Alianza Team

PERSONAL DATA PROCESSING POLICY

Code: TE-JUR-PO-003	Type: POLICY	Effective date: 2025-09-18	Version: 005

1. OBJECTIVE:

The objective of this personal data processing policy (hereinafter, the "Policy")—in which Team Foods Colombia S.A. and Grasas S.A. act as Data Controllers (hereinafter the "Companies," without prejudice to the fact that the reference should be understood as the entity that applies in each case)—is to guarantee compliance with the applicable law regarding personal data protection, with respect to the information of the data subjects on which the Companies perform any type of processing. This Policy also seeks to ensure the rights of the data subjects in any phase of processing.

DATA CONTROLLERS

Here is the information for the Companies that act as data controllers for personal data within the framework of this Policy:

Company	Tax Nit.	Address	Phone	Email	Link
Team Foods Colombia S.A.	860.000.006-4	Calle 45A Sur#21-56 Bogotá D.C.	(601) 770 9000	notificaciones@alianzateam.com	https://alianzateam.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@alianzateam.com	https://alianzateam.com/politica-de-datos-personales-alianza-team/

2. SCOPE:

This Policy must be strictly and obligatorily followed by the Companies, as well as by their senior management, employees, and any other third party that represents them or acts on their behalf, or has any type of legal or commercial relationship that involves the processing of personal data on behalf of and for the benefit of the Companies. Additionally, employees of the Companies who, in the course of their duties, perform operations related to personal data processing must know, respect, and enforce the guidelines of this document. All employees who work at the Companies are obligated to maintain the confidentiality of the personal data they come into contact with due to their roles, even after their employment or contractual relationship with the Companies has ended.

Based on Article 15 of the Political Constitution of Colombia, Law 1581 of 2012, and regulatory decrees 1377 of 2013 and 886 of 2014—now contained in chapters 25 and 26 of the Single Decree 1074 of 2015—which established the general framework for data protection in Colombia, ALIANZA TEAM has implemented these guidelines. These guidelines will govern all areas of the company and any third parties entrusted with processing personal data provided to ALIANZA TEAM, in order to respect all rights and guarantees regarding the privacy of data subjects 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 risks associated with personal data processing to ensure the privacy and security of personal information, such as:

1. **Unauthorized access.**
2. **Loss of information.**
3. **Unauthorized modification.**
4. **Unauthorized disclosure.**
5. **Unconsented use.**
6. **Legal non-compliance.**

4. DEFINITIONS :

The words and concepts below will have the meanings specified to facilitate a proper understanding of this Policy:

A. **Authorization:** Prior, express, and informed consent from the data subject for the processing of personal data.

B. **Privacy Notice:** A verbal or written communication generated by the Data Controller, addressed to the Data Subject for the Processing of their personal data, which informs them about the existence of applicable information processing policies, how to access them, and the purposes for which the personal data is intended to be used.

C. **Database:** An organized set of personal data that is subject to processing.

D. **Personal Data:** Any information linked to or that can be associated with one or more specific or identifiable natural persons. In general, when referring to Personal Data, it is understood to include Sensitive Data, unless otherwise stated or an explicit distinction is made.

E. **Sensitive Data:** Data that affects the data subject's privacy or whose improper use can lead to discrimination. This includes information revealing racial or ethnic origin, political views, religious or philosophical beliefs, membership in unions, social or human rights organizations, or political parties, as well as data related to health, sexual life, and biometric data. Examples of biometric data include still or moving images, fingerprints, photographs, iris scans, and voice or facial recognition.

F. **Habeas Data Right:** In accordance with Article 15 of the Political Constitution of Colombia, all individuals have the right to personal and family privacy and to their good name, and the State must respect and enforce these rights. Similarly, they have the right to know, update, and correct information collected about them in databases and files of public and private entities. The collection, processing, and circulation of data must respect freedom and other guarantees established in the Constitution.

G. **Data Processor:** A natural or legal person, public or private, who, alone or in association with others, processes personal data on behalf of the Data Controller.

H. **Data Controller:** A natural or legal person, public or private, who, alone 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):** The 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 is also a Data Controller and is located inside or outside the country.

L. **Transmission:** The processing of personal data that involves communicating the data inside or outside the territory of the Republic of Colombia when the purpose is for a Processor to perform processing on behalf of the Controller.

