



PERSONAL DATA

PROCESSING POLICY



1. PURPOSE

The purpose of this personal data processing policy (hereinafter, the “Policy”), under which Team Foods Colombia S.A. and Grasas S.A. act as Data Controllers (hereinafter, the “Companies”, notwithstanding which any reference shall be understood as made to the entity that is applicable in each case), is to ensure compliance with the applicable law on personal data protection with respect to the information of data subjects over which the Companies carry out any type of processing. Likewise, this Policy seeks to safeguard the rights of data subjects at any stage of processing.

DATA CONTROLLERS

The following is the information of the Companies that act as Data Controllers of personal data within the framework of this Policy:

LEGAL NAME	TAX ID (NIT)	ADDRESS	TELEPHONE	EMAIL	POLICY LINK
Team Foods Colombia S.A.	860.000.006-4	Calle 45A Sur #21-56 Bogotá D.C.	(601) 770 9000	notificaciones@alanzateam.com	alanzateam.com/politica-de-datos-personales-alianza-team
Grasas S.A.	891.300.529-4	Calle 11 # 18-113 Buga, Valle del Cauca	(602) 237 5000	notificaciones@alanzateam.com	alanzateam.com/politica-de-datos-personales-alianza-team



2. SCOPE

This Policy must be complied with on a mandatory and strict basis by the Companies, as well as by their directors, employees and any other third party that represents them or acts on their behalf, or that has any type of legal or commercial relationship and processes personal data in the name and on behalf of the Companies. In turn, the Companies’ employees who, in the exercise of their duties, carry out operations relating to the processing of personal data must know, observe and enforce the guidelines set out in this document. All employees who work at the Companies are required to keep confidential the personal data with which they come into contact by virtue of their duties, including after the termination of their employment or contractual relationship with the Companies.

Based on Article 15 of the Political Constitution of Colombia, on Law 1581 of 2012, and on regulatory Decrees 1377 of 2013 and 886 of 2014 – now contained in Chapters 25 and 26 of Sole Decree 1074 of 2015, which developed the general framework for data protection in Colombia – ALIANZA TEAM has implemented these guidelines, by which all areas of the company and the third parties entrusted with the processing of personal data provided to ALIANZA TEAM shall be governed, in order to respect all the rights and guarantees regarding the privacy of the data subjects whose

personal data we process and to fully comply with the parameters established in the aforementioned regulations.



3. ASSOCIATED RISK(S)

This Policy also seeks to prevent and/or control the risks associated with the processing of personal data, in order to ensure the privacy and security of personal information, such as:

- Unauthorized access.
- Loss of information.
- Unauthorized modification.
- Unauthorized disclosure.
- Unconsented use.
- Legal non-compliance.



4. DEFINITIONS

The following words and concepts shall have the meanings set out below, in order to facilitate a proper understanding of this Policy:

- A. Authorization:** Prior, express and informed consent of the data subject to carry out the processing of personal data.
- B. Privacy notice:** Verbal or written communication generated by the Data Controller, addressed to the data subject for the processing of their personal data, by means of which they are informed of the existence of the information processing policies applicable to them, the manner of accessing them, and the purposes of the processing intended for the personal data.
- C. Database:** An organized set of personal data that is subject to processing.
- D. Personal data:** Any information linked to, or that may be associated with, one or more specific or identifiable natural persons. In general terms, any reference to Personal data shall be understood to include Sensitive data, unless otherwise stated or an explicit distinction is made.
- E. Sensitive data:** Sensitive data is understood to be data that affects the privacy of the data subject or whose improper use may give rise to their discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions, social or human rights organizations, or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties, as well as data relating to health, sexual life, and biometric data, among others, the capture of still or moving images, fingerprints, photographs, iris, voice, facial or palm recognition, among others.

- F. Habeas Data right:** In accordance with Article 15 of the Political Constitution of Colombia, all persons have the right to their personal and family privacy and to their good name, and the State must respect them and cause them to be respected. Likewise, they have the right to know, update and rectify the information collected about them in databases and in the files of public and private entities. In the collection, processing and circulation of data, the freedom and other guarantees enshrined in the Constitution shall be respected.
- G. Data Processor:** A natural or legal person, public or private, who, by itself or in association with others, carries out the processing of personal data on behalf of the Data Controller.
- H. Data Controller:** A natural or legal person, public or private, who, by itself or in association with others, decides on the Database and/or the processing of the data. For the purposes of this Policy, the Companies are the Data Controllers.
- I. Data subject(s):** A natural person whose personal data is subject to processing.
- J. Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.
- K. Transfer:** Occurs when the Data Controller and/or Data Processor of personal data, located in the Republic of Colombia, sends the information or personal data to a recipient who, in turn, is a data controller and is located inside or outside the country.
- L. Transmission:** The processing of personal data that involves the communication thereof inside or outside the territory of the Republic of Colombia when its purpose is the carrying out of processing by the Data Processor on behalf of the Data Controller.
- M. Data Protection Officer:** The Data Protection Officer (DPO) is the person designated by ALIANZA TEAM to ensure compliance with the Personal Data Protection Program, its policy, Law 1581 of 2012 and other applicable regulations on personal data protection.

