VIRGINIA FOOD, INC.

DATA PRIVACY POLICY

TABLE OF CONTENTS

Virginia Food, Inc. ("VFI" or "we," "our," or "us) recognizes the value of ensuring that all personal information and data of its customers, suppliers, employees, visitors, and other data subjects are protected against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

In compliance with the general data privacy principles embodied in Republic Act No. 10173 or the Philippine Data Privacy Act of 2012 ("Data Privacy Act"), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission ("NPC") (the "Data Privacy Laws"), VFI issues this Policy to serve as guidelines and to show its commitment to the protection of personal information and data. This Data Privacy Policy (the "Policy") shall also encapsulate the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

VFI shall exercise its responsibility with the due diligence expected from the nature of the industry, and ensure that its directors, officers, and employees perform their duties with a strict and faithful compliance with these guidelines on personal information and data security and confidentiality.

A. Definition of Terms

"Data Subject" refers to an individual whose personal, sensitive, or privileged information is processed ("you");

"Personal Data" refers to all types of personal information;

"Personal Information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

"Personal Information Processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

"Processing" refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data; and

"Sensitive Personal Information" refers to personal data:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

B. Scope and Limitations

All personnel of VFI including but not limited to its directors, officers, and employees, regardless of their type of employment or contractual arrangement, must comply with this Policy.

C. Processing of Personal Data

1. Collection

1.1 Personal data that VFI collects refers to personal information, sensitive personal information and other data or information about you from which you can be identified either (a) from that data alone; or (b) from that data combined with other information.

1.2 Examples of personal data which you may provide to us include:

a. your name, national registration identification number, passport number or other identification number, date of birth, gender, nationality, telephone number(s), residential and/or mailing address, email address, facial images in a photograph or video recording, fingerprint and any other information relating to you which you have provided to us in any form you have submitted to us, or in other forms of interaction with you;
b. information about your use of our websites and services, including cookies, IP addresses, subscription account details and membership details;
c. employment details, education background and income levels; and
d. your payment related information, such as your bank account or credit card information and your credit history.

1.3 Personal data may be collected by us, directly or indirectly, for instance:

a. when you respond to our promotions and other initiatives, subscribe to our mailing lists or mobile applications, or respond to our market surveys;
b. when you use or purchase our products or services or when you submit forms relating to any of our products or services;
c. when you attend events organized by us or participate in our promotional activities;
d. when you visit our websites and/or when you register for or use or as a member on any of our services on websites owned or operated by us;
e. when your images are captured by us via CCTV cameras while you visit premises we own, manage or operate;

f. when you enter into transactions with us, or express any interest in doing so;
g. when you enter into an agreement with us, such as a sale and purchase agreement, supply agreement, and service agreement;
h. when you communicate with us by telephone, email, via our website or through other communication channels including social media platforms;
i. when you request that we contact you;
j. when we receive references from business partners and third parties, for example, where you have been referred by them;
k. when you submit a job application to us;
l. when we seek information about you and receive your personal data in connection with your relationship with us;
m. when you submit your personal data to us for any reason.

1.4 We also collect personal data from third party sources, for example:

a. from our business partners and third party service providers who provide advertising, marketing or promotional, and other services to VFI;
b. from public agencies or other public sources.

1.5 In certain circumstances, you may also provide us with personal data of persons other than yourself. If you do so, you warrant that you have informed him/her of the purposes for which we are collecting his/her personal data and that he/she has consented to your disclosure of his/her personal data to us for those purposes, including all purposes as set out in this Policy.

You agree to indemnify and hold us harmless from and against any and all claims by such individuals relating to our collection, use and disclosure of such personal data in accordance with the terms of this Policy.

2. Purposes of Collection, Use or Disclosure

2.1 Personal Information and Sensitive Personal Information is collected by VFI for the following main reasons:

a. To allow VFI to comply with its duties and responsibilities with the relevant government regulators or legal authorities;
b. To allow VFI to carry out its business, including for internal and administrative purposes.