M. **Data Protection Officer:** The Data Protection Officer (DPO) is the person designated by ALIANZA TEAM S.A. to ensure compliance with the Personal Data Protection Program, its policy, Law 1581 of 2012, and other applicable regulations regarding personal data protection.

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

5. GENERAL CONDITIONS:

PRINCIPLES APPLIED TO THE PROCESSING OF PERSONAL DATA

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

A. **Principle of Legality:** Data processing is subject to what is established in the Law and in other provisions that develop it. The collection, use, access, transfer, storage, and destruction of personal data are not carried out illegally, fraudulently, by unfair means, or in a manner contrary to current legislation.

B. **Principle of Purpose:** The processing of personal data will always be carried out in accordance with the purpose that was communicated to the Data Subject at the time of collection. This purpose must be legitimate according to the Constitution and applicable regulations.

C. **Principle of Freedom:** The processing of personal data will only be carried out with the prior authorization of the Data Subject, and data may not be obtained or disclosed without express authorization for that purpose. An exception may be made if the data is obtained and disclosed by legal mandate or a court order that waives the obligation to obtain the aforementioned authorization.

D. **Principle of Truthfulness or Quality:** The information subject to processing must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The processing of partial, incomplete, fragmented, or misleading data is prohibited. Appropriate measures must be implemented to guarantee the accuracy and sufficiency of the data. When the Data Subject requests it or when the Companies deem it relevant, the data will be updated, rectified, or deleted.

E. **Principle of Transparency:** The processing must guarantee the right of the data subject to obtain from the Data Controller or Processor, at any time and without restrictions, information about the existence of data that concerns them.

F. **Principle of Restricted Access and Circulation:** Access to personal data will only be permitted to: i) the Data Subject, their successors, or their legal representatives ; ii) third parties authorized by the Data Subject or the law ; and iii) public and administrative entities in the exercise of their legal functions or by court order.

G. **Principle of Security:** Personal data must be processed with the necessary technical, human, and administrative measures to guarantee its security, preventing its alteration, loss, unauthorized or fraudulent consultation, use, or access.

H. **Principle of Confidentiality:** All individuals involved in the processing of non-public personal data are obligated to guarantee the confidentiality of the information. They must do so even after their relationship with any of the tasks that comprise the processing has ended. They may only provide or communicate personal data when it corresponds to the development of activities authorized by law.

I. **Principle of Information Temporality:** The Data Subject's information may not be provided to third parties or users 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 current regulations and is not used for purposes other than those established in the Data Subject's authorization, in the company's privacy policies, or those legally authorized.

J. **Principle of Comprehensive Interpretation of Constitutional Rights:** The rights will be interpreted in harmony and in balance with the right to information provided in Article 20 of the Constitution and with the applicable constitutional rights. The principle of confidentiality requires that all persons involved in the processing of non-public personal data guarantee the confidentiality of the information, even after their relationship with the processing tasks has ended.

6. GUIDELINES:

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

The Companies process personal data under applicable legal parameters, in accordance with which, as a general rule and unless a legal exception applies, 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 generally requires the free, prior, express, and informed consent of the Data Subject, unless a legal exception applies.

B. **Form and Mechanisms for Granting Authorization:** Authorization can be documented by any mechanism that allows for proof and guarantees its later consultation. This can be done: i) in writing, ii) orally, or iii) through the Data Subject's unequivocal actions that reasonably lead to the conclusion that Authorization was granted. Silence can never be considered an unequivocal action.

C. **Proof of Authorization:** The Companies will maintain the necessary records or mechanisms 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 Necessary:** The following are events where, in accordance with applicable law, the Data Subject's Authorization is not necessary:

i. Information required by a public or administrative entity in the exercise of its legal functions or by court order.

ii. Public data.

iii. Medical or sanitary emergencies.

iv. Processing of information authorized by law for historical, statistical, or scientific purposes.

v. Data related to the civil registry of individuals.

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 Article 15 of Law 1581 of 2012, a process described in section 8 of this Policy.

F. **Authorization for the Processing of Sensitive Data:** When processing sensitive personal data, the Companies will comply with the special requirements established by applicable law. This includes informing the Data Subject that they are not obligated to authorize the processing, and explicitly and beforehand informing them which data is

sensitive and the specific purpose of its processing.