These definitions have been established in Law 1581 of 2012, Decree 1377 of 2013 and the regulations that clarify, amend or supplement them.

5. GENERAL CONDITIONS

PRINCIPLES APPLIED TO THE PROCESSING OF PERSONAL DATA

The Companies shall carry out the processing of personal data under the following principles:

- A. Principle of legality:** The processing of data is subject to the provisions of the Law and other regulations that develop it. The collection, use, access, transfer, storage and destruction of personal data shall not be carried out unlawfully, fraudulently, by unfair means or contrary to the legislation in force.
- B. Principle of purpose:** The processing of personal data shall always be carried out in accordance with the purpose communicated to the data subject at the time of collection, which must be legitimate in accordance with the Constitution and the applicable regulations.
- C. Principle of freedom:** The processing of personal data shall only be carried out with the prior authorization of the data subject, and the data may not be obtained or disclosed without express authorization for that purpose. As an exception, data may be obtained and disclosed pursuant to a legal mandate or judicial order that waives the obligation to obtain such authorization.

- D. Principle of accuracy or quality:** The information subject to processing must be truthful, complete, accurate, up to date, verifiable and comprehensible. The processing of partial, incomplete, fragmented or misleading data is prohibited. Appropriate measures must be implemented to ensure the accuracy and sufficiency of the data. When the data subject so requests, or when the Companies deem it appropriate, the data shall be updated, rectified or deleted.
- E. Principle of transparency:** In processing, the right of the data subject to obtain from the Data Controller or the Data Processor, at any time and without restrictions, information about the existence of data concerning them must be ensured.
- F. Principle of restricted access and circulation:** Access to personal data shall be permitted only to: (i) the data subject, their successors in title or their legal representatives; (ii) third parties authorized by the data subject or by law; and (iii) public and administrative entities in the exercise of their legal functions or by judicial order.
- G. Principle of security:** Personal data must be processed under the technical, human and administrative measures necessary to ensure its security, preventing its alteration, loss, unauthorized or fraudulent consultation, use or access.
- H. Principle of confidentiality:** All persons involved in the processing of personal data that is not public in nature are required to ensure the confidentiality of the information, including after the end of their relationship with any of the tasks comprising the processing, and may only supply or communicate personal data when this corresponds to the carrying out of the activities authorized by law.
- I. Principle of temporality of information:** The data subject's information may not be supplied to third parties or to a user when it ceases to serve the purpose for which it was obtained and stored in the database. The purpose of ALIANZA TEAM's databases is established by the regulations in force, and they are not used for purposes other than those established in the data subject's authorization, in the company's privacy policies, or in those legally authorized.
- J. Comprehensive interpretation of constitutional rights:** The rights shall be interpreted in harmony and in balance with the right to information provided for in Article 20 of the Constitution and with the applicable constitutional rights.
- K. Principle of confidentiality (data under dispute):** All persons involved in the processing of personal data that is not public in nature are required to ensure the confidentiality of the information, including after the end of their relationship with any of the tasks comprising the processing, and may only supply or communicate personal data when this corresponds to the carrying out of the activities authorized by law.



6. GUIDELINES

A) AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA AND PRIVACY NOTICES

The Companies carry out the processing of personal data under the applicable regulatory parameters, pursuant to which, as a general rule and save for an applicable legal exception, they obtain Authorization from the data subjects before carrying out any type of processing. The Authorization takes into account the following fundamental parameters:

- A. Authorization:** The processing of personal data by the Companies requires, as a general rule and save for an applicable legal exception, the free, prior, express and informed consent of the data subject.
- B. Form and mechanisms for granting authorization:** The Authorization may be recorded by any mechanism that allows evidence to be obtained and ensures its subsequent consultation, which may occur: (i) in writing, (ii) orally, or (iii) through unequivocal conduct of the data subject that reasonably allows it to be concluded that Authorization was granted. Under no circumstances may silence be equated with unequivocal conduct.
- C. Evidence of Authorization:** The Companies shall maintain the records or mechanisms necessary to demonstrate when and how Authorization was obtained from the data subjects for the processing of their personal data.
- D. Cases in which Authorization is not required:** The following are events in which, in accordance with applicable law, the data subject's Authorization is not required, that is, where the matter concerns:
 - Information required by a public or administrative entity in the exercise of its legal functions or by judicial order.
 - Data of a public nature.
 - Cases of medical or health emergency.
 - Processing of information authorized by law for historical, statistical or scientific purposes.
 - Data relating to the civil registry of persons.
- E. Revocation of Authorization and/or deletion of data:** Data subjects may at any time request the Companies to delete their personal data and/or revoke the Authorization granted for processing, by submitting a claim, in accordance with the provisions of Article 15 of Law 1581 of 2012, a process that is described in Title 8 of this Policy.
- F. Authorization for the processing of sensitive data:** Where the processing of sensitive personal data is concerned, the Companies shall comply with the special requirements established by applicable law, such as informing the data subject that they are not obliged to authorize its processing, and informing them explicitly and in advance of the data that is sensitive in nature and the specific purpose of its processing.
- G. Privacy notice:** The privacy notice is the document, whether physical, electronic or in any format, that is made known to the data subject before or at the time of the collection of their personal data, and is the means by which they are informed of everything relating to the information processing policies that will be applicable to them, the ways to access them and, in general, the purposes for which their personal data has been obtained and the processing that the Companies will give to it. The Companies shall make available the privacy notices they deem appropriate for the processing they carry out, always in compliance with applicable law.