We may also collect, use, process, store and/or disclose personal data for one or more of the following purposes:

a. to conduct and complete transactions (e.g. processing orders and payments; providing products or services that have been requested), performing our obligations or exercising our rights as set out in binding contractual terms, and otherwise to manage your relationship with us;
b. to provide customer service (e.g. providing information on status and updates);
c. to process your application for a membership account or subscription to a mailing list of VFI, establish user profiles and maintain such account, including verification of personal particulars and processing payment requests;
d. to process your participation in our promotions, contests and other marketing and promotional events;
e. to deliver correspondences or notices as may be required for documentation, execution of contracts between us, or as you may have requested or agreed to;
f. to process payments or credit transactions;
g. to communicate with you and respond to your queries or requests;
h. to conduct research and analysis for review, development, management and improvement of our products and/or services;
i. to manage the business operations of VFI and to comply with internal policies and procedures;

j. to respond to legal processes or to comply generally with any applicable laws, governmental or regulatory requirements of any relevant jurisdiction (and any applicable rules, codes of practice or guidelines), and requests of any governmental or other regulatory authority with jurisdiction over us, including, without limitation, assisting in law enforcement and investigations by relevant authorities;
k. security and safety purposes within the premises of VFI, including the conduct of security screening and issuance of access passes;
l. to communicate with you any changes and development to policies, terms and conditions and other administrative information of VFI;
m. to protect and enforce our contractual and legal rights and obligations and to handle disputes and conduct and facilitate investigations and proceedings;
n. if you submit an application to us as a candidate for employment, to process your application, conduct pre-recruitment checks and background screening, collect information about your suitability for the position applied for, organize training and staff development programs, assess your performance, administer benefits and payroll processing, provide you with tools to do your job and to communicate with you to comply with our policies and processes;
o. such purposes that may be informed to you when your personal data is collected;
p. any other reasonable purposes related to the aforesaid or for which you have provided any information to us; and/or
q. any other incidental business purposes related to or in connection with the above.

Our processing of your personal data for the above purposes may be made on the legal basis of legitimate interests, entering into or performance of contract with you, legal compliance, consent, or any other basis as permitted by laws applicable in any relevant jurisdiction, as the case may be.

2.2 We may also collect, use, process, store and/or disclose personal data for other legitimate purposes related to our business and which are not incompatible with the original purposes for which you have provided the personal data, and also in circumstances other than set out in this policy where required, or permitted, by laws applicable in any relevant jurisdiction.

2.3 For the purposes set out above where your personal data are required for entering into or performance of contract with you or for our legal compliance, if you do not provide us with the required personal data, we may not be able to effectively provide or continue providing you with the products and/or services which you have requested from us.

3. Storage, Retention and Destruction

Any Personal Data, Personal Information and Sensitive Personal Information provided to VFI is retained only for a period of five (5) years or for such duration that is necessary to fulfill whatever purpose for which it is collected subject to compliance with applicable laws, rules and regulations. VFI will exercise reasonable security measures to prevent unauthorized, accidental, or unlawful access, processing, deletion, loss or use, including providing standard restrictions to physical access to data within VFI's systems, and encryption of sensitive data when transmitting such data. Such reasonable measures will also be taken to remove information when no longer necessary.

4. Transfer, Disclosure and Sharing of Personal Data

4.1 VFI may disclose your personal data to the following parties, whether located within or outside the Philippines, for the purposes set out or otherwise referred to in this Policy:

a. VFI's business partners, affiliates, associated companies and related parties for legitimate business purposes;
b. agents, contractors, third party service providers and specialist advisors of VFI and their respective affiliates, associated companies and related parties, who have been contracted to provide administrative, financial, research, operational or other services;
c. third party business partners who offer goods and services or sponsor contests or other promotional programs, whether in conjunction with VFI or not, and where permitted by applicable laws;
d. third parties to whom you authorize disclosure of your personal data (through this Policy or otherwise);
e. the auditors, professional consultants, lawyers and other advisors of VFI and its business partners, affiliates, associated companies and related parties;
f. insurers, credit providers, courts, tribunals, law enforcement agencies, regulatory authorities and other governmental agencies as agreed or authorized by law;
g. credit reporting or reference agencies or investigators, credit bureau and in the event of default or disputes, any debt collection agencies or dispute resolution centers;
h. any business partner, investor, assignee or transferee (actual or prospective) to facilitate business asset transactions (which may extend to any merger, acquisition or asset sale) involving VFI and its business partners, affiliates, associated companies and related parties;
i. banks, credit card companies and their respective service providers.

5. Access

Due to the sensitive and confidential nature of the personal data under the custody of VFI, only the Data Subject and the authorized representative of VFI shall be allowed to access your personal data, for such purpose/s not contrary to law, public policy, public order or morals.

However, for personal data shared over the Internet, it is important to be aware that despite our efforts to secure our systems and applications, we make no guarantee, warranty or any representation that our systems or applications are completely secure and absolutely invulnerable to security breaches.

6. Security Measures

VFI will take appropriate organizational, physical, and technical measures which are consistent with the Data Privacy Laws. VFI will use security procedures and technology to protect the information it holds.

6.1 Organizational Security Measures

A Data Protection Officer ("DPO") shall be appointed by VFI. The DPO is responsible for ensuring VFI's compliance with the Data Privacy Laws.

General Qualifications:

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

b. The DPO shall be a full-time or organic employee of VFI. Where the employment of the DPO is based on a contract, the term or duration thereof shall be at least be two (2) years to ensure stability.

c. A DPO must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by VFI. In his or her capacity as DPO, an individual may perform (or be assigned to perform) other tasks or assume other functions that do not give rise to any conflict of interest.

Duties and Responsibilities:

a. Monitor VFI's compliance with the Data Privacy Laws. For this purpose, he or she may:

- Collect information to identify the processing operations, activities, measures, projects, programs, or systems of VFI, and maintain a record thereof;
- Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
- Inform, advise, and issue recommendations to VFI;
- Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
- Advice VFI as regards the necessity of executing a data sharing agreement with third parties, and ensure its compliance with the law;

b. Ensure the conduct of privacy impact assessments relative to activities, measures, projects, programs, or systems of VFI;
c. Advice VFI regarding complaints and/or the exercise by Data Subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
d. Ensure proper data breach and security incident management by VFI, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
e. Inform and cultivate awareness on privacy and data protection within the organization of VFI, including all relevant laws, rules and regulations and issuances of the NPC;
f. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of VFI relating to privacy and data protection, by adopting a privacy by design approach;
g. Serve as the contact person of VFI vis-à-vis Data Subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;
h. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
i. Perform other duties and tasks that may be assigned by VFI that will further the interest of data privacy and security and uphold the rights of the Data Subjects.

6.2 Physical Security and Technical Security Measures

VFI shall ensure that physical security measures are in place, which shall, include, among others, monitoring and limiting access to, and activities in, the departments and offices of VFI where personal data is processed, including guidelines that specify the proper use of and access to electronic media. In addition, VFI shall implement technical security measures to ensure that, among others, VFI's processing systems are not vulnerable to data breach. VFI shall faithfully comply with the standards and guidelines in the Data Privacy Act on physical security and technical security measures.

6.3 Breach and Security Incidents

a. Data Breach Notification

All employees and agents of VFI involved in the processing of personal data are tasked with regularly monitoring for signs of a possible data breach or security incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or security incident.

The DPO shall notify the NPC and affected Data Subjects of any incident of data breach pursuant to requirements and procedures prescribed by the Data Privacy Act.

The notification to the NPC and affected Data Subjects shall describe, among others, the nature of the breach, the personal data possibly involved, and the measures taken by VFI to address the breach.

b. Breach Reports

VFI shall ensure that all security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller as defined under the Data Privacy Act. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted by the DPO to the NPC annually.

