Personal data processing policy

The policies outlined below apply to the Processing of Personal Data controlled by Team Foods Colombia S.A. and / or Grasas S.A. (hereinafter referred to as "the Companies"), regarding customer, supplier, employee and general third party Personal Data.

SECTION I – GENERAL

Article 1 Applicable regulations: This Policy is governed by the considerations set forth under articles 15 and 20 of the Political Constitution of Colombia, Law 1581 of 2012 "By which the general provisions for personal data protection are outlined", and SECTION 25 of Decree 1074 of 2015 "By which Law 1581 of 2012 is partially regulated".

Article 2. Scope of Application: This Policy shall apply to Personal Data managed by the Companies and which are subject to Data Processing.

2.1 Territorial Scope: The Policy shall apply to the Processing of Personal Data managed by the Companies, including data collected from individuals accessing the webpage from jurisdictions different from Colombia.

Article 3. Purpose: The purpose of this Policy is to comply with the obligations stipulated under literal k) Article 17 of Law 1581, 2012, as well as regulating the procedures for collection, handling and processing of Personal Data collected by the Companies.

Article 4. Contact Information: Team Foods Colombia S.A. is domiciled at Calle 45a Sur No. 56 – 21, Bogota D.C., Colombia and may be contacted at the aforementioned address or email notification@alianzateam.com

Article 5. Definition: For the purposes of this Processing of Personal Data Policy, it shall be defined as:

Authorization: Prior, explicit and informed consent of the Holder of the Personal Data to execute the

Processing of Personal Data.

Database: Organized set of Personal Data subject to processing .

Personal Data: Any information that may be associated with one or more specific or determinable natural persons. Some examples of Personal Data are as follows: name, citizenship ID details, address, email, telephone number, marital status, health related data, fingerprint, salary, assets, among others.

Public Personal Data: Refers to Personal Data which is not Semi-Private, Private or Sensitive in nature.

Public data, among others, is data concerning people's marital status, their profession or trade and their commercial/trading status or public employee.

Private Personal Data: Refers to data, which due to its intimate or reserved nature, is only relevant to Holder of the same.

Semi-private Personal Data: Personal Data which is not intimate, reserved, nor public in nature and which information or disclosure may be of interest not only to its Holder but also to a certain segment or group of people or to society in general, for example, the compliance and non-compliance with financial obligations or data concerning affiliations with the social security system.

Sensitive Personal Data: Information which involves the privacy of the Holder or which improper use may produce discrimination, such as racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations, human rights or the promoting interests of any political party or which guarantees the rights and opposition of political parties as well as data related to health, sexual life and biometric data, among others; capture of images or images in movement, fingerprints, photographs, iris, voice, facial or palm recognition, among others.

Responsible for the Processing : Natural person or company, public or private, independently or in association with others, perform the Processing of Personal Data on behalf of the Responsible Party .

Claim: Request from the Holder of the Data or the persons duly authorized by the same or by Law, to correct, update or delete their Personal Data or to revoke the authorization as set forth under Law.

Responsible for the Processing : Natural Person or legally established company, public or private, that individually or in association with others, make decisions in terms of database and / or the Processing of data.

Holder: Natural person whose Personal Data is subject to Processing .

Transfer: The Transfer of Personal Data takes place when the Responsible and / or Person in Charge of the Processing of Personal Data, located in Colombia, sends the information or Personal Data to a recipient, who in turn is Responsible for the Processing located in Colombia or abroad.

Diffusion: Processing of Personal Data which implies communication of the same in the Republic of Colombia or abroad, when the purpose is to perform personal data processing by the Manager on behalf of the Responsible party.

Processing : Any Personal Data operation or set of operations such as collection, storage, use, circulation or deletion.

Article 6. Principles applicable to the Processing of Personal Data: For the Processing of Personal Data, the Companies shall apply the principles outlined below, which establish the instructions to be followed within the Processing of Personal Data:

Legality: The Processing of Personal Data must be performed in accordance with the applicable legal provisions (Statutory Law 1581 of 2012 and its regulatory decrees).

