service provider or providers. The DPO or COP shall also remain the contact person of the Group or Organization vis-à-vis the NPC.

e. *Independence, Autonomy and Conflict of Interest*

A DPO or COP must be independent in the performance of his functions and should be accorded a significant degree of autonomy by the Group and/or the relevant Organization.

In his capacity as DPO or COP, an individual may perform (or be assigned to perform) other tasks or assume other functions that do not give rise to any Conflict of Interest.

f. *General Obligations of Group or Organization Relative to the DPO or COP*

The Group and/or the relevant Organization should:

i. effectively communicate to its personnel, the designation of the DPO or COP and his functions;

ii. allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;

iii. provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep himself updated with the developments in data privacy and security and to carry out his tasks effectively and efficiently;

iv. grant the DPO or COP appropriate access to the Personal Data it is Processing, including the processing systems;

v. where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;

vi. promptly consult the DPO or COP in the event of a Personal Data Breach or Security Incident; and

vii. ensure that the DPO or COP is made a part of all relevant working groups that deal with Personal Data Processing activities conducted inside the Organization or the Group, or with other organizations.

To strengthen the autonomy of the DPO and COPs and ensure their independence, the Group or the relevant Organization should not directly or indirectly penalize or dismiss the DPO or COP for performing his tasks. It is not necessary that the penalty be actually imposed or meted out. A mere threat shall be considered sufficient if it has the effect of impeding or preventing the DPO or COP from performing his tasks. However, nothing shall preclude the legitimate application of

labor, administrative, civil, or criminal laws against the DPO or COP, based on just or authorized causes.

g. *Publication and Communication of Contact Details*

To ensure that its own personnel, the Data Subjects, the NPC, or any other concerned party, are able to easily, directly, and confidentially contact the DPO or COP, the Group or the relevant Organization must publish the DPO's or COP's contact details through at least, the following:

- the Group or the Organization's website;
- privacy policy; and
- this Manual.

At their discretion, the Organizations, may introduce or offer additional means for Data Subjects to communicate (*e.g.*, telefax, social media platforms, etc.) with the DPO or COPs.

For this purpose, the contact details of the DPO or COPs should include the following information:

- title or designation
- postal address
- a dedicated telephone number
- a dedicated email address

The name or names of the DPO or COPs need not be published. However, it should be made available upon request by a Data Subject or the NPC.

2. *Maintaining Organizational Competency*

An Organization must require all its employees to attend periodic information security awareness trainings and data privacy and security trainings.

3. *Conduct of Privacy Impact Assessment*

The Organization shall conduct a Privacy Impact Assessment relative to all activities, projects, and systems involving the Processing of Personal Data. It may choose to outsource the conduct of such assessment to a third party.

4. *Recording and Documentation*

The DPO and COPs shall maintain adequate records and documentation of activities it has carried out to ensure compliance with the Rules.

5. *Duty of Confidentiality*

All individuals subject to this Manual must operate and hold Personal Data under strict confidentiality. This obligation shall continue even after such individual transfers to another position in an Organization or is terminated or terminates his employment or contractual relations with an Organization. The employee's obligation to maintain secrecy and confidentiality shall be

provided in the Employee Confidentiality Agreement which all employees are required to sign as a condition for employment or continued employment.

On the other hand, the duty of confidentiality for contractors, providers, and other individuals who have access to Personal Data shall be as provided in their respective Non-Disclosure and Confidentiality Agreements, and/or Confidentiality undertakings in their respective contracts.

6. *Review of Privacy Manual*

This Manual shall be reviewed and evaluated annually. The privacy and security policies and practices of the Group shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

The Group shall use reasonable and appropriate physical measures to ensure protection of Personal Information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful Processing.

1. *Format of Data to be Collected*

Personal Data collected may be in digital/electronic format and paper-based/physical format.

2. *Storage Type and Location*

Personal Data shall be stored in secured locations designated by the Data Owner. As far as practicable, such data shall be physically locked in Data Storage Areas.

When outside the Organization's premises, employees are likewise required to keep under their possession all Mobile Devices assigned to them. When necessary, employees shall deposit them in a secure location such as a locker or a hotel safe. When travelling, Mobile Devices should not be left inside a car, even if it is locked. Moreover, Mobile Devices should be stored in a hand luggage instead of putting them in the hold of the plane.

All assets associated with the Processing of Personal Data shall be identified and an inventory of all important assets drawn up and maintained to provide control and accountability to support management's strategic planning and enhance response time for critical incidents, system's planning, protection, maintenance, and recovery.

3. *Access Procedure for Employees and Contractors*

Access to Personal Data shall be strictly limited to individuals, employees, and contractors alike, who need such data in the performance of their functions. The Group Head of the Data Owner shall identify in a written document the individuals who are allowed access to Personal Data Processed by such Data Owner as well as the type (whether full or limited) and duration of access allowed. A written authorization by the Group Head of the Data Owner is required before any person other than those identified may be allowed access to the Personal Data.

The keys to the Data Storage Areas shall be held by a person designated by the Group Head of the Data Owner.

