# CEMENTOS ARGOS S.A.

## PERSONAL DATA PROCESSING POLICY

# TABLE OF CONTENTS

CEMENTOS ARGOS S.A. and its affiliated companies (hereinafter "ARGOS"), in compliance with the provisions of Law 1581 of 2012 and any other standards that modify it, supplement it or replace it (hereinafter “DP Normativity), regulating the collection and treatment of personal data and establishing the legal guarantees that must be met by all persons in Colombia for the proper treatment of said information (hereinafter "treatment"), issues the following policy of treatment of personal data (hereinafter “Policy”) which develops the information security strategy for the treatment of personal data (hereinafter "PD") within ARGOS, with the following prior considerations:

**CONSIDERATIONS**

1. ARGOS has been working on the regulation of the PD treatment process within the framework of ISO Standard 27001/27002, which involves the subjection of ARGOS to comply with the current regulations regarding the protections of PD.
2. The DP Normativity which dictates the general provisions for the protection of PD, grants companies a period of six (6) months as of the enactment of the law to adapt to said provisions.
3. In order to fulfill ARGOS' obligation to improve its Information Security Management System within a Plan-Do-Check-Act scheme, it is necessary to issue a Policy that establishes the rules applicable to the treatment of the PD in the custody of the business entity.
4. It is the responsibility of ARGOS directors, employees and external contractors to observe, abide by and comply with the orders and instructions imparted specifically by ARGOS regarding PD whose disclosure or improper use may cause detriment to the Holders thereof, in compliance with the rights contained in Article 15 of the Political Constitution of Colombia, and the DP Normativity.
5. The legal regulations related to PD establish economic, commercial and custodial sanctions, which is why cooperation between ARGOS and the addressees of this Policy is essential in order to guarantee the rights to intimacy, habeas data and to the protection of PD and thus avoid damages to any of the parties and/or third parties.
6. The regulations of the Policy, particularly those regarding work relationships and rendering of services, must include the protection of the PD related to human resources while respecting the minimum rights and guarantees of employees and service providers, under penalty of the stipulations losing effect.

7. Pursuant to labor legislation, the employer has a duty to protect its employees, and they have the duty of compliance and loyalty to ARGOS in order to contribute to the secure management of personal information.
8. This Policy complements and does not contravene the employees' or ARGOS' obligations contained in the labor legislation.
9. It is the duty of ARGOS employees to lend their full assistance in the event of an accident or imminent risk that affects or threatens the information assets, especially those related to the PD in the custody of ARGOS, so that ARGOS has the cooperation it requires to investigate, analyze and capture evidence of security incidents that compromise said information, whether or not they have a judicial mandate, in compliance with the instructions contained in ARGOS' chain of custody protocol.

Based on the above considerations that underlie the protection of PD at ARGOS, the following mandatory provisions are formulated for their treatment.

**I. DEFINITIONS**

**Personal Data Base**. It is any organized set of personal data regardless of its manner of creation, storage, organization and access.

**Automated Data Base**. It is an organized set of personal data created, processed and/or stored through computer or software programs.

**Non-Automated Data Base**. It is an organized set of personal data created, processed and/or stored manually without computer or software programs.

**Transfer of Data**. Treatment of data that supposes their disclosure to a person other than the Holder of the data, or other than the person authorized as transferee.

**Data Base Custodian.** It is the individual under whose custody the PD is.

**Personal Data**. It is any piece of data or information that identifies an individual or makes them identifiable. The data may be numeric, alphabetic, graphic, visual, biometric, auditory, profile or any other type.

**Sensitive Personal Data**. It is a special category of especially protected personal data because they are related to health, gender, political affiliation, race or ethnicity, and biometric prints, among other things, which are part of a person's private life and can only be collected with the express and informed consent of their Holder in the cases provided by law.

**Treatment Supervisor.** It is the individual or legal person, public or private authority, that by itself

or jointly with others, performs the treatment of the PD on behalf of the Manager.

**Sources Accessible to the Public.** This refers to sources that contain PD and may be queried by anyone; this may or may not include payment in exchange for access to such data. Sources accessible to the public include phone books, industry or sector directories, among others, as along as the information is limited to general PD or contains general aspects of the law. This condition includes print media, official newspapers and other types of media.

**Habeas Data.** Fundamental right of every person to know, update, rectify and/or cancel information and PD that has been collected from them and/or is processed in public or private databases, as provided by law and other applicable regulations.

**Procedure for the Analysis and Creation of Information**. It is the creation of information regarding a person based on the analysis and treatment of the collected and authorized PD for purposes of analyzing and extracting behavioral habits or profiles that generate added value to the information obtained from the Holder of every piece of personal data.