Purpose: The Personal Data collected must be used for a specific and explicit purpose which must be informed to the Holder or as set forth under Law. The Holder must be informed clearly, sufficiently and in advance about the purpose of the information provided.

Voluntary authorization: The collection of Personal Data may only be exercised with prior, explicit and informed authorization of the Holder.

Veracity or Quality: The information subject to the Processing of Personal Data must be truthful, comprehensive, exact, updated, verifiable and understandable.

Transparency: Within the Processing of Personal Data, the Holder´s right to obtain, at any time and without restrictions, information about the existence of data concerning him/her must be guaranteed.

Access and restricted circulation: The Processing of Personal Data shall only be performed by the persons authorized by the Holder and / or as set forth under Law.

Safety: The Personal Data subject to Processing must be handled in accordance with all necessary safety standards in order to prevent loss, adulteration, consultation, use or unauthorized or fraudulent access.

Confidentiality: All employees that work in the Companies are obliged to keep Personal Data confidential, even after their employment or contractual relationship has ended.

SECTION II.- AUTHORIZATION

Article 7. Authorization: The Processing of Personal Data by the Companies requires voluntary, prior, explicit and informed consent of the Holder.

Article 8. Form and mechanisms for granting Authorization: The Authorization may appear in any manner which guarantees its consequent consultation, specifically: i) in writing, ii) orally, or iii) by means of absolute authorization of the Holder which leads to reasonably conclusion that the Authorization was granted. In no case may silence be interpreted as absolute authorization.

Article 9. Proof of Authorization: The Companies shall keep necessary records or mechanisms in order to establish when and how the authorization was obtained from the Personal Data Holders for the processing thereof.

SECTION III.- RIGHTS AND OBLIGATIONS

Article 10. Rights of the Holders: In accordance with the provisions of article 8 of Law 1581 of 2012, the Holder of Personal Data has the right to:

1. Know, update and rectify Personal Data before those responsible for the processing or corresponding Processing Managers. This right may be

exercised, among others, against partial, inaccurate, incomplete, fractioned, misleading data, or when processing is explicitly prohibited or has not been authorized;

2. Request proof of authorization granted to the Responsible Processing Officer, except when explicitly excepted as a requirement for the Processing, in accordance with the provisions of article 10 of Law 1581 of 2012;
3. Be informed by the Processing Manager, upon request, regarding the use that has been given of Personal Data;
4. Submit complaints due to violations of the provisions of Law 1581 of 2012 and other regulations which may have modified, added or complemented the same, before the Superintendence of Industry and Commerce.
5. Revoke the Authorization and / or request deletion of data when during the Processing, the principles, rights and constitutional and legal guarantees have not been not met. The revocation and / or deletion shall proceed when the Superintendence of Industry and Commerce has established that during the processing, the responsible party or Person in Charge have engaged in actions that violate Law 1581 of 2012 and / or the Constitution of Colombia;
6. Unrestricted free of charge access to Personal Data subject to processing .

Article 11. Obligations of the Companies: The Companies recognize that the Personal Data is property of the people to whom they refer and that only they can decide in regards to the same. Therefore, the Companies shall use the Personal Data collected only for the purposes for which they are duly empowered to do so and recognizing, in any case, the current regulations on the Protection of Personal Data.