Employees are also advised to take extra care when exposing their Mobile Devices in public places such as coffee shops and airport security checkpoints. Users of Mobile Devices in public places must be mindful and take care to avoid the risk of overlooking by unauthorized persons.

4. *Monitoring and Limitation of Access to Room and Facility*

Only individuals properly identified or authorized to have access to Personal Data shall be allowed entry to the Data Storage Areas. The Data Owner and, when applicable, the Data Custodian, shall maintain a log which records access to the Data Storage Areas. Such log shall also indicate whether copies of Personal Data were made and for what purpose.

Security personnel shall monitor or shall have a mechanism to monitor the Data Storage Areas to ensure that there are no signs of break-ins or unauthorized or unlawful entries. Any signs of break-ins shall be promptly reported to the Data Owner, and when applicable, the Data Custodian, and investigated.

All maintenance personnel who are assigned to clean the Data Storage Areas shall be screened and their names and work schedules recorded.

5. *Design of Office Space/Work Station*

The Group shall ensure that the design of office spaces and workstations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to the public. Employees should only be aware of the existence of, or activities within, a secure area on a need to know basis. Recording and photographic equipment should not be allowed in the Data Storage Areas, unless specifically authorized.

The rooms and work stations used in Processing Personal Data shall, as far as practicable be secured against natural disasters, power disturbances, external access, and other similar threats.

6. *Persons Involved in Processing, and their Duties and Responsibilities*

The Group shall ensure that the duties, responsibilities, and schedule of individuals involved in the Processing of Personal Data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time.

The Group Heads of the departments in an Organization, or their equivalents, should periodically review and validate roles and responsibilities related to security of Personal Data in contracts, job descriptions, job offers, or in user agreements. This is to ensure that roles and responsibilities of all employees are up-to-date and adheres to the Information Security Policy of the Organization. The review and validation of roles and responsibilities should be conducted annually; or when implementing new changes in the information system; or during restructuring and staffing of the Organization, its groups, divisions, or departments.

7. *Modes of Transfer of Personal Data*

The Organization shall be responsible for any Personal Data under its control or custody, including information that have been outsourced or transferred to a PIP or a third party for Processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Transfers of Personal Data via electronic mail shall use a secure email facility. Facsimile technology shall not be used for transmitting documents containing Personal Data.

8. *Retention and Disposal Procedure*

Please refer to Article V, Section C on Storage, Retention, and Destruction of files containing Personal Data for guidelines on the retention and disposal procedure.

C. Technical Security Measures

1. *Monitoring for Security Breach*

The Group shall use an intrusion detection system to monitor security breaches to the network and alert the relevant Organization of any attempt to interrupt or disturb the system.

2. *Security Features of the Software/s and Application/s Used*

The Organization's IT Department 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. Moreover, custody of software installers must be with the Organization's IT Department, or any other department or group tasked with similar functions, and not the individual users. This is because any installation requires administrative privilege.

All production application systems which handle Sensitive Personal Information are required to have system logs. Systems shall be monitored and information security events must be recorded to detect unauthorized information Processing activities. Operator logs and fault logging must be used to ensure information system problems are identified. System monitoring must be used to check the effectiveness of controls adopted and to verify conformity to an access policy model, subject to compliance with relevant laws, rules, and regulations applicable to its monitoring and logging activities.

3. *Regular Testing, Assessment, and Evaluation*

To prevent third parties from gaining unauthorized access to the Organization's information systems, employees are enjoined not to use any externally-provided software from a person or organization other than a known and trusted supplier. The only exception to this is when a software application has first been tested and approved by the Organization's IT Department. All employees and individuals provided with official IT computing resources and connecting to the Organization's systems are also required to have virus screening software. Virus screening software must be installed and enabled on all the Organization's mail users, firewalls, internet servers, and desktop machines.

The Organization's IT Department shall also install in official IT computing resources, and regularly update, malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis perform the following tasks:

- Check any file on electronic or optical media, and files received over networks, for viruses, malware and other malicious code and scripts before use.

- Check electronic mail attachments and downloads for malicious code before use. This check may be carried out at different places, (*e.g.* at electronic mail servers, on client computers or when entering the network of the Organization).

To prevent any inadvertent disclosure of Personal Data to third parties or the introduction of malware to the system through human error, the Organization shall periodically conduct personnel awareness training involving security threats and issues. Employees shall also be trained or given information on how to report and recover from malicious code attacks.

4. *Technical Security Measures to Control and Limit Access*

Aside from the built-in security features of the software and applications used, the Group likewise implements an additional layer of security by requiring all employees to use strong passwords and providing guidelines for generating strong passwords and providing specific guidelines for password resets. Employees are likewise given guidelines regarding choice of passwords as well as reusing similar passwords. Further, to prevent a brute force attack, after three (3) unsuccessful attempts to enter a password, the involved user-id is either: (a) suspended until reset by a system administrator, or (b) if dial-up or other external network connections are involved, disconnected. Erroneous password entries will likewise be recorded in an audit log for later inspection and action, as necessary. The Organization's IT department is also tasked to ensure that the Organization's network has appropriate controls to protect it from malicious external intrusion such as putting up firewalls for internet access.