**Dissociation Procedure**. This refers to all PD treatment in such a way that the obtained information cannot be associated with an identified or identifiable person.

**Principles for Data Treatment.** They are the fundamental legal and/or jurisprudential rules that inspire and guide the treatment of PD, and serve as the basis to determine the actions and criteria to solve possible collisions between the right to privacy, habeas data and PD protection, and the right to information.

**Data Base Owner.**

Within ARGOS' business processes, the database owner is the department responsible for the treatment and management of said data.

**Treatment Manager**.

It is the individual or legal person, of a public or private nature, who collects the PD and determines the purpose, content, and use of the database for treatment.

**Personal Data Holder**. It is the individual whose data is the object of treatment.

Regarding legal persons, the name is considered a fundamental right protected by the Constitution.

**Data Treatment.** Any operation or set of operations and technical procedures - that may or may not be automated - performed on PD such as collection, recording, storage, conservation, use, circulation, modification, blocking, and cancellation, among others.

**User**. Is the natural or legal person who has a stake in the use of the personal information.

**Violation of Personal Data.** It is a crime pursuant to Law 1273 of 2009 contained in Article 269 F

of the Colombian Penal Code. The prohibited conduct is as follows: "Whosoever, without being entitled to do so, for his own benefit or on behalf of a third party, obtains, complies, extracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or employs personal codes, PD contained in databases, archives, or similar, shall incur in a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1,000 current minimum monthly wages."

**Violations to Personal Data Security Measures.** A security incident will be deemed as any situation that involves a violation of the security measures adopted by ARGOS to protect the PD in its custody, either as Manager and/or Supervisor, as well as any other behavior that constitutes improper treatment of the PD, in opposition to the provisions contained herein or as provided by law. All security incidents that compromise the PD in ARGOS' custody must be reported to the appropriate authority.

## II. OBJECTIVE

To adopt and establish the rules applicable to the treatment of the PD that has been collected, processed and/or stored by ARGOS in the exercise of its corporate purpose, either as Treatment Supervisor and/or Manager.

The rules contained in this Policy comply with the provisions of the DP Normativity, in terms of guaranteeing people's right to privacy, exercise of habeas data and protection of PD, in accordance with the right to information, so that these rights are regulated proportionally at ARGOS and their violation can be prevented.

The rules adopted in this Policy by ARGOS conform to international standards related to the protection of PD.

## III. SCOPE OF IMPLEMENTATION

This Policy shall apply to the treatment of PD carried out by ARGOS where it has presence or when the Policy applies to the Manager and/or Supervisor located outside Colombian territory by virtue of international treaties, contractual relationships, etc.

The principles and provisions contained in this Policy shall apply to any PD database in ARGOS' custody, either as Treatment Manager and/or Treatment.

All organizational processes at ARGOS that involve the treatment of PD shall be subject to the provisions of this Policy

**IV. ADDRESSEES OF THIS POLICY.**

This Policy shall apply and therefore bind the following persons:

**4.1.** Legal representatives and/or corporate administrators.

**4.2.** ARGOS internal staff, directors or otherwise, who guard and process PD.

**4.3.** Contractors and natural or legal persons who render services to ARGOS under any type of contract by virtue of which any kind of PD is processed.

**4.4.** Shareholders, tax auditors and persons with whom there is a statutory legal relationship.

**4.5.** Public and private persons as PD users.

**4.6.** Other persons as provided by law.

**V. PRINCIPLES APPLICABLE TO THE TREATMENT OF PERSONAL DATA**

The protection of PD at ARGOS shall be subject to the following principles or fundamental rules, which shall serve as the basis to establish the internal processes related to PD treatment and shall be processed in a harmonious, integral and systematic manner to resolve any conflicts that may arise related to this matter. These principles are enshrined in international standards, Colombian laws, and the jurisprudence of the Constitutional Court, which has developed the fundamental rights related to personal data.

**5.1. Informed Consent or Principle of Freedom**.

The treatment of PD within ARGOS can only occur with the prior, informed, express consent of the Holder. PD may not be obtained, processed or disclosed without the authorization of the Holder except through a legal or judicial mandate that substitutes the consent of the Holder.

**5.2. Legality.**

The treatment of PD in Colombia is a regulated activity, therefore, the business processes and addressees of this Policy will be subject to the provisions thereof.

**5.3. Purpose of the Data**.

The treatment of PD must obey a legitimate purpose, in accordance with the Constitution and the law, which the Holder must be informed of correctly, accurately and previously in order for them to express their informed consent.

**5.4. Quality or Veracity of the Data.**

Personal data collected by ARGOS must be truthful, complete, accurate, verifiable, comprehensible, and must be kept updated. Providing partial, fractioned, incomplete or error-inducing data is prohibited.

