CLARIOS	**Personal Dara Protection Policy – Clarios Andina**

1. OBJECTIVE

Establish the personal data protection policy for **CLARIOS ANDINA S.A.S** in accordance with the principle of demonstrated responsibility (Accountability) of the Superintendence of Industry and Commerce (SIC), to preserve the confidentiality, integrity and availability of the Holders personal data which the company manages.

2. SCOPE

This document contains the personal data protection policy of **CLARIOS ANDINA S.A.S.**

3. GENERAL CONDITIONS

In compliance with the provisions contained in the law 1581 of 2012 for the personal data protection and the article 13 of Decree No. 1377 of 2013, regulatory of the Statutory Law for the personal data protection, **CLARIOS ANDINA S.A.S – NIT 900.388.600-1**, commercial company located in the city of Yumbo (Valle del Cauca), can disclose their policy related to the processing of personal data, for knowledge of their Holders and general public.

- **CONTROLLER: CLARIOS ANDINA SAS.**
- **Address:** Car 35 N° 10-300 Acopi - Yumbo, Valle del Cauca
- **Phone:** (+57) (2) 6911800.
- **Email:** protecciondedatospersonales@clarios.com

4. RESPONSIBILITIES

- **Senior Management:** Designate the person in charge and the resources necessary for the protection of the personal data managed by the company, approve and monitor the PIGDP, and promote the organizational culture in privacy.
- **Information Security and Privacy Committee:** Make decisions regarding risks and incidents that affect the privacy of the personal data of the holders associated with the company.
- **Local Data Privacy Responsible:** responsible for coordinating, reporting and promoting compliance with locally applicable data protection regulations in alignment with CLARIOS Global Privacy Program for a defined geography, business, and/or group of legal entities. Address requests from the Holders when they require action on their personal data. Report to government entities the incidents that affect the personal data processed.
- **Holders:** Provide the signed authorization for the treatment of your personal data by the company.
- **Controller:** Take decisions about the processing of the personal data of the holders throughout their life cycle. Defines policies, procedures, controls, use, disposal, means, and in general all the government related to the processing of personal data for the company. Must demonstrate responsibility in the processing of personal data before government entities at any time.
- **Processor:** The processor is the party engaged by the controller to process personal data.

5. DEFINITIONS

- **Consent:** Prior, express and informed consent of the Holder to carry out the processing of personal data.
- **Information asset:** Highly valid resources for the company that contains information which must guarantee confidentiality, integrity and availability.
- **Privacy notice:** Verbal or written communication generated by the Responsible, directed to the Owner for the Processing of their personal data, by means of which they are informed about the existence of the Information Processing policies that will be applicable to them, the form of access to them and the purposes of the treatment that is intended to give personal data.
- **Database:** Organized set of personal data that is subject to Treatment.
- **Confidentiality:** Property to prevent unauthorized access to information according to its classification level.
- **Control:** It is a measure that modifies the risk. The policies, procedures, practices and organizational structures designed to keep information security risks below the level of risk assumed. Control is also used as a synonym of safeguard or countermeasure.
- **Personal data:** Any information linked to or associated with one or several natural persons determined or determinable.
- **Private data:** It is the data that due to its intimate or reserved nature is only relevant for the owner.
- **Public data:** It is the data that is not semi-private, private or sensitive. They are considered public data, among others, the data relative to the civil status of the people, to their profession or trade and to their quality of merchant or public servant. By its nature, public data may be contained, among others, in public records, public documents, gazettes and official bulletins and judicial sentences duly executed that are not subject to reservation.
- **Semi-private data:** Information that is not private, reserved, or public in nature and whose knowledge or disclosure may be of interest not only to its owner but to a certain sector or group of people or to society in general, such as financial and credit data of commercial activity or services referred to in Law 1266 of 2008.
- **Sensitive data:** Any information that affects the privacy of the Owner or whose improper use can generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations, of human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data.
- **Availability:** Property of the information to be accessible and usable when required by an authorized entity.
- **Data Controller:** Natural or legal person, public or private, that by itself or in association with others, performs the processing of personal data.
- **Risk management:** Coordinated activities to direct and control an organization with respect to risk. It consists of the evaluation and treatment of risks.
- **Information security incident:** Single event or series of unexpected or unwanted information security events that have a significant likelihood of compromising business operations and threatening information security.
- **Integrity:** Property of information regarding its accuracy and completeness.