G. **Privacy Notice:** The privacy notice is a document in physical, electronic, or any other format that is made known to the data subject before or at the time of collecting their personal data. It is the means by which they are informed about everything related to the information processing policies that will apply to them, the ways to access them, and, in general, the purposes for which their personal data has been obtained and the processing the Companies will give it. The Companies will provide the privacy notices that they find relevant for the processing they carry out, always in compliance with applicable law.

B) RIGHTS OF THE DATA SUBJECTS

In accordance with what is established in Article 8 of Law 1581 of 2012, the Data Subject has the right to:

A. Know, update, and correct their personal data with the Companies. This right can be exercised, among other things, with respect to partial, inaccurate, incomplete, fragmented, or misleading data, or data whose processing is expressly prohibited or has not been authorized.

B. Request proof of the Authorization granted to the Companies when they act as Data Controllers, unless it is expressly exempted as a requirement for processing, in accordance with what is provided in Article 10 of Law 1581 of 2012.

C. Be informed by the Companies, upon request, about the use that has been made of their personal data.

D. File complaints with the Superintendence of Industry and Commerce for violations of Law 1581 of 2012 and other regulations that modify, add to, or supplement it.

E. Revoke Authorization and/or request the deletion of data when the processing does not respect constitutional and legal principles, rights, and guarantees. Revocation and/or deletion will proceed in the terms of Article 9 of Decree 1377 of 2013. This will not apply in cases where 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 their personal data that has been processed, free of charge.

G. PROCESSING OF SENSITIVE PERSONAL DATA:

In the development of their commercial activity, the Companies only process sensitive personal data for specific purposes, and as long as it has been previously authorized by the respective Data Subject. This is always done under the security and confidentiality standards corresponding to its nature. In any case, the collection of sensitive personal data will state that authorizing its processing is optional and does not constitute a condition for accessing any of our products or services. In this sense, the aforementioned authorization granted by the Data Subjects will comply with the special requirements established by applicable law, such as explicitly and beforehand informing the Data Subject which data is sensitive and the specific

purpose of its processing. ALIANZA TEAM may process it as long as:

A. The Data Subject has given their explicit authorization for such processing, except in cases where the law does not require such authorization.

B. The processing is necessary to protect the vital interest of the data subject and they are physically or legally incapacitated. In these events, the legal representatives must grant their authorization.

C. The processing refers to data that is necessary for the recognition, exercise, or defense of a right in a judicial process.

D. The processing has a historical, statistical, or scientific purpose. In this event, measures must be adopted to suppress the identity of the Data Subjects.

H. RIGHTS OF CHILDREN AND ADOLESCENTS:

In general terms, ALIANZA TEAM does not process personal data of children and adolescents. However, in exceptional cases, it may process such data as long as:

A. It is public data.

B. The processing performed by ALIANZA TEAM responds to and respects the best interests of the children and adolescents.

C. The processing performed by ALIANZA TEAM ensures the respect of their fundamental rights.

Once the above requirements are met, the legal representative of the children or adolescents will grant the authorization, after the minor exercises their right to be heard, and their opinion will be valued considering their maturity, autonomy, and capacity to understand the matter.

C) PROCEDURE FOR EXERCISING THE RIGHTS OF THE DATA SUBJECTS

A. **Service Channels:** Data Subjects may exercise their rights granted by applicable law and this Policy with the Companies by submitting a request to one 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.**
Phone: **01 8000 12 7474 en Colombia o (601) 307 3980 in Bogotá**
Email: **notificaciones@alianzateam.com**

Grasas S.A.

NIT: **891.300.529-4**

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

Phone: **01 8000 12 7474 en Colombia**

Email: **notificaciones@alianzateam.com**

B. **Legitimacy for Exercising Data Subjects' Rights:** The rights of the Data Subjects established in applicable law and indicated above may be exercised by the following persons:

i. The Data Subject, who must sufficiently prove their identity.

ii. Their successors, who must prove this status.

iii. The representative and/or attorney-in-fact of the Data Subject, by providing proof of representation or power of attorney.

iv. By stipulation in favor of or for another.

The rights of children or adolescents will be exercised by the people who are authorized to represent them.

C. **Types of Requests:** The following are the types of requests that can be made in relation to the processing of personal data by the Companies, in accordance with applicable law:

i. Consultation: In accordance with Article 14 of Law 1581 of 2012, the Data Subject, their successor, or their representative may consult the Data Subject's personal data that is in the Companies' databases, free of charge. The Companies will provide legitimate persons with all the information contained in the individual record or that is linked to the Data Subject's identification.