B) RIGHTS OF DATA SUBJECTS

In accordance with the provisions of Article 8 of Law 1581 of 2012, the data subject has the right to:

- A.** Know, update and rectify their personal data vis-à-vis the Companies. This right may be exercised, among others, with respect to partial, inaccurate, incomplete, fragmented or misleading data, or data whose processing is expressly prohibited or has not been authorized.
- B.** Request evidence of the Authorization granted to the Companies when they act as Data Controllers, except where it is expressly exempted as a requirement for processing, in accordance with the provisions of Article 10 of Law 1581 of 2012.
- C.** Be informed by the Companies, upon request, of the use that has been made of their personal data.
- D.** File complaints with the Superintendence of Industry and Commerce for infringements of the provisions of Law 1581 of 2012 and other regulations that amend, add to or supplement it.
- E.** Revoke the Authorization and/or request the deletion of the data when the principles, rights and constitutional and legal guarantees are not respected in the processing. Revocation and/or deletion shall proceed under the terms of Article 9 of Decree 1377 of 2013. The foregoing shall not apply in cases in which the data subject has a legal or contractual duty to remain in the database, in accordance with Article 2.2.2.25.2.6 of Decree 1074 of 2015.
- F.** Access, free of charge, their personal data that has been subject to processing.

PROCESSING OF SENSITIVE PERSONAL DATA

In the course of their commercial activity, the Companies process sensitive personal data only for specific purposes, and only insofar as it has been previously authorized by the respective data subject, always under the security and confidentiality standards corresponding to its nature. In any event, the collection of sensitive personal data shall warn that the authorization for its processing is optional and does not constitute a condition for accessing any of our products or services. In this regard, the aforementioned authorization granted by the data subjects shall comply with the special requirements established by the applicable law in this respect, such as informing the data subject explicitly and in advance of the data that is sensitive in nature and the specific purpose of its processing, among others that may be applicable. ALIANZA TEAM may process such data provided that: (a) the data subject has given their explicit authorization for such processing, except in cases where the granting of such authorization is not required by law; (b) the processing is necessary to safeguard the vital interest of the data subject and the latter is physically or legally incapacitated – in these events, the legal representatives must grant their authorization; (c) the processing relates to data that is necessary for the recognition, exercise or defense of a right in judicial proceedings; (e) the processing has a historical, statistical or scientific purpose – in this event, measures conducive to the suppression of the data subjects' identity must be adopted.

RIGHTS OF CHILDREN AND ADOLESCENTS

In general terms, ALIANZA TEAM does not process the personal data of children and adolescents; however, in exceptional cases, it may process such data provided that:

1. The data is public in nature.
2. The processing carried out by ALIANZA TEAM responds to and respects the best interests of children and adolescents.
3. The processing carried out by ALIANZA TEAM ensures respect for their fundamental rights.

Once the foregoing requirements have been met, the legal representative of the children or adolescents shall grant the authorization, after the minor has exercised their right to be heard, an opinion that shall be assessed taking into account their maturity, autonomy and capacity to understand the matter.

C) PROCEDURE FOR EXERCISING THE RIGHTS OF DATA SUBJECTS

a. Service channels

Data subjects may exercise the rights granted to them by applicable law and this Policy vis-à-vis the Companies, through the means that the Companies have implemented for this purpose, by submitting a request addressed to any of the following service channels:

Team Foods Colombia S.A.

NIT: 860.000.006-4

Address: Calle 45 A Sur No. 56 – 21, Bogotá D.C., Colombia

Telephone: 01 8000 12 7474 in Colombia or (601) 307 3980 in Bogotá

Email: notificaciones@alanzateam.com

Grasas S.A.

NIT: 891.300.529-4

Address: Calle 11 No. 18 – 113, Buga, Valle del Cauca, Colombia

Telephone: 01 8000 12 7474 in Colombia

Email: notificaciones@alanzateam.com

b. Standing to exercise the rights of data subjects

The rights of data subjects established by applicable law and indicated above may be exercised by the following persons:

- By the data subject, who must sufficiently prove their identity.
- By their successors in title, who must prove such capacity.
- By the representative and/or attorney-in-fact of the data subject, upon proof of the representation or power of attorney.
- By stipulation in favor of, or for, another (third-party beneficiary).