**5.5. Transparency.**

The treatment of PD shall guarantee the Holder's right to obtain from the Treatment Manager and/or Supervisor at any time and without restriction information about the existence of the data concerning the Holder.

**5.6. Relevance of the Data**.

PD collection by ARGOS will take into account the purpose of the treatment and/or database; therefore, the data must be appropriate, relevant and not excessive or disproportionate to the purpose. The collection of PD disproportionate to the purpose they are obtained for is prohibited.

**5.7. Access and Restricted Circulation.**

PD collected or processed by ARGOS will be used by the company solely within the scope of the purpose and authorization granted by the Holder of the personal data; therefore, the data may not be accessed by, transferred or disclosed to third parties.

The PD in the custody of ARGOS will not be available on the Internet or on any other means of mass dissemination, except if the access is technically controllable and secure and for the purpose of providing knowledge strictly to Holders and authorized third parties as provided by law and the principles that govern the matter.

**5.8. Temporality of the Data**.

Once the purpose for which the PD was collected and/or processed has been exhausted, ARGOS will cease to use it and will adopt the necessary security measures for handling the PD while complying with the commercial law obligations related to the maintenance of trade books and merchant correspondence.

**5.9. Security of the Data.**

ARGOS, in its capacity as Treatment Manager or Supervisor of the PD shall, depending on the case, adopt the necessary physical, technological and/or administrative measures to ensure the attributes of integrity, authenticity and reliability of the PD. ARGOS, pursuant to the classification of the PD, shall implement high, medium and low security measures in order to prevent the adulteration, loss, leak, query, or unauthorized or fraudulent use or access.

**5.10. Confidentiality**.

ARGOS and all persons who intervene in the treatment of the PD have the professional obligation to maintain the confidentiality of said data; this obligation remains even after the contractual relationship has been completed. ARGOS shall implement data protection clauses in its contractual relationships for such a purpose.

**5.11. Duty of Information.**

ARGOS shall inform the Holders of the PD as well as the Treatment Managers and Supervisors about the PD protection policy adopted by ARGOS, and about the purpose and other principles that regulate treatment. Similarly, ARGOS shall disclose the existence of PD databases in its custody, the rights, and the exercise of habeas data by the Holders, in accordance with applicable

laws.

**5.12. Special Protection of Sensitive Data.**

ARGOS will not collect or process sensitive data linked to political ideologies, union affiliation, religious beliefs, sexual life, ethnicity, health data, and underage people data, except in cases that do not require consent or only with the express authorization of the Holder or its representative - while making it clear that it is optional and voluntary to answer questions regarding this kind of data. Sensitive PD that may be obtained through processes related to ARGOS activities will be protected with high security measures.

**VI. RIGHTS OF DATA HOLDERS**

The Holders of PD contained in databases that reside in ARGOS information systems possess the rights described in this section in compliance with the fundamental guarantees enshrined in the Political Constitution and the Law.

The exercise of these rights shall be free and unlimited by the Holder, without prejudice to legal provisions that regulate the exercise thereof.

The exercise of habeas data, expressed in the following rights, constitutes personal power and shall be exercised exclusively by the Holder, except as provided by law.

**6.1. Right to Access.**

This right encompasses the ability of the Holder to obtain all information regarding his or her own PD, whether it is partial or complete, the treatment thereof, the purpose of such treatment, the location of the databases that contain their PD, and communications and/or transfers made regarding the PD, authorized or otherwise.

**6.2. Right to Update.**

This right includes the ability of the Data Holder to update his or her PD when it has changed.

**6.3. Right to Rectify.**

This right includes the ability of the Holder to modify data that is inaccurate, incomplete or non-existent.

**6.4. Right to Cancel.**

This right includes the right of the Holder to cancel his or her PD, or to suppress it when it is excessive, irrelevant or its treatment goes against regulations, except in those cases contemplated as exceptions by law.

**6.5. Right to Revoke Consent.**

The Holder has the right to revoke the consent and authorization provided to ARGOS for a specific process, except in those cases contemplated as exceptions by law and/or in which it is necessary under a specific contractual framework.

**6.6. Right of Opposition.**

This right includes the ability of the Holder to oppose the processing of his or her PD, except in cases where such a right does not apply due to legal provisions or when it infringes upon general interests greater than private interests. Based on the legitimate rights argued by the Holder, ARGOS' Legal and Institutional Affairs Vice Presidency shall issue a judgment based on proportionality or weighting in order to determine the preeminence or not of the Holder's particular right to other rights, e.g. the right of information.

**6.7. Right to File Complaints and Claims or to Exercise Actions.**

The Holder has the right to file claims and complaints with the Superintendency of Industry and Commerce, or with the competent authority, as well as to file pertinent actions for the protection of his or her data. ARGOS shall respond to the requirements made by the competent authorities regarding these Holder's rights.