For this purpose, the Data Subject, their successor, or their representative must submit a query indicating the information they wish to know, addressed to any of the service channels mentioned above. The Companies will respond to the query within a maximum of ten (10) business days from the date of its receipt. If it is not possible to respond within that time frame, the interested party will be informed of the reasons for the delay and the date on which their query will be answered, which can in no case exceed five (5) business days following the expiration of the initial term.

ii. Claims: In accordance with Article 15 of Law 1581 of 2012, when the Data Subject, their successor, or their representative believes that the information processed by the Companies should be corrected, updated, or deleted, or they notice an alleged non-compliance with any of the duties contained in applicable law, they may file a claim with the Companies. This will 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:

   A. The identity of the Data Subject and documents proving the identity of the applicant and the capacity in which they are acting (in case they are not the Data Subject themselves).

   B. The address or written communication method through which the applicant expects to receive a response.

   C. Clear and precise description of the facts leading to the claim, as well as the personal data regarding which they seek to exercise their rights and the specific request.

3. The maximum time the Companies will have to respond to a claim will be fifteen (15) business days from the day after its receipt. If it is not possible to respond within that time frame, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which can in no case exceed eight (8) business days following the expiration of the initial term.

4. If the claim is incomplete, the interested party will be required to correct the deficiencies within five (5) business days following the receipt of the claim. If two (2) months pass from the date of the request without the applicant providing the required information, the claim will be considered withdrawn.

5. If the person who receives the claim within the Company is not competent to resolve it, they will transfer it to the appropriate person within a maximum of two (2) business days and will inform the interested party of the situation.

6. Once the complete claim is received, a note will be included in the database that says "claim in process" and the reason for it, within a term no longer than two (2) business days. This note must be kept until the claim is resolved.

   1. Rectification and updating: When the claims are for the purpose of rectifying or updating information, the applicant must indicate the corrections to be made and provide documentation that supports their request.

   2. **Revocation of Authorization or Deletion of Personal Data:** ALIANZA TEAM and/or the Processors guarantee the right of Data Subjects in their databases or their successors to request the revocation of authorization or the deletion of information contained in their individual record or any information linked to their identification when they believe the parameters established by law are met. The right to file claims is also guaranteed when they notice an alleged non-compliance with Law 1581 of 2012 or the present Personal Data Processing Policies.

3. Procedural Requirement: In accordance with Article 16 of Law 1581 of 2012, the Data Subject, their successor, and their representatives may only file a complaint with the Superintendence of Industry and Commerce once they have exhausted the consultation or claim process with the Companies.

D. Person and Area Responsible for Responding to Data Subjects' Requests: The area within the Companies responsible for responding to Data Subjects' requests is the Legal and Corporate Affairs Vice Presidency.

Data Subjects may submit their requests through the service channels indicated in section 8, letter a) of this Policy.

E. Data Protection Officer: In accordance with Article 2.2.2.25.4.4 of Decree 1074 of 2015, every Data Controller and Processor must designate a person or area to "assume the function of personal data protection" and to "process the requests of the 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 the area in charge of data protection at ALIANZA TEAM is to ensure the effective implementation of the policies and procedures adopted to comply with regulations, supervise regulatory compliance, manage security incidents, and serve as a liaison with the Superintendence of Industry and Commerce (SIC). The DPO will also be responsible for implementing good personal data management practices within the company. The DATA PROTECTION OFFICER will be tasked with structuring, designing, and managing the program that allows the organization to comply with personal data protection regulations, as well as establishing the controls for that program, its evaluation, and continuous review.

F. DUTIES OF THE COMPANIES AS DATA CONTROLLERS AND PROCESSORS: The Companies recognize that personal data is the property of the Data Subjects it refers to and that only they can make decisions about it. In this sense, the Companies will use the collected personal data only for the purposes for which the Data Subject has expressly authorized its processing. They will also process it when they can do so without authorization, for purposes linked to the exception for which no authorization is required, and will always respect current regulations on personal data protection.

