



Policy Title: **DATA PRIVACY**

1. POLICY STATEMENT

Mabuhay Vinyl Corporation (the "Company") puts premium value on the privacy and security of personal data entrusted to it by its stakeholders (stockholders, employees, suppliers, customers, affiliates and non-affiliates) for legitimate purposes hence adopts this Policy to comply with Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), its Implementing Rules and Regulations ("IRR"), and other relevant policies, including issuances of the National Privacy Commission ("NPC"), which govern the collection, use, and disclosure of individuals' personal data by organizations in a manner that recognizes both the individuals' right to protect their personal data, and organizations' need to collect, use, and disclose personal data for purposes that a reasonable person would consider appropriate under the circumstances.


The DPA ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding the individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

This Data Privacy Policy shall serve as a guide or handbook for ensuring the compliance of the Company with the Philippine Privacy laws, DPA, its IRR, and other relevant issuances of the NPC. It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances from collection to destruction, directed toward the fulfilment and realization of the rights of the data subjects.


2. DEFINITIONS

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

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



CORPORATE POLICY
Mabuhay Vinyl Corporation

Document No. :

Revision Code : 00

Effectivity date : August 1, 2020

Page 2 of 18

Policy Title: **DATA PRIVACY**

- C. "Data Privacy Act" or "DPA" refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations.

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

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

- F. "Data Subject" refers to an individual whose Personal Information, Sensitive Personal Information, or Privileged Information is processed.


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

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

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

- J. "Personal Data" collectively refers to Personal Information, Sensitive Personal Information, and Privileged Information.


Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



CORPORATE POLICY
Mabuhay Vinyl Corporation

Document No. :

Revision Code : 00

Effectivity date : August 1, 2020

Page 3 of 18

Policy Title: **DATA PRIVACY**

K. "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;

L. "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.

M. "Personal information controller" ("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 its behalf. The term excludes:

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


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

N. "Personal information processor" ("PIP") refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

O. "Processing" refers to any operation or set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system.

P. "Privileged Information" refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.


Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.O. Pangilinan
President/COO



CORPORATE POLICY
Mabuhay Vinyl Corporation

Document No. :

Revision Code : 00


Effectivity date : August 1, 2020

Page 4 of 18


Policy Title: **DATA PRIVACY**

- Q. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
- R. "Public authority" refers to any government entity created by the Philippines Constitution or law, and vested with law enforcement or regulatory authority and functions;
- S. "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.
- T. "Sensitive Personal Information" refers to Personal Data:
1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 2. About an individual's health, education, genetic, or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
 3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and
 4. Specifically established by an executive order or an act of Congress to be kept classified.


Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

3. SCOPE AND LIMITATION

This Policy shall lay down the data protection and Security Measures of the Company. It shall govern the Processing of Personal Data of Data Subjects by the Company and its PIP/s if any. All Employees regardless of type of employment, as well as PIP/s are instructed to comply with all the provisions stated in this Policy.

4. ORGANIZATIONAL SECURITY MEASURES

A. Data Protection Officer

A Data Protection Officer ("DPO") shall be appointed by the Company.

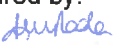
The DPO is responsible for ensuring the Company's compliance with applicable laws and regulations for the protection of data privacy and security.

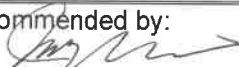
The functions and responsibilities of the DPO shall particularly include, among others:

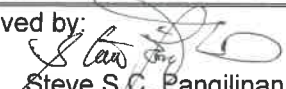
1. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
2. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
3. Inform, advise, and issue recommendations to the PIC or PIP;
4. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
5. Advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law.

B. Data Privacy Principles

All Processing of Personal Data within the Company should be conducted in compliance with the following data privacy principles in the DPA:

Prepared by:

Angelita M. Rada
Data Privacy Officer

Recommended by:

Kate Morgan E. Quiobe
HRD Manager

Approved by:

Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

a. **Transparency:**

The Data Subject must be aware of the nature, purpose, and extent of the Processing of his or her Personal Data by the Company, including the risks and safeguards involved, the identity of persons and entities involved in Processing his or her Personal Data including the identity of the Company, the Company's DPO, and the Company's Personal Data Processor, his or her rights as a Data Subject, and how these can be exercised.

Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.

b. **Legitimate purpose:** The collection, processing, use, and disclosure of Personal Data by the Company shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. **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 shall be processed by the Company only if the purpose of the Processing could not reasonably be fulfilled by other means.

C. Data Processing Records

Adequate records of the Company's Personal Data Processing activities shall be maintained at all times.

Responsible Persons: The DPO, with the cooperation and assistance of all the concerned business and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date.

Minimum Requirements: At the minimum, the following information must be recorded:

Prepared by:

A. Rada
Angelita M. Rada
Data Privacy Officer

Recommended by:

Kate Morgan E. Quiobe
Kate Morgan E. Quiobe
HRD Manager

Approved by:

Steve S.C. Pangilinan
Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

1. Information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;
2. A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;
3. General information about the data flow within the Company, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;
4. A general description of the organizational, physical, and technical security measures in place within the Company; and
5. The name and contact details of the DPO, Personal Data processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.


D. Management of Human Resources

Persons Responsible: The DPO, with the cooperation of the Company's Human Resources ("HR") department, shall develop and implement measures to ensure that all the Company's personnel who have access to Personal Data will strictly process such data in compliance with the requirements of the DPA and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of the Company and conducting training programs to educate employees and agents on data privacy related concerns.

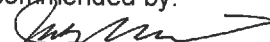
Employee Consent: The DPO, with the assistance of HR, shall ensure that Company shall obtain the employee's informed consent, evidenced by written, electronic or recorded means, to:

1. The Processing of his or her Personal Data, for purposes of maintaining the Company's records; and
2. A continuing obligation of confidentiality on the employee's part in connection with the Personal Data that he or she may encounter during the period of employment with the Company. This obligation shall apply even after the employee has left the Company for whatever reasons.


Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

E. Data Collection Procedures

Responsible Persons: The DPO, with the assistance of the Company's HR and any other departments of the Company responsible for the Processing of Personal Data, shall document the Company's Personal Data Processing procedures.

The DPO shall ensure that such procedures are updated and that the consent of the Data Subjects (when required by the DPA or other applicable laws or regulations) is properly obtained and evidenced by written, electronic, or recorded means.

Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that Processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

F. Data Retention Schedules


Retention Policy: Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by the Company for a period longer than necessary and/or proportionate to the purposes for which such data was collected. MVC shall comply with the retention period specified in the Files Management System.

Responsible Persons: The DPO, with the assistance of the Company's HR and any other departments of the Company responsible for the Processing of Personal Data, shall be responsible for developing measures to determine the applicable data retention schedules, and procedures to allow for the withdrawal of previously given consent of the Data Subject, as well as to safeguard the destruction and disposal of such Personal Data in accordance with the DPA and other applicable laws and regulations.

5. PHYSICAL SECURITY MEASURES

- 1) **Responsible Persons:** The DPO, with the assistance of HR and the Corporate Planning - MIS department, shall develop and implement policies and procedures for the Company to monitor and limit access to, and activities of HR, as well as any other departments and/or workstations in the Company where Personal Data is


Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

processed, including guidelines that specify the proper use of, and access to, electronic media.

- 2) **Evaluation and Readjustment of Office:** The design and layout of the office spaces and work stations of the above-mentioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons.
- 3) **Office Access Restrictions:** The duties, responsibilities, and schedules 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.
- 4) **Physical Risk Management:** The rooms and workstations used in the Processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.
- 5) **Maintenance Policies:** The Company shall establish policies and procedures preventing the mechanical destruction of files and equipment.


6. TECHNICAL SECURITY MEASURES

Responsible Persons: The DPO, with the cooperation and assistance of Corplan - MIS, shall continuously develop and evaluate the Company's security policy with respect to the Processing of Personal Data.

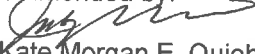
Minimum Requirements: The security policy should include the following minimum requirements:

- a. Safeguards to protect the Company's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;
- b. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Company's data processing systems and services;
- c. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Company's computer

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

- network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a Personal Data breach;
- d. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - e. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and
 - f. Encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

7. RIGHTS OF THE DATA SUBJECT

As provided under the DPA, Data Subjects have the following rights in connection with the Processing of their Personal Data: (1) Right to be Informed; (2) Right to Object; (3) Right to Access; (4) Right to Rectification; (5) Right to Erasure or Blocking; and (6) Right to Damages.

Employees and agents of the Company are required to strictly respect and obey the rights of the Data Subjects.