**6.8. Right to Grant Authorization for the Treatment of Data.**

In pursuance of the principle of Informed Consent, the Holder has the right to grant authorization, by any means that may be subject to subsequent query, to have his or her PD processed by ARGOS.

Said authorization shall not be required in the following, exceptional, cases:

**6.8.1.** When required by a public or administrative entity in fulfillment of its legal duties, or by court order.

**6.8.2.** When dealing with data of a public nature.

**6.8.3.** In cases of medical or public health emergencies.

**6.8.4.** When the information treatment is authorized by law for historical, statistical, or scientific purposes.

**6.8.5**. When dealing with PD related to people's Civil Registration.

In these cases, while the Holder's authorization is not required, all other principles and legal provisions concerning the protection of PD shall apply.

## VII. DUTIES OF THE ADDRESSEES OF THIS STANDARD REGARDING PERSONAL DATABASES WHEN ACTING AS MANAGERS AND SUPERVISORS.

### 7.1. Duties of Treatment Managers.

When ARGOS, or any of the addressees of this Policy, assume the quality of Treatment Managers of the PD in their custody, they shall fulfill the following duties without prejudice to the other provisions provided by law and otherwise that govern their activities:

a) To guarantee the Holder, at all times, the full and effective exercise of the right to habeas data.
b) To request and maintain, under the conditions provided by this standard, a copy of the authorization and consent granted by the Holder.
c) To inform the Holder in a timely manner about the purpose of the collection of data and about the rights conferred by virtue of the authorization that was granted.

d) To keep the information under the necessary conditions of security to prevent their adulteration, loss, or unauthorized or fraudulent query, use or access.
e) To ensure that the information provided to the Treatment Supervisor is truthful, complete, accurate, updated, verifiable and comprehensible.
f) To update the information and inform the Treatment Supervisor in a timely manner of any changes regarding the data that was provided previously, and to adopt other necessary measures to ensure the provided information stays updated.
g) To correct the information when it is inaccurate and to inform the Treatment Supervisor of any relevant changes.
h) To provide the Treatment Supervisor, as the case may be, solely with data whose treatment has been previously authorized in accordance with the law.
i) To demand from the Treatment Supervisor respect at all times for the security and privacy of the Holder's information.
j) To process queries and claims formulated under the terms provided by this Policy and by law.
k) To adopt an internal handbook of policies and procedures to ensure compliance with the law and, especially, to process queries and claims.
l) To inform the Treatment Supervisor of any situation in which the information is in dispute by the Holder, when a claim has been filed and its respective process has not been completed.
m) To inform the Holder, by request, about the use given to his or her data.
n) To inform the data protection authority when there are breaches to the security codes and when there are risks associated with the administration of the Holders' information.
o) To comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

**7.2. Duties of Personal Data Treatment Supervisors.**

When ARGOS, or any of the addressees of this Policy, assume the quality of Treatment Managers of the PD in their custody, they shall fulfill the following duties without prejudice to the other provisions provided by law and otherwise that govern their activities:

a) To guarantee the Holder, at all times, the full and effective exercise of the right to habeas data.
b) To keep the information under the necessary conditions of security to prevent their adulteration, loss, or unauthorized or fraudulent query, use or access.
c) To update, correct or suppress the data in a timely manner as established by law.

d) To update the information reported by the Treatment Managers within five (5) business days as of the date of receipt.
e) To process queries and claims formulated by Holders under the terms provided by this Policy and by law. This duty shall be the responsibility of ARGOS' Legal and Sustainability Vice Presidency.
f) To adopt an internal handbook of policies and procedures to ensure compliance with the law and, especially, to process queries and claims by the Holders.
g) To record the note "claim in process" in the database, as provided by law, for unresolved claims and complaints filed by the Holders of the PD.
h) To insert the note "information under judicial discussion" in the database once the competent authority has reported any legal proceedings related to the quality of the personal data.
i) To abstain from circulating information that is being disputed by the Holder and which has been ordered to be blocked by the Superintendency of Industry and Commerce.
j) To allow access to the information only to persons authorized to do so.
k) To inform the Superintendency of Industry and Commerce when there are breaches to the security codes and when there are risks associated with the administration of the Holders' information.
l) To comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

**7.3. Common Duties of Treatment Managers and Supervisors.**

In addition to the duties described above for ARGOS and for anyone who assumes the condition of Treatment Manager or Supervisor, the following duties shall be assumed as well regardless of condition:

a) To apply security measures in accordance with the classification of the PD ARGOS processes.
b) To adopt disaster recovery procedures applicable to databases that contain PD.
c) To adopt back up procedures for databases that contain PD.
d) To conduct regular audits of compliance with this Policy by its addressees.
e) To manage databases that contain PD in a secure manner.
f) To apply this Policy jointly with the Information Security Policy.
g) To keep a central registry of databases that contain PD, and that includes their history since creation, information treatment and cancellation of databases.

h) To manage access to PD databases contained in the information systems in a secure manner, when involved as a Treatment Manager or Supervisor.
i) To have a procedure to manage security incidents concerning databases that contain PD.
j) To include clauses in contracts with third parties that regulate access to data bases that contain PD.