VII. Breach and Security Incidents

A. Security Incident Response Team

There shall be a Security Incident Response Team comprising of the Organization's DPO or COP, as the case may be, and one (1) officer from each of the following departments, as designated by the relevant Group Heads:

- Legal Department
- Human Resources Department
- IT Department
- Internal Audit Department

If the Security Incident involves a specific department of the Organization, the Group Head of that department shall designate an officer from its department to be the sixth member of the Security Incident Response Team. The team shall be headed by the Organization's DPO or COP, as the case may be.

The Security Incident Response Team shall collectively assess and evaluate a Security Incident or Personal Data Breach, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with the reporting requirements under the Rules.

The Security Incident Response Team shall, as soon as practicable, ideally within 24 hours from the occurrence of the Security Incident or Personal Data Breach, conduct an initial assessment of the incident or breach to ascertain the nature and extent thereof.

B. Measures to Prevent and Minimize Breach and Security Incidents

Each Organization shall ensure that all new employees, personnel, and contractors are oriented on the proper Processing of Personal Data as provided in Article V. All new employees must attend information security awareness trainings and data privacy and security trainings within the fiscal year of their employment. Each Organization shall also ensure that a copy of this Manual is available and accessible to all employees.

Certain employees who regularly deal with and Process Personal Data will also be included in the capacity building trainings to be conducted.

To monitor for security breaches and identify risks in the processing system as well as assess any changes that need to be made to the Group's policies, each Organization shall conduct periodic Privacy Impact Assessment. The Privacy Impact Assessment shall be conducted as necessary based on the determination of the DPO and/or COP, or at least once a year.

C. 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 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.

D. Notification Protocol

The NPC and affected Data Subjects must be notified within 72 hours upon knowledge of, or when there is reasonable belief that, a Personal Data Breach requiring notification has occurred, as follows:

a. Sensitive Personal Information or any 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
b. The PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Data Subject.

The DPO shall determine whether there is a need to notify the NPC and the Data Subjects affected by the Security Incident or Personal Data Breach. The DPO may delegate the actual notification to any member of the Security Incident Response Team.

E. Documentation and Reporting Procedure of Security Incidents or a Personal Data Breach

The Security Incident Response Team shall come up with a written report for all Security Incidents and Personal Data Breaches. The report shall include the facts surrounding the incident/breach, the effects of such incident/breach, and the remedial actions taken by the Organization. For other Security Incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation.

The Security Incident Response Team, in coordination with the DPO, shall likewise be responsible for preparing a summary of all reports to be submitted to the NPC annually, comprised of general

information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of Personal Data.

VIII. Inquiries and Complaints

Should a Data Subject raise any inaccuracy or error in his Personal Data, the relevant Organization should immediately and accordingly correct the same or provide means for which the Data Subject can correct the Personal Data (*e.g.* updating of online Personal Information records, or online profile), unless the request is vexatious or otherwise unreasonable.

If Personal Data have been corrected, the relevant Organization should ensure that both the new and the retracted information are accessible to the Data Subject and that the intended recipients thereof simultaneously receive the new and the retracted information. However, there is no obligation on the part of the Organization to inform recipients or third parties who have previously received such Processed Personal Data of their inaccuracy and their rectification unless reasonably requested to do so by the Data Subject.

The employee should also be given an opportunity to add a supplementary statement if he objects to the accuracy, relevance, or completeness of the information appearing in his personnel file.

Data Subjects also have the right to suspend, withdraw, or order the blocking, removal, or destruction of his Personal Data from an Organization's filing system upon discovery and substantial proof of any of the following:

a. The Personal Data are incomplete, outdated, false, or unlawfully obtained;
b. The Personal Data are being used for purposes not authorized by the Data Subject;
c. The Personal Data are 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 concern 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; and
g. The PIP or PIC violated the rights of the Data Subject.

The relevant Organization may notify third parties who have previously received such Processed Personal Data.

Inquiries and complaints from Data Subjects may be sent or forwarded to the following:

Data Protection Officer
JY Campos Centre
9th Avenue corner 30th Street
Bonifacio Global City
Taguig City 1634
Philippines
+632 8562888
dpo@delmonte-phil.com

IX. Effectivity

The provisions of this Manual shall be effective immediately.

Schedule 1

Full name,
Addresses and Contact Details e.g. home, mailing and/or business address,),
Contact Details e.g. email address, contact numbers (landline, mobile, fax),
Product Interest e.g. whether they are interested in certain products
Remuneration information including Bank Account numbers (payroll), Payslips
Date of birth
Place of birth
Photos
Government Issued Unique Identifiers (TIN, UMID ID number, SSS Number, Pag-Ibig Number, Philhealth Number, Driver's License number, Passport number)
Age
Religious, philosophical, or political affiliations
Health information and records
Any proceeding for any offense committed or alleged to have committed, the disposal of such proceedings, or the sentence of any court in such proceedings
Employment contract
Tax returns
Gender
Physical attributes (Height, Weight, Blood Type, Eye Color, and the like)
Civil Status
Civil Status Date
Citizenship
Citizenship Date
Religion
Educational information
Names, addresses, contact details, occupations, and birthdays of dependents