The DPO, with the assistance of HR shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

The Data Subjects' Rights are elaborated upon as follows:


A. Right to be Informed

The Data Subject has the right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.


The Data Subject shall be notified in writing and furnished with information indicated hereunder before the entry of his or her Personal Data into the processing system of the Company, or at the next practical opportunity:

- a. Description of the Personal Data to be entered into the data processing system;

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

- b. Purposes for which the personal data are being or will be processed, including Processing for profiling or historical, statistical, or scientific purposes;
- c. Basis of Processing, when Processing is not based on the consent of the Data Subject;
- d. Scope and method of the Personal Data Processing;
- e. The recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;
- f. 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 foreseen consequences of such Processing for the Data Subject;
- g. The identity and contact details of the DPO;
- h. The period for which the Personal Data will be stored; and
- i. The existence of their rights as Data Subjects, including the right to access, correction, and to object to the Processing, as well as the right to lodge a complaint before the NPC; and
- j. When applicable, the nature and purpose of data sharing and/ or transfer of personal data outside the Philippines.

B. 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.

The Data Subject 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 Company shall no longer process the Personal Data, unless:

- 1. The Personal Data is needed pursuant to a subpoena;
- 2. The Processing is 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 Company and the Data Subject; or

Prepared by:

Angelita M. Rada
Angelita M. Rada
Data Privacy Officer

Recommended by:

Kate Morgan E. Quiobe
Kate Morgan E. Quiobe
HRD Manager

Approved by:

Steve S.C. Pangilinan
Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

3. The Personal Data is being collected and processed to comply with a legal obligation.

C. Right to Access

The Data Subject, upon written request, has the right to reasonable access to the following:

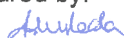
1. Contents of his or her Personal Data that were processed;
2. Sources from which Personal Data were obtained;
3. Names and addresses of recipients of the Personal Data;
4. Manner by which his or her Personal Data were processed;
5. Reasons for the disclosure of the Personal Data to recipients, if any;
6. Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;
7. Date when Personal Data concerning the Data Subject were last accessed and modified; and
8. The designation, name or identity, and address of the Company's DPO.

D. Right to Rectification

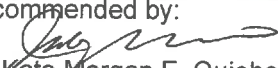
The Data Subject has the right to dispute the inaccuracy or rectify the error in his or her Personal Data, and the Company shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.

If the Personal Data has been corrected, the Company shall ensure the accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data 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.

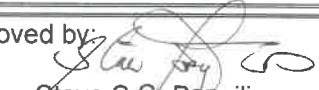
Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

E. 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 Company's filing system.

1. **Conditions for Erasure/ Blocking:** 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 by the Company;
 - 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; or
 - g. The Data Subject's rights have been violated by the Company.

2. The Company or its DPO may notify third parties who have previously received such processed Personal Data that the Data Subject has withdrawn his or her consent to the Processing thereof upon reasonable request by the Data Subject.

F. 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 the violation by the Company of their rights and freedoms as Data Subject.

Prepared by:

Angelita M. Rada
Angelita M. Rada
Data Privacy Officer

Recommended by:

Kate Morgan E. Quiobe
Kate Morgan E. Quiobe
HRD Manager

Approved by:

Steve S.C. Pangilinan
Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

G. Transmissibility of Rights of Data Subjects

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 his/her rights.

H. Data Portability

Where his or her Personal Data is processed by the Company through electronic means and in a structured and commonly used format, the Data Subject shall have the right, upon request, to obtain 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 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.

The DPO shall regularly monitor and implement the NPC's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.


8. DATA BREACHES & SECURITY INCIDENTS

A. Data Breach Notification

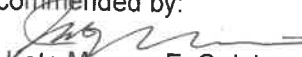
Responsible Persons: All employees and agents of the Company involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or Security Incident.

Internal Reporting Timeline: In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the DPA has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or Security Incident.

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

NPC Reporting Timeline: The DPO shall notify the NPC and the affected Data Subjects within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by, the Company that a personal data breach requiring notification has occurred, pursuant to requirements and procedures prescribed by the DPA.

Minimum Contents:

- 1) The notification to the NPC and the affected Data Subjects shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by the Company to address the breach.
- 2) The notification shall also include measures taken to reduce the harm or negative consequences of the breach and the name and contact details of the DPO from whom the Data Subject can obtain additional information about the breach, and any assistance to be provided to the affected Data Subjects.
- 3) The form and procedure for notification shall conform to the regulations and circulars issued by the NPC, as may be updated from time to time.


B. Breach Reports

Documentation Requirement: All Security Incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements.


Contents of Report for Personal Data Breaches: In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the Company, such as:

- 1) Facts
 - a. Main people responsible
 - b. Events surrounding the breach
 - c. Where data was located, stored, or otherwise processed
 - d. When the data breach happened
 - e. How the breach was detected
 - f. Why did the data breach happen
- 2) Effects
 - a. Effects/ consequences of the data breach
 - b. How data was affected
 - c. Who were the affected data subjects

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



Policy Title: **DATA PRIVACY**

- d. How were the data subjects affected
- e. How long did it take to affect the data subjects
- 3) Remedial Actions
 - a. How long did it take to resolve the matter
 - b. Who took charge of the remedial efforts
 - c. What actions were taken by the person in charge
 - d. When was the situation completely resolved
 - e. What measures were taken to ensure that the breach does not happen again

Contents of Report for Other Security Incidents: In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation.

Availability for NPC: All reports shall be made available when requested by the NPC.

Annual Summary: A general summary of the reports shall be submitted by the DPO to the NPC annually.

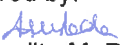
9. OUTSOURCING AGREEMENTS

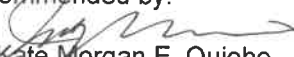
Documentation Requirement: Any Personal Data Processing conducted by an external agent or entity (third party service provider) on behalf of the Company should be evidenced by a valid written contract with the Company.

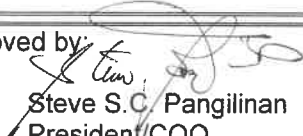
Subcontracting by Third Party Service Provider: The fact that the Company entered into such contract or arrangement does not give the said external agent or entity the authority to subcontract to another entity the whole or part of the subject matter of said contract or arrangement, unless expressly stipulated in writing in the same contract or evidenced by a separate written consent/agreement of the Company.

Required Contents: Such contract should expressly set out: (1) The subject matter and duration of the Processing; (2) The nature and purpose of the Processing; (3) The type of Personal Data and categories of Data Subjects; (4) The obligations and rights of the Company; and (5) The geographic location of the Processing under the contract.

Required Stipulations: In addition, the contract shall include express stipulations requiring the external agent or entity to:

Prepared by:

 Angelita M. Rada
 Data Privacy Officer

Recommended by:

 Kate Morgan E. Quiobe
 HRD Manager

Approved by:

 Steve S.C. Pangilinan
 President/COO



Policy Title: **DATA PRIVACY**

- A. Process the Personal Data only upon the documented instructions of the Company, including transfers of Personal Data to another country or an international organization, unless such transfer is required by law;

- B. Ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process the Personal Data;

- C. Implement appropriate security measures;

- D. Comply with the DPA, its IRR, and other issuances of the NPC, and other applicable laws, in addition to the obligations provided in the contract, or other legal act with the external party;


- E. Not engage another processor without prior instruction from the Company: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the Processing;

- F. Assist the Company, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;


- G. Assist the Company in ensuring compliance with the DPA, its IRR, and other issuances of the NPC, taking into account the nature of Processing and the information available to the external party who acts as a Personal Information Processor as defined under the DPA;

- H. At the choice of the Company, delete or return all Personal Data to it 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 other applicable laws or regulations;

Prepared by:


Angelita M. Rada
Data Privacy Officer

Recommended by:


Kate Morgan E. Quiobe
HRD Manager

Approved by:


Steve S.C. Pangilinan
President/COO



CORPORATE POLICY
Mabuhay Vinyl Corporation

Document No. :

Revision Code : 00

Effectivity date : August 1, 2020

Page **18** of **18**

Policy Title: **DATA PRIVACY**

- I. Make available to the Company all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the Company or another auditor mandated by the latter; and
- J. Immediately inform the Company if, in its opinion, an instruction violates the DPA, its IRR, or any other issuance of the NPC.

Prepared by:

Angelita M. Rada
Angelita M. Rada
Data Privacy Officer

Recommended by:

Kate Morgan E. Quiobe
Kate Morgan E. Quiobe
HRD Manager

Approved by:

Steve S.C. Pangilinan
Steve S.C. Pangilinan
President/COO