Without prejudice to the above, the Companies will have the following duties as Data Controllers and Processors, when acting in these capacities:

A. Duties of the Companies as Data Controllers: The Companies, as Data Controllers, must fulfill the following duties, without prejudice to other provisions in the law and other regulations governing their activity:

i. Guarantee the Data Subject, at all times, the full and effective exercise of the Habeas Data right.

ii. Request and keep a copy of the respective Authorization granted by the Data Subject, under the conditions provided in Law 1581 of 2012.

iii. Properly inform the Data Subject about the purpose of the collection and the rights they have by virtue of the Authorization granted.

iv. Keep personal data under the necessary security conditions to prevent its alteration, loss, unauthorized or fraudulent consultation, use, or access.

v. Ensure that the information supplied to the Data Processors is truthful, complete, accurate, up-to-date, verifiable, and understandable.

vi. Update the information, communicating all changes regarding the data previously supplied to the Data Processors in a timely manner and adopting other necessary measures to keep the information supplied to them updated.

vii. Rectify the information when it is incorrect and communicate the relevant changes to the Data Processor.

viii. Supply Data Processors, as the case may be, only with data whose processing is previously authorized in accordance with Law 1581 of 2012.

ix. At all times, require Data Processors to respect the security and privacy conditions of the Data Subject's information.

x. Process consultations and claims submitted in the terms specified in Law 1581 of 2012.

xi. Inform the Data Processors when certain information is being disputed by the Data Subject, once a claim has been filed and the respective process has not concluded.

xii. Inform the Data Subject, upon their request, about the use of their data.

xiii. Inform the data protection authority when security codes are violated and there are risks in the administration of the Data Subjects' information.

xiv. 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 they concurrently hold the roles of Data Controller and Data Processor, must fulfill the following duties, without prejudice to other provisions in the law and other regulations governing their activity:

i. Guarantee the Data Subject, at all times, the full and effective exercise of the Habeas Data right.

ii. Keep the information under the necessary security conditions to prevent its alteration, loss, unauthorized or fraudulent consultation, use, or access.

iii. Timely update, rectify, or delete the data in the terms of the present law.

iv. Update the information reported by the Data Controllers within five (5) business days from its receipt.

v. Process consultations and claims filed by the Data Subjects in the terms specified in the Colombian personal data protection regime.

vi. Adopt an internal manual of policies and procedures to ensure proper compliance with the Colombian personal data protection regime, and especially for responding to consultations and claims from Data Subjects.

vii. Register the legend "claim in process" in the database in the manner regulated by law.

viii. Insert the legend "information in judicial dispute" in the database once notified by the competent authority about judicial processes related to the quality of the personal data.

ix. Refrain from circulating information that is being disputed by the data subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.

x. Allow access to the information only to people who are authorized to have access to it.

xi. Inform the Superintendence of Industry and Commerce when security codes are violated and there are risks in the administration of the Data Subjects' information.

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

E. **PURPOSES OF PROCESSING:** The purpose is the reason for which people's data has been collected. The processing and the purpose given to personal data by ALIANZA TEAM and/or the processors must be those established in the respective authorization granted by the Data Subject.

Without prejudice to the purposes of the processing informed to the Data Subjects in a timely manner and prior to processing through Privacy Notices and as stated in each of the Authorizations for Processing, the personal data managed by the Companies will be collected, used, stored, updated, transmitted, and/or transferred, and in general will be processed, for the following purposes:

A. **In relation to the nature and activities of the Companies' corporate purpose:** The processing of personal data carried out by the Companies will have the following general purposes related to the nature and activities of the Companies' corporate purpose, applicable to the different types of counterparties and/or Data Subjects whose data is processed by the Companies as Data Controller:

i. Manage and maintain the relationship with the Data Subject or with the entity they are linked to, regardless of its nature, in order to comply with internal policies, standard operating procedures, and the Companies' guidelines. This implies executing and fulfilling the obligations derived from this relationship, as well as carrying out the corresponding administrative and accounting management.

ii. Review information to comply with regulations related to due diligence at the SAGRILAFT, Business Ethics PTEE, Environmental Crimes Prevention, and Human Rights levels.

iii. Carry out internal or external audit processes related to the commercial activity that the Companies perform.

iv. Handle any procedures with authorities and/or public or private individuals and/or entities, to whom the information is relevant, as well as to address administrative and judicial requirements, and the data may be given to external lawyers, advisors, or auditors for these purposes.