D. Rights of Data Subjects

VFI shall ensure that your rights as Data Subjects are protected and recognized. Towards this purpose, VFI shall ensure that all Data Subjects shall be given the following rights:

1. Right to be informed

The Data Subject has the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed. The Data Subject shall be furnished with information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

a. Description of the personal data to be entered into the system;

b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;

c. Basis of processing, when processing is not based on the consent of the Data Subject;

d. Scope and method of the personal data processing;

e. The recipients or classes of recipients to whom the personal data are or may be disclosed;

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

g. The identity and contact details of the personal data controller or its representative;

h. The period for which the information will be stored; and

i. The existence of their rights as Data Subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the NPC.

2. Right to object

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

When a Data Subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the Data Subject; or
3. The information is being collected and processed as a result of a legal obligation.

3. Right to access

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

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

4. Right to rectification

The Data Subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the

retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

5. Right to erasure or blocking

The Data Subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

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

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

2. The personal information controller may notify third parties who have previously received such processed personal information.

6. Right to damages

The Data Subject has the right to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

7. Transmissibility of Rights

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

8. Right to Data Portability

The Data Subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the Data Subject. The NPC may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

VFI may engage a Personal Information Processor to process the Personal Data, Personal Information and Sensitive Personal Information of the its Data Subjects. Such engagement shall comply with the requirements of the Data Privacy Act and shall at all times be covered by the appropriate contractual agreements. VFI shall ensure that such Personal Information Processor shall also, where applicable, implement the security measures of the Data Privacy Act. At all times the

Personal Information Processor must ensure the confidentiality, integrity and availability of the personal data processed, and prevent its use for unauthorized purposes.

E. Consent Withdrawals

The consent that you provide for the collection, use and disclosure of your personal data will remain valid as long as the purpose for which it is collected exists or until such time it is being withdrawn by you in writing. An individual may withdraw consent and request us to stop using and/or disclosing their personal data by submitting a request in writing to our Data Protection Officer at the contact details provided below.

If you withdraw your consent to any or all use of your personal data or do not consent to the collection of your personal data by us, where it is mandatory for you to provide us with such personal data, we may not be able to provide or continue providing you with products and/or services which you have requested and such withdrawal may also constitute a termination event which results in legal consequences such as forfeiture of deposits. You understand and agree that in such instances where VFI requires your personal data to fulfill a contractual obligation to you and you withdraw your consent to collect, use or disclose the relevant personal data for those purposes, VFI cannot be held liable for breach of that agreement. VFI's legal rights and remedies in such event are expressly reserved.

Please note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws in any relevant jurisdiction.

F. Accuracy

We generally rely on personal data provided by you (or your authorized representative). In order to ensure that your personal data is current, complete and accurate, please update us if there are changes to your personal data by informing our Data Protection Officer in writing at the contact details provided below.

G. Cookies and WebsiteTracking

When you visit our websites, please note that we may use cookies and similar tracking mechanisms and devices, for purposes such as monitoring the number of times you visit the websites, which pages you go to, and how long you spend browsing each page. This information helps us build a profile of our users and improve our websites and other products and services. Where data is only used on an aggregated basis, we will be unable to identify any particular individual, and we generally track on per-device basis.

H. Other Websites

Our websites may contain links to other websites. However, this Policy only applies to VFI, and if you visit other websites, including through such links, different privacy policies will apply.

I. How to Contact Us/Data Protection Officer Details

If you have any queries or comments on this Policy or the use of your personal data, or if you wish to lodge a privacy-related complaint, please contact our Data Protection Officer at:

Data Protection Officer
Email address: dataprivacy.dpo@virginiafood.com.ph
Phone number: 09178055068

VFI will investigate your queries, comments or complaint, and will use reasonable endeavours to respond, in accordance with applicable laws.

J. Effectivity

This Policy shall be effective as of 1 March 2023.