**VIII. HABEAS DATA PROCEDURE FOR THE EXERCISE OF RIGHTS OF INFORMATION, ACCESS, UPDATE, RECTIFICATION, CANCELLATION AND OPPOSITION.**

In pursuit of the constitutional guarantee of Habeas Data regarding rights of access, update, rectification, cancellation and opposition by the Holder or legally qualified stakeholder, that is, their assignees or legal representatives, ARGOS shall adopt the following procedure:

**8.1.** The Holder and/or stakeholder in exercising one of these rights shall accredit such a condition by means of a copy of the relevant document and of their identification, which may be provided physically or digitally. In the event the Holder is represented by a third party, a notarized power of attorney must be provided.

The proxy must also accredit their identity under the terms described above.

**8.2.** The request to exercise any of the aforementioned rights shall be made in writing, either physically or digitally. The request to exercise any of the aforementioned rights may be sent to the main address or to the e-mail address enabled by ARGOS for the exercise of Habeas Data. ARGOS may provide other means for the Holders to exercise their rights.

**8.3.** The request to exercise any of the aforementioned rights shall contain the following information:

**8.3.1.** Name of the Holder and his or representatives, if applicable.

**8.3.2.** A precise request for information, access, update, rectification, cancellation, opposition or revocation of consent. In every case the request must be reasonably justified in order for ARGOS to provide a response as Database Manager.

**8.3.3.** Mailing and/or e-mail address for notifications.

**8.3.4.** Documents to support the request.

**8.3.5.** Signature of the Holder on the request.

If any of the aforementioned requirements are not fulfilled, ARGOS shall notify the stakeholder within 5 days following receipt of the request so that it may be corrected and ARGOS can respond to the Habeas Data request. If the required information is not provided after two (2) months, it will be understood that the request has been withdrawn. ARGOS may have physical and/or digital formats to exercise this right, and they will indicate whether they are related to a query or a claim by the stakeholder. Within two (2) business days after the reception of the complete request, ARGOS will indicate that the claim is in process. The respective database (PQR) must contain a box with the following captions: "Claim in process" and "Claim resolved".

When ARGOS is responsible for the databases with PD contained in its information systems, it will respond to requests within a period of ten (10) days for queries, and fifteen (15) days for claims.

ARGOS will also respond when it verifies that its information systems do not contain PD of the stakeholder exercising one of the aforementioned rights.

In the event of a claim, if it is not possible to respond within a period of fifteen (15) days, the stakeholder will be informed of the reason for the delay and the date on which the claim will be dealt with, which cannot, under any circumstances, be more than 8 business days following the expiration of the initial 15 days.

In cases in which ARGOS is the Treatment Supervisor, said situation will be informed to the Holder or party interested in the personal data and communicated to the person responsible for the request in order for this person to respond to the request that has been filed. A copy of this communication shall be addressed to the Holder or stakeholder so that they may be aware of the identity of the personal data Manager and, consequently, the identity of the principal obliged to ensure the exercise of their right.

ARGOS shall document and store requests made by data Holders or stakeholders associated with the exercise of any of their rights, as well as the responses to said requests. This information will be processed in accordance with regulations applicable to ARGOS correspondence.

In order to resort to the Superintendency of Industry and Commerce to exercise the legal actions contemplated for data Holders or stakeholders, the query and/or claims process described herein must first be exhausted.

**IX. CENTRAL REGISTRY OF PERSONAL DATABASES**

As Treatment Manager for the PD in its custody and in pursuit of its business activities, as well as regarding the data for which it acts as Supervisor, ARGOS shall keep a central registry where it will list each of the databases contained in its information systems.

The central registry of PD databases will permit the following:

**9.1.** The registration of all PD databases contained in ARGOS' information systems. Each one will be assigned a registration number.