v. Make calls and send communications to physical mail, email, cell phone, or mobile device, via text messages or through any other similar and/or digital communication means, with information relevant to the Data Subject or the entity with which the Data Subject is linked and that has a relationship with the Companies.

vi. Carry out any type of act or diligence of judicial or extrajudicial collection and/or exercise the rights that correspond to the Companies.

vii. Verify data and information related to the Data Subject or the entity they are linked to, as well as expand the information provided through public sources.

viii. Address and manage requests, complaints, claims, or suggestions made by Data Subjects and control bodies, including responding or providing personal data to other authorities that require it in the exercise of their functions and by virtue of applicable law.

ix. Manage and process information through tools that use artificial intelligence, to fulfill activities related to the corporate purpose of the companies and their relationship with each interest group.

x. Manage security in the Companies' facilities through video surveillance systems. As this involves the processing of sensitive data such as people's images, the information captured through video surveillance systems will be processed with the relevant security and confidentiality measures. Compliance with other requirements established by applicable law for the processing of sensitive personal data will also be ensured.

x. Comply with and apply the constitutional, legal, and regulatory provisions provided in the Colombian legal system and applicable to the Companies.

xii. 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.

xiii. Comply with the Companies' legal, pre-contractual, contractual, post-contractual, tax, financial, and accounting obligations.

xiv. Comply with the Companies' Policy Guidelines.

xv. Transmit, Transfer, or share the collected information with different areas of the Companies and their associated companies in Colombia and abroad, within the framework of the purposes authorized by the Data Subject.

B. **With respect to the personal data of our corporate and consumer clients, and our suppliers, the previously mentioned purposes will apply, plus the following:**

- Commercial Purposes:

- Purposes common to Corporate Clients and Consumer Clients:

i. Inform about changes or modifications to our products or services, or about new products or services, whether or not they are related to the one contracted or acquired by the Data Subject, through any of the communication means provided by the Data Subject.

ii. 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 communication means provided by the Data Subject.

iii. Facilitate the design and implementation of loyalty programs.

iv. Conduct internal studies on compliance with commercial relationships and market studies at all levels.

v. Allow third-party companies—with whom the Companies have entered into data Transmission or Transfer contracts that include provisions to ensure the security and proper processing of personal data—to contact the Data Subject to offer them goods or services of interest, to the extent that this has been expressly authorized by the data subject.

vi. Populate the Companies' databases with information from Data Subjects through marketing activities, as long as they have expressly agreed to their inclusion.

- **Service Purposes:**

Purposes common to Corporate Clients and Consumer Clients:

i. 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.

ii. Manage the Data Subject's use of the various services corresponding to websites managed by the Companies, including filling out 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 allows the Companies' databases to be populated, and this is explicitly communicated to the Data Subjects.

iii. Contact the Data Subject after their inactivity to evaluate the resumption of the relationship, as long as the Data Subject has not requested the removal of their information from the database or revoked the authorization.

- **Purpose applicable only to Corporate Clients:** Prepare, present, and follow up on quotes, commercial proposals, and offers of goods or services from the Companies and/or request, study, and follow up on quotes, commercial proposals, and offers of goods or services presented to the Companies.
- **Purpose applicable only to Consumer Clients:** Manage the Data Subject's requests related to the acquisition of products or services via e-commerce.
- **Purposes applicable only to Suppliers:**

i. Receive the products and/or services offered by the supplier.

ii. Manage the Data Subject's use of the various services corresponding to websites managed by the Companies, including filling out content and forms and downloading by the Data Subject.

- **With respect to the personal data of the Companies' job candidates:**

i. Open a file on the candidate in relation to the selection process they are applying for or have been invited to participate in.

ii. Carry out all activities typical of a personnel selection process such as medical exams, skills and competency tests, among others.

iii. Administer and operate, directly or through third parties, the selection and hiring processes, including the evaluation and qualification of participants and the performance of security studies to verify due diligence at the risk level of the Compliance Programs, verification of judicial records, or conducting home visits, among others. To the extent that some of this information may be considered sensitive data, such as that related to judicial records, the Companies will comply with the special requirements contemplated in the applicable legislation for this type of data.

iv. The process may also include contacting the candidate or contacting third parties through the information that the candidate has provided, including the confirmation of personal and work references that the candidate has provided, as well as all the information that the data subject provides as part of the selection process.

v. Request resume attachments such as medical or psychotechnical exams, references, and work certifications, among others. To the extent that this involves sensitive personal data such as that related to health, the Companies will comply with the special requirements contemplated in the applicable legislation for this type of data.

vi. Verify documents related to the data subject's studies, such as diplomas, grade transcripts, and other documents related to their work history, among others.

vii. Data may also be processed after the selection process has ended to consider the data subject's profile for future job openings and to contact them if their profile may be suitable for one of these.

viii. Send information about subsequent job openings similar to those for which the candidate has applied.

ix. Even after the selection process has ended, comply with legal obligations, internal corporate requirements, and document retention rules.

- **With respect to the personal data of the Companies' employees:**

i. Store and manage the personal data of employees and former employees in their databases. Also, perform the activities required in the contractual and post-contractual stage of the employment relationship.

ii. Comply with the obligations derived from the employment relationship, as well as the constitutional, legal, and regulatory provisions provided in the Colombian legal system that are applicable to the employment relationship. This may include sharing the personal data of employees and their beneficiaries with competent judicial and administrative authorities, social security system entities (Pension Fund, EPS, ARL, Severance Fund, ICBF, Family Compensation Fund, SENA), and assisted payroll operators. This is required to comply with their legal functions and existing labor legislation, and especially for the generation of electronic payroll payment support and the adjustment notes that arise from that document.

iii. Carry out the due diligence process at the risk level of the Compliance Programs, verification of judicial records, financial behavior, or conducting home visits, among others, to update their security study.

iv. Develop the activities inherent to human resources management within the Companies, such as payroll, affiliations with general social security system entities, wellness and occupational health activities, exercising the employer's disciplinary authority, among others.

v. Make the necessary payments derived from the execution of the employment contract and/or its termination, and other social benefits that may apply in accordance with applicable law.

vi. Contract for employee benefits with third parties, such as life insurance, medical expenses, among others.

vii. Notify authorized contacts in case of emergencies during work hours or as a result of the work being performed.

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

ix. Plan business or work wellness activities and events.

x. Transmit information to third-party companies in Colombia and abroad when necessary for the development of the purposes authorized by the Data Subject, such as payroll management.

xi. Control access to the Companies' offices and plants, including the establishment of video-monitored zones. To the extent that this involves the processing of sensitive data such as people's images, the information captured through video surveillance systems will be processed with the relevant security and confidentiality measures, and compliance with other requirements established by applicable law for the processing of sensitive personal data will be ensured.

xii. Carry out the processing of sensitive data such as information related to health, medical, or psychotechnical exams of the employee for the purpose of carrying out the registration and monitoring of this information exclusively within the framework of the employment relationship. To the extent that this involves sensitive personal data such as that related to health, the Companies will comply with the special requirements contemplated in the applicable legislation for this type of data.

xiii. Carry out the processing of sensitive data such as information related to minor children for the purpose of carrying out the relevant registrations with 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, if applicable. The Companies will comply with the special requirements contemplated in the applicable legislation for this type of data.

xiv. Provide training on the Companies' guidelines and policies.

xv. Register Data Subjects in the Companies' computer systems and platforms.

xvi. Use personal information and images produced during the Companies' activities and events to share them 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, as long as it has been authorized by the Data Subject. To the extent that this involves the processing of sensitive data such as people's images, it will be processed with the relevant security and confidentiality measures, and compliance with other requirements established by applicable law for the processing of sensitive personal data will be ensured.

xvii. Process selection processes that the Companies have internally, with clients, or for tenders, using the information contained in the employee's resume, academic certifications, and work certifications.

xviii. Respond to questions or requests for information made by the Companies' clients, for which the personal data of employees or former employees is relevant.

xix. Register, manage, and carry out the processing and archiving of the information supplied in the reports and consultations submitted through the Companies' Integrity and Labor Affairs Line Channel.

xx. Maintain efficient communication with the employee to obtain or update information that is useful by virtue of the employment/contractual relationships in which they are a part.

xxi. Give references to third parties about the employee's performance, in case the Companies are contacted by third parties for this purpose, during or after the termination of the employment relationship.

xxii. Any other activity of a similar and/or complementary nature to those previously described that are necessary to develop the employment relationship between the data subject and one of the Companies.

