PERSONAL DATA PROTECTION POLICY

IMAGINE WHAT
WE CAN BUILD TOGETHER

ARGOS

PERSONAL DATA PROTECTION POLICY

ARGOS

CEMENTOS ARGOS S.A. and its subordinated companies (hereinafter “ARGOS”) in compliance with the provisions related to the collection and treatment of personal data (hereinafter “PD”), have adopted the following policy of information security and treatment of personal data, prior to the following considerations:

1. ARGOS has been working on the process for regulating PD treatment under the framework of ISO 27001/27002, which means that ARGOS is subject to compliance with current regulations on PD.

2. In compliance of ARGOS´ obligation to improve its Information Security Management System within a *Plan-Do-Verify-Act* scheme, it is required to issue a standard that establishes the rules applicable to the treatment of PD that are under the responsibility of ARGOS.

3. It is ARGOS’ directives responsibility, as well as employees and vendors, to observe, obey and comply the orders and instructions that ARGOS issues regarding PD whose disclosure or improper use may harm its Data Holders.

4. Applicable regulations related to PD establish economic, commercial and criminal sanctions, and for that reason cooperation between ARGOS and the recipients of this policy is essential, to guarantee the rights of privacy, *Habeas Data* and protection of PD to prevent damages to Data Holders.

5. Internal regulation related to the protection of PD must include guidelines about the protection of personal information related to labor relations and provision of services, respecting the minimum rights and guarantees of employees and contractors. Contrary stipulations stated in internal regulation shall not produce any effect.

6. In accordance to labor law, employer has the duty to protect employees and employees have the duties of comply and behave loyalty to ARGOS, so that these duties contribute to the secure management of personal information.

7. This policy complements and does not contravene the obligations of employee and ARGOS contained in labor law.

8. It is ARGOS employees’ duty to fully support in case of an imminent risk or incident that affect or threaten the information assets, especially those related to the PD that ARGOS guards, assuring the provision of the cooperation required by ARGOS to investigate, analyze and capture evidence of security incidents that compromise this information (whether they have a judicial vocation or not) and complying with the instructions contained in the ARGOS chain of custody protocol.

Based on the above considerations that underlie the protection of PD in ARGOS, we adopted the following provisions which are mandatory for the recipients of this policy.

I. DEFINITIONS

1. **Automated Personal Database.** Organized set of personal data that is created, processed or stored through computer programs or software.

2. **Database Guard.** Is the employee, contractor or person who has the PD base in his custody within ARGOS.

3. **Data Administrator.** Natural or legal person, public or private authority, that by itself or in association with others, performs the PD treatment on behalf of the Database Responsible.

4. **Data Holder.** Natural person whose PD is being processed. Regarding legal persons, the name is preached as a fundamental right protected by the Constitution.

5. **Data Owner.** Each department that within the ARGOS business processes is responsible of the treatment and management of a specific PD Database.

6. **Data Responsible.** Natural or legal person, of a public or private nature, who collects the PD and decides on the purpose, content and use of the database.

7. **Data User.** Natural or legal person interested in the use of PD.

8. **Dissociation Process.** It refers to all PD treatment so that the information obtained cannot be associated to an identified Data Holder or identifiable person.

9. **Habeas Data.** Fundamental right of Data Holders to know, update, rectify or request suppression of the information and PD that have been collected or processed in public or private databases, in accordance with the provisions of the law and other applicable regulations.

10. **Information analysis and creation process.** Creation of information regarding a person, from the analysis and treatment of the collected and authorized PDs, for the purpose of analyzing and extracting profiles or behavior habits, which generate an added value on the information obtained from the Data Holders.

11. **Non-automated Database**. It is the organized set of personal data that is created, processed or stored manually, with the absence of computer programs or software.

12. **Personal Data.** It is any data or information that identifies a natural person or makes it identifiable, that can be numerical, alphabetical, graphic, visual, biometric, auditory, profiles or any other type of data.

13. **Personal Database.** Any organized set of personal data, whatever the form or modality of its creation, storage, organization and access

14. **Principles for data processing**. Fundamental rules of a legal or jurisprudential nature that inspire and guide the treatment of PD. Based on these principles, are determined the actions and criteria to solve the possible collision between the right to privacy, *Habeas Data*, protection of PD and the information right.

15. **Sensitive Personal Data.** It is a special category of personal data that is specially protected due to been related to health, sex, political affiliation, race or ethnic origin, biometric traces, among others, that are part of the person's privacy and can only be collected with the express and informed consent of its Data Holder and in the cases provided by law.