In accordance with the provisions of article 17 of Law 1581 of 2012, the Companies are obliged to comply with the following obligations :

1. Guarantee the Holder full and effective exercise of the right to habeas data at all times.
2. Request and keep, as set forth under Law 1581 of 2012, a copy of the corresponding authorization

granted by the Holder;

1. Duly inform the Holder about the purpose of the collection and his/her rights by virtue of the authorization granted;
2. Keep Personal Data under required safety standards in order to prevent adulteration,

loss, consultation, use or unauthorized or fraudulent access;

1. Guarantee that the information provided to the Processing Manager is truthful, comprehensive, accurate, updated, verifiable and understandable;
2. Update the information, informing the Person in Charge of Processing in a timely manner, of all updates regarding previously provided data and implement other necessary measures so that the information provided is kept updated;
3. Rectify the information when it is incorrect and inform any pertinent issues to the Processing Manager;
4. Provide the Processing Manager, as corresponds, only data which Processing is previously authorized in accordance with the provisions of Law 1581 of 2012;
5. Require the Processing Manager to respect safety and privacy conditions of the Holder's information at all times.
6. Process inquiries and claims formulated in the terms indicated under Law 1581 of 2012;
7. Inform the Processing Manager when certain information is under discussion with the Holder, once the claim has been submitted and the corresponding procedure has not been completed;

8. Inform, at the request of the Holder, about the use given of their data;
9. Inform the data protection authority in the event of safety and code violations, and

in case of risks in the administration of the holders ´ information.

1. Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

SECTION IV- PRIVACY NOTICE

Article 12. The privacy notice is a physical or electronic document, or in any other format made known to the Holder, before or at the time of collection of their Personal Data, and is the means by which information is informed in regards to Information Processing Policies which shall be applicable, the ways to access them and, in general, the purposes for which Personal Data has been obtained and the processing that the Companies proceed.

SECTION V- PURPOSES OF THE PROCESSING

Article 13. Information processing. The Personal Data managed by the Companies shall be collected, used, stored, updated, transmitted and / or transferred, for the following purpose or purposes:

Regarding the Personal Data of our Clients and Suppliers:

1. To provide required services and products;

2. Inform about changes, modifications or new products or services related or not with the products or services contracted or acquired by the Holder by any means of communication;
3. Comply with obligations contracted with the Holder;
4. Evaluate the quality of the product and service, perform market studies and statistical analysis for internal uses and participation of the Holders in marketing and promotional activities.
5. Provide design and implementation of customer loyalty programs;
6. Share Personal Data, including the Transfer and Transmission of Personal Data to third parties for purposes related to the operation of the Companies;
7. Perform internal studies in regards to the fulfillment of commercial relations and market studies at any level;
8. Perform internal or external audit processes typical of the commercial activity that the Companies carry out;
9. Allow companies associated to the Companies, with which it has entered into contracts including provisions to guarantee the safety and proper Processing of the Personal Data processed, to contact the Holder with the purpose of offering goods or services of interest;
10. Control access to the offices and plants of the Companies, including the establishment of video-monitored areas;
11. Respond queries, requests, complaints and claims made by the Holders and control bodies and process the Personal Data to other authorities that by virtue of law must receive Personal Data;
12. Use the different services corresponding to websites, including content and format downloads;
13. Transfer information collected to different areas of the Companies and associated companies in Colombia and abroad when necessary for operational development and payroll management (collection of portfolio and administrative charges, treasury, accounting, among others);
14. Register the Holders in the Companies ´ systems and process their payments or collections;

15. Any other similar and / or complementary activity in nature, to those previously outlined, necessary for the development of the corporate purpose of the Companies.

Regarding the Personal Data of our candidates:

1. Manage and operate, directly or by means of third parties, the personnel selection and hiring processes, including the evaluation and qualification of participants and verification of work based and personal references, and the performance of safety related studies;
2. Any other similar and / or complementary activity in nature to those previously outlined and necessary for the development of the corporate purpose of the Companies.