The rights of children and adolescents shall be exercised by the persons empowered to represent them.

c. Types of requests

The following are the types of requests that may be submitted in relation to the processing of personal data carried out by the Companies, in accordance with applicable law:

A. Inquiry: In accordance with the provisions of Article 14 of Law 1581 of 2012, the data subject, their successor in title or their representative may consult, free of charge, the data subject's personal data held in the Companies' databases. The Companies shall provide to the entitled persons all the information contained in the individual record or that is linked to the identification of the data subject. To this end, the data subject, their successor in title or their representative must submit an inquiry indicating the information they wish to know, addressed to any of the service channels indicated above. The inquiry shall be handled by the Companies within a maximum term of ten (10) business days from the date of its receipt. When it is not possible to handle the inquiry within that term, this fact shall be communicated to the interested party, stating the reasons for the delay and indicating the date on which the inquiry will be handled, which in no case may exceed five (5) business days following the expiration of the first term.

B. Claims: In accordance with the provisions of Article 15 of Law 1581 of 2012, when the data subject, their successor in title or their representative considers that the information processed by the Companies should be subject to correction, update or deletion, or notes the alleged breach of any of the duties contained in applicable law, they may submit a claim to the Companies, which shall be processed under the following rules:

1. The claim must be submitted through the service channels enabled by the Companies and indicated in this document.
2. The claim must contain, at a minimum, the following information:
 - The identity of the data subject, as well as the documents proving the identity of the applicant and the capacity in which they act, the latter in the event that they are not the data subject themselves.
 - The address or written means of communication through which the applicant expects to receive a response.
 - A clear and precise description of the facts giving rise to the claim, as well as of the personal data with respect to which one of the rights is sought to be exercised, and the specific request.
3. The maximum term that the Companies shall have to handle a claim shall be fifteen (15) business days counted from the day following the date of its receipt. When it is not possible to handle it within that term, the interested party shall be informed of the reasons for the delay and the date on which their claim will be handled, which in no case may exceed eight (8) business days following the expiration of the first term.
4. If the claim is incomplete, the interested party shall be requested, within the five (5) business days following its receipt, to remedy the deficiencies. If two (2) months elapse from the date of the request without the applicant submitting the required information, it shall be understood that they have withdrawn the claim.
5. In the event that the person who receives the claim within the Company is not competent to resolve it, they shall forward it to the appropriate party within a maximum term of two (2) business days and shall inform the interested party of the situation.
6. Once the complete claim has been received, a legend stating "claim in process" and the reason therefor shall be included in the database within a term of no more than two (2) business days. Said legend shall be maintained until the claim is decided.

– **Rectification and update:** When claims seek the rectification or update of information, the applicant must indicate the corrections to be made and provide the documentation supporting their request.

– **Revocation of authorization or Deletion of Personal data:** ALIANZA TEAM and/or the Data Processors guarantee to the data subjects whose personal data is contained in their databases, or to their successors in title, the right to request the Revocation of the authorization or to request the deletion of the information contained in their individual record or of all information linked to their identification when they consider that the parameters established by law, or those indicated in subparagraph e) of Chapter V of these Personal Data Processing Policies, are met. Likewise, the right to file claims when they note the alleged breach of Law 1581 of 2012 or of these personal data processing policies is guaranteed.

– **Procedural prerequisite (condition precedent):** In accordance with the provisions of Article 16 of Law 1581 of 2012, the data subject, successor in title and their representatives may only file a complaint with the Superintendence of Industry and Commerce once they have exhausted the inquiry or claim procedure before the Companies.

d. Person and area responsible for handling data subject requests

The area responsible within the Companies for handling data subject requests is:

Area: Vice-Presidency of Legal and Corporate Affairs.

Data subjects may submit their requests through the service channels indicated in subparagraph a) of Title 8 of this Policy.

e. Personal Data Protection Officer

In accordance with Article 2.2.2.25.4.4 of Decree 1074 of 2015, every data controller and data processor must designate a person or area that “assumes the personal data protection function” and that “shall process the requests of data subjects”, for the exercise of the rights referred to in Law 1581 of 2012 and the decree.

The function of the DATA PROTECTION OFFICER or of the area in charge of data protection at ALIANZA TEAM is to ensure the effective implementation of the policies and procedures adopted by it to comply with the regulations, the supervision of regulatory compliance, the management of security incidents and the liaison with the Superintendence of Industry and Commerce (SIC), as well as the implementation of good personal data management practices within the company.

The DATA PROTECTION OFFICER shall have the task of structuring, designing and administering the program that enables the organization to comply with the regulations on personal data protection, as well as establishing the controls of that program and its ongoing evaluation and review.

D) DUTIES OF THE COMPANIES AS DATA CONTROLLERS AND DATA PROCESSORS

The Companies acknowledge that personal data is the property of the data subjects to whom it refers and that only they may decide on it. In this regard, the Companies shall use the personal data collected solely for the purposes for which the data subject has expressly authorized its processing, or where they may carry out the processing without such Authorization for purposes

linked to the exception by virtue of which Authorization is not required, and respecting, in any event, the regulations in force on personal data protection.