- **PIGDP:** Comprehensive Personal Data Management Program. Set of policies, principles, standards, procedures and verification and evaluation mechanisms established by the company to provide personal data protection standards complying with the principle of demonstrated liability according to law 1581 of 2012.
- **Policy:** Intentions and directions of an organization as formally expressed by Senior Management.
- **Holder:** Natural person whose personal data is subject to Treatment.
- **Treatment:** Any operation or set of operations on personal data, such as collection, storage, use, circulation, or deletion.

For the understanding of the terms that are not listed above, you must refer to the current legislation, especially Law 1581 of 2012 and the other complementary regulations.

6. PRINCIPLES

- **LEGALITY IN MATTERS OF DATA PROCESSING:** Treatment is a regulated activity that must be subject to the provisions of the law and other provisions that develop it.

- **PURPOSE:** The Treatment must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the Holder.

- **FREEDOM:** The Treatment can only be exercised with the prior, express and informed consent of the Holder. Personal data may not be obtained or disclosed without prior authorization, or in the absence of legal or judicial mandate that relieves consent.

- **TRUTHFULNESS OR QUALITY:** The information subject to Treatment must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fractioned or misleading data is prohibited.

- **TRANSPARENCY:** In the Treatment the right of the Holder must be guaranteed to obtain from the data Controller at any time and without restrictions, information about the existence of data that concerns him.

- **RESTRICTED ACCESS AND CIRCULATION:** The Treatment is subject to the limits that derive from the nature of the personal data and the provisions of the law. In this sense, the Treatment can only be done by persons authorized by the Holder and / or by the persons provided for in the Law 1581 of 2012. Personal data, except public information, may not be available on the Internet or other means of dissemination or mass communication, unless the access is technically controllable to provide restricted knowledge only to the Holders or authorized third parties.

- **SECURITY:** The information subject to Treatment by the data Controller, should be handled with the technical, human and administrative measures that are necessary to grant security to the records avoiding their adulteration, loss, consultation, use or non-access authorized or fraudulent.

- **CONFIDENTIALITY:** All persons involved in the processing of personal data that do not have the nature of public are obliged to guarantee the reservation of information, even after the end of

their relationship with any of the tasks involved in the treatment and can only perform supply or communication of personal data.

7. TREATMENT

The treatment that the society gives and will give to personal data for its collection, storage, use, circulation, update, retention and / or deletion, aims to achieve efficient communication and commercial relationship with our collaborators, customers, and suppliers, through the purposes that are listed in the following numeral.

8. USE AND PURPOSE OF DATA PROCESSING

The personal data of employees, candidates, suppliers, customers, visitors, and final consumers will be used for the development of the corporate purpose of **CLARIOS ANDINA S.A.S**, as well as in the development of their legal, administrative, operational, contractual and commercial obligations.

The following are the purposes that the company will give in the processing of personal data according to the holder type:

8.1. CANDIDATES AND EMPLOYESS: CLARIOS ANDINA S.A.S may process personal data of applicants for employment, employees, and retired workers for the following purposes:

- Recruitment, selection and filing processes for statistical purposes.
- Perform directly or through third parties in the inhibitory or restrictive lists and databases of the Attorney General's Office, Comptroller's Office, Cifin, Data Credit, among others.
- Manage the contracting process and comply with contractual obligations.
- Comply with legal and contractual obligations.
- Comply with labor legislation, social security, health care, and other provisions related to labor issues.
- Affiliation with the different entities of the General Social Security and Para-fiscal System.
- Provide tax and / or tax information on the operations performed with employees.
- Control of the company's physical security through video surveillance systems.
- Control of employee access to company facilities.
- Payroll and social benefits management.
- Processing of the work resume of active, inactive and aspiring employees.
- Management of active and inactive temporary employees of the company.
- Information management of educational and academic training of active and inactive employees.
- Control of employee entry and exit times through biometric markings.
- Verification of conflicts of interest between employees and suppliers.

8.2. CLIENTS, SUPPLIERS AND CUSTOMERS: CLARIOS ANDINA S.A.S may use the personal data of suppliers, former suppliers, customers, former customers, potential customers and consumers for the following purposes:

- Sort, catalog, classify, store and separate the information provided for easy identification.
- Consult, compare and evaluate all the information that is stored in the judicial Databases or of any public entity of surveillance, control or security legitimately constituted.