**9.2.** The registration of the databases shall indicate: **(i)** The type of personal data it contains; **(ii)** The purpose and intended use of the database; **(iii)** Identification of the department at ARGOS that processes the database; **(iv)** Treatment system utilized (automatic or manual) for the database; **(v)** Indication of the security level and measures that apply to the database by virtue of the type of personal data it contains; **(vi)** Location of the database in ARGOS' information systems; **(vii)** The groups of people or stakeholders whose data are contained in the database; **(viii)** ARGOS' condition as database Treatment MANAGER or SUPERVISOR; **(ix)** Authorization of communication or transfer of the database, if it exists; **(x)** Origin of the data and procedure to obtain consent; **(xi)** ARGOS employee who is the custodian of the database; **(xii)** All other requirements applicable by any laws that may be issued.

**9.3.** Any changes that arise in the PD databases regarding the aforementioned requirements shall be recorded monthly for purposes of compliance and auditing. In the event the databases have not undergone any changes, their custodian shall record that as well.

**9.4.** The occurrence and history of security incidents that arise against any of the PD databases in ARGOS' custody shall be recorded in this central registry.

**9.5.** The registry will indicate any penalties that may be imposed regarding the use of the database as well as the origin thereof.

**9.6.** The cancellation of PD databases shall be recorded indicating the reasons and technical measures adopted by ARGOS to make the cancellation effective.

**X. TREATMENT OF PERSONAL DATA**

The operations that constitute the treatment of PD by ARGOS, as Manager or Supervisor thereof, shall be governed by the following parameters.

**10.1. Personal Data Related to Human Resources.**

**10.1.1. Treatment of Data before the Contractual Relationship.**

ARGOS shall process the PD of its employees, contractors, and applicants to new jobs during three instances: before, during, and after the employment and/or service relationship.

Treatment before the employment relationship. ARGOS shall inform in advance the people interested in participating in a hiring progress of the rules applicable to the treatment of PD provided by the applicant, as well as to the data obtained during the hiring process.

Once the hiring process is finished, ARGOS shall inform the persons not hired of the decision and return to them the PD that was provided, except when the Holders of the data authorize in writing the destruction of said data, so long as the Holder of the data has not been hired. The information obtained by ARGOS regarding persons who were not hired, results of psycho-technical tests and interviews shall be eliminated from their information systems, thus complying with the principle of purpose.

When ARGOS engages a third party to conduct the hiring processes, ARGOS shall include clauses in the contracts to regulate the treatment of PD provided by applicants, as well as the intended

purpose of the personal information obtained from the respective processes.

The PD and information obtained from the hiring process regarding the persons hired to work at ARGOS shall be stored in the personal folder, and high levels and measures of security shall be applied to this information, by virtue of the potential of this information to contain sensitive data.

The purpose of the data provided by applicants to jobs at ARGOS and the personal information obtained from the hiring process is limited to the participation in said process. Therefore, its use for other purposes is prohibited.

**10.1.2. Treatment of Data during the Contractual Relationship.**

ARGOS shall store the PD and information obtained during the employee hiring process in a folder identified with the name of each one. This physical or digital folder may only be accessed and processed by the Labor Relations department for the purpose of managing the contractual relationship between ARGOS and its employees.

The use of employees' information for purposes other than managing the contractual relationship is prohibited at ARGOS. The different use of employees' PD may only take place by order of a competent authority, as long as it has the power to do so. It will be the responsibility of the Legal and Institutional Affairs Vice Presidency to assess the competence and effectiveness of the order issued by the competent authority in order to prevent an unauthorized transfer of PD.

**10.1.3. Treatment of Data after the Termination of the Contractual Relationship.**

Once the employment relationship has been terminated, regardless of the cause, ARGOS will store the PD obtained from the hiring process and documentation generated during the employment relationship in a central archive and subject this information to high levels and measures of security, given the potential of the employment information to contain sensitive data.

ARGOS is prohibited from giving this information to third parties, as this fact may constitute a

deviation from the purpose for which the PD was provided by the Holders. The foregoing is excepted by the previous written authorization that documents the consent of the Holder of the personal data.

**10.2. Treatment of Shareholders' Personal Data.**

ARGOS is prohibited from giving this information to third parties, as this fact may constitute a deviation from the purpose for which the PD was provided by the Holders.
Consequently, access to such personal information shall occur in accordance with the rules contained in the Commercial Code that regulates the matter.

ARGOS will only use the PD of shareholders for purposes derived from the existing statutory relationship.

**10.3. Treatment of Suppliers' Personal Data.**

ARGOS will only collect from its suppliers the data that is necessary, relevant and not excessive for the purpose of selecting, evaluating and executing the contract that may arise. When ARGOS is required by law to disclose the data of an individual supplier (individual) as a consequence of a hiring process, this shall occur under the provisions that comply with this Policy and that alert third parties about the purpose of the information being disclosed.

ARGOS shall collect from its suppliers the PD of the suppliers' employees that are necessary, relevant, and non-excessive, that for security reasons ARGOS needs to analyze and evaluate in relation to the characteristics of the services provided by the supplier.