Without prejudice to the foregoing, the Companies shall have the following duties as Data Controllers and Data Processors, when acting in such capacities:

a. Duties of the Companies as Data Controllers

The Companies, as Data Controllers, must comply with the following duties, without prejudice to the other provisions set out in the law and in others that govern their activity:

- Guarantee the data subject, at all times, the full and effective exercise of the Habeas Data right.
- Request and retain, under the conditions set out in Law 1581 of 2012, a copy of the respective Authorization granted by the data subject.
- Duly inform the data subject of the purpose of the collection and of the rights afforded to them by virtue of the Authorization granted.
- Retain the personal data under the security conditions necessary to prevent its alteration, loss, unauthorized or fraudulent consultation, use or access.
- Ensure that the information supplied to the Data Processors is truthful, complete, accurate, up to date, verifiable and comprehensible.
- Update the information, communicating in a timely manner to the Data Processors all updates regarding the data previously supplied to them, and adopt the other measures necessary to keep the information supplied to them up to date.
- Rectify the information when it is incorrect and communicate the relevant matter to the Data Processor.
- Supply to the Data Processors, as the case may be, only data whose processing has been previously authorized in accordance with the provisions of Law 1581 of 2012.
- Require the Data Processors, at all times, to respect the security and privacy conditions of the data subject's information.
- Process the inquiries and claims made under the terms indicated in Law 1581 of 2012.
- Inform the Data Processors when certain information is under dispute by the data subject, once the claim has been submitted and the respective procedure has not been completed.
- Inform, at the data subject's request, of the use given to their data.
- Inform the data protection authority when there are breaches of the security codes and there are risks in the administration of the data subjects' information.
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

b. Duties of the Companies as Data Processors

The Companies, when acting as Data Processors, or when the capacities of Data Controller and Data Processor concur in them, must comply with the following duties, without prejudice to the other provisions set out in the law and in others that govern their activity:

- Guarantee the data subject, at all times, the full and effective exercise of the Habeas Data right.
- Retain the information under the security conditions necessary to prevent its alteration, loss, unauthorized or fraudulent consultation, use or access.
- Carry out, in a timely manner, the update, rectification or deletion of the data under the terms of this law.
- Update the information reported by the Data Controllers within the five (5) business days counted from its receipt.
- Process the inquiries and claims made by the data subjects under the terms indicated in the Colombian personal data protection regime.
- Adopt an internal manual of policies and procedures to ensure proper compliance with the Colombian personal data protection regime and, in particular, for the handling of inquiries and claims by data subjects.
- Record in the database the legend “claim in process” in the manner regulated by law.
- Insert in the database the legend “information under judicial dispute” once notified by the competent authority of judicial proceedings relating to the quality of the personal data.
- Refrain from circulating information that is being contested by the data subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.
- Allow access to the information only to the persons who may have access to it.
- Inform the Superintendence of Industry and Commerce when there are breaches of the security codes and there are risks in the administration of the data subjects’ information.
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

E) PURPOSES OF PROCESSING

Purpose is understood to be the aim for which persons’ data has been collected. The processing of, and the purpose given to, personal data by ALIANZA TEAM and/or the data processors must be those established in the respective authorization granted by the data subject.

Without prejudice to the purposes of processing communicated to the data subjects in a timely manner and prior to processing by means of Privacy Notices and as recorded in each of the Processing Authorizations, the personal data managed by the Companies shall be collected, used, stored, updated, transmitted and/or transferred, and in general terms processed, for the following purposes:

a. In relation to the nature and activities inherent to the corporate purpose of the Companies

The processing of personal data carried out by the Companies shall have the following general purposes relating to the nature and activities inherent to the corporate purpose of the Companies, applicable to the different types of counterparties and/or data subjects whose data is subject to processing by the Companies as Data Controller:

- Manage and maintain the relationship with the data subject or with the entity to which they are linked, regardless of its nature, in order to comply with the Companies' internal policies, standard operating procedures and guidelines. This entails performing and complying with the obligations arising from such relationship, as well as carrying out the corresponding administrative and accounting management.
- Review of the information to comply with the regulations relating to due diligence at the level of SAGRILAF, PTEE Business Ethics, Prevention of Environmental Crimes and Human Rights.
- Carry out internal or external audit processes inherent to the commercial activity that the Companies conduct.
- Carry out any procedure before authorities and/or persons and/or public or private entities, with respect to which the information is relevant, as well as respond to administrative and judicial requirements, the data being deliverable for these purposes to external lawyers and advisors or auditors.
- Make calls and send communications to physical mail, email, mobile phone or mobile device, via text messages or through any other analog and/or digital means of communication, with information relevant to the data subject or to the entity with which the data subject is linked and that has a relationship with the Companies.
- Carry out any type of judicial or extrajudicial collection act or proceeding and/or exercise the rights that correspond to the Companies.
- Verify the data and information relating to the data subject or the entity with which they are linked, as well as expand the information provided through public sources.
- Attend to and manage the requests, complaints, claims or suggestions made by data subjects and by oversight bodies, including responding to or providing to the other authorities that, in the exercise of their functions and by virtue of applicable law, require the personal data.