- Analyze, process, evaluate, treat or compare the information provided and use it for the specific purposes of the business to be held.
- Consult the lists for the prevention and control of money laundering and financing of terrorism.
- Sending information of interest, advertising material, offers and invitations to events scheduled by the Company.
- Comply with Colombian or foreign law and the orders of judicial, administrative or private entities in the exercise of public services when they require it.
- If the Company hires technology-based platforms in the cloud, or delegates to a third party, the data Controller must authorize the transfer of the data to the third party and to the countries where the data centers of the service provider are located who will act as a Processor.
- Execution and fulfillment of the contracts that are celebrated.
- Issuance of certifications relative to the relationship of the data holder with the Company.

8.3. **SHAREHOLDERS**: **CLARIOS ANDINA S.A.S** may or treat the personal data of shareholders in order to comply with the laws and other agreements of the shareholders, additionally for the following purposes:

- The creation and registration as a shareholder or member of the company's Board of Directors.
- Schedule to assemblies or meetings.
- Sending/receiving messages for the purpose of developing one's own activities as a shareholder and member of the Board of Directors.
- Any other purpose that results in the development of functions that correspond to it by virtue of the relationship between shareholder and / or board member and the company.

8.4. **VISITORS: CLARIOS ANDINA S.A.S** may process the personal data of visitors for the following purposes:

- Verify affiliation with ARL risk entities for legal compliance with occupational safety and health.
- Control of the physical security of the company through video surveillance systems.
- Registration and control of access of visitors to the physical facilities of the company.
- Consult and evaluate information from judicial databases or public surveillance entities.
- Consult the lists for the control of money laundering and terrorist financing.

For the treatment of personal data, **CLARIOS ANDINA SAS**, with the purpose of fulfilling the requirements mentioned in this policy, may transfer and / or transmit in specific cases the data to other Controllers and/or Processor inside or outside of Colombia, taking into account the restrictions on the international transfer of the SIC to countries that have personal data protection policies and the existing binding corporate standards for the company.

Video surveillance systems are used for the registration and control of personnel (employees, customers, suppliers, visitors or third parties) that enter the company's facilities. The privacy notice that relates the authorization for the video registration of personnel entering the facilities, is located at the main entrance of the company.

9. TREATMENT OF SENSITIVE PERSONAL DATA

In accordance with article 6 of Law 1581 of 2012, article 6 of Decree 1377 of 2013 and article 2.2.2.25.2.3 of the single regulatory decree 1074 of 2015 informs the holders that because they are

sensitive data are not required to authorize their treatment taking into account the exceptions of law. The holder has the option on the answers to the questions on sensitive personal data. No activity may condition the holder to provide sensitive personal data, as long as there is no legal or contractual duty. The personal data identified as sensitive that the company will treat according to its express consent are:

- **Biometric data** (*photographs, videos, fingerprints and facial recognition*). Photos on resume (CV), employees and visitors cards. Video records for physical security control. Fingerprint and facial recognition for employee time control markings.
- **Occupational health data** (*laboratories, medical and psychological diagnoses, medications, treatments, disabilities, pregnant or lactating mothers*). Related to compliance with occupational safety and health for employees.

10. BINDING CORPORATE RULES

The Binding Corporate Rules are the mechanism that allows to demonstrate the commitment and the guidelines of privacy and protection of personal data for the company and all its subsidiaries, independent of the global location site. **CLARIOS ANDINA SAS**, at the head of its parent company **CLARIOS**, undertakes to guarantee the security and privacy of the information at the head of the global office for the protection of personal data, whose point of contact is the **Ethics and Compliance Officer** in the email privacyoffice@clarios.com.

11. RIGHTS OF PERSONAL DATA HOLDERS

The Holder has the following rights contained in article 8 of Law 1581 of 2012:

a) Know, update and rectify your personal data in front of the data Controller or data Processor. This right may be exercised, among others, against partial, inaccurate, incomplete, fractioned, misleading data, or those whose treatment is expressly prohibited or has not been authorized.
b) Request proof of the consent granted to the data Controller, unless when expressly excepted as a requisite for the treatment, in accordance with the article 10 of this law.
c) To be informed by the data Controller or the data Processor, upon request, regarding the use that has been given to their personal data.
d) Submit complaints to the Superintendence of Industry and Commerce (SIC) for infractions of the provisions of this law and other regulations that modify, add or complement it.
e) Revoke the consent and/or request the deletion of the data when the Treatment does not respect the principles, rights and constitutional and legal guarantees. The revocation and / or suppression will proceed when the Superintendence of Industry and Commerce has determined that in the Treatment the Controller has incurred in conducts contrary to this law and the Constitution.
f) Access free of charge to your personal data that have been subject to processing.