F. **NATIONAL AND INTERNATIONAL TRANSFERS:** The Companies may, as long as the Data Subject authorizes it, Transfer personal data to third parties, who may be located in Colombia or in jurisdictions other than Colombia. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Superintendence of Industry and Commerce on the matter, which can in no case be lower than those required by Law 1581 of 2012.

The above is without prejudice to the cases contemplated in Article 26 of Law 1581 of 2012. In cases not contemplated as an exception, the Companies will obtain a declaration of conformity regarding the international transfer of personal data from the Superintendence of Industry and Commerce.

In any case, the third parties to whom the Companies Transfer data will at all times comply with confidentiality and security obligations that guarantee the integrity, confidentiality, and security of the data. The third parties who receive the data may process it as Data Controllers, and for the purposes that have been authorized by the Data Subject. In the case of Transfers, the Data Subject will be informed of the mechanisms to exercise their rights and the identification of the new Data Controller.

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 processors located inside or outside the territory of the Republic of Colombia, to the extent that the Transmission has been authorized by the Data Subject. Otherwise, the Companies must establish contractual clauses or enter into personal data Transmission contracts with the Data Processors in which, among other things, they establish the following:

A. The scope and purposes of the processing by the Processor.

B. The activities that the Processor will perform on the data on behalf of the Companies.

C. The obligations of the Processor to the Data Subject and the Companies, which will include at a minimum: (i) applying the Companies' obligations under this Policy and performing data processing in accordance with the purpose that the Data Subjects have authorized and with applicable laws; (ii) processing personal data on behalf of

the Companies in accordance with the principles that protect them; (iii) safeguarding the security of the databases that contain personal data ; and (iv) maintaining confidentiality with respect to the processing of personal data.

H. **VALIDITY OF DATABASES:** Personal data under the control of the Companies will be kept for a reasonable and necessary time, in accordance with the purposes that justified the processing, taking into account the provisions applicable to the matter in question and the administrative, accounting, tax, legal, and historical aspects of the information. Notwithstanding the foregoing, personal data must be kept when 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. **POLICY VALIDITY AND MODIFICATIONS:** This Policy is effective as of June 1, 2017, and was modified on September 16, 2025. The Companies may amend, modify, or withdraw any part of the content of this Policy at any time, and when there are substantial changes, the Data Subjects will be informed before or at the time of implementing the new policies. This will be done by publishing the updated text on this site and/or by sending it to the personal data subject through another mechanism. Any substantial changes in the personal data processing policies will be communicated to the data subjects in a timely manner through the usual contact methods and/or through the website:

https://www.alianzateam.com/politicas/

J. **SECURITY MEASURES:** In accordance with the principle of security established in Law 1581 of 2012, the Companies will adopt the necessary technical, human, and administrative measures to guarantee the security of the personal data subject to processing, thus preventing its alteration, loss, unauthorized or fraudulent consultation, use, or access.

7. APPENDICES:

[TE-JUR-MA-003]: PROCEDURE MANUAL - V001 - MANUAL

INCIDENT MANAGEMENT -V001 - FORM

RIGHTS RESPONSE - V001 - FORM

8. CONTROL DE CAMBIOS:

Control de **Cambios**

Version	Date	Brief description of the change
003	2024-02-27	The wording and structure of this Policy are modified, the information of the Controllers is specified, functions are included for the Personal Data Protection Officer, the purposes of the processing are categorized, and the modification date is included.

Version	Date	Brief description of the change
002	2020-11-11	No changes apply to the current version; it is placed in a cycle for review and approval of the document, according to the guidelines of TE-SIG-PR-001 DOCUMENT MANAGEMENT section 6.2.4. All documents in the Management System are reviewed and updated every two years.
002	2017-06-01	Change control in red
001	2013-07-27	Document issued

Created By	Edited By	Reviewed By	In Testing	Approved By
JUAN DAVID PÉREZ ESPINOSA QUALITY ASSISTANT	**GRETTA MARTINEZ BRICEÑO** ANALYST	**JUAN SEBASTIAN NINO ROMERO** COMPLIANCE OFFICER QUALITY ASSISTANT		**JHON DIDIER RESTREPO DEDIEGO** QUALITY ASSISTANT

Alianza Team

PERSONAL DATA PROCESSING POLICY

Code: TE-JUR-PO-003	Type: POLITICA	Eff ective date: 2025-09-18	Version: 005