The PD of supplier employees collected by ARGOS shall have the sole purpose of verifying the moral suitability and competence of the employees. Therefore, once this requirement has been fulfilled ARGOS may return said information to the suppliers, except when it is necessary to keep such data.

When ARGOS provides its employees' PD to suppliers, they shall protect the PD provided in accordance with the provisions of this Policy. For such a purpose, the respective audit provision

shall be included in the contract or document that legitimates the delivery of the PD. ARGOS will verify that the requested data is necessary, relevant and not excessive in terms of the purpose that justifies the request to access the data.

**10.4. Treatment of Personal Data during Hiring Processes.**

Third parties that during hiring processes, partnerships or cooperation agreements with ARGOS access, use, process and/or store PD belonging to ARGOS employees or to a third party's employees related to such contractual processes will adopt the relevant provisions of this Policy, as well as the security measures indicated by ARGOS according to the processed PD.

For such a purpose, the respective audit provision shall be included in the contract or document that legitimates the delivery of the PD. ARGOS will verify that the requested data is necessary, relevant and not excessive in terms of the purpose of the treatment

**10.5. Treatment of the Personal Data of the Community at Large.**

The collection of data belonging to individuals that ARGOS processes while conducting actions related to the community, either as a consequence of corporate social responsibility or any other activity, shall be subject to the provisions of this Policy. For such a purpose, ARGOS shall previously inform and obtain authorization from the Holders of the data in the documents and instruments related to these activities that are used for such a purpose.

In all of the cases described above, the departments at ARGOS that conduct business processes in which PD is involved must consider in their action strategies the formulation of rules and procedures that permit complying with and enforcing this Policy, as well as preventing possible legal sanctions.

**XI. PROHIBITIONS**

For the implementation of this PD treatment policy, the following prohibitions and sanctions are

established as a consequence of their non-compliance.

**11.1.** ARGOS forbids the access, use, management, transfer, communication, storage, and any other treatment of sensitive PD without the authorization of the Holder of the personal data and/or ARGOS.
Failure to comply with this prohibition by ARGOS employees shall be considered a serious offense, which may lead to the termination of employment. The foregoing is without prejudice to any legal actions that may arise.

Failure to comply with this prohibition by suppliers hired by ARGOS shall be considered a serious enough offense to terminate the contract without prejudice to any actions that may arise.

When the object of the contract is related to PD, contracts with suppliers will include a provision related to the damages that ARGOS may incur and the consequences such as fines, operational penalties, and other sanctions that may be imposed on ARGOS by competent authorities as a result of the reckless and negligent actions of the supplier.

**11.2.** ARGOS forbids the transfer, communication or circulation of PD without the previous, written and express consent of the Holder or without the authorization of ARGOS. The transfer or communication of PD must be recorded in ARGOS' central registry of PD, and must be authorized by the database custodian.

**11.3.** ARGOS forbids the access, use, transfer, communication, treatment, storage, and any other type of treatment of sensitive PD that may identified during an audit in compliance with the Policy on the proper use of ARGOS' IT resources and/or other Policy issued by ARGOS for such a purpose.

Any sensitive data that is identified shall be reported to the Holder thereof in order for him or her to delete them. If this is not an option, ARGOS will delete them in a secure manner.

**11.4.** ARGOS forbids addressees of this Policy from any treatment of PD that may result in one of the behaviors described in Cybercrime Law 1273 of 2009, unless authorized by the Holder of the data and/or ARGOS, as the case may be.

**11.5.** ARGOS forbids the treatment of PD belonging to children and underage teenagers, except with the express authorization of their legal representatives. All treatment of data belonging to minors must ensure that the prevailing rights in the Political Constitution are recognized together with the Code for Children and Adolescents.

**XII. INTERNATIONAL TRANSFER OF DATA**

The transfer of PD to countries that do not provide adequate protection of data is forbidden. Safe countries are understood as those that meet the standards issued by the Superintendency of Industry and Commerce.

As an exception, ARGOS may transfer data internationally when:

**12.1.** The Holder of the data has granted authorization previously, expressly, and unequivocally for the transfer.

**12.2.** The transfer is necessary for the execution of a contract between the Holder and ARGOS as Treatment Manager and/or Supervisor.

**12.3.** Dealing with bank and stock transfers according to legislation applicable to such transactions.

**12.4.** Dealing with transfers within a framework of international treaties that are part of the Colombian legal system.

**12.5.** Transfers are legally required to safeguard the public interest.

At the time of an international transfer of PD, prior to sending or receiving such data, ARGOS shall sign agreements that regulate in detail the obligations, burdens and duties that arise for the participating parties.

Any agreements or contracts entered into shall abide by the provisions of this Policy, as well as by the legislation and jurisprudence applicable to the protection of PD.