12. DUTIES OF DATA CONTROLLERS

The data Controller must comply with the following as contained in article 17 of Law 1581 of 2012:

a) Guarantee to the Holder, at all times, the full and effective exercise of the right of habeas data.
b) Request and keep, under the conditions provided for in this law, a copy of the respective consent granted by the Holder.

c) To duly inform the Holder about the purpose of the collection and the rights that assist him by virtue of the authorization granted.
d) Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
e) Ensure that the information provided to the Processor is true, complete, accurate, updated, verifiable and understandable.
f) Update the information, communicating in a timely manner to the data Processor, all the news regarding the data that he has previously provided and take the other necessary measures so that the information provided to him is kept updated.
g) Rectify the information when it is incorrect and communicate the pertinent to the data Processor.
h) Provide to the data Processor, as appropriate, only data whose treatment is previously authorized in accordance with the provisions of this law.
i) Require to the data Processor at all times to respect the security and privacy conditions of the Holder's information.
j) To process the queries and claims made in the terms indicated in the law and in this policy.
k) Adopt an internal manual of policies and procedures to ensure adequate compliance with the law and especially for the attention of inquiries and complaints.
l) Inform to the data Processor when certain information is under discussion by the Holder, once the claim has been submitted and the respective procedure has not been completed.
m) Inform at the request of the Holder about the use given to their data.
n) Inform the data protection authority when there are violations of security codes and there are risks in the management of the information of the Holders.
o) Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.
p) The other duties established in the law for the person responsible for the treatment.

13. DUTIES OF DATA PROCESSORS

Attending the stated regulations, the manager for personal data must comply with the following as contained in Article 18 of Law 1581 of 2012:

a) Guarantee to the Holder, at all times, the full and effective exercise of the right of habeas data.
b) Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
c) Timely update, rectify or delete the data in the terms of this law.
d) Update the information reported by the data Controller within five (5) business days from their receipt.
e) To process the consultations and claims made by the Holders in the terms indicated in this law.
f) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, for the attention of inquiries and complaints by the Holders.
g) Register in the database the legend "**claim in proces**s" in the form in which it is regulated in this law.
h) Insert in the database the legend "**information in judicial discussion**" once notified by the competent authority about judicial processes related to the quality of personal data.
i) Refrain from circulating information that is being controversial by the Holder and whose blockade has been ordered by the Superintendence of Industry and Commerce.
j) Allow access to information only to people who may have access to it.
k) Inform the Superintendence of Industry and Commerce when there are violations of security codes and there are risks in the administration of the information of the Holders.

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

14. PERSONAL DATA PROTECTIONS PROCEDURE

To facilitate the exercise of their rights by the owner of the data, the following is the procedure established for this purpose:

14.1. CONSULTATION:

The Holders or their successors in title may consult the personal information of the Holder storage in any database of **CLARIOS ANDINA SAS** by written request for the channel defined within this policy.

Once the communication or Holder e-mail has been received, it will proceed in accordance with the same within the term of ten (10) business days from the date of reception. When it is not possible to attend the consultation within said term, the interested party will be informed, stating the reasons for the delay and indicating the date on which his inquiry will be attended, which in no case may exceed five (5) business days following the expiration of the first term.

14.2. CLAIMS:

The Holder or his successors who consider that the information contained in a database of **CLARIOS ANDINA SAS** must be corrected, updated or deleted, or when they notice the alleged breach of any of the duties contained in the regulations personal data protection, may file a claim with **CLARIOS ANDINA SAS** or the Processor.

The claim will be formulated by means of a written request by the channel defined in this policy with the identification of the Holder, the description of the facts that give rise to the claim, the address, and accompanying the documents to be asserted.

If the claim is incomplete, the interested party will be required within five (5) days after receipt of the claim to correct the faults.

After two (2) months from the date of the request, without the applicant submitting the required information, it shall be understood that the claim has been abandoned.