16. **Sources Accessible to the Public.** Databases containing PD whose consultation can be made by any person, which may or may not require a payment to access such data. Public databases include, among others, telephone directories, industry or sector directories as long as the information contained within these databases is limited to PD of a general nature or that contains generalities of law. The print media, official newspaper and other media will have this condition.

17. **Transfer of Data**. Data processing that involves its disclosure to a person different from the Data Holder or different from the person who was authorized process data.

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

19. **Violations of PD Security Measures.** Situation that implies a violation of the security measures adopted by ARGOS to protect the PD in custody, whether ARGOS acts as Data Responsible or Data Administrator, as well as any other conduct that according to this policy and law constitutes inappropriate treatment of PD. Any security incident involving the PD held by ARGOS must be reported to the supervisory authority.

II. OBJECTIVE

Adopt and establish the rules applicable to the treatment of the PD collected, processed or stored by ARGOS in the performance of its corporate purpose, either as Data Responsible or Data Administrator.

The rules adopted by ARGOS in this policy are in accordance with international standards regarding PD protection.

III. APPLICATION

The principles and provisions contained in this policy will be applied to any PD database that is in the custody of ARGOS, either as Data Responsible or Data Administrator.

All ARGOS organizational processes that involve the treatment of PD, must be subject to the provisions of this policy.

If there is a difference between the applicable regulations in any jurisdiction and this policy, the application of local regulations will prevail over this policy.

IV. SCOPE

This policy will be applied and therefore will bind the following people:

1. Legal Representatives or administrators of ARGOS.
2. ARGOS employees, with directive level or not, who guard and treat Personal databases.
3. Contractors and natural or legal persons who provide their services to ARGOS under any type of contractual modality, by which they carry out any PD treatment.
4. Shareholders, external auditors and those other persons with whom there is a statutory legal relationship.
5. Data Users including public and private persons.
6. The other persons established by law

V. APPLICABLE PRINCIPLES

The protection of PD in ARGOS will be subject to the following fundamental principles or rules. Internal processes related to the treatment of PD will be determined and interpreted in a harmonious, comprehensive and systematic way with these principles to resolve conflicts that arise in this matter..

1. **Informed consent or freedom principle.** PD treatment within ARGOS can only be done with the prior, express and informed consent of the Data Holder. PD may not be obtained, processed or disclosed without the authorization of the Data Holder unless a legal or judicial mandate supplants the Holder's consent.
2. **Legality.** PD treatment is a regulated activity and therefore the business processes and recipients of this policy must be subject to the provisions of this guideline.
3. **Purpose of data.** PD treatment must obey to a legitimate purpose, in accordance with the Constitution and the law, which must be informed in a concrete, precise and prior way to the Data Holder so that he expresses his informed consent.
4. **Data quality or veracity.** PD collected by ARGOS must be truthful, complete, accurate, verifiable, understandable and kept up to date. The treatment of partial, fractional, incomplete or misleading data is prohibited.

5. **Transparency.** In PD treatment Data Responsible or Data Administrator must grant, at any time and without restrictions, the Holder's right to obtain and know information about the existence of data that concerns him.

6. **Relevance of data.** In the collection of PD by ARGOS, the purpose of the treatment or the database must be considered. Therefore, PD must be adequate, pertinent and not excessive or disproportionate data in relation to the purpose. The collection of disproportionate PD in relation to the purpose for which they are obtained is prohibited.

7. **Restricted access and circulation.** The PD collected or processed by ARGOS will be used by the company only in the scope of the purpose and authorization granted by the Data Holder. Therefore, PD may not be accessed, transferred, assigned or communicated to third parties not authorized. PD in custody of ARGOS may not be available on the Internet or by any other means of mass disclosure, unless access is technically controllable and secure, and with the purpose of providing restricted knowledge to the Data Holders or authorized third parties in accordance with the provisions of the law and the principles that govern PD Treatment.

8. **Data temporality**. Once the purpose by which the PD was collected or processed has been finished, ARGOS must cease PD use and will adopt the appropriate security measures to do it. Commercial and legal obligations regarding the conservation of merchant books and correspondence will be considered.

9. **Data Security.** As Data Responsible or Data Administrator, ARGOS will adopt the physical, technological or administrative security measures that are necessary to guarantee the attributes of integrity, authenticity and reliability of PD. According to the PD classification, ARGOS will implement high, medium or low level security measures, applicable as appropriate, to prevent adulteration, loss, leakage, consultation, use or unauthorized or fraudulent access.

10. **Non-Disclosure:** ARGOS and all persons involved in PD treatment, have a professional obligation to save and maintain the reserve of such data, and this obligation remains even after the contractual relationship has ended. ARGOS will implement, in its contractual relations, data protection clauses associated to this principle.

11. **Information duty:** ARGOS will inform Data Holders, Data Responsible or Data Administrators the PD protection regime adopted by ARGOS, as well as the purpose and other principles that regulate the PD treatment. Additionally, complying with the registration required by law, ARGOS will report the existence of the personal databases guarded, the rights and the exercise of habeas data by Data Holders.

12. **Special protection of Sensitive Personal Data:** ARGOS will not collect or process PD exclusively linked to political ideologies, union affiliation, religious beliefs, sexual life, ethnic origin, and health data, except in cases of express consent of the Data Holder, making it clear that it is optional to answer questions that are related to Sensitive Personal Data or to minors or in those

cases of law in which consent is not required. Sensitive Personal Data can be obtained in the development of ARGOS activities, will be protected through high security measures.

VI. DATA HOLDERS' RIGHTS

In compliance with the fundamental guarantees enshrined in the Political Constitution and Law, Data Holders of the personal data bases contained in ARGOS information systems, have the rights described in this section. The exercise of these rights will be free and unlimited for the Data Holder, in accordance to legal provisions that regulate the exercise thereof. The exercise of Habeas Data, expressed in the following rights, constitutes a very personal power and will be exercised exclusively by the Data Holder, with the exceptions of law.

1. **Access right.** This right includes the Data Holders' power to obtain all the information regarding their own PD, whether partial or complete, information of the treatment applied, of the purpose of treatment, the location of the databases containing their PD, and about communications or assignments made regarding them, whether authorized or not.

2. **Update right.** This right includes the power of the Data Holders to update their PD when they have had any variation.

3. **Correction right.** This Right includes the power of the Data Holder to modify the data that turns out to be inaccurate, incomplete or non-existent.

4. **Cancelation right.** This Right includes the power of Data Holders to cancel their PD or delete them when they are excessive, not relevant, or the treatment is contrary law, except in those cases contemplated as law exceptions.

5. **Right to revoke Consent.** The Holder has the right to revoke the consent or authorization that enabled ARGOS for PD treatment with a certain purpose, except in those cases contemplated as law exceptions or when treatment is necessary in a specific contractual framework.

6. **Opposition right.** This right includes the power of Data Holders to oppose the treatment of their PD, except in cases where such right does not proceed by legal provision or for violating general superior interests to the private interest. ARGOS Legal Vice-Presidency, based on the legitimate rights that the Holder argues, will make a proportionality or weight judgment to determine the preeminence or not of the Data Holder's right over other rights, as information right.

7. **Right to file complaints and claims.** The Holder has the right to file complaints and claims, as well as the actions that may be pertinent, for the protection of his data before the competent authority. ARGOS will respond to the requests made by the competent authorities in relation to the rights of Data Holders.

8. **Right to grant authorization for data processing.** In development of the principle of informed consent, Data Holders have the right to grant their authorization to process their PD in ARGOS, by

any means that may be subject to subsequent consultation. Exceptionally, this authorization will not be required in the following cases: when required by a public or administrative entity in compliance with its legal functions, or by court order, in the case of data of a public nature, in cases of medical or health emergency, when it is information processing authorized by law for historical, statistical or scientific purposes, in the case of PP related to the Civil Registry of people. In these cases, although the Data Holder's authorization is not required, the other principles and legal provisions on PD protection will apply.

VII. DATA RESPONSIBLE AND DATA ADMINISTRADOR DUTIES

When ARGOS or any of the recipients of this policy, assume the role of Data Responsible, they must fulfill the following duties, as well as the other provisions stablished in the applicable law and in other regulations that govern their activity:

1. Guarantee to the Data Holder, at all times, the full exercise of the right of Habeas Data.
2. Request and keep, under the conditions set forth in this law, a copy of the respective authorization and consent granted by the Data Holder.
3. To inform the Data Holder about the purpose of the collection and the rights that are granted by virtue of the authorization given.
4. Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
5. Guarantee that the information provided to the Data Administrator is truthful, complete, exact, updated, verifiable and understandable.
6. Update the information, communicating in a timely manner to the Data Administrator, when there are changes regarding the data that has previously been provided and adopt the other necessary measures so that the information is kept updated.
7. Rectify the information when it is incorrect and communicate it to the Data Administrator.
8. Provide in each case to the Data Administrator only the PD whose Treatment is previously authorized in accordance with the provisions of the law.
9. Require always to the Data Administrator, respect for the security and privacy conditions of the Data Holders' information.
10. Process queries and claims in the conditions indicated in this norm and in the law.
11. Adopt internal guidelines that include the policies and procedures to guarantee adequate compliance with the law and especially for the attention of queries and complaints.

12. Inform the Data Administrator the cases when certain information is under discussion by the Data Holder, once the claim has been presented and the respective procedure has not been completed.

13. Inform, under request of the Data Holder about the use given to their PD.

14. Inform the data protection authority when there are violations of the security codes and there are risks in the management of the information of Data Holders.

15. Comply with the instructions and requirements issued by the competent authority.

When ARGOS or any of the recipients of this policy, assume the role of Data Administrator, they must fulfill the following duties, as well as the other provisions stablished in the applicable law and in other regulations that govern their activity:

1. Guarantee to the Data Holder, at all times, the full exercise of the right of Habeas Data.

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

3. Timely update, rectify or delete the data in accordance with the law.

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

5. Process the queries and claims made by the Data Holders in the terms indicated in this norm and in the law. This function will be headed by the ARGOS Legal Vice-presidency.

6. Adopt internal guidelines that include the policies and procedures to guarantee adequate compliance with the law and especially for the attention of queries and complaints.

7. Register in the database the legend "pending claim" in the way that is regulated by law, regarding those unresolved complaints or claims presented by Data Holders.

8. Insert in the database the legend "information in judicial discussion" once notified by the competent authority about judicial processes related to the quality of PD.

9. Abstain from circulating information that is being discussed by the Data Holder and whose blocking has been ordered by the competent authority.

10. Allow access to information only to people who by applicable laws are able to access it.

11. Inform the competent authority when there are violations of the security codes and there are risks in the administration of the information of the Data Holders.

12. Comply with the instructions and requirements issued by the competent authority.

In addition to ARGOS duties described above and complementing the obligations of any other person who assumes their condition of Data Responsible or Data Administrator, they will assume the following duties regardless of their condition:

1. Apply security measures according to the classification of the PD that ARGOS treats.
2. Adopt disaster recovery procedures applicable to databases.
3. Adopt Back Up procedures for databases containing PD.
4. Periodically audit compliance with this rule by its recipients.
5. Securely manage databases containing PD.
6. Apply this standard on PD protection in harmony with the Information Security Policy.
7. Maintain a central registry of the databases containing PD.
8. Securely manage access to the personal databases included in the information systems, in which this policy recipients act as Data Responsible or Data Administrator.
9. Have a procedure to manage security incidents with respect to databases containing PD.
10. Regulate access to databases containing PD in contracts with third parties.

VIII. PROCEDURE TO EXERCISE RIGHTS

In development of the constitutional guarantee of *Habeas Data* and regarding the rights of access, updating, rectification, cancellation and opposition by the Data Holder or the legally authorized interested party (Data Holders successors in title and legal representatives), ARGOS adopts the following procedure:

1. The Data Holder or the or the legally authorized person interested in exercising one of these rights, will accredit this condition by means of a physical or digital copy of the pertinent document and of his identity document. If the Data Holder is represented by a third party, the respective power of attorney must be submitted, which must have recognition of the content before a notary. The attorney must also prove his identity in the terms indicated before.

2. The request to exercise any of the aforementioned rights must be made in a physical or digital written support. The request to exercise those rights may be addressed to Argos offices, to the email datospersonales@argos.com.co or through the Transparency Hotline (lintransparencia@argos.com.co).

3. The request to exercise any of the rights will contain the following information:

- Name of the Data Holder, and his representatives, if applicable.
- Concrete and precise request for information, access, updating, rectification, cancellation, opposition or revocation of consent. In each case, the request must be reasonably substantiated so that ARGOS can answer as Data Responsible.
- Physical or electronic address for notifications.
- Documents that support the request.
- Signature of the request by the Data Holder.

If any of the requirements indicated above are missing, ARGOS will notify the interested party within five (5) days of receipt of the request, so that they can be rectified and then proceeding to respond to the Habeas Data request submitted. After two (2) months without submitting the required information, it will be understood that the request has been withdrawn.

When Argos acts as Data Responsible for the personal base contained in its information systems, will respond to the request within ten (10) days if it is a query; and fifteen days (15) days if it is a claim. ARGOS will answer in the same term when there is no PD of the interested party that exercises any of the indicated rights in the information systems.

In case of claim, if it is not possible to respond within fifteen (15) days, the interested party will be informed of the reasons for the delay and the date on which the claim will be attended, which in no case may exceed eight (8) days after the expiration of the first fifteen (15) days.

When Argos acts as Data Administrator, ARGOS will inform the Data Holder or the person interested in the personal data of such situation, and will communicate the request to the Data Responsible so that he responds the request, consultation or claim presented. A copy of such communication to the Data Responsible will be addressed to the Data Holder or interested party, so that they have knowledge of the identity of the Data Responsible who is the person obligated to guarantee the exercise of rights.

ARGOS will document and store the requests made by the Data Holders or by those interