



**SHAKEY'S PIZZA ASIA VENTURES INC.**  
 15KM East Service Road, Brgy. San Martin de Porres, Paranaque City 1700  
 www.shakeyspizza.ph

# DATA POLICY MANUAL

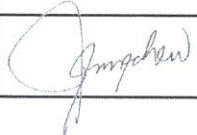
Version 01.2024

## Document History:

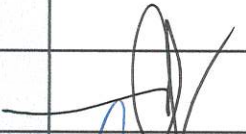



- Revision Number 00 always means Official Release
- For Revision Number 01 onwards, Description of Change must indicate which Section Numbers have been revised.

Revision Number	Description of Change	Author	Signature	Issued Date
00	Official Release			

## Reviewed by:

Department	Name	Designation	Signature	Date
Legal	Atty. James Earl Chew	DPO		

## Approved by:

Designation	Name	Signature	Date
President and Chief Executive Officer	Vicente L. Gregorio		
Chief Finance Officer	Manuel T. Del Barrio		
Chief Operating Officer	Jorge Ma. Q. Concepcion		5/20
Chief Human Resource Officer	Ma. Elma C. Santos		5/20

CONTENTS	PAGE NO.
<b>ARTICLE 1. THIS MANUAL</b>	3
Sec. 1. Introduction	3
Sec. 2. Purpose of the Data Privacy Manual	3
Sec. 3. Scope and Application	4
Sec. 4. Ownership	4
Sec. 5. Definitions	4
Sec. 6. References	7
<b>ARTICLE II. DATA PRIVACY PRINCIPLES</b>	8
Sec. 1. Transparency	8
Sec. 2. Legitimate Purpose	8
Sec. 3. Proportionality	8
<b>ARTICLE III. PROCESSING OF PERSONAL DATA</b>	9
Sec. 1. Collection	9
Sec. 2. Use	12
Sec. 3. Storage, Retention and Disposal	12
Sec. 4. Access	13
Sec. 5. Disclosure and Sharing	14
<b>ARTICLE IV. SECURITY MEASURES</b>	14
Sec. 1. Organizational Security Measures	14
Sec. 2. Physical Security Measures	16
Sec. 3. Technical Security Measures	17
<b>ARTICLE V. PERSONAL DATA BREACH AND SECURITY INCIDENTS</b>	18
Sec. 1. Data Privacy Breach Response Team	18
Sec. 2. Duties of the Breach Response Team	18
Sec. 3. Measures to Prevent Security Incidents and Personal Data Breach	19
Sec. 4. Procedure for Recovery and Restoration of Personal Data	19
Sec. 5. Response and Notification Protocols for Security Incidents and Data Breaches	19
Sec. 6. Documentation and Reporting Procedure for Security Incidents	21
<b>ARTICLE VI. RIGHTS OF DATA SUBJECTS</b>	22
Sec. 1. Right to Be Informed	22
Sec. 2. Right to Reasonable Access	22
Sec. 3. Right to Object	23
Sec. 4. Right to Correction	23
Sec. 5. Right to Erasure or Blocking	23
Sec. 6. Right to Data Portability	24
Sec. 7. Right to File a Complaint	24
Sec. 8. Right to Damages	24
Sec. 9. Transmissibility of Rights	24

CONTENTS	PAGE NO
----------	---------

ARTICLE VII. NOTIFICATIONS, REQUESTS, INQUIRIES, AND COMPLAINTS	24
Sec. 1. Requests and Inquiries Pertaining to Data Privacy Issues	25
Sec. 2. Procedure for Complaints	25
ARTICLE VIII. EFFECTIVITY	26
ANNEXES	
Annex A. Privacy Notice and Consent Form	27
Annex B. Privacy Notice	28
Annex C. Standard Clauses/Provisions for Outsourcing/Subcontracting	31
Annex C-1. Template for Outsourcing/Subcontracting Agreements	34
Annex D. Standard Clauses/Provisions for Data Sharing	40
Annex D-1. Template for Data Sharing Agreement	41
Annex E. Privacy Impact Assessment Questionnaire	49
Annex F. Contact List of DPO and COPs	53
Annex G. Confidentiality/Non-Disclosure/Non-Compete/Proprietary Information Agreement	54
Annex H. Data Privacy Trackers	58
Annex I. Security Incident Report Form	60
Annex J. Data Privacy Request Form	62

# ARTICLE I THIS DATA PRIVACY MANUAL

## Sec. 1. Introduction

Shakey's Pizza Asia Ventures, Inc. and its subsidiaries (referred herein as "the Group") hereby adopts this Data Privacy Manual (the "Manual") in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (the "DPA"), its Implementing Rules and Regulations (the "IRR"), and other relevant policies and issuances (collectively known as "Privacy Laws") of the National Privacy Commission (the "Commission"). Below is the list of subsidiaries within the Group:

Wow Brand Holdings Inc.  
Shakey's Pizza Commerce Inc.  
Shakey's Seacrest Inc.

The DPA was passed into law in 2012, consistent with the Philippines' policy of protecting the fundamental human right of privacy, while ensuring free flow of information. To promote such policy, the DPA, along with its IRR, shall govern the processing of personal data by any natural or juridical person in the government or private sector, who must in turn establish policies and implement measures to guarantee the security of personal data under their control and/or custody.

With the Privacy Laws, and the principles of transparency, legitimate purpose and proportionality as its backdrop, the Group abides by this Manual in carrying out its principal business. This is to ensure that personal data under its control remain safe and secured while being processed in the course of its business.

## Sec. 2. Purpose of the Data Privacy Manual

This Manual shall serve as a guide for ensuring compliance with the DPA, its IRR and other relevant issuances of the Commission. This Manual shall encapsulate the privacy and data protection protocols to be observed and carried out for specific circumstances (e.g., from collection to destruction) and activities performed by the Group. Likewise, this manual aims to inform clients, employees, partners and stakeholders of the Group's data protection and security measures, and to guide them in the exercise of their rights under the Privacy Laws.

This Manual is designed to inform Employees of:

- a. The purposes and guidelines the processing of Personal Data and Sensitive Personal Data undertaken by the Group;
- b. The data protection and security measures implemented by the Group to ensure protection of Personal Data;
- c. How Employee can contact the Group or any of its subsidiaries with any inquiries or complaints;

- d. Data Subject's rights in relation to the processing of their Personal Data and Sensitive Personal Data; and
- e. How contracts with all vendors requiring the vendors shall be governed and provide adequate levels of privacy protection as requested under the Data Privacy Act of the Philippines and other data protection legislations.

### **Sec. 3. Scope and Application**

This Manual shall lay down the data protection and security measures of the Group. It shall govern the processing of personal data of data subjects by the Group and the latter's PIPs, if any. All employees of the Company, regardless of the type of employment, as well as all PIPs, are enjoined to comply with the terms laid down in this Manual.

This Manual applies to all Personal Data and Sensitive Personal Data (as defined below) received by the Group in any format related to any current and former employees, their respective family members, officers, consultants, contractors, temporary and agency Employee, as well as applicants for employment ("Employee"), vendors, suppliers, third-party processors and customers and clients.

This Manual is not exclusive and conclusive. The Group's policies, measures and procedures, as explained in this Manual, may be amended as deemed necessary due to legislation and issuances of the NPC. Moreover, the Group shall periodically review this Manual and its policies, measures and procedures for continued propriety with respect to the applicable risks identified and assessed. As such, the Group reserves the right to modify, add or alter this Manual anytime in accordance with data privacy laws, regulations, issuances of the NPC and jurisprudence, all of which are read into and are an integral part of this document.

### **Sec. 4. Ownership**

This document is the responsibility of the Data Protection and Security Team (DPST). It is kept up to date by the Data Protection Officer (DPO). Recommendation for improvements is the responsibility of the DPO as owner of the document.

### **Sec. 5. Definitions**

Authorized Personnel	Employee/s or officer/s of the Group authorized to collect and/or to process personal data either by the function of their office or position, or through specific authority given in accordance with the policies of the Group
Breach Response Team or BRT	The group of individuals designated by the Group to respond to security incidents and personal data breaches, and to ensure that data breaches are reported to the NPC.
Commission or NPC	The National Privacy Commission

Compliance Officer for Privacy or COP	An individual duly appointed and authorized by the Group to perform some of the functions of the DPO for a subsidiary, division, or business unit, if any.
Consent of the Data Subject	Any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and processing of his/her Personal, Sensitive Personal, or Privileged Information. It shall be evidenced by written, electronic, or recorded means.
Data Protection and Security Team or DPST	The group of individuals designated by the Group to respond to inquiries and complaints relating to data privacy, and to assist in ensuring the Company's compliance with the Privacy Laws, as well as in implementing this Manual.
Data Processing Systems or DPS	The systems and procedures by which Personal Data is collected and further processed by the Group in its Information and Communications System/s and/or relevant Filing System/s. A DPS may refer to both electronic and manual processes
Data Protection Officer or DPO	The officer duly designated and appointed by the Group to be responsible for ensuring the Group's compliance with Privacy Laws for the protection of data privacy and security. The DPO shall also act as liaison between the Group and the NPC for privacy-related compliance matters
Data Sharing	The disclosure or transfer to a third party of Personal Data under the control or custody of the Group.
Data Sharing Agreement	Any written contract or agreement that contains the terms and conditions of a Personal Data Sharing arrangement entered by the Group with a third party.
Data Subject	An individual whose Personal, Sensitive Personal, and/or Privileged Information are being collected and/or processed by the Group in the course of its business operations. For purposes of this Manual, it refers to employees, trainees, applicants, members of the Board of Directors, consultants, clients, stockholders, partners, suppliers, subcontractors, service providers, office visitors, and other persons with business dealings with the Group
Filing System	Any system or process referring to the collection and storage of documents containing personal data to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible

Information and Communications System	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
Outsourcing	The disclosure or transfer of Personal Data by the Group to a Personal Information Processor (PIP) for the latter's Processing, which shall be done strictly in accordance with the instructions of the Company
Outsourcing Agreement	Any written contract entered by the Group with a PIP, including its service providers for the processing of personal information on behalf of the Group.
Personal Information	Any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual
Personal Data	Collective term for personal information and sensitive personal information, including privileged information.
Privileged Information	Any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication
Personal Data Breach	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed
Personal Information Controller or PIC	A natural or juridical person, including the Group, who/which controls the collection, holding, processing and use of Personal Data, or instructs another person to process Personal Data on its behalf
Personal Information Processor or PIP	Any natural or juridical person, or any other body, to whom a PIC, which may include the Group, outsources, or gives instructions as regards the Processing of Personal Data of a Data Subject or group of Data Subjects
Privacy Impact Assessment or PIA	A process of review used to evaluate and manage the impact on privacy of a particular program, project, process, measure, system, or technology product of the Group or its PIP/s. It takes into account the nature of the Personal Data to be protected, the Personal Data flow, the risks to privacy and security posed by the Processing, current data privacy best practices, and the cost of security implementation.

Privacy Laws	Collectively refers to the DPA, its Implementing Rules and Regulations (the "IRR"), the issuances of the NPC and other applicable laws and regulations
Privacy Policy	The internal statement that governs the Group's practices of handling personal data. It instructs the users of Personal Data (i.e., Authorized Personnel) on the processing of Personal Data and informs them of the rights of the Data Subjects.
Privacy Notice	The statement, substantially in the format specified under Annex "D" of this Manual, made to a Data Subject to inform him/her of how the Group processes his/her Personal Data
Processing	Any operation or set of operations performed upon Personal Data including, but not limited to, its collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction. Processing may be performed through automated means or by manual processing
Security Incident	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
Security Measures	The physical, technical, and organizational measures employed by the Company to protect Personal Data from natural and human dangers
Sensitive Personal Information	<p>Personal Information that is:</p> <ol style="list-style-type: none"> <li>1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.</li> <li>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.</li> <li>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; or</li> <li>4. Specifically established by an executive order or an act of Congress to be kept classified.</li> </ol>

## Sec. 6. References



- Republic Act 10173 - Data Privacy Act of 2012
- Implementing Rules and Regulations of the Data Privacy Act of 2012
- NPC Privacy Toolkit, Third Edition 2018
- NPC Issuances

## ARTICLE II DATA PRIVACY PRINCIPLES

In processing Personal Data, the Group, its employees and PIPs shall abide by the following principles:

### **Sec. 1. Transparency.**

The Data Subject shall be informed of the nature, purpose, and extent of the Processing of his/her Personal Data, including the risks and safeguards involved, the identity of the Group, his/her rights as a Data Subject, and how these rights may be exercised.

### **Sec. 2. Legitimate Purpose.**

The Processing of Personal Data shall only be for the purpose declared and specified to the Data Subject. No further processing of Personal Data shall be done without the consent of the Data Subject.

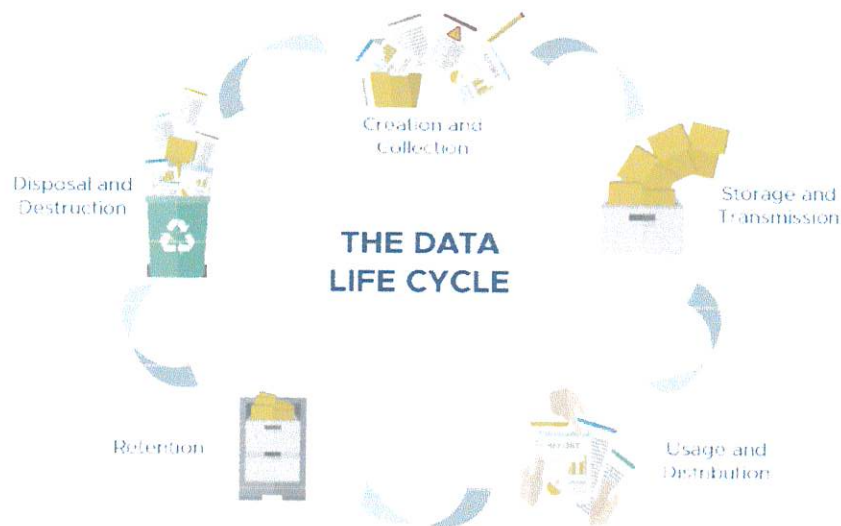
### **Sec. 3. Proportionality.**

The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data will be processed by the Group only if the purpose of the Processing could not be reasonably fulfilled by other means, and if required by the Group's business operations.

## ARTICLE III PROCESSING OF PERSONAL DATA

Whenever necessary, the Group shall process Personal Data to achieve its legitimate business purposes and may modify or update any of its Data Processing Systems.

Processing of personal data commences from the collection thereof until its disposal and destruction<sup>1</sup>:



This section shall provide the various guidelines to be applied to the various parts of the life cycles of Personal Data or processing systems within the Organization.

### Sec. 1. Collection

#### 1.1 General Principles for Collecting Personal Information.

1.1.1 *Consent.* Consent is generally required prior to the collection and processing of personal data, subject to the exemptions provided under the DPA and other applicable laws and regulations. When required, consent must be time-bound in relation to the declared, specified and legitimate purpose.

To be valid, consent must be freely given, specific, express and an informed indication of will, whereby the data subject agrees or voluntarily assents to the collection and processing of personal information about and/or relating to him or her. The Data Subject must also be informed and provided the means to withdraw consent already given.

Where the Group must collect and process the Personal Data of a Data Subject under any contract with such Data Subject, it shall ensure that the Data Subject to has signed

---

<sup>1</sup> Diagram from the Third Edition of the NPC Toolkit, 2018.

a Consent Form substantially in the form provided in Annex "A". Consent may also be given on behalf of a Data Subject by a lawful representative, or an agent authorized by the Data Subject to do so.

The detailed guidelines on consent are contained in the Group's Consent Documentation Guidelines.

1.1.2 *Informing Data Subjects of their Rights.* Before processing any personal data, the Group's responsible personnel shall apprise the Data Subject/s concerned of specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her Personal Data for profiling, or processing for direct marketing, and data sharing. Data Subjects must also be informed of their rights under the DPA, its IRR and other related issuances of the NPC.

1.1.3 *Purpose.* Personal Data shall only be collected and used for the purpose/s specified and declared to the Data Subject, and subject to the Consent of the Data Subject. The Group's use of the Personal Data shall only be for the purpose of carrying out the business operation of the Group or for the following general purposes, among others:

- a. To document and manage the Group records;
- b. conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract thereafter;
- c. To respond to queries, complaints, and requests;
- d. To provide information about the Group's services;
- e. To conduct research and analysis to improve customer experience;
- f. To maintain security; and
- g. To comply with legal, regulatory, and contractual requirements or obligations.

The use and processing of Personal Data may also depend on the specific activities and transactions of the various subsidiaries and business units involved.

1.1.4 *Accuracy and Relevance.* Only Personal Data that is necessary and compatible with the declared, specified and legitimate purpose shall be collected. The Group shall regularly review forms used to ensure that the information being collected are still accurate and relevant.

1.2 **Data Subjects from whom Personal Data are obtained.** The Group processes personal data of the following:

- a. Customers and participants in various promotions;
- b. Vendors, service providers and representatives of its third-party vendors, service providers;
- c. Prospective, active, resigned, and separated employees;
- d. Student interns; and
- e. Visitors.

1.3. **Type of Data Collected and Mode of Collection.** The Group processes all kinds of personal data, including sensitive personal data. These personal data may include, among others,

names, date and year of birth, marital status, gender, citizenship/nationality, residence, contact information, government-issued documents and information peculiar to an individual, and bank account information. In this regard, all departments shall collect only such personal data and maintain only such records and documents that are necessary to carry out a legitimate purpose. The Personal Data in the custody of the Group may be in digital/electronic format and/or paper-based/physical format.

1.3.1 Employee Data - The Group processes the following Personal Data necessary for management of payroll and Employee administration: (i) name; (ii) address; (iii) date of birth; (iv) gender; (v) current position and effective date; (vi) salary information and bank details; (vii) emergency contact information; (viii) education and certification; (ix) sickness, accident and work records; (x) leave entitlement and leave balance; (xi) bonus, pensions, insurance and benefits details; and (xii) general information on the member of Employee's dependents (e.g., number of dependents, age, and relationship).

In addition, the Group may process any other information that it deems necessary to function as a business, some of which may or may not constitute Personal Data, including, but not limited to: (a) hire date; (b) job grading; (c) training courses; (d) previous employers; and (e) recruitment information (e.g., personal curricula).

The above Personal Data and other information is processed at the beginning of and throughout the Employee's working relationship with the Group through various forms and submissions and is updated as necessary.

1.3.2 Customer Data - The Group may collect the basic contact information of clients and customers, including their full name, address, contact number, together with the information on the products that they patronize. This information may be collected by sales representatives or other agents through accomplished order forms or from third party providers engaged by the Group process customer data on its behalf in order to provide services and customer support.

1.3.3 Vendor Data - The Group may collect the basic contact information of vendors' or suppliers' representatives for purposes of coordination and provision of services or supplies as part of vendor accreditation and onboarding and preparation and execution of contracts with vendors and third-party suppliers or providers.

1.4 **Privacy Notice.** Information on the collection and Processing of Personal Data of the Data Subject, shall be relayed to the Data Subject through a Privacy Notice, which shall be posted in the Group's websites and made readily available to the Data Subject including the following information:

- a. Types of Personal Data collected;
- b. Purpose/s for the collection and Processing of Personal Data;
- c. Transfer and/or sharing of Personal Data and recipients thereof;
- d. Extent of Processing of Personal Data;;
- e. Rights of the Data Subject with regard to privacy and data protection; and
- f. Contact information of the DPO.

The Privacy Notice shall be in substantially the same form as provided in Annex "B".

## Sec. 2. Use

### 2.1 General Principles on the Use of Personal Data.

2.1.1 *Personal Data must be processed fairly and lawfully.* Personal Data to be processed should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards and in accordance with the consent of the Data Subject/s or other conditions of processing provided under the DPA.

Processing of Personal Data shall be in accordance with the conditions for processing of regular Personal information and Sensitive Personal Information as provided in the DPA.

2.1.2 *Quality of Personal Data.* Personal Data processed by the Group must be accurate, relevant and, to the extent necessary, up to date. Personal Data that is inaccurate or incomplete shall be corrected, supplemented, and/or erased by the Group, in accordance with the appropriate request procedure as provided in Par. XII Sec. 3 of this Manual.

2.1.3 *Adequacy of Processing.* Processing of Personal Data must be adequate and not excessive in relation to the purposes for which they are collected and processed. The Group must ensure that processing is conducted in a manner compatible with declared, specified, and legitimate purpose.

2.1.4 *Rights of Data Subjects.* In processing Personal Data, the Group shall uphold the rights of the Data Subject, provide the Data Subject with sufficient information about the nature and extent of processing and allow the Data Subject to exercise his or her rights at all stages of processing. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.

2.2 **Government-Mandated Use.** The Group may use and process the Personal Data in compliance with government regulatory requirements, company disclosures, and reportorial requirements, and pursuant to a lawful order of any court or tribunal. In such instances, the Group shall ensure that the any disclosure or sharing of Personal Data with government agencies and regulators are supported by and pursuant to relevant statutory or regulatory requirements and are covered by sufficient safeguards.

2.3 **Notification on Use of Personal Data for Marketing and Profiling.** A Data Subject must be notified before entry of his/her Personal Data into the Group's Data Processing Systems whenever such Personal Data shall be used for direct marketing, profiling, or historical or scientific purpose/s. Notification shall be made through electronic mail to the address of the Data Subject found in the Group records. Use of personal data for future marketing and profiling should be indicated in the consent statement prior to the collection of personal data.

### Sec. 3. Storage, Retention and Disposal

Personal Data should only be stored for as long as necessary to carry out an aspect or specific purpose of the business operations the Group. The guidelines for the storage, retention and disposal of Personal Data collected and processed by the Group shall be as specified in the Group's Document Classification and Management Policy.

**3.1 Storage.** Personal Data of Data Subjects shall be stored in the Group's manual, automated and electronic Data Processing Systems, such as but not limited to, password-protected computer devices, secure filing cabinets, secure filing rooms. Where necessary to further its business and to keep its security software tools up to date, the Company shall regularly review, upgrade and test its Data Processing Systems.

**3.2 Retention.** Personal data collected but are no longer processed shall only be retained for a reasonable period, provided such period is supported by proper justification. The purpose/s for which it was collected and processed, as well as the applicable periods prescribed by law, if any, shall be considered in retaining the Personal Data. This is applicable to both physical and electronic files.

3.2.1 Retention of personal data shall only for as long as necessary:

- i. for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- ii. for the establishment, exercise or defense of legal claims; or
- i. for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

3.2.2 Retention of personal data shall be allowed in cases provided by law.

3.2.3 Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the DPA in order to safeguard the rights and freedoms of the data subject.

3.2.4 Personal data which is 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.

3.2.5 Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

3.2.6 The Group shall, as far as practicable, conduct a periodic inventory of all physical and electronic files to ensure that documents are kept in accordance with the applicable retention period and that only relevant information are retained.

**3.3 Disposal of Personal Data.** All physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure means that would prevent further processing,

unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects. The method of disposal and/or destruction should render the Personal Data unreadable and irretrievable and prevent the occurrence of any Personal Data Breach and other Security Incidents.

#### **Sec. 4. Access**

- 4.1 Confidentiality.** At every stage of the Data Processing Systems employed by the Group, and even after the termination of the relation of the Data Subject with the Group, the Group, its employees, particularly its Authorized Personnel, and its PIP/s shall maintain the confidentiality and secrecy of the Personal Data that come to their knowledge and possession.
- 4.2 Access.** In accessing and processing Personal Data, all Authorized Personnel and PIP/s, as well as employees who request to access Personal Data of Data Subjects are enjoined to comply with this Manual. Anyone with access to Personal Data shall only process the same in accordance with the purpose of the Processing, and may not share, disclose, or distribute the Personal Data unless instructed by the Group, and with the consent of the Data Subject.

#### **Section 5. Disclosure and Sharing**

- 5.1 Permitted Disclosure.** All employees, consultants and PIPs of the Group shall maintain the confidentiality and secrecy of all Personal Data that come to their knowledge and possession, even after resignation, separation, termination of contract, or other contractual relations. Personal Data under the custody of the Group shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.
- 5.2 Outsourcing or Subcontracting of Processing of Personal Data.** In cases where the processing of Personal Data has been outsourced to or is performed by a third party, the Group shall ensure that the appropriate outsourcing agreements and contracts with vendors or third-party processors acting as a Personal Information Processor, is executed and includes the mandatory provisions required by the DPA and its IRR. Any outsourcing or subcontracting agreement or contract shall substantially contain the standard clauses prescribed in Annex "C" or which shall substantially be in the form prescribed in Annex "C-1".
- 5.3 Data Sharing.** In cases where the Group, acting as a Personal Information Controller, has agreed to disclose and share Personal Data under its custody and control to any approved third party acting as a Personal Information Controller, shall comply with the requirements stated in the DPA, its IRR, and the related issuances of the NPC and is covered by the appropriate Data Sharing Agreement which shall substantially contain the terms and conditions prescribed in Annex "D", or which shall substantially be in the form prescribed in Annex "D-1".

### **ARTICLE IV SECURITY MEASURES**



These Security Measures aim to maintain the availability, integrity and confidentiality of Personal Data and protect them from the accidental loss or destruction, unlawful access to, fraudulent misuse, unlawful destruction, alteration, and contamination of Personal Data.

## **Sec. 1. Organizational Security Measures**

- 1.1 Privacy Impact Assessment.** The Group shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data in accordance with the DPA and applicable issuances of the NPC. To the extent possible a PIA shall be conducted before the implementation of any activity, project or system. The Privacy Impact Assessment Questionnaire is provided in Annex "E".
- 1.2 Primary responsibility lies with PIC and PIP.** The responsibility for complying with the DPA, its IRR, issuances by the Commission, and all other applicable laws lies with the Group and its PIPs. The Group shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party, as provided in the preceding article on the outsourcing or subcontracting of processing of Personal Data and data sharing.
- 1.3 Key Personnel.** The Group has designated a Data Protection Officer ("DPO") and Compliance Officers for Privacy ("COP") for each subsidiary and relevant business unit who may be contacted via e-mail as provided for in Annex "F" and shall constitute a Breach Response Team in accordance with Article V, Section 1 hereof.
  - 1.3.1 Compliance Officer for Privacy.** Each subsidiary, and relevant division, department, and/or business unit of the Group may appoint among its ranks a Compliance Officer for Privacy or COP, who shall assist the DPO in ensuring that the subsidiary, department, and/or business unit assigned to him/her complies with the Privacy Laws, and this Manual.
  - 1.3.2 Functions of the DPO and COPs.** The DPO and COPs shall be responsible for overseeing the compliance of the Group with the Privacy Laws, and this Manual, including the conduct of the Privacy Impact Assessment, implementation of security measures, security incident and breach protocol, and the inquiry and complaints procedure.
- 1.4 Continuing Education on Data Privacy.** All Employees of the Group shall be required to undergo training on data privacy upon employment and shall participate in periodic refresher training sessions as necessary. The Group shall hold mandatory trainings on privacy and data protection at least once a year or as often as may be necessary. Intra-office memoranda shall be distributed to inform employees of the most current government issuances on data privacy, as well as of any update of this Manual.
- 1.5 Duty of Confidentiality.** All employees will be asked to sign a Confidentiality/Non-Disclosure Agreement, if not expressly stated in their employment contract with the Group. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

The Confidentiality/Non-Disclosure/Non-Compete/Proprietary Information Agreement, substantially in the same form as provided in Annex "G" hereof, may be executed by the Group to protect confidential information and/or Personal Data given to an employee or any other party.

- 1.6 Breach Reporting.** All employees and agents of the Group involved in the processing of Personal Data are tasked with regularly monitoring for signs of security incidents or a potential data breach. In case of doubt as to whether an incident is a Security Incident or a Data Breach, report the incident as soon as possible.
- 1.7 Company Records.** Adequate records of the Group's Personal Data Processing activities, projects and processing systems shall be maintained and kept up to date. These records shall include, at the minimum, general information about the Data Processing Systems of the Group. The Group shall maintain an inventory of the Data Processing Systems used and the Personal Data and method of processing involved.

The Group, through its Authorized and key personnel, shall maintain Data Privacy Trackers, which shall contain a log of all privacy-related incident/s, complaint/s and/or request/s from Data Subjects, access request/s, as well as a list of all Personal Data Sharing Agreements and Outsourcing Agreements entered into by the Group. The Data Privacy Tracker shall substantially be in the form prescribed in Annex "H".

- 1.8 Review of Data Privacy Manual.** This Manual shall be reviewed and evaluated periodically. Privacy and security policies and practices within the Company shall be updated to remain consistent with current data privacy best practices.

## **Section 2. Physical Security Measures**

- 2.1 Format of Data.** Personal Data in the custody of the Group may be in digital/electronic format and paper-based/physical format.
- 2.2 Storage Type and Location.** All Personal Data being processed by the Group shall be stored in a secure facility or location, whether virtual or physical. Papers or physical documents bearing Personal Data shall be stored in locked filing cabinets, access keys to which shall be entrusted only to Authorized Personnel. Digital or electronic documents containing Personal Data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes. Security considerations shall be based on the criticality of documents determined under the Group's Document Classification Matrix.
- 2.3 Access and Security Clearances.** Due to the sensitive and confidential nature of Personal Data being handled by the Group, only the Group's Authorized Personnel and PIP/s contracted by the Group shall be allowed to access and process the Personal Data of the Group. Rules regarding such access shall be provided for in the Access matrix/policy of the Group.
- 2.4 Office Spaces and/or Workstations.** Workstations and computers shall be positioned with considerable spaces between them to maintain the privacy and protect the processing of

## Personal Data.

2.4.1 *Clean Desk Policy.* Employees are required to lock their screens or put their computers in sleep mode upon leaving their workstations. All confidential papers and other records or files containing personal data must be kept secured when not in use by authorized personnel and are not allowed to be left on desks or any other area in plain sight.

2.5 **Maintenance of Confidentiality.** To the extent possible, each department or business unit shall clearly identify individuals who will handle and process Personal Data and define the duties, responsibilities, and schedule of individuals involved in the processing of Personal Data to ensure that only such individuals are granted access to such Personal Data.

2.5.1 Employees involved in processing Personal Data shall maintain the confidentiality of electronic and physical data and/or files at every stage of the collection, handling and processing of data.

2.5.2 Employees, whether Authorized Personnel or not, shall not be allowed to bring, connect, and/or use their personal gadgets or storage devices of any form when processing Personal Data.

2.6 **Modes of Transfer of Personal Data within the Company or to Other Parties.** Transfer of Personal Data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. To the extent possible, facsimile technology shall not be used for transmitting documents containing Personal Data.

The Information Security Officer shall ensure that employee emails and data are encrypted whenever portable media, such as disks or USB drives, to store or transfer personal data, are used, while laptops used to store personal data must utilize full disk encryption.

2.7 **Retention and Disposal Procedure.** The Group shall retain Personal Data in its custody following the retention periods indicated in the Group's retention policy.

## Sec. 3. Technical Security Measures

The Group shall implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access, in accordance with the relevant provisions of the DPA and its IRR, NPC Circular No. 16-01, and related issuances of the NPC.

3.1 **Monitoring for Security Breaches.** The Group shall cause the monitoring of access to Personal Data so as to minimize the risk of Personal Data Breach and other Security Incident/s. For this purpose, the Group shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

- 3.2 **Security Features of Software/s and Application/s Used.** To ensure compatibility and data security, the Group shall first ensure that the software applications have been reviewed and evaluated before the installation and utilization thereof in the Group computers and devices.
- 3.2.1 The Group shall procure and install an antivirus software for all Group devices where Personal Data are stored, including tablets and smartphones, that regularly access the Internet. The Information Security Officer shall ensure that the antivirus software is updated, and a system check is done periodically.
- 3.2.2 The Group shall use web application firewall to protect its servers and databases from malicious online attacks.
- 3.3 **Regular Assessment and Evaluation of Security Measures.** The Group shall regularly review security policies and perform periodic penetration testing of the firewall appliance from outside the Group's premises and from within to conduct vulnerability assessment and test the effectiveness of the same.
- 3.4 **Encryption, Authentication, and Other Technical Security Measures.** Each employee with access to Personal Data shall verify his/her identity using a secure encrypted link and multi-level authentication. Passwords or passcodes used to access Personal Data should be of sufficient strength to deter password attacks. Computers, portable disks, and other devices used by the Group and its PIP/s in Processing Personal Data shall be encrypted with the most appropriate encryption standard in accordance with the recommended standard by the NPC.
- 3.5 **Other Technical Security Measures.** The Group shall employ such other technical Security Measures as may be available and necessary to keep its software security tools up to date.

## ARTICLE V PERSONAL DATA BREACH AND SECURITY INCIDENTS

The detailed procedure for breach response, reporting and documentation are specified in the Group's Data Breach and Security Incident Management Policy.

### Sec. 1. Data Privacy Breach Response Team

A Data Privacy Breach Response Team, consisting of key officers of the Group, the DPO and COPs of the Group, shall be constituted, and shall be responsible for ensuring immediate action in the event of a Personal Data Breach.

The Breach Response Team shall be composed of the following:

1. Representative from the Human Resources Department

2. Representative from the Information Technology Department
3. Representative from the Legal and Compliance Department
4. Representative from the Investor Relations
5. Chief Operating Officer
6. The Data Protection Officer ("DPO")
7. The Compliance Officers for Privacy ("COP") from the relevant entity or Business Unit where the security incident or breach occurred.
8. The President and CFO/CIO/CRO shall be de facto members of the BRT for necessary approvals for recommended actions.

## **Sec. 2. Duties of the Breach Response Team**

The Breach Response Team shall be responsible for:

- a. Assessing and evaluating security incidents and possible data breaches;
- b. Managing the restoration of integrity to the information and communications system
- c. Investigating reported personal data breaches;
- d. Mitigating and remedying any resulting damage;
- e. Recommend and implement immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system; and
- f. Complying with reporting requirements.

## **Sec. 3. Measures to Prevent Security Incidents and Personal Data Breach**

To minimize, if not prevent, the occurrence of breach and security incidents, the Group shall implement organizational, physical and technical measures, such as, but not limited to, the following:

- a. Regularly conduct a PIA to identify risks in the processing of personal data. It shall take into account the size and sensitivity of the personal data being processed, and impact and likely harm of a personal data breach;
- b. Regular monitoring of security breaches and vulnerability scanning of computer networks;
- c. Capacity building of the Group's employees to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents;
- d. Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;
- e. Implementation of appropriate security measures that protect the availability, integrity and confidentiality of personal data being processed, such as, but not limited to, the following:
  - i. Implementation of back-up solutions;
  - ii. Access control and secure log files;
  - iii. Encryption;

- iv. Data disposal and return of assets policy.
- f. Periodic review of policies and procedures being implemented by the Club, including the testing, assessment, and evaluation of the effectiveness of the security measures.

#### **Sec. 4. Procedure for Recovery and Restoration of Personal Data**

The Group shall always maintain a backup file for all Personal Data under its custody. In the event of a Security Incident or Personal Data Breach, the Group shall compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the Security Incident or Personal Data Breach.

#### **Sec. 5. Response and Notification Protocol for Security Incidents and Data Breach**

- 5.1 Reporting of Security Incidents and Possible Data Breach.** All employees are required to monitor and report any suspected security incident to their respective COP and/or directly to the DPO immediately upon knowledge thereof. Upon receipt of an initial Security Incident Report to be accomplished by the reporting employee or party, the DPO shall convene the BRT to review/evaluate the report submitted and determine if there is a valid personal breach covered by the mandatory breach notification requirement. If no personal data is involved, the incident shall be included in the Annual Security Incident Report for submission to NPC.
- 5.2 Mandatory Notification of the Data Breach.** Upon knowledge of, or reasonable belief that a Data Breach has occurred, the Breach Response Team shall inform and seek the approval of the Group's management. The DPO shall notify the Commission and the affected Data Subjects of the occurrence of the Data Breach within seventy-two (72) hours from knowledge of the breach. If a Personal Data Breach occurred, the DPO may immediately halt the affected process.

#### **Sec. 6. Documentation and Reporting Procedure for Security Incidents and Personal Data Breach**

The Breach Response Team shall prepare detailed documentation of every incident or breach encountered by the Group, as well as an annual report, to be submitted to management and the NPC, within the prescribed period. All security incidents and personal data breaches, including those not covered by the mandatory notification requirement, shall be documented through written reports. Any or all reports shall be made available when requested by the NPC.

- 6.1 Documentation of Personal Data Breaches.** Upon the completion of the investigation and post incident review of the incident or breach, the Breach Response Team or the relevant personal information processor (in case the breach occurred during processing by the third-party processor), shall prepare the Personal Data Breach Report for both reportable and non-reportable data breaches.
- 6.2 Annual Security Incident Report.** The Annual Security Incident Report must be submitted to the Commission annually before the end of the first quarter of every year (i.e., every end of March of each year) covering all the security incidents that occurred from the previous year. The Annual Security Incident Report shall contain aggregated data or general information including the number of incidents (including malicious code, software and hardware failure, hacking, logical infiltration, and hardware maintenance error) and breach encountered,

classified according to their impact on the availability, integrity, or confidentiality of personal data and shall be in the form provided by the Commission.

## **ARTICLE VI RIGHTS OF DATA SUBJECTS**

Data Subjects have the right to control the use and Processing of his/her Personal Data, which the Group's employees and PIP/s shall respect and take into consideration in the performance of all types of Processing activities.

### **Sec. 1. Right to be Informed**

The Data Subject has the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed. Before the entry of his/her Personal Data into the Group's Data Processing Systems, or at the next practicable opportunity, the Data Subject must be notified and furnished with the following information:

- a. A description of the Personal Data to be collected and processed;
- b. The purpose/s for which Personal Data are being or will be processed;
- c. The basis of Processing, in case Processing is not based on the Consent of the Data Subject;
- d. The scope and method of the Processing of Personal Data;
- e. The recipient/s or classes of recipient/s to whom the Personal Data are or may be disclosed or shared; in case of automated access, and where allowed by the Data Subject, the methods utilized therefor, 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;
- f. The identity and contact details of the Company, its representative, and/or, upon request, the DPO and/or COP/s, if any;
- g. The period for which the Personal Data will be stored; and
- h. The existence of his/her rights as a Data Subject, including the right to lodge a complaint before the Commission.

### **Sec. 2. Right to Reasonable Access**

The Data Subject has the right to gain reasonable access to the following:

- a. Contents of his/her Personal Data that were processed;
- b. Sources from which Personal Data were obtained;
- c. Names and addresses of recipient/s of the Personal Data;
- d. The manner by which his/her Personal Data were processed;
- e. Reasons for the disclosure of the Personal Data to recipient/s, if any;
- f. 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;
- g. Date when Personal Data concerning the Data Subject were last accessed and modified; and
- h. Identity and address of the Group.

### **Sec. 3. Right to Object**

The Data Subject shall have the right to object to the Processing of his/her Personal Data. The Data Subject shall also be notified and given an opportunity to object and withhold his/her consent to the Processing of his/her Personal Data in case of changes or any amendment to the information supplied or declared to the Data Subject prior to or in relation to the Processing. When a Data Subject objects or withholds consent, the Group shall no longer Process the Personal Data, unless:

- a. the Personal Data is needed pursuant to a subpoena;
- b. 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 Group and the Data Subject (e.g., to assess the qualification of an applicant or the suitability of a current employee for promotion or transfer, the Company may require information as regards the person's educational attainment); or
- c. the Personal Data is being collected and processed pursuant to a legal obligation (e.g., to make the mandatory contributions to an employee's Social Security System, Pag-Ibig Home Development Mutual Fund, and PhilHealth accounts, the Company has to obtain the pertinent social security numbers of the employee).

### **Sec. 4. Right to Correction**

The Data Subject has the right to dispute any inaccuracy or error in his/her Personal Data, and have the Group correct or cause the correction thereof, unless the request is vexatious or unreasonable. If the Personal Data has been corrected, the Group 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 recipient/s thereof. 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.

### **Sec. 5. Right to Erasure or Blocking**

The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his/her Personal Data from the Group's Data Processing Systems and may exercise such right, upon discovery and/or substantial proof of any of the following:

- a. Personal Data collected and/or being processed is incomplete, outdated, false, or unlawfully obtained;
- b. Personal Data is being used for purpose/s not authorized by the Data Subject;
- c. Personal Data is no longer necessary for the purpose/s for which they were collected;
- d. The Data Subject has withdrawn his/her consent or objects to the Processing, and there is no other legal ground or overriding legitimate interest for the Processing;
- e. Personal Data concerns information prejudicial to the Data Subject, unless justified by the freedom of speech, of expression, or of the press, or otherwise authorized;
- f. The Processing is unlawful; or
- g. The Right/s of the Data Subjects has/have been violated.



Upon reasonable request of the Data Subject, the Group shall notify third parties who have previously received such processed Personal Data of the Data Subject's decision to exercise such right.

#### **Sec. 6. Right to Data Portability**

Where Personal Data is processed by electronic means, the Data Subject has the right to obtain from the Group a copy of such Personal Data in an electronic or structured format that is commonly used and allows for further use by the Data Subject. This right may be exercised upon a reasonable request by the Data Subject.

#### **Sec. 7. Right to File a Complaint**

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

#### **Sec. 8. Right to Damages**

The Data Subject has the right to be indemnified for any damages sustained due to the inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, as may be imposed by the courts in a relevant proceeding accordance with the DPA.

#### **Sec. 9. Transmissibility Of Rights**

Any lawful heir and/or assign of the Data Subject may invoke the Rights of the Data Subject to which he/ she is an heir and/or assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her right. Such right may be exercised subject to proper verification of authority of the heir or assign.

### **ARTICLE VII NOTIFICATIONS, REQUESTS, INQUIRIES AND COMPLAINTS**

The exercise of the Data Subject's rights as discussed in the preceding Article VI shall be subject to reasonable procedures and guidelines that may be imposed by the relevant business unit, department, or entity within the Group. Data Subjects may also inquire or request information regarding any matter relating to the Processing of his or her Personal Data under the custody of the Group, including the data privacy and security policies implemented to ensure the protection of their Personal Data.

#### **Sec. 1. Requests And Inquiries Pertaining to Data Privacy Issues**

To exercise his or her rights, the Data Subject may accomplish the Data Privacy Request Form prescribed in Annex "J" indicating therein the right he/she wishes to exercise with respect to his/her Personal Data and transmit the same to the Group through its Authorized Personnel, the COP of the relevant business unit, department or entity or DPO.

The following procedure shall apply for the exercise of the Data Subject's rights:

1. The Data Subject who seeks to access to and/or seeks to modify his/her Personal Data with the Group shall accomplish the Data Privacy Request Form and file the same with the Authorized Personnel and previously dealt with by the Data Subject as processor of his/her Personal Data or the COP for the subsidiary, division or relevant business unit or department concerned, or in the COP's absence, the head of subsidiary, division or business unit or department.
2. The COP for the subsidiary, division or relevant business unit or department concerned, or in the COP's absence, the head of subsidiary, division or business unit or department, shall determine the reasonableness of the exercise of the right. If found reasonable, the COP, the head of subsidiary, division or business unit or department shall approve and transmit the same to the subsidiary, division, business unit, or department concerned for implementation.
3. In case of doubt on the propriety of the exercise of right and/or access request, as the case may be, the COP, if any, or the head of the subsidiary, division or business unit, or department concerned shall consult and/or seek assistance or advice from the DPO and/or the approval of the Chief Legal Officer of the Group.

## **Sec. 2. Procedure For Complaints**

The procedure to be observed in case of complaints for data privacy violation shall be as follows:

- a. Should a Data Subject file a complaint for violation of his or her rights under the DPA relative to the Processing of their Personal Data under the custody of the Group, including the data privacy and security policies implemented to ensure the protection of their personal data, the complaint shall be filed in three (3) printed copies, or sent to the relevant dedicated email address of the COP for the relevant business unit, department or entity or to **dpo@shakeys.biz**. The concerned department or unit shall confirm with the complainant its receipt of the complaint.
- b. Upon receipt of the complaint, the COP shall:
  - i. verify the allegations of the complaint;
  - ii. if warranted, conduct an initial investigation in case of serious security breach as provided under the Data Privacy Act and its IRR; and
  - iii. report the Security Incident or Personal Data Breach to the Commission following the procedure laid down in Article VI, Section 6 of this Manual.
- c. When the complaint violation is serious or causes or has the potential to cause material damage to the Group or any of its Data Subjects, the Breach Response Team may also be convened as an investigation committee to recommend actions to address the complaint. Such recommendation shall be submitted to the management of the Group for approval.

## **ARTICLE VIII EFFECTIVITY**

The provisions of this Manual are effective this 01<sup>st</sup> day of January 2024, until revoked or amended by the Group, through a Board Resolution.

## ANNEXES

### Annex A. Data Privacy Notice and Consent Form

In the course of determining whether to hire you for employment purposes, [insert name of entity] will collect and process Personal Data relating to you and, if applicable, your relatives. These Personal Data include information for [insert purposes for collection and processing of personal information]. Collection of Personal Data shall be made thru various channels such as [insert means and methods for collecting personal information].

By signing this consent form, you provide consent to [insert name of entity] to:

1. Collect and process your Personal Data, as provided under applicable laws, regulations, and [insert name of entity]'s policies, for its and its affiliates' and partners' [insert purposes];
2. Make your Personal Data available to [insert name of entity] affiliates and partners for them to process the Personal Data for their own benefit, for the same purposes as indicated above. A list of our affiliates and partners are available at [insert URL link, if any/applicable. If not, the list of recipients should be prepared in case requested by a Data Subject]; and
3. Make your Personal Data available, and to permit [insert name of entity]'s affiliates and partners also to make your Personal Data available:
  - a. To third parties who provide products or services to [insert name of entity] or its affiliates and partners for the same \_\_\_\_\_ purposes as described above; and
  - b. To other third parties, where required or permitted by law, including regulatory authorities, government agencies, as well as parties with whom you voluntarily transact.

[In case the signatory will provide Personal Data for third parties/contacts/relatives] You also confirm that, before providing us with the Personal Data of your relatives ("Your Contacts"), you have obtained their consent to: (i) you collecting their Personal Data; (ii) you sharing the same with [insert name of entity]; its affiliates and partners, and the third parties as indicated above; and (iii) to the processing (for purposes of \_\_\_\_\_) of their Personal Data by [insert name of entity] and its affiliates and partners indicated above as provided herein.

The Personal Data will be retained in [insert name of entity]'s records as part of its potential talent pool for a period of six (6) months, ("Personal Data Retention Period"). Unless retention for a longer period is required for reasonable cause, the disposition of Personal Data shall, upon the lapse of the Personal Data Retention Period, be effected by [insert name of entity] in accordance with applicable laws and regulations.

You and your contacts are entitled to certain rights in relation to the Personal Data that may be collected from you (and from your contacts), including the right to access, correction, and to object to the processing, as well as the right to lodge a complaint before the National Privacy Commission in case of violation of your or your contacts' rights as data subjects. You may consult the [insert name of entity]'s Data Protection Officer at [insert e-mail address and/or phone number, and business address] for any concerns regarding your Personal Data.

---

Name

Date

## Annex B. Privacy Notice

Shakey's Pizza Asia Ventures Inc. (SPAVI) operates the [shakeyspizza.com.ph](https://shakeyspizza.com.ph) (the "Site"). This Privacy Policy page informs you of our policies regarding the collection, use and disclosure of Personal Information that we receive from users of the Site.

We use your Personal Information only for providing and improving the Site. By using the Site, you agree to the collection and use of information in accordance with this policy.

### Information Collection and Use

While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you if you wish to provide feedback or make an inquiry. Personally identifiable information may include, but is not limited to your name, mailing address, email address and contact numbers.

### How We Collect Personal Information

We will primarily collect personal information you knowingly and voluntarily provide when you contact us to enable us to provide the service you requested, or indirectly from your interactions with us (such as by monitoring your use of our websites). In some cases, we may also need to collect personal Information about you from third parties (such as recruitment agencies and government agencies).

### Why We collect Personal Information

We collect only the Personal Information needed to effectively serve you and carry out our business operations. We may collect, use, and process your Personal Information for the following general purposes [these purposes may be limited or expanded depending on the actual activities of the relevant entity, brand or division]:

- to respond to your queries, complaints, and requests;
- to provide information about our services;
- to conduct research and analysis to improve customer experience;
- to maintain security; and
- to comply with legal, regulatory, and contractual requirements or obligations.

We may also use your Personal Information to contact you with reference to your feedbacks, answers to your inquiries, send you newsletters, marketing and/or promotional materials.

### Consent

Before processing your Personal Data, you will be required to provide your permission for our collection, use, and processing of your Personal Data, and confirm you have accepted the policies and practices described in this Privacy Notice. By clicking the tick box [in our contact form], you acknowledge that you have read, understood, and accept the terms and conditions of this Privacy Policy and that you consent to the collection and use of your Personal Information by us, for the

purposes stated in this Privacy Policy. [In case any Personal Data is transferred or shared to parties abroad, this may be added: You also consent to the disclosure and transfer of the Personal Information within and outside Philippines, solely in connection with these purposes.]

## Disclosures

We may share your personal information (which may sometimes include sensitive personal information) within our corporate group who require the information for the purposes in this notice. We may also engage the services of third parties to perform functions on our behalf that are consistent with this Privacy policy. Examples of these third parties include data analysts, customer support specialists, email vendors, web hosting companies and fulfilment companies (including companies that coordinate mailings) [Recipients or categories of recipients shall be included in this portion]. These third parties may be provided with access to or may process Personal Information needed to perform their functions but only upon our instructions. When it is necessary, we will enter into contractual undertakings to ensure that the Personal Information accessed by third parties is adequately protected to a standard comparable to the protection under applicable Data Privacy Laws.

If it may be necessary to disclose Personal Information to third parties in a different country, we will take steps to ensure that there is a lawful basis for the disclosure and that the disclosure complies with all applicable laws.

## Cookies

We use "cookies" on this site. A cookie is a piece of data stored on a site visitor's hard drive to help us improve your access to our site and identify repeat visitors to our site. Cookies can also enable us to track and target the interests of our visitors to enhance the experience on our site. Usage of a cookie is in no way linked to any personally identifiable information on our site.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.

## Log Data

We may also collect the log data your browser sends which may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.

## Security

The security of your Personal Information is important to us, but please note that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

## Storage and Retention

Any Personal Information we collect and use shall not be kept longer than is necessary for the fulfilment of the purposes stated in this Privacy Policy or to comply with our legal obligations. We

will delete Personal Information that is no longer required for business or legal purposes, as soon as reasonably possible and in accordance with the SPAVI's retention policy.

## Your Rights

You are entitled to certain rights in relation to the Personal Information that may be collected from you, including the right to access, request for correction or deletion, and to object to the processing, as well as the right to lodge a complaint before the National Privacy Commission in case of violation of your rights as data subjects. If you wish to access, correct or update any personal information that we hold about you, then you should contact our Data Privacy Officer as provided below.

It is important to us that all of the information we hold about you is correct and up-to-date, so let us know promptly if there are any errors or other changes should be made.

## Changes To This Privacy Policy

SPAVI reserves the right to update or change this Privacy Policy at any time without prior notification to the site users and visitors. You may want to check for changes to this policy periodically for any update. Your continued use of the Service after we post any modifications to the Privacy Policy on this page will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Privacy Policy.

We may also choose to place a prominent notice on the Site if material changes to this Privacy Policy is made.

## Contact Us

If you have any questions about this Privacy Policy, you may contact us by sending an email to the [dpo@shakeys.biz](mailto:dpo@shakeys.biz) *[the email address of the COP may also be indicated]*.

## Annex C. Standard Clauses for Outsourcing/Subcontracting

1. Whenever applicable, in performing its obligations under this contract, the [PROVIDER] shall, at all times, comply with the provisions of Republic Act No. 10173 or "the Data Privacy Act of 2012," its implementing rules and regulations, and all other laws and government issuances which are now or will be promulgated relating to data privacy and the protection of personal information. The [PROVIDER], its officers, employees, agents, and representatives, shall, among others:
  - a) Process personal data only upon the documented instructions of the [CLIENT/COMPANY], including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
  - b) Implement measures and systems such as clear written guidelines and training for its employees, agents, and representatives, that will enable data subjects or subscribers to exercise any and all of their rights under the Data Privacy Act of 2012;
  - c) Implement such measures and systems that will allow data subjects to exercise their right to object or withhold consent to further processing as provided under the Data Privacy Act of 2012;
  - d) Implement such measures and systems that will allow data subjects to exercise their right to access under the Data Privacy Act of 2012;
  - e) Maintain proper records, and provide the [CLIENT/COMPANY] access to such records, as will allow the [CLIENT/COMPANY] to comply with the exercise by data subjects of their right to access under the Data Privacy Act of 2012;
  - f) Ensure that data subjects will be able to exercise their right to rectification, modification, or blocking of data under the Data Privacy Act of 2012;
  - g) Determine the appropriate level of security measures, subject to, and in conjunction with, that of the [CLIENT/COMPANY], taking into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and cost of security implementation;
  - h) Implement security measures for data protection (i.e., generally, the physical, organization, and technical security measures prescribed by the Data Privacy Act and its implementing rules and regulations), including policies for evaluation, monitoring, and review of operations and security risks. These measures may include clear written guidelines, training modules for its employees, agents, and representatives, and audit measures in relation to the (1) collection, processing, maintenance, and deletion/disposal of personal data and records; and (2) the sharing of these information, especially on the specific persons to whom the information may be given access. Such measures shall aim to maintain the availability, integrity, and confidentiality of personal data, and prevent negligent, unlawful, or fraudulent processing, access, and other interference, use, disclosure, alteration, loss, and destruction of personal data;



- i) Implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing, or for such other purposes as may be required under the Data Privacy Act of 2012 or any other applicable law or regulation;
- j) Implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination;
- k) Ensure that its employees, agents, and representatives who are involved in the processing of personal information operate and hold personal information under strict confidentiality. This obligation shall continue even after their transfer to another position or upon termination of their employment or contractual relations;
- l) Not to engage another processor without prior the [CLIENT/COMPANY]: Provided, that any such arrangement shall ensure that the same obligations for data protection under this document are implemented, taking into account the nature of the processing;
- m) In case of data breach, promptly notify the [CLIENT/COMPANY] within twenty-four (24) hours or earlier from the time of discovery, to enable the [CLIENT/COMPANY] to notify the National Privacy Commission and the affected data subject within the period prescribed under the Data Privacy Act of 2012, when sensitive personal information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, the [CLIENT/COMPANY], the [PROVIDER], or the National Privacy Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject or subscriber;
- n) Document all occurrence of security incidents and personal data breaches and prepare Personal Data Breach Reports detailing the incidents surrounding each data breach, including facts surrounding the incident, the effects of such incident, and the remedial action taken by the [PROVIDER], as required by the NPC;
- o) Timely provide a copy of the Personal Data Breach Reports to the [CLIENT/COMPANY] through a secure channel and keep copies of the Personal Data Breach Reports in its premises for at least six (6) years, or unless otherwise directed by the NPC;
- p) Promptly inform [CLIENT/COMPANY] if, in its opinion, any instructions of the [CLIENT/COMPANY] violates, or may be construed to violate, any provision of the Data Privacy Act of 2012 or any other issuance of the National Privacy Commission;
- q) Assist THE [CLIENT/COMPANY] in ensuring compliance with the Data Privacy Act of 2012, its implementing rules and regulations, other relevant laws, and other issuances of the National Privacy Commission, taking into account the nature of processing and the information available to the [PROVIDER];

- r) At the choice of the [CLIENT/COMPANY], delete, destroy, or return all personal data to the former after the end of the provision of services relating to the processing: Provided, that this includes deleting or destroying existing copies unless storage is authorized by the Data Privacy Act of 2012 or another law;
  - s) Make available to the [CLIENT/COMPANY] all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act of 2012, and allow for and contribute to audits, including inspections, conducted by the [CLIENT/COMPANY] or another auditor mandated by the latter; and
  - t) Include all the foregoing in the privacy and security policy of the [PROVIDER].
2. The [CLIENT/COMPANY] shall have the right to test and monitor compliance by the [PROVIDER] with the aforementioned data privacy laws, administrative orders, and government issuances, and the provisions of this paragraph. The [PROVIDER] agrees to immediately correct or introduce improvements to its system should the results show failure by [THE PROVIDER] to comply with the requirements of this paragraph, without prejudice to other remedies available to the [CLIENT/COMPANY] under this Agreement.

## Annex C-1. Template for Outsourcing/Subcontracting Agreement

### OUTSOURCING/SUBCONTRACTING AGREEMENT

#### KNOW ALL MEN BY THESE PRESENTS:

This Outsourcing Agreement ("Agreement") is being executed by and between:

\_\_\_\_\_, a duly organized and registered corporation under the laws of the Philippines with principal office at \_\_\_\_\_, represented herein by its \_\_\_\_\_ and its \_\_\_\_\_, hereinafter referred to as "CLIENT",

-and-

\_\_\_\_\_, a duly organized and registered corporation under the laws of the Philippines with principal office at \_\_\_\_\_, represented herein by its \_\_\_\_\_, hereinafter referred to as "PROCESSOR".

(Hereinafter collectively referred to as the "PARTIES")

#### WITNESSETH: That -

**WHEREAS**, the CLIENT is engaged in the business of \_\_\_\_\_ and desires to collect and process the Personal Data of its \_\_\_\_\_ (the "Data Subjects") to \_\_\_\_\_ (the "Purpose"), and for such purpose, has to collect and process Personal Data.

**WHEREAS**, the PROCESSOR is engaged in the business of \_\_\_\_\_.

**WHEREAS**, the CLIENT desires to engage the services of PROCESSOR in the collection and processing of Personal Data of its Data Subjects.

**WHEREAS**, the PROCESSOR has accepted the offer of the CLIENT to collect and process the Personal Data of Data Subject for the declared Purpose; and

**WHEREAS**, the PARTIES have agreed to enter into this Agreement to provide the terms and conditions for the outsourcing of the collection and processing of the Personal Data of Data Subjects; NOW THEREFORE, and in consideration of the foregoing premises and mutual covenants hereinafter set forth, the PARTIES hereto have agreed and do hereby agree as follows:

#### 1. Purpose of the Agreement

The Purpose of this Agreement is \_\_\_\_\_.

#### 2. Term

The Term of this Agreement, and its subsequent renewals, if applicable, shall not exceed five (5) years. The same shall continue to be in effect unless terminated in writing by both PARTIES.

### **3. Personal Data**

- 3.1. Personal Data covered by Outsourcing – The Personal Data of Data Subjects covered by this Agreement are enumerated in detail in Annex “A” of this Agreement.
- 3.2. Control over Processing – CLIENT shall control the processing of the Personal Data of Data Subjects, pursuant to this Agreement, and for such purpose, shall give instructions to the PROCESSOR.
- 3.3. Further Outsourcing of Personal Data – It is only upon prior written instruction of CLIENT that the PROCESSOR may engage the services of another Processor, provided that that such engagement shall be covered by a duly executed Outsourcing Agreement.
- 3.4. Format of Personal Data – Personal Data processed by the Parties may be in digital/electronic format or physical format.
- 3.5. Personal Data Storage – The Personal Data processed by the Parties shall be stored in secure facilities, whether in digital/electronic format or physical format. Personal Data stored in computers or in any electronic storage facility shall be protected by passwords and/or encryption. On the other hand, Personal Data in physical format shall be stored in locked filing cabinets/drawers and/or vaults, the access keys or codes shall be entrusted to an authorized personnel/s.

### **4. Representations and Warranties of the CLIENT:**

The CLIENT represents, warrants, and undertakes that:

- (i) It has obtained the specific consent of the Data Subjects to the Outsourcing; and
- (ii) The Data Subjects have been provided the following information before the Personal Data is shared:
  - a. Identity of the personal information controllers or processors that will be given access to Personal Data;
  - b. Purpose of the Data Sharing;
  - c. Categories of Personal Data concerned;
  - d. Intended recipients or categories of recipients of the Personal Data;
  - e. Existence of their rights as data subjects, including the right to access and correction, and the right to object; and
  - f. Other information that would sufficiently notify the data subject of the nature and extent of the Data Sharing and the manner of processing.
- (iii) It shall not disclose the Personal Data to third parties without the written consent of the Data Subjects;
- (iv) It shall at all times comply with the requirements of the Data Privacy Act of 2012 and all other applicable data privacy laws and regulations and issuances of the National Privacy Commission (“Privacy Laws”);

- (v) It shall implement such measures and systems that will enable the Data Subjects to exercise their rights under the Privacy Laws, including without limitation the rights access, rectification, modification, blocking, and to object to the processing of data;
- (vi) It shall implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing;
- (vii) It shall ensure that its Representatives who are involved in the processing of personal information operate and hold personal information under strict confidentiality. This obligation shall continue even after their transfer to another position or upon termination of their employment or contractual relations; and
- (viii) Immediately inform the other party, through its Data Privacy Officer, within Twenty-Four (24) hours if, in its opinion, there is a security incident in relation to the Privacy Laws.

## **5. Representations and Warranties of the Processor**

The PROCESSOR represents, warrants, and undertakes that:

- (i) process the Personal Data only upon the documented instructions of the CLIENT, including transfers of Personal Data to another country or an international organization, unless such transfer is authorized by law;
- (ii) ensure that an obligation of confidentiality is imposed on its authorized personnel and other persons authorized to process the Personal Data;
- (iii) implement appropriate security measures and comply with the Privacy Laws;
- (iv) not engage another processor without prior written approval from CLIENT: 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;
- (v) assist the CLIENT, 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;
- (vi) assist the CLIENT in ensuring compliance with the Privacy Laws, regulations, and relevant government issuances, taking into account the nature of Processing and the information available to the PROCESSOR;
- (vii) at the choice of CLIENT, delete or return all Personal Data to CLIENT after the end of the term or provision of services relating to the Processing: Provided, that this includes deleting existing copies unless storage is authorized by law;
- (viii) make available to CLIENT all information necessary to demonstrate compliance with the obligations laid down in Privacy Laws, and allow for and contribute to audits, including inspections, conducted by CLIENT or an auditor mandated by the latter; and
- (ix) immediately inform CLIENT if, in its opinion, an instruction infringes data privacy laws, regulations, and relevant government issuances.

## **6. Confidentiality**

The Parties shall treat the Personal Data processed pursuant to this Agreement with utmost confidentiality. Further, the Parties shall ensure that their respective personnel, agents and/or representatives, as well as PIP/s, if any, engaged in the Processing of Personal Data under this Agreement, understand and are fully informed of the confidential nature of the Personal Data

being processed, and that their obligation to keep the same in confidence survives the termination of their engagement, employment, and/or any relationship with either Party.

## **7. Data Subjects Access to the Agreement**

Data Subjects have the right to obtain a copy of this Agreement and the (any related documents/renewal of agreement, etc.). The Data Subjects also have the right to access, update or correct certain Personal Data, or withdraw consent to the use of any of their Personal Data, provided that they must first submit a formal request to any of the PARTIES. Likewise, all requests must be communicated to the other party first before any changes be made and applied.

## **8. Data Subject Requests and Complaints**

In the event of any complaints or requests for data or information on this Agreement and the Personal Data, whoever receives any complaints or requests first shall be responsible for addressing such complaints or requests. Complaints or requests shall be referred to the respective Data Privacy Officer of the company to which the complaints or requests were first received, provided that the Data Privacy Officer of the company who first received the complaint shall inform his/her counterpart from the other company, within twenty-four (24) hours from notice or receipt of the complaint, that they it has received such notice or complaint. The contact details of the respective Data Privacy Officer are as follows:

For the CLIENT:

Company:  
Registered Address:  
E-mail:

For the PROCESSOR:

Company:  
Registered Address:  
E-mail:

## **9. Breach Management**

Within twenty-four (24) hours from discovery of a security breach or in case of receipt of complaint from a Data Subject, the Data Privacy Officer of the company who discovered such security breach or who has received the Data Subject's complaint must inform his/her counterpart from the other company of such fact. Should such form of breach or complaint be reportable to the National Privacy Commission ("NPC"), both Parties shall notify the NPC and the concerned data subjects within seventy-two (72) hours pursuant to NPC Circular No. 16-03.

## **10. Retention of Personal Data**

The Retention of Personal Data of Data Subjects by the PROCESSOR shall be coterminous to the term of this Agreement, unless a written agreement for an extension is executed by the PARTIES and/or as needed in accordance to a lawful order by a government agency.

## 11. Return, Destruction, or Disposal of Personal Data

All shared Personal Data, at the option of the CLIENT, shall be returned to the CLIENT after the termination of the Agreement. The Destruction or Disposal of Personal Data of Data Subjects shall be covered by the policy of Party who has in their possession any documents, whether physical or digital, containing Personal Data.

## 12. Indemnification

The defaulting party shall indemnify the aggrieved party all losses and expenses arising out of the following:

- a) Complaint brought by a Data Subject or the Aggrieved Party;
- b) Breach of Obligations in this Agreement; and/or
- c) Defaulting Party's willful misconduct and gross negligence.

## 13. General Terms

- a) This Agreement may be amended, modified, superseded or cancelled only in writing by the PARTIES.
- b) The rights and obligations of the PARTIES under this Agreement shall not be assigned to any person without the prior written consent of the other party.
- c) No delay, failure, refusal or neglect of a party to exercise any right or power under this Agreement or to insist upon full compliance by the other party of its obligations under this Agreement shall constitute a waiver of any provision of this Agreement or the further exercise of any of its rights herein. Any waiver expressly granted by a party must be in writing.
- d) Should any provision of this Agreement be declared null, void or unenforceable by any competent government agency or court, this shall not affect the other provisions of this Agreement which are capable of severance and which will continue unaffected. The PARTIES agree that any provision declared null, void or unenforceable by any competent government agency or court shall be replaced with valid or enforceable provisions as closely aligned with the original intention of the PARTIES.
- e) The laws of the Philippines shall govern and apply to any matter involving the interpretation, construction or performance of any provision of this Agreement. In case of suit arising from or in connection with the interpretation, implementation or enforcement of this Agreement, the parties agree to submit to the jurisdiction of the proper court of Pasig City, Philippines, to the exclusion of all other courts.
- f) All notices and communications relating to this Agreement shall be sent to the registered address stated in Clause No. 6.

IN WITNESS WHEREOF, the parties have set their hands on this Agreement on the respective dates and place stated in their respective Acknowledgements.

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

Signed in the presence of:

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

### ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)

) S.S.

BEFORE ME, a Notary Public for and in \_\_\_\_\_, this \_\_\_\_\_  
day of \_\_\_\_\_ 20\_\_ at \_\_\_\_\_, Philippines, personally  
appeared the following persons and exhibiting to me:

Name

Competent Evidence  
Issued of Identity

Date/Place

known to me and to me known to be the same persons who executed the foregoing  
**Outsourcing Agreement**, including the Annexes thereto, and they acknowledged the same  
to be their free and voluntary act and deed and that of their respective principals.

IN WITNESS WHEREOF, I have hereunto set my hand and seal on the date and at  
the place first above written.

Doc. No.: \_\_\_\_\_;

Page No.: \_\_\_\_\_;

Book No.: \_\_\_\_\_;

Series of 20\_\_.



## Annex D - Standard Clauses for Data Sharing

### 1. Representations and Warranties of [entity sharing the personal data]

[Entity sharing the personal data] represents, warrants, and undertakes that:

- (i) It has obtained the specific consent of the data subjects to the Data Sharing; and
- (ii) The data subjects have been provided the following information before the data is shared:
  - a. Identity of the personal information controllers or processors that will be given access to personal data;
  - b. Purpose of the data sharing;
  - c. Categories of personal data concerned;
  - d. Intended recipients or categories of recipients of the personal data;
  - e. Existence of their rights as data subjects, including the right to access and correction, and the right to object; and
  - f. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

### 2. Representations and Warranties of [entity receiving the personal data]

[Entity receiving the personal data] represents, warrants and undertakes that:

- (i) It shall at all times comply with the requirements of the Data Privacy Act of 2012 (DPA, for brevity) and all other applicable data privacy laws and regulations;
- (ii) It shall implement such measures and systems that will enable data subjects to exercise their rights under the DPA, including without limitation the rights access, rectification, modification, blocking, and to object to the processing of data;
- (iii) It shall implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing; and
- (iv) It shall ensure that its employees, agents, and representatives who are involved in the processing of personal information operate and hold personal information under strict confidentiality. This obligation shall continue even after their transfer to another position or upon termination of their employment or contractual relations.

## Annex D-1 Template for Data Sharing Agreement

### DATA SHARING AGREEMENT

#### KNOW ALL MEN BY THESE PRESENTS:

This Data Sharing Agreement ("Agreement") this \_\_\_\_ day of \_\_\_\_\_, 202x at \_\_\_\_\_, is being executed by and between:

\_\_\_\_\_, a duly organized and registered corporation under the laws of the Philippines with principal office at \_\_\_\_\_, represented herein by its \_\_\_\_\_ and its \_\_\_\_\_, hereinafter referred to as "\_\_\_\_\_",

-and-

\_\_\_\_\_, a duly organized and registered corporation under the laws of the Philippines with principal office at \_\_\_\_\_, represented herein by its \_\_\_\_\_, hereinafter referred to as "\_\_\_\_\_".

(Hereinafter collectively referred to as the "PARTIES")

#### WITNESSETH: That -

WHEREAS, the PARTIES have entered into a \_\_\_\_\_ (the "Contract"), which is attached herewith as Annex "A", executed on \_\_\_\_\_ for the purpose of \_\_\_\_\_.

WHEREAS, the PARTIES, in order to complete the purpose of the Contract, are required to share Personal Data of \_\_\_\_\_ ("Data Subjects") through the submission of \_\_\_\_\_, and other documents ("Personal Data").

WHEREAS, the PARTIES deemed it necessary to share with each other the Personal Data of \_\_\_\_\_, pursuant to the Contract; and

WHEREAS, the PARTIES have agreed to enter into this Agreement to provide the terms and conditions for the sharing and processing of the Personal Data;

NOW THEREFORE, and in consideration of the foregoing premises and mutual covenants hereinafter set forth, the PARTIES hereto have agreed and do hereby agree as follows:

#### Section 1. Purpose of Data Sharing

- 1.1 The Parties are entering into this Agreement, and [Personal Information Controller A] is granting [Personal Information Controller B] access to the personal data described under Section 2 hereof for the following purposes:

- a. *[Main Purpose]*
  - b. *[Public Function, Public Service or Business Activity the performance of which the agreement is meant to facilitate]*
  - c. *[If the purpose includes the grant of online access to personal data, or if access is open to the public or private entities, these shall also be clearly specified herein.]*
- 1.2 *[Personal Information Controller B]*, on the other hand, is granting *[Personal Information Controller A]* access to the personal data described under Section 2 hereof for the following purposes.

- a. *[Main Purpose]*
- b. *[Public Function, Public Service or Business Activity the performance of which the agreement is meant to facilitate]*

*[If the purpose includes the grant of online access to personal data, or if access is open to the public or private entities, these shall also be clearly specified herein.]*

## **Section 2. Personal Data to be Shared**

*[Type of personal data to be shared under the agreement for every party]*

*[Categories of personal data whether personal information or sensitive personal information]*

## **Section 3. Representation and Warranties of the Parties**

3.1 Entity sharing Personal Data] represents, warrants and undertakes that:

- a. It has obtained the specific consent of the data subject to the Data Sharing prior to collection and processing, except where such consent is not required for the lawful processing of personal data, as provided by law.
- b. The data subjects have been provided the following information prior to the Data Sharing:
  - i. The identity of personal information controllers or personal information processors that will be given access to the personal data;
  - ii. The purpose of data sharing;
  - iii. The categories of personal data concerned;
  - iv. Intended recipients or categories of recipients of the personal data;
  - v. Existence of the rights of data subjects, including the right to access and correction, and the right to object. However, the other party shall be informed of any request to access or correct personal information which is the subject matter of this sharing agreement; and
  - vi. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

3.2 [Entity receiving the personal data] represents, warrants and undertakes that:

- a. It shall at all times comply with the requirements of the DPA) and all other applicable data privacy laws and regulations;
- b. It shall implement such measures and systems that will enable data subjects to exercise their rights under the DPA, including without limitation the rights access, rectification, modification, blocking, and to object to the processing of data;
- c. It shall implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing; and
- d. It shall ensure that its employees, agents, and representatives who are involved in the processing of personal information operate and hold personal information under strict confidentiality. This obligation shall continue even after their transfer to another position or upon termination of their employment or contractual relations.

#### **Section 4. Procedures for Use or Process of Personal Data**

- 4.1 **Manner of Sharing** [*How parties may use or provide access to the personal data, including, but not limited to, online access*]. Provided that processing and sharing must adhere to the data privacy principles laid down in Republic Act No. 10173, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission.
- 4.2 **Standard of Care.** A party to this Agreement who receives personal data from the other party warrants that it shall exercise at least the same degree of care as it uses with its own personal data and confidential information, but in no event less than reasonable care, to protect the personal data from misuse and unauthorized access or disclosure.
- 4.3 **Permitted Disclosure.** Parties may disclose the personal data only to:
  - a. The extent necessary;
  - b. To authorized persons only;
  - c. With notice to the other party; and
  - d. With the consent of the data subject or when expressly authorized by law.
- 4.4 **Required Disclosure.** If a party is compelled by law to disclose any personal data, it shall notify the other party of such fact before disclosing the compelled personal data.
- 4.5 **Breach Management**
  - a. **Report.** Within twenty-four (24) hours of becoming aware of any unauthorized use or disclosure of the personal data or any security incident or possible security breach, a party shall promptly report such fact to the other party who shared the personal data. Both Parties shall, within seventy-two (72) hours from such occurrence, notify the National Privacy Commission and the concerned data subjects in accordance with NPC Circular 16-03.
  - b. **Cooperation and Mitigation.** A party who receives the personal data shall cooperate with any mediation that the other party, in its discretion, determines is necessary to:

- i. address any applicable reporting requirements, and
- ii. mitigate any effects of such unauthorized use or disclosure of the personal data or any security incident or possible security breach, including measures necessary to restore goodwill with stakeholders, including research subjects, collaborators, governmental authorities, and the public.

## **Section 5. Operational Details of the Sharing or Transfer of Personal Data**

*[Overview of the operational details of the sharing or transfer of personal data and must explain to a data subject the need for the agreement, and the procedure that the parties intend to observe in implementing the same.]*

## **Section 6. Security Measures**

*[General description of the security measures to maintain the confidentiality, integrity and availability of personal data and to ensure the protection of the personal data of data subjects, including the policy for retention or disposal of records.]*

*[Adequate safeguards for data privacy and security must be detailed and reiterate the duty to uphold the rights of the data subjects.]*

## **Section 7. Online Access to Personal Data**

*[If a party shall grant online access (as referred in section 4.1) to personal data under its control or custody to the other, it shall specify the following information:*

- a. Justification for allowing online access;
- b. Parties that shall be granted online access;
- c. Types of personal data that shall be made accessible online;
- d. Estimated frequency and volume of the proposed access; and
- e. Program, middleware and encryption method/ standard that will be used.]

*[Where a government agency grants online access to personal data under its control or custody, such access must be done via a secure encrypted link. The government agency concerned must deploy middleware that shall have full control over such online access.]*

## **Section 8. Mutual Representations**

- a. No Restriction. Neither party is under any restriction or obligation that could affect its performance of its obligations under this Agreement.
- b. No Violation, Breach, or Conflict. Neither party's execution, delivery, and performance of this Agreement and the other documents to which it is a party, and the consummation of the transactions contemplated in this Agreement, do or will result in its violation or breach of the Data Privacy Act of 2012, its IRR and other issuances of the National Privacy Commission, and other related and applicable laws, or conflict with, result in a violation or breach of, constitute a default under, or result in the acceleration of any material contract.

- c. Ownership. The party sharing personal data has the [exclusive] right to grant the other party use of the personal data.

## **Section 9. Return, Destruction, or Disposal of Transferred Personal Data**

*[Unless otherwise provided by the data sharing agreement, all personal data transferred to other parties by virtue of such agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement.]*

*[Identify the method that shall be adopted for the secure return, destruction or disposal of the shared data and the timeline therefor.]*

On the expiration or termination of the Agreement, or on a party's request, the other party shall promptly:

- a) return the personal data and any other property, information, and documents, including confidential information, provided by it;
- b) delete all the personal data including confidential information provided by it, relating to the data processing and sharing;
- c) destroy all copies it made of personal data and any other property, information, and documents, including confidential information; and
- d) if requested, deliver to the requesting party an affidavit or certification confirming the other party's compliance with the return or destruction obligation under this section.

Upon termination or expiration of this Agreement, the party who receives the personal data shall cease all further use of any personal data, whether in tangible or intangible form.

## **Section 10. Use of Name**

Neither party will use the other party's name, logos, trademarks, or other marks without that party's written consent.

## **Section 11. Term**

*[Specify the term or duration of the agreement, which may be renewed on the ground that the purpose/s of such agreement continues to exist: provided, that in no case shall such term or any subsequent extensions thereof exceed five (5) years, without prejudice to entering into a new data sharing agreement.]*

- 11.1 Effectivity. This Agreement is effective upon the date last signed and executed by the duly authorized representatives of the Parties to this Agreement and shall remain in full force and effect until modified or terminated by mutual agreement, in writing, by both Parties.

11.2 Termination on Notice. Either party may terminate this agreement on any valuable cause on through a written notice delivered to the other party [*Termination notice days*] days prior to the termination date.

11.3 Termination for Material Breach. So long as the rights and welfare of the data subjects will not be prejudiced, each party may terminate this agreement with immediate effect by delivering notice of the termination to the other party, if:

- a. the other party fails to perform, has made or makes any inaccuracy in, or otherwise materially breaches, any of its obligations, covenants, or representations, and
- b. the failure, inaccuracy, or breach continues for a period of [*Breach continuation days*] days after the injured party delivers notice to the breaching party reasonably detailing the breach.

11.4 This Agreement may likewise be extended, by mutual consent, through a written notice by either party of its intention to extend this Agreement thirty (30) days before the termination period set.

## **Section 12. Remedies of the Data Subject**

*[Remedies available to a data subject, in case the processing of personal data violates his or her rights, and how these may be exercised.]*

## **Section 13. Indemnification**

The defaulting party shall indemnify the aggrieved party against all losses and expenses arising out of any proceeding:

- a. Brought by either a third party or by the aggrieved party;
- b. Arising out of the party's breach of its obligations, representations, warranties, or covenants under this agreement; and
- c. Arising out of the defaulting party's willful misconduct or gross negligence.

## **Section 14. Authorized Personal Information Processor**

*[Any personal information processor, not party to this agreement, that will have access to or process the same personal data shared to and by any of the parties including the types of processing it shall be allowed to perform.]*

## **Section 15. Data Protection Officer or Compliance Officer**

*[Designated data protection officers and compliance officers for privacy of the parties, their positions in the company/ agency and their contact details.]*

## **Section 16. Personal Information Controller Responsible for Information Request, or Any Complaint**

*[Personal information controller responsible for addressing any information request, or any complaint filed by a data subject and/ or any investigation by the national privacy commission.]*

## **Section 17. General Provisions**

- 17.1 **Security of Personal Data.** Data sharing shall only be allowed where there are adequate safeguards for data privacy and security. Parties shall use contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred.
- 17.2 **Responsibility of the Parties.** Parties shall comply with the Act, its IRR, and all applicable issuances of the National Privacy Commission, including putting in place adequate safeguards for data privacy and security.
- 17.3 **Confidentiality Obligations.** The party who receives shall hold the other party's personal data in strict confidence. Each party will use the same degree of care to protect the data as it uses to protect its own data of like nature, but in no circumstances less than reasonable care. The party who receives shall ensure that its employees or agents are bound to the same obligations of confidentiality as the other party. The obligation of confidentiality shall be maintained even after the termination of this Agreement but shall not apply with respect to information that is independently developed by the Parties, lawfully becomes a part of the public domain, or of which the Parties gained knowledge or possession free of any confidentiality obligation.
- 17.4 **Accountability for Cross-border Transfer of Personal Data.** Each party shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.
- 17.5 **Assignment.** Neither party may assign this Agreement or any of their rights or obligations under this Agreement without the other party's written consent and notice to the data subjects.
- 17.6 **Governing Law.** This Agreement shall be governed, construed, and enforced in accordance with the laws of the Republic of the Philippines.
- 17.7 **Mandatory Periodic Review.** The terms and conditions of this Agreement shall be subject to a mandatory review by the Parties thereto upon the expiration of its term, and any subsequent extensions thereof. The Parties shall document and include in its records:
  - a. reason for terminating the agreement or, in the alternative, for renewing its term; and
  - b. in case of renewal, any changes made to the terms and conditions of the agreement.
- 17.8 **Review and Modification.** Parties hereby authorizes the National Privacy Commission to review the contents of this Agreement and, whenever it becomes necessary, suggest any amendment or revision hereof. In such a case, Parties shall execute an amended Agreement



within fifteen (15) days from Notice of Review by the National Privacy Commission containing its observations and suggestions in order to be compliant with the provisions of the Data Privacy Act, its Implementing Rules and Regulations and other issuances of the National Privacy Commission.

17.9 Severability. If any part of this Agreement is declared unenforceable or invalid, the remainder will continue to be valid and enforceable.

17.10 Alternative Dispute Resolution. In the event of any dispute or difference of any kind whatsoever arising out of or relating to this Agreement, the Parties shall, at first instance, exercise their best efforts to resolve the dispute or difference by mutual consultation as soon as possible. In case best efforts fail, the dispute or difference shall be referred to alternative dispute resolution which shall be governed in accordance with the provisions provided in Republic Act No. 9285, otherwise known as the "Alternative Dispute Resolution Law." The seat of the arbitration shall be the Philippines.

17.11 Venue of Actions. In case of a court suit, the venue shall be the courts of competent jurisdiction in [CITY OR MUNICIPALITY WHERE THE ACTIONS WILL BE FILED] to the exclusion of all other courts subject to prior resort to alternative dispute resolution as herein prescribed.

IN WITNESS WHEREOF, the Parties hereto have affixed their respective signatures this \_\_\_\_\_ day of \_\_\_\_\_ 202x, at \_\_\_\_\_, Philippines.

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

\_\_\_\_\_  
Name  
Position  
Name of Organization/Institution

Signed in the presence of:

\_\_\_\_\_

#### ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)

Before me this \_\_\_\_ day of \_\_\_\_\_ 202x in \_\_\_\_\_ personally appeared:

Names	Government Issued Identification Document			
	ID No.	Date	Place	Expiry Date

all known to me and to me known to be the same persons who executed the foregoing instrument consisting of \_\_\_\_ pages including this page, and they acknowledged to me that the same is their own free and voluntary act and deed and the entities they represent.

IN WITNESS WHEREOF, I have hereunto set my hand this \_\_\_\_\_ day of \_\_\_\_\_, 202x.

Doc No. \_\_\_\_\_;

Page No. \_\_\_\_\_;  
Book No. \_\_\_\_\_;  
Series of 202x.

## Annex E. Privacy Impact Assessment Questionnaire

### PRIVACY IMPACT ASSESMENT QUESTIONNNAIRE

Please provide a brief response and indicate if there is an applicable Group policy.

Department / Unit	
Respondent	
Brief Description of the Department/Unit	
No. of team members	
Which team member handle personal data	
Are there any contractual employees handling personal data	
Brief description of the data processing activities of the Department/Unit	
Personal Data / Category of personal data	
Data Subject / Category of Data Subjects	
Use/s or Purpose/s of Processing	
Recipients / Category of Recipients of personal data	
Collection Point - how is personal data collected?	
With Consent Forms? Manner of Obtaining Consent	
Storage- Where and how is the Personal Data stored?	
Retention - Length of time the data will be stored	
Access to personal data - Who are given access and how is access determined and controlled?	
Disclosure of personal data -To whom are personal data disclosed?	
Disposal of personal data	
Is Personal Data is transferred or shared with any party outside the Philippines?	
What Data Processing Systems are used? (indicate whether manual, or electronic or automated).	

Are decisions relating to the Data Subject to be made based on the processed data, or that would significantly affect the rights and freedoms of the data subject?	
Does the system support fully automated decision-making operation/s?	
What is the impact of the System on the Data Subject/s? (Low / Medium / High)	

If the Department/Unit performs multiple Processing activities, please fill in the table below for each processing activity.

Category of Personal Data: this refers to the type of personal data collected by each department. E.g. name, address, phone no., email address, ID documentation no., health record, CV, photograph, credit card no. and any other type of information that can be used (either on its own or together with other information) to identify an individual. Please indicate whether the Personal Data collected refers to regular personal information or sensitive personal information.

For each Category of Data identified, the following shall be considered:

- Collection Point: this refers to when and where the specified data is collected.
- Storage: this refers to where the specified data is stored or resides. E.g. data management system (please specify the system), shared folder (please specify the shared folder), sharepoint (please specify the sharepoint site), department filing system, office handphone, personal handphone etc. For each storage medium identified, please specify:
- Access: who authorizes access to that identified storage medium, and who currently has access to the data in that identified storage medium.
- Use: this refers to what purposes the data is being used for. E.g. KYC, marketing, payment, etc.
- Disclosure: this refers to the parties (outside of INGS) to whom data may be disclosed in the course of the use of the data. E.g. government authorities, agents, counterparties, correspondent banks, service providers etc.
- Retention: this refers to how long the data is being retained after the purpose for which it is collected has expired.
- Disposal : this refers to when and how the data is disposed.

Processing Activity	
Category of Personal Data	
Collection Point	
Storage	
Access	

Use	
Purpose of collection and processing	
Disclosure - To whom disclosed	
Retention	
Disposal	

## PIA FOR DPS

Data processing System: this refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

Data Processing System	
Purpose of the System	
Personal information controller or processor	
If the system, application or software is outsourced or subcontracted, name and contact information of personal information processor	
Is the contract with third party processor compliant with DPA and related rules	
Data Subject / Category of Data Subjects	
Personal Data / Category of personal data	
Recipients / Category of Recipients of personal data	
Is Personal Data is transferred outside the Philippines	
Does the system support a fully-automated decision-making operation/s	
What is the impact of the System on the Data Subject/s in case of breach? (Low / Medium / High)	

--	--

Where automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject, please fill in the table below.

Note: No decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of the data subject.

Purpose of Processing	
Categories of personal data to undergo processing	
Category/ies of Data Subjects	
Has the Data Subject consented to the automated processing of Personal Data? Manner of Obtaining Consent	
Recipients or Categories of Recipients to whom the data are to be disclosed	
Length of time the data will be stored	
Methods and logic utilized for automated processing	
Decisions relating to the Data Subject to be made based on the processed data, or that would significantly affect the rights and freedoms of the data subject	



## Annex F. Contact List of Data Privacy Officer and Compliance Officers for Privacy

DPO Business Unit	DPO email
Group DPO; DPO for SPAVI	<a href="mailto:dpo@shakeys.biz">dpo@shakeys.biz</a>
WBHI	<a href="mailto:dpo@periperichicken.biz">dpo@periperichicken.biz</a>
SPCI	<a href="mailto:dpo@shakeys.biz">dpo@shakeys.biz</a>



Annex G. Confidentiality/Non-Disclosure/Non-Compete/Proprietary Information Agreement

CONFIDENTIALITY / NON-DISCLOSURE / NON-COMPETE /  
PROPRIETARY INFORMATION AGREEMENT

This Agreement is made and executed on \_\_\_\_\_ 20\_\_ by and between:

SHAKEY'S PIZZA ASIA VENTURES, INC., with office address at the 7<sup>th</sup> Floor,  
Centerpoint Building, Julia Vargas corner Garnet Road, Ortigas Center,  
Pasig City, Philippines, herein referred to as the "**COMPANY**"

-and-

\_\_\_\_\_, Filipino, of legal age, with address  
\_\_\_\_\_, hereinafter referred  
to as the "**EMPLOYEE**."

In consideration of the mutual covenants and premises contained herein, the parties agree to the following terms:

1. **Proprietary Information and Confidentiality**

"**Proprietary Information**" as used in this Agreement shall refer to any of the following:

- a. All information disclosed to the **Employee** by the **Company** or any third party, including but not limited to clients, suppliers, manufacturers, and purchasers, and all information received by the **Employee** during his/her employment with the **Company**;
- b. All information generated by the **Employee** based, in whole or in part, upon the information included in paragraph 1 (a), in any form, tangible, electronic or otherwise, including, but not limited to, oral, written, graphic, demonstrative, sample, product or machine recognizable forms, and including but not limited to, diagrams, flow charts, drawings, photographs, computer files, computer listings, equipment, business plans, marketing plans, patent disclosures, patent applications or other intellectual property documents, including copyright application, proposed trademarks, service marks, grant applications and contract proposals, financing sources, phone lists, customer lists, descriptions of materials, service or contract agreements, purchasing and accounting information and documents, testing, financing;
- c. All information pertaining and relating to employee compensation (including all remuneration, allowances, bonuses, privileges and other benefits) and such related information or documents, which the **Employee** may have acquired in the course of his employment with the **Company**;
- d. All information pertaining to selling and business methods used, belonging to or designed or developed by or for the **Company**;

- e. All types of personal information of employees, customers, vendors and other individuals which the **Employee** may have acquired or been given access to relative and as an incident to his employment with the **Company**;
- f. Information relating to the technical know-how required during and relative to the **Employee's** employment, as well as trade secrets, business activities, product formula, operations, organizations, finances, pricing, clients, and dealings of and concerning the **Company** and/or any of its associated companies and any of its products, which the **Employee** may have acquired relative and as an incident to his employment with the **Company**; and
- g. The terms and conditions of any contract between the **Company** and any client, and information acquired, obtained or developed by or revealed to the **Company** or its representatives or EMPLOYEES in the course of or in connection with the provisions of the said contract, which the **Employee** became aware of during his/her employment with the **Company**.

The **Employee** agrees that the Proprietary Information shall be retained in confidence and shall not be reproduced, used, disseminated, displayed, tested, published, or disclosed to any third party without the prior written approval of the Company President, provided that personal information may only be collected, processed, used and disclosed in accordance with applicable laws and the Company's internal policies.

Disciplinary action for the disclosure of any Proprietary, confidential and/or personal information may range from any of the following penalties: suspension, demotion, or immediate termination of employment, without prejudice to the **Company's** right to resort to the other legal recourse and remedies.

In addition, disclosure of compensations and benefits to unauthorized persons, whether co-employees or not, may result in penalties, including but not limited to the loss of compensations or benefits, or privileges if the discloser is the recipient.

Furthermore, the **Employee** undertakes to safeguard all such confidential information, keep informed of and abide by the company's policies and regulations as established from time to time for the protection of such information.

The **Employee** hereby assigns to the **Company** any and all inventions, procedures, process and/or innovations which may have been conceived and/or developed by the **Employee** during his/her employment with the **Company**. The **Employee** further agrees that any invention, innovation, procedure and/or process developed and/or conceived by him/her shall become part of the **Company's Proprietary Information**.

### 3. Non-Competition

The **Employee** shall not, during the term of his/her employment or after termination of his/her employment thereof, directly or indirectly, use any Proprietary Information and/or skills training other than in the course of performing his/her duties as an **Employee** of the **Company**, nor shall the **Employee** promote, engage in or assist in any capacity, any business, organization, or activity competing with or damaging to the **Company** or any of its activities or affiliates.

Engagement in said activity is cause for immediate transfer, suspension from duties, termination, the filing of a legal case and claim for damages, or other commensurate adjustments or penalties, including but not limited to the withholding of any forms of compensation and benefits at no liability to the **Company**.

Furthermore the **Employee** agrees, during the period of his/her employment with the **Company** or after the termination of his/her employment not to, directly or indirectly, whether on the **Employee's** behalf or on-behalf of any person, firm or organization, solicit, recruit, canvass or obtain as a customer, employee, or supplier any person, firm, or company that is now or was at any time a customer, employee, or exclusive supplier of the **Company** and/or its affiliates. Neither shall the **Employee** use his/her personal knowledge, relationship or influence over another employee, customer or supplier known to him/her as having dealings with the **Company** to compromise or put the **Company** and/or its affiliates at a disadvantage, whether now or in the future.

The **Employee** agrees that he/she will not, during the period of contract or service with the **Company** or for a period of one (1) year from the termination of his/her employment, directly or indirectly, engage in any employment or vocation in any capacity whether gratuitously or otherwise which would conflict with his/her employment with the **Company** or compete or be in competition with the **Company** in any place from any branch and/or operation of the **Company**, either in his/her behalf or on behalf of any person, firm and **Company**.

In any event, in case of separation of the **Employee** from the **Company**, with or without cause, he/she agrees not to recruit, employ or engage the services of other employees of the **Company**, directly or indirectly for whatever purpose especially engaging in any business or activity competing with the **Company** or its affiliates.

#### 4. Accurate Disclosure of Information

The **Employee** agrees that any misrepresentation and/or misleading or false statements supplied in, or any material omission in the application form or other documents, submissions and statements (including verbal) relative to the **Employee's** civil status, liabilities, cases, previous employment, family and educational background, associations or other vital information including the existence of cases filed against the **Employee**, conflicts or interests, and/or the presence of relatives in the **Company** and/or its affiliates, it being the policy of the **Company** and its affiliates not to allow employment of relations within the **Company** and its affiliates, shall be a ground for disciplinary action including, but not limited to, the suspension and/or dismissal of the **Employee**.

The **Employee** acknowledges and agrees that any breach by him/her of any provisions of this Agreement would result in irreparable damage and injury to the **Company** such that any monetary compensation would therefore be an inadequate remedy for any such breach. Accordingly, the **Employee** agrees that if he/she breaches any provisions of the Agreement, the **Company** shall be entitled, in addition to all remedies available to it, to seek an injunction or other appropriate judicial remedies/relief to restrain any such threatened or continuing breach by the **Employee** without showing or proving any actual damage sustained by the **Company**. Nothing in this clause shall preclude the **Company** from pursuing any other remedies, which may be available for the breach or threatened breach of the Agreement by the **Employee**, including the right of the **Company** to suspend and/or terminate the **Employee** or to pursue cases in court or to claim damages for such breach of contract.

## 5. Liquidated and Other Damages

Notwithstanding the above provisions, in the event of breach, violation or circumvention, directly or indirectly, of any of the terms of this Agreement by the **Employee**, the **Company** shall be entitled to liquidated damages in the amount of Two Hundred Thousand Pesos (Php200,000.00) and to damages equal to the amount of damages caused to the **Company** for such breach, violation or circumvention of this Agreement, as well as all expenses incurred in the recovery of said damages including, but not limited to, legal fees.

Notwithstanding the foregoing, the **EMPLOYEE** acknowledges that the value of the Confidential Information and his/her undertakings contained herein is such that an award of damages or an account of profits may not adequately compensate the **COMPANY** in the event of a breach of this Undertaking. The **EMPLOYEE** acknowledges that, without in any way compromising its rights to seek damages or any other form of relief in the event of a breach of this Undertaking, the **COMPANY** shall have the following remedies:

- a. to seek and obtain an ex-parte interlocutory or final injunction to prohibit or restrain any breach or threatened breach of this Undertaking; and
- b. to demand a penalty equivalent to the actual damages suffered. This penalty shall be without prejudice to other judicial or extra-judicial actions which the injured party may maintain for breach of this Undertaking.

## 6. Binding Agreement

This Agreement is the entire agreement between the parties hereto relating to the subject matter hereof and shall be modified only in writing signed by the parties hereto. This Agreement shall be binding upon and inure to the benefit of the heirs, successors and assigns of the parties hereto; provided, however, that **Employee** shall not assign any of **Employee's** duties hereunder without the prior written consent of the President of the Company.

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the date first written above.

For **SHAKEY'S PIZZA ASIA VENTURES, INC.**

\_\_\_\_\_  
\_\_\_\_\_  
—

I have read, understood and been provided with a copy of the above agreement.

CONFORME:

\_\_\_\_\_  
Signature over Printed Name

\_\_\_\_\_  
Date signed

SIGNED IN THE PRESENCE OF:

## Annex H. Data Privacy Trackers

The Data Privacy Tracker is a log of all privacy-related incident/s, complaint/s and/or request/s from Data Subjects, access request/s, as well as a list of all Data Sharing and Outsourcing Agreements entered into by the Company.

SECURITY INCIDENTS LOG				
Date of Incident	Type of Security Incident (e.g., Denial Of Service, Malware, Phishing, Theft of Data, etc.)	Incident Count	Number of Data Subjects Affected	Measures Taken (Measures Undertaken, Assistance Provided to Data Subjects, Outcome)

PERSONAL DATA BREACH LOG				
Date of Breach	Nature of the Breach (Brief Description of The Incident)	Incident Count	Number of Data Subjects Affected	Measures Taken (Measures Undertaken, Assistance Provided to Data Subjects, Outcome)

COMPLAINTS LOG			
Date of Complaint	Data Subject - Complainant	Nature and Description of Complaint	Actions Taken

--	--	--	--

DATA PRIVACY REQUESTS LOG			
Date of Request	Requesting Data Subject	Nature and Description of Data Privacy Right Invoked	Actions Taken

DATA SHARING AGREEMENTS			
Date of Execution	Term	Recipient / Second Party	Purpose of DSA and Personal Data Shared

OUTSOURCING AGREEMENTS					
Date of Execution	Term	Processor	Nature of Service	Purpose	Personal Data Processed

## Annex J. Security Incident Report Form

### Security Incident Report

Shakey's Pizza Asia Ventures, Inc.  
Data Protection and Security Team

This form should be used to report events or occurrences 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. Such events include, but are not limited to:

- malicious code;
- hacking/logical infiltration;
- misuse of resources
- hardware and/or software failure
- violation of IT security policies
- hardware maintenance error
- loss of personal information or sensitive personal information
- suspected breach

<b>Details of Reporting Party</b>	
Employee ID (if SPAVI employee)	
Full Name	
Phone /Mobile number	
Email	
Department/Division	
If SPAVI Vendor:	
Name of Vendor	
Address of Vendor	

<b>Details of Incident</b>		
Date of Incident		
Time of Incident		
Location of Incident		
What personal data is involved?		
Is the incident arising internally or externally (at a vendor)?		
Is the incident still in progress?	Yes	No
Do you need immediate assistance from IT Security?	Yes	No
Has this incident already been reported to the IT Service Desk?	Yes	No
If yes, provide ticket number		
Date and time of report		

<b>Brief Description of the Incident</b> Include details on what type of personal information is affected (or suspected to be affected) and number of individuals that could be affected)



Comments

Prepared By:	
First Point of Contact:	
Department:	Position:
Telephone/Mobile number:	Email:
Date:	Signature:

Please forward to COP / DPO for evaluation and recording.

## Annex K. Data Privacy Request Form

### DATA PRIVACY REQUEST FORM

Note: The Data Privacy Request Form may be filed with the Authorized Personnel previously dealt with by the Data Subject as processor of his/her Personal Data. The Authorized Personnel shall then endorse the same to the Compliance Officer for Privacy (COP) for the branch, sub-office, or department concerned, or in his absence, the Head of such branch, sub-office, or department, for assessment of the reasonableness and approval of the exercise of the right.

DATA SUBJECT INFORMATION		
Name of Data Subject:		
Atty-in-Fact/ Authorized Representative of the Data Subject		
Mobile Number:		
Postal Address and Email Address:		
Proof of Identity Presented: (If Atty-in-Fact or Authorized Representative, SPA should also be presented)		
Right/s to be exercised:  (Please encircle corresponding letter)	a. Right to be informed b. Right to Object c. Right to Access d. Right to Correction	e. Right to Erasure or Blocking f. Right to Data Portability
Description or type of Personal Data:		
Other Instructions or Requests, if any:		
Preferred Method of Compliance: (Please encircle corresponding letter)	a. Send me a paper-based/physical copy of the Updated/Requested Personal Data through my Postal Address. b. Send through E-mail an electronic copy of the Updated/Requested Personal Data through my email address. c. Others, please specify below: _____ _____	

I hereby attest that all information stated in this form are all true and correct to the best of my knowledge. Any concealment, false statement, and/or non-declaration shall constitute fraud, which shall be ground to file a legal action against me; I therefore waive my rights to institute any case arising from this situation.

Likewise, I hereby attest that I been informed of the purpose for the processing of the Information that I provided, and that I expressly give my consent therefor.

Furthermore, as an Attorney-in-Fact / Authorized Representative of the Data Subject (if applicable in this request), I warrant that I have: (i) obtained authorization from the Data Subject to disclose their information included in this form; and that (ii) the Data Subject has been informed of the purpose for the disclosure and collection of information.

I agree to indemnify and hold the Company free and harmless from any and all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, if any.

This consent for the Company to use or process the information herein shall be valid for the purpose of the request herein.

\_\_\_\_\_  
Signature over printed name

\_\_\_\_\_  
Date signed