In case the person who receives the claim is not competent to resolve it, it will transfer to the corresponding one in a maximum term of two (2) business days and will inform the interested party of the situation.

Once the complete claim has been received, a legend that says "**claim in process**" and the reason thereof will be included in the database, in a term not exceeding two (2) business days. This legend must be maintained until the claim is decided.

The maximum term to attend the claim will be fifteen (15) business days counted from the day following the date of receipt of the complete claim. When it is not possible to meet the claim within said term, the interested party will be informed of the reasons for the delay and the date on which his claim will be handled, which in no case may exceed eight (8) business days following the expiration of the first finished. The request for suppression of information does not proceed when the Holder has a legal duty or contractual link to remain in the database.

14.3. DATA UPDATING/RECTIFICATION REQUEST: The data Controller will update and/or rectify, at the request of the Holder, the information that is incomplete or inaccurate by means of a written request for the channel defined in this policy. For this, the Holder or successor will indicate the pertinent updates and/or corrections together with the documents that support the request.

14.4. CONSENT REVOKE AND/OR DATA DELETION: The Holder of personal data may request to the Controller revoke and/or delete their personal data by written request through the channel defined in this policy, provided that it is not prevented by a legal or contractual provision that indicates their permanence in the databases. If the respective legal term has expired, personal data have not been eliminated, the Holder shall have the right to request the Superintendence of Industry and Commerce to order the deletion of personal data.

15. POLICIES

- The Controller and Processor of personal data processing have the obligation to guarantee the confidentiality, integrity and availability of the Holders personal data associated with the company at each stage of their life cycle. The Controller and Processors implement security measures to collect, storage, use and share data. The Controller determines the archiving time and the secure procedures for deletion either at the request of the Holder, legal requirements or retention time.

- To guarantee the confidentiality of the information, the data Controller implements confidentiality and authorization agreements for the processing of personal data with the Holders associated with the company and third parties.

- The company identifies, analyzes, evaluates, treats, monitors and communicates the risks that affect the security of information and personal data through a methodology of continuous improvement. The evaluation is carried out annually or when required.

- The company plans, implements, maintains and improves an Information Security Management System (ISMS) and a Personal Data Protection Program (PDPP) to guarantee the privacy, confidentiality, integrity and availability of personal data headlines associated with the company.

- The company implements physical and logical access controls to information, especially the Holders personal data, through the assignment of roles, privileges and segregation of duties which are periodically verified by the responsible areas.

- Personal data of a sensitive nature are classified as **CRITICAL AND HIGHLY CONFIDENTIAL** by the company, and both physical/logical access and its treatment is restricted only to persons of interest, prior authorization. Its disclosure without authorization of the Holder is totally prohibited and will be penalized in accordance with the current law of protection of personal data.

- The company implements backup procedures for information, especially for information that contains personal data. The backup copies of logical databases are made according to the procedures established in a corporate manner where their periodicity and retention time are established according to the type of data. Physical databases (paper or similar) are digitally backed by the area responsible for their processing and their archiving time is determined according to the document retention tables established for the company.

- Remote access to company information, and especially that containing personal data, is done through the access control mechanisms established by the company with prior authorization. Authorized users who can access and process information are responsible for implementing and enforcing established information security procedures.

- The company identifies and implements information security requirements for its own or outsourced systems that process and store information, especially personal data.

- The company implements change management procedures for its own or outsourced information systems that process information, especially personal data. Changes that impact the confidentiality, integrity and / or availability of personal data must have the prior authorization of the data Controller.

- Compliance with security and privacy controls is verified through audits.

- Both the Controller and Processors are obliged to report the occurrence of incidents that affect the confidentiality, integrity, availability or other privacy requirements of the Holders, to the entities in charge at the time established. The company has established communication channels for the attention and reporting of incidents.

The databases with personal information of the Holders treated by the company and located in the National Registry of Databases (NRDB) of the Superintendence of Industry and Commerce of Colombia (SIC) on June 02, 2017 and later, will be valid while the company **CLARIOS ANDINA SAS**, collect, store, use, circulate and/or retain the related data for the reasonable and necessary time according to the specified purposes and the document retention tables of the company, always in compliance with current legal regulations.

This personal data treatment policy is effective in accordance with the requirements contained in the aforementioned regulations.