It will be the responsibility of the Legal and Institutional Affairs Vice Presidency to approve the agreements or contracts that involve an international transfer of PD, by using the applicable principles in this Policy as guidelines.

It will also be the responsibility of this Office to make the pertinent queries to the Superintendency of Industry and Commerce to ensure the quality of "safe country" in relation to the destination and/or origin of the data.

**XIII. ROLES AND RESPONSIBILITIES FOR COMPLIANCE WITH THE PROTECTION OF PERSONAL DATA**

The responsibility of ensuring the appropriate treatment of PD within ARGOS belongs to all of its employees and corporate administrators. Consequently, every department that handles business processes that involve the treatment of PD must adopt rules and procedures for the implementation of and compliance with this standard, given their condition as custodians of the personal information contained in ARGOS' information systems. In the event of doubts regarding the treatment of PD, the department responsible for the security of the information and/or the Legal and Institutional Affairs Vice Presidency will indicate the guidelines to be followed, as the case may be.

**XIV. TEMPORALITY OF THE PERSONAL DATA**

When ARGOS processes PD, the permanence of the data in its information systems will be determined by the purpose of such treatment. Consequently, once the purpose for which the data was collected has been exhausted, ARGOS shall destroy or return the data, as the case may be, or else keep it as provided by law, while adopting the necessary technical measures to prevent inappropriate treatment.

**XV. SECURITY MEASURES**

When processing the PD regulated by this Policy, ARGOS shall adopt physical, logical, and administrative measures - which are classified as high, medium and low level - in accordance with the risk that may arise from the criticality of the processed PD.

In pursuit of the principle of PD Security, ARGOS shall adopt general guidelines for these measures, which shall be of mandatory compliance for the addressees of this Policy.

The addressees of this Policy are obligated to inform ARGOS of any suspicion that may involve the violation of the security measures adopted by ARGOS to protect the PD entrusted to them, as well as of any inappropriate treatment thereof, whenever they are aware of such a situation.

In these cases, ARGOS will communicate the situation to the controlling authorities and will manage the PD security incident in order to determine the legal repercussions, be they criminal, labor related, disciplinary or civil.

**XVI. PROCEDURES AND SANCTIONS**

ARGOS informs the addressees of this Policy of the sanctions regime provided by Law 1581 of 2012 in Article 23, which materializes the risks assumed by an undue treatment of PD:

*"ARTICLE 23. Sanctions. The Superintendency of Industry and Commerce may impose the following sanctions on Treatment Managers and Supervisors:*

*a) Personal and institutional fines up to the equivalent of two thousand (2,000) legal minimum monthly wages in force at the time of the sanction. Fines may be successive while the breach that gave rise to them subsists.*

*b) Suspension of activities related to treatment for a period of up to six (6) months.The suspension act will indicate the corrective measures that need to be adopted.*

*c) Temporary closure of treatment-related operations once the suspension term has expired without having adopted the corrective measures ordered by the Superintendency of Industry and Commerce.*

*d) Immediate and definitive closure of operations involving the treatment of sensitive data."*

The notification of any investigation procedure by any authority related to the treatment of PD shall be reported immediately to ARGOS' Legal and Institutional Affairs Vice Presidency in order to take the necessary measures to defend the actions of the company and prevent the imposition of the sanctions provided by Colombian legislation, in particular those contained in Title VI, Chapter 3 of Law 1581 of 2012 described above.

As a consequence of the risks assumed by ARGOS, both as PD Treatment Manager and/or Supervisor, failure to comply with this Policy by its addressees is considered a serious offense and will result in the termination of the respective contract without prejudice to any other legal actions that may arise.

**XVII. DELIVERY OF PERSONAL DATA TO AUTHORITIES**

Whenever government authorities request from ARGOS access to and/or delivery of PD contained in any of its databases, the legality of the request will be verified as well as the relevance of the requested data in terms of the purpose expressed by the authorities, and the delivery of the requested personal information will be documented, provided it meets all its attributes (authenticity, reliability and integrity), while warning the official making the request, the official who receives it, and the entity they work for, of the duty to protect such data. The authorities requesting the personal information shall be forewarned about the security measures applied to the PD they are receiving and of the risks involved in its undue use and inappropriate treatment.

**XVIII. RESTRICTIONS TO THE USE OF THIS POLICY**

This Policy is for the exclusive use of ARGOS, therefore, its copy, reproduction, distribution, transfer, publication, translation or any other use by persons outside of ARGOS is strictly prohibited, in

consideration of the respect for the intellectual property of its creators as well as for information security reasons.

**XIX. VALIDITY**

This Policy has been approved by ARGOS on April 8th of two thousand thirteen (2013).