- Manage and process information through tools that use artificial intelligence, language models (including but not limited to foundational and generative models), machine learning, advanced analytics, computer vision and intelligent automation, for the performance of activities relating to the corporate purpose of the Companies, the operational efficiency of the supply chain, information security and their relationship with each stakeholder group. In furtherance of this purpose, the Companies may, among others: (a) use AI models for the optimization of operational processes, predictive analysis of supply and demand, quality control, predictive and corrective maintenance, and supply chain management; (b) implement virtual assistants, chatbots or automated service systems for the management of requests, qualification of business opportunities, commercial prospecting and support of customers, suppliers and employees; (c) apply AI tools for the selection, evaluation, performance analytics and human talent management, ensuring human oversight in decisions that affect labor rights or that produce legal effects for persons; (d) use analytical and predictive models for fraud detection, compliance risks, audits, internal reviews and corporate due diligence; (e) process data through AI platforms for the personalization of products and services, audience profiling, market prospecting and commercial communications; (f) employ artificial vision, pattern recognition and AI systems for the management of physical security at facilities and plants; and (g) use AI tools for the analysis of financial, accounting and tax data, provided that this does not entail automated decisions that produce legal effects or significantly affect the data subject.
 - Manage security at the Companies' facilities through video surveillance systems. Insofar as this involves the processing of sensitive data such as persons' images, the information captured through video surveillance systems shall be processed with the relevant security and confidentiality measures, and the other requirements established by applicable law for the processing of sensitive personal data shall be complied with.
 - Comply with and apply the constitutional, legal and regulatory provisions set out in the Colombian legal system and applicable to the Companies.
 - Ensure and guarantee the physical and digital security of the data subject and their information, and the improvement of the visit experience at the Companies' establishments and facilities.
 - Comply with the legal, pre-contractual, contractual, post-contractual, tax, financial and accounting obligations of the Companies.
 - Comply with the Companies' Policy Guidelines.
 - Transmit, Transfer or share the information collected with different areas of the Companies and with their associated companies in Colombia and abroad, within the framework of the purposes authorized by the data subject.
- b. Respecting the personal data of our customers — corporate and consumer — and our suppliers, the purposes previously mentioned shall apply and, additionally, the following**

Commercial purposes

PURPOSES COMMON TO CORPORATE CUSTOMERS AND CONSUMER CUSTOMERS

- Inform about changes or modifications to our products or services, or about new products or services, whether or not related to the one contracted or acquired by the data subject, through any of the means of communication provided by the data subject.
- Evaluate the quality of our products and services, conduct market studies and statistical analyses for internal use, and invite data subjects to participate in marketing and promotional activities developed by the Companies, through any of the means of communication provided by the data subject.
- Facilitate the design and implementation of loyalty programs.
- Conduct internal studies on the performance of commercial relationships and market studies at all levels.
- Allow third-party companies, with which the Companies have entered into Transmission or Transfer of data agreements that include provisions to ensure the security and proper processing of personal data, to contact the data subject for the purpose of offering them goods or services of interest, insofar as this has been expressly authorized by the data subject.
- Feed the Companies' Databases with information of the data subjects through marketing activities, provided that they have expressly accepted their inclusion.

Service purposes

PURPOSES COMMON TO CORPORATE CUSTOMERS AND CONSUMER CUSTOMERS

- Share personal data, including the Transfer and Transmission of personal data, with third parties for the development of the purposes authorized by the data subject.
- Manage the use by the data subject of the various services corresponding to websites managed by the Companies, including the completion of content and forms and downloading by the data subject. Some of these websites contain marketing activities or content of interest to the data subject, which allow the Companies' Databases to be fed, which is expressly communicated to the data subjects.
- Contact the data subject after their deactivation to evaluate the resumption of the relationship, provided that the data subject has not requested the removal of their information from the database, nor revoked the authorization.

Purpose applicable only to Corporate Customers

Prepare, submit and follow up on quotations, commercial proposals and offers of goods or services of the Companies and/or request, study and follow up on quotations, commercial proposals and offers of goods or services submitted to the Companies.

Purpose applicable only to Consumer Customers

Manage the data subject's requests relating to the acquisition of products or services via electronic commerce.

Purposes applicable only to Suppliers

- Receive the products and/or services offered by the supplier.
- Manage the use by the data subject of the various services corresponding to websites managed by the Companies, including the completion of content and forms and downloading by the data subject.

WITH RESPECT TO THE PERSONAL DATA OF THE COMPANIES' JOB CANDIDATES

- Open a file on the candidate in relation to the selection process for which they apply or have been invited to participate.
- Carry out all the activities inherent to a personnel selection process, such as medical examinations, skills and competency tests, among others.
- Administer and operate, directly or through third parties, the personnel selection and recruitment processes, including the evaluation and grading of participants and the conduct of security screenings to verify due diligence at the level of the Compliance Programs' risks, verification of judicial records or the conduct of home visits, among others. Insofar as some of this information may be considered sensitive data, such as that relating to judicial records, the Companies shall comply with the special requirements contemplated in the applicable legislation for this type of data.
- Likewise, the process may also include contacting the candidate or contacting third parties through the information that the candidate has provided, including the confirmation of the personal and professional references that the candidate has listed, as well as all the information that the data subject provides as part of the selection process.
- Require attachments to the résumé, such as medical or psychometric examinations, references and employment certifications, among others. Insofar as sensitive personal data is concerned, such as that relating to health, the Companies shall comply with the special requirements contemplated in the applicable legislation for this type of data.
- Verify the documents relating to the data subject's studies, such as diplomas, transcripts, and other documents relating to their employment history, among others.
- The data may also be processed after the end of the selection process in order to consider the data subject's profile in future job openings and to contact them in the event that their profile may fit one of these.
- Send information about subsequent vacancies similar to those for which the candidate has applied.
- Even after the end of the selection process, comply with legal obligations, meet internal corporate requirements and comply with the document retention rules.