Regarding the Personal Data of our staff:

1. Develop activities of human resource management within the Companies, such as payroll, affiliations to the general social safety system, occupational health and welfare activities, exercise employer's sanctioning power, among others;
2. Make necessary payments resulting from the employment contract execution and/or its termination, and any other social benefits applicable in accordance with law;
3. Contract employment benefits with third parties, such as life insurance, medical expenses, among others;
4. Notify authorized contacts in case of emergencies during working hours or during the

development of the same;

5. Coordinate professional development of employees, employee access to computer resources of the Companies and assist in their use;

6. Plan business activities;
7. Transfer information collected to different areas of the Companies and associated companies in Colombia and abroad when necessary for the development of the operations and payroll management (collection of portfolio and administrative collections, treasury, accounting, among others);
8. Control offices and plant access of the Companies, including the set up of video-monitored areas;
9. Manage training;
10. Register the holders in the different systems of the Companies;
11. Any other similar and / or complementary activities nature to those outlined herein, necessary for the development of the corporate purpose of the Companies.

SECTION VI- PERSON AND AREA RESPONSIBLE FOR REQUESTS, COMPLAINTS OR CLAIMS OF HOLDERS OF INFORMATION.

Article 14. The division responsible for access request, rectification, updating, data deletion or revocation of consent or Authorization granted for the Processing of Personal Data to any of the Companies, is the Legal and Corporate Affairs Vice Presidency, located at Calle 45a Sur No. 56 – 21, Bogota DC, Colombia, email Notifications@alianzateam.com

The Personal Data Protection Officer ´s main functions is to ensure effective implementation of policies and procedures accepted by the Companies in order to comply with the Colombian System for the Protection of Personal Data, and to take charge of the structuring, design and administration of the Comprehensive Personal Data Management program.

The Company's Personal Data Protection Officer shall:

1. Manage the appropriate procedure of any claim submitted by the Holders in accordance with the provisions of this Policy.
2. Verify that the information received by the Holder is sufficient in order to provide a response;
3. Evaluate the need to extend the term for responding Claims;
4. Allocated the claim within the Companies as appropriate;
5. Assign responses to claims;
6. Send responses to the Holders in accordance with the terms established under Law, in this Policy and in the Policies and Procedures Guidelines of the Companies;
7. Order warning inclusion in the databases against claims or those under judicial evaluation;
8. Ensure compliance with this Policy;
9. Provide support to the divisions of IT, Structure and Design and administer the Comprehensive Data Management Program staff in line with the indications approved for this purpose by the Board of Directors and the Company Presidency;
10. Keep the Presidency informed of the progress status of the implementation of the Comprehensive Personal Data Management Program, by means of semi-annual reports outlining detailed activities, outstanding activities, execution timeframe and resources required for said purpose;
11. Prepare annual reports on the implementation and operational processes of the Comprehensive Personal Data Program Management before the General Assembly of Shareholders .
12. Implement a training program of protection of Personal Data within the Companies and ensure

permanent training activities for the staff;

13. As part of his/her duties, the Company's Personal Data Protection Officer shall supervise the training of new staff members in appropriate Processing of Personal Data and, especially, the obligations to be complied with in his/her job position;

14. Audit the compliance of the different areas of the Companies regarding adequate compliance with the

Colombian System for the Protection of Personal Data, this Policy and those resulting from the

implementation of the Comprehensive Personal Data Management Program;

15. Develop required control in order to guarantee the implementation and effectiveness of the Comprehensive Personal Data Management Program together with the support of the Technology Area, and strict compliance

of the Companies´ terms and obligations under the Colombian System of Protection of Personal Data;

16. Coordinate and encourage definition and implementation of the risk management system

associated with the Processing of Personal Data;

17. Coordinate and promote the definition and implementation of the Comprehensive Data Management Program that controls the staff.
18. Operate as bridge and coordinate the implementation of the Comprehensive Personal Data Management Program with the areas of the Companies.
19. Maintain the inventory of Companies' Personal Databases permanently updated. Finally, perform semi-annual audits directly or with the support of the internal audit area.
20. Validate the formation of Personal Databases and register it in the National Registry of Databases

of the Superintendence of Industry and Commerce;

21. Update the information of the National Registry of Databases whenever required in compliance with the applicable law; including the management of safety and incidents reports before the Superintendence of Industry and Commerce;
22. Manage contracts for the international transfer of Personal Data or manage compliance declarations, as required, in accordance with the National Registry of Databases;
23. Respond inquiries submitted within the organization regarding the Comprehensive Management Program

of Databases and the Colombian System for Protection of Personal Data;

24. Confirm the responsibilities of each of the Companies' divisions in regards to Data Processing

Personnel under his/her responsibility, and establish due compliance indicators for frequent compliance verification;

25. Attend visits of the Superintendence of Industry and Commerce concerning the supervision of the

Colombian System for the Protection of Personal Data within the organization.

SECTION VII ACCESS, CONSULTATION AND CLAIM PROCEDURES

Article 15. Access Rights. The Holders of Personal Data processed by the Companies have the right to access their Personal Data and the details of said Processing, as well as to rectify and update the same if they are inaccurate or

to request elimination when considered that they are disproportionate or unnecessary for its purposes or contrasting to the specific purpose processing.

Submission of requests and for the purpose of guaranteeing the herein referred to rights, enquires should be addressed to:

- Physical mail:

Team Foods Colombia S.A. Calle 45a Sur No. 56 – 21, Bogotá D.C.

Grasas S.A. Calle 45a Sur No. 56 – 21, Bogotá D.C.

By email:

Team Foods Colombia S.A. notifications@alianzateam.com

Grasas S.A. notifications@alianzateam.com

These channels may be used by Personal Data Holders, or third parties to act on their behalf as authorized by law, in order to exercise the following rights:

a.Queries: The Holder may access his/her Personal Data free of charge. Thus, the holder may submit a request indicating the information required by means of any of the mechanisms indicated above. The request shall be answered by

the Companies within a maximum term of ten (10) business days as of the date of receipt. When it is not possible to answer the request within said term, this circumstance shall be reported to the applicant, stating the reasons for the delay and indicating the date on which their query shall be answered, which in no case may exceed five (5) business days following the expiration of the first term.

1. **Claims:** In accordance with the provisions of Article 14 of Law 1581 of 2012, when the Holder or his/her duly authorized third party considers that the information processed by the Companies should be subject to correction, update or deletion, or when it should be revoked due to presumed violations of any legal obligations, they may submit a request to the Companies, which shall be processed under the following set of rules:

- The Holder or or his/her duly authorized third party must provide evidence of identity, authorization, representation or provision in favor of another or for another third party. When the request is performed by a third party and it is not proven that he/she acts on his/her behalf, the request shall not be processed.
- The request for rectification, updating, deletion or revocation must be submitted by means of the instruments enabled by the Companies and outlined in this document and enclose, at least, the following information:

1. The name and address of the Holder or any other methods for receiving response.
2. Documents showing the identity of the applicant and, if applicable of his/her duly authorized representative including the corresponding authorization.
3. Clear and precise description of the Holder's Personal Data to which he/she pursues to exercise the rights and the specific request.

The maximum term to meet this request shall be fifteen (15) business days as of the day following the date of receipt.

When it is not possible to answer the request within said term, this circumstance shall be reported to the applicant, stating the reasons for the delay and indicating the date on which their query shall be answered, which in no case may exceed five (8) business days following the expiration of the first term.

If the claim is incomplete, the interested party shall, within five (5) days after receiving it, correct the corresponding errors. If after two (2) months as of the date of the request, without the applicant submitting the required information, the claim shall be interpreted as a withdrawn claim. Once a complete claim has been received, a reference indicating "claim in process" and due reason shall be included in the Database, within a term not exceeding two (2) business days. Said reference must be preserved until the claim is decided upon.

First Paragraph. Rectification and update: When the claims are intended for rectification or update, the Holder must indicate the corresponding corrections and submit documentation that supports their request.

Second paragraph. Deletion: The deletion of Personal Data is performed by means of total or partial elimination of personal information as requested by the Holder, notwithstanding, the Companies may deny such request when the Holder has a legal or contractual duty to remain in the Database.

Article 16. Revocation of Authorization. Holders of personal data may revoke the Authorization previously granted at any time, except in those events in which a legal or contractual provision impedes such action. In any case, the Holder must indicate in his/her corresponding request if it is a full or partial revocation, the latter, when he/she requests to eliminate only some of the authorized data, the Holder must clearly indicate which data to be delete.

SECTION VIII- DATABASES VALIDITY PERIOD

Article 17. Personal Data stored by the Companies shall be kept as long as required according to the purpose of the Processing and / or for the term required in order to comply with a legal or contractual obligation. The Companies have adopted measures for timely and safe elimination of their Personal Data, outlined in the Policies and Procedure Guidelines.

SECTION IX – PROCESSING OF SENSITIVE PERSONAL DATA

Article 18. Upon performing the corresponding commercial activity, the Companies process Sensitive Personal Data for specific purposes. The Companies shall only perform the Processing of sensitive Personal Data as long as it has been previously authorized by the corresponding Holder and shall handle them under safety and confidentiality standards in accordance with their nature.

In accordance with the above, the Companies have implemented administrative, technical and legal procedures as duly outlined in the Policies

and Procedures Guidelines, which are mandatory for The Companies' employees and, as applicable, their suppliers, associated companies and / or commercial allies.

However, it shall be notified that the collection of Sensitive Personal Data is not meant as a condition for accessing any of our products or services.

SECTION X- TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 19. In accordance with article 26 of Law 1581 of 2012, the Transfer of Personal Data of any kind to countries that do not provide adequate levels of data protection is prohibited. A country that offers an adequate level of data protection is considered when the standards set by the Superintendence of Industry and Commerce have been met. They may, however, never be less than those required by law 1581 of 2012.

This prohibition shall not apply when it refers to:

1. Information for which the Holder has granted his/her explicit and unequivocal authorization for the Transfer;
2. Exchange of medical data, when required by the Holder's Processing for health matter reasons or public hygiene;
3. Bank or stock transfers, in accordance with the legislation applicable;
4. Transfers agreed within the framework of international treaties in which the Republic of Colombia is

included, based on the principle of reciprocity;

5. Transfers required for contractual execution between the Holder and the Data Controller, or for the execution of pre-contractual measures as long as the Holder's Authorization is available;
6. Transfers legally required in order to safeguard public interest, or for the recognition, exercise

or defense of a right within a judicial process.

SECTION XI- INTERNATIONAL AND NATIONAL TRANSMISSIONS OF DATA TO MANAGERS

Article 20. When the Companies send or transmit data to one or more Managers located within or outside the territory of the Republic of Colombia, they must establish contractual clauses or enter into a Personal Data Transmission contract in which, among others, as outlined below:

1. The capacity and purposes of the processing .
2. The activities that the Person in Charge shall perform on behalf of the Companies.
3. The obligations that the Manager must fulfill in regards to the Holder of the Companies´ data.
4. The duty of the person in charge of processing the data in accordance with the authorized purpose for the same and in view of the principles of the Colombian Law and this Policy.

5. The obligation of the Person in Charge in order to adequately protect the Personal Data and the Databases as well as keeping confidentiality regarding the Processing of the transmitted data.
6. A description of the specific safety measures to be adopted by both the Companies and

by the final user Data Controller.

The Companies shall not request Authorization when international transmission of data is protected by any of the exceptions provided within the Law and corresponding Regulatory Decrees.

SECTION XII- FINAL PROVISIONS

Article 21 The Companies shall be responsible for the protection of Personal Data, shall process the requests of the Holders, and shall guarantee the exercise of the corresponding rights.

Article 22. Safety measures: Upon exercising the safety principles established under Law 1581 of 2012, the Companies shall undertake the necessary technical, human and administrative measures in order to guarantee the safety of the Personal Data subject to Processing, thus avoiding its adulteration, loss, consultation, use or unauthorized or fraudulent access.

Article 23. Validity: This Policy is effective as of June 1, 2017.