WITH RESPECT TO THE PERSONAL DATA OF THE COMPANIES' EMPLOYEES

- Store and administer in their databases the personal data of employees and former employees; as well as carry out the activities required in the contractual and post-contractual stage of the employment relationship.

- Comply with the obligations arising from the employment relationship, as well as with the constitutional, legal and regulatory provisions set out in the Colombian legal system that are applicable to the employment relationship. The foregoing may include sharing the personal data of employees — and that of their beneficiaries — with the competent judicial and administrative authorities, social security system entities (Pension Fund, EPS, ARL, Severance Fund, ICBF, Family Compensation Fund, SENA), and assisted payroll operators, as required in compliance with their legal functions and the existing labor legislation; as well as making electronic payroll reports to the DIAN and, in particular, for the generation of the electronic payroll payment voucher and the adjustment notes derived from the aforementioned document.
- Carry out the due diligence process at the level of the Compliance Programs' risks, verification of judicial records, financial behaviors or the conduct of home visits, among others, for the updating of their security screening.
- Carry out the activities inherent to human resources management within the Companies, such as payroll, affiliations to entities of the general social security system, well-being and occupational health activities, exercise of the employer's disciplinary authority, among others.
- Make the necessary payments arising from the performance of the employment contract and/or its termination, and the other social benefits that may be due in accordance with applicable law.
- Contract employment benefits with third parties, such as life insurance, medical expenses, among others.
- Notify authorized contacts in the event of emergencies during working hours or in connection with the performance thereof.
- Coordinate the professional development of employees, employees' access to the Companies' IT resources and assist in their use.
- Plan business or employee well-being activities and events.
- Transmit the information with third-party companies in Colombia and abroad when this is necessary for the development of the purposes authorized by the data subject, such as payroll management.
- Control access to the Companies' offices and plants, including the establishment of video-surveilled areas. Insofar as this involves the processing of sensitive data such as persons' images, the information captured through video surveillance systems shall be processed with the relevant security and confidentiality measures, and the other requirements established by applicable law for the processing of sensitive personal data shall be complied with.
- Carry out the processing of sensitive data such as information relating to health, medical or psychometric examinations of the employee for the purpose of carrying out the registration and follow-up of this information exclusively within the framework of the employment relationship. Insofar as sensitive personal data is concerned, such as that relating to health, the Companies shall comply with the special requirements contemplated in the applicable legislation for this type of data.

- Carry out the processing of sensitive data such as information relating to minor children for the purpose of carrying out the relevant registrations before the social security system entities, as well as to manage possible benefits and/or information that is relevant exclusively within the framework of the employment relationship, where applicable. The Companies shall comply with the special requirements contemplated in the applicable legislation for this type of data.
- Conduct training on the Companies' guidelines and policies.
- Register the data subjects in the Companies' IT systems and platforms.
- Use the personal information and images produced during the Companies' activities and events in order to share them both internally and externally through digital platforms, social networks, emails or other communication channels. This includes the creation and dissemination of material to communicate in physical, digital or audiovisual formats, provided that it has been authorized by the data subject. Insofar as this involves the processing of sensitive data such as persons' images, it shall be processed with the relevant security and confidentiality measures, and the other requirements established by applicable law for the processing of sensitive personal data shall be complied with.
- Process selection processes that the Companies have internally, with customers or in tenders, using the information contained in the employee's résumé, academic certifications and employment certifications.
- Respond to questions or requests for information made by the Companies' customers, for which the personal data of employees or former employees is relevant.
- Register, manage, and carry out the processing and filing of the information supplied in the reports and inquiries submitted through the Companies' Integrity and Labor Affairs Hotline channel.
- Maintain efficient communication with the employee in order to obtain or update the information that is useful to them by virtue of the employment/contractual relationships to which they are a party.
- Provide references to third parties on the employee's performance, in the event that the Companies are contacted by third parties for this purpose, during or after the termination of the employment relationship.
- Any other activity of a similar and/or complementary nature to those described above that is necessary to develop the employment relationship between the data subject and one of the Companies.

F) NATIONAL AND INTERNATIONAL TRANSFERS

In line with the purposes mentioned above, the Companies may store and process the personal data of third parties in (i) any country where we have facilities; and (ii) any country in which we contract service providers. These transfers are necessary to support the purposes described in this Privacy Policy. When the destination jurisdiction does not have an adequate level of data protection, the Companies shall seek the authorizations or declarations of conformity required under the law. The foregoing is without prejudice to the cases contemplated in Article 26 of Law 1581 of 2012.

In the context of the transfer for the use of platforms, artificial intelligence tools and global storage infrastructure (including the migration, hosting and processing of databases in data centers located in the United States of America or other global jurisdictions), whose servers or providers are located in jurisdictions other than Colombia, the Companies have implemented the appropriate safeguards, including Standard Contractual Clauses (SCCs), data processing agreements (DPAs) and equivalent mechanisms that ensure an adequate level of protection provided that they comply with applicable law.

G) INTERNATIONAL AND NATIONAL TRANSMISSIONS

Within the framework of the processing activities and the purposes authorized by the data subject, the Companies may Transmit data to one or more data processors located inside or outside the territory of the Republic of Colombia, insofar as the said Transmission has been authorized by the data subject. Otherwise, the Companies must establish contractual clauses or enter into personal data Transmission agreements with the Data Processors in which, among others, they establish the following:

- The scope and purposes of the processing by the Data Processor.
- The activities that the Data Processor will carry out on the data on behalf of the Companies.
- The obligations of the Data Processor towards the data subject and the Companies, which shall comprise at a minimum: (i) applying the Companies' obligations under this Policy and processing the data in accordance with the purpose that the data subjects have authorized and with applicable laws; (ii) processing, on behalf of the Companies, the personal data in accordance with the principles that protect it; (iii) safeguarding the security of the databases containing personal data; and (iv) maintaining confidentiality regarding the processing of personal data.

H) VALIDITY OF THE DATABASES

The personal data under the control of the Companies shall be retained for as long as is reasonable and necessary, in accordance with the purposes that justified the processing, having regard to the provisions applicable to the matter in question and to the administrative, accounting, fiscal, legal and historical aspects of the information. Notwithstanding the foregoing, personal data must be retained when so required to comply with a legal or contractual obligation. The Companies have adopted measures for the timely and secure deletion of their personal data.

I) VALIDITY OF THE POLICY AND AMENDMENTS

This Policy is effective as of the first (01) of June 2017, and was amended on the eighteenth (18) of June 2026.

The Companies may amend, modify or withdraw any part of the content of this Policy at any time, and where substantial changes are concerned, the data subjects shall be informed before or at the time of implementing the new policies, through the publication of the updated text on this site and/or by sending it to the data subject by another mechanism.

Any substantial change in the personal data processing policies shall be communicated in a timely manner to the data subjects through the usual means of contact and/or through the

website: <https://www.alianzateam.com/politicas/>

J) SECURITY MEASURES

In furtherance of the principle of security established in Law 1581 of 2012, the Companies shall adopt the technical, human and administrative measures necessary to ensure the security of the personal data subject to processing, thereby preventing its alteration, loss, unauthorized or fraudulent consultation, use or access.

K) AUTOMATED DECISIONS AND ARTIFICIAL INTELLIGENCE

The Companies may use artificial intelligence tools and automated decision-making systems in the conduct of their activities, provided that their implementation and use are carried out in accordance with the applicable regulations on personal data protection, information security and corporate ethical principles. In all cases, the Companies shall adopt reasonable measures to: (i) ensure transparency regarding the processing of personal data carried out by means of AI systems and facilitate the exercise of the rights of data subjects; (ii) implement adequate human oversight mechanisms when automated decisions may produce legal effects or significant impacts on data subjects; (iii) identify, assess, document and mitigate the risks associated with the use of AI systems, and carry out data protection impact assessments when the nature, scope or purpose of the processing entails high risks to the rights and freedoms of data subjects; (iv) adopt measures to ensure the quality, accuracy, relevance and minimization of the data used by AI systems, among others.

The Companies may refrain from implementing or using AI systems when risks are identified that cannot be reasonably mitigated, or when there is a significant probability of an adverse effect on the rights of data subjects.



7. ANNEXES

No annexes were listed in the source document at the time this Policy was issued.



8. CHANGE CONTROL

Change Control

VERSION	DATE	DESCRIPTION OF CHANGE
006	2026-05-12	Purposes and controls associated with the responsible use of AI within the organization are included.
005	2025-09-18	The purposes and the processing of sensitive data are updated; the rights-of-children-and-adolescents approach to processing and definitions are included.
004	2024-06-13	No changes apply to the current version; it is placed in cycle for review and approval of the document, in accordance with the guidelines of TE-SIG-PR-001 Documentation Management, section 6.2.4 — all Management System documents are reviewed and updated every two years.
003	2024-02-27	The wording and structure of this Policy are modified; the information of the Data Controllers is specified; functions are added to the Personal Data Protection Officer; the purposes of processing are categorized; a modification date is included.
002	2020-11-11	No changes apply to the current version; it is placed in cycle for review and approval of the document, in accordance with the guidelines of TE-SIG-PR-001 Documentation Management, section 6.2.4 — all Management System documents are reviewed and updated every two years.
002	2017-06-01	Change control in red.
001	2013-07-27	Issuance of the document.

CREATED BY	EDITED BY	REVIEWED BY	APPROVED BY
JUAN DAVID PEREZ ESPINOSA Quality Assistant	GRETTA MARTINEZ BRICEÑO Compliance Analyst	JUAN SEBASTIAN NINO ROMERO Vice-President of Corporate Affairs	LINA MARIA MUÑOZ VARELA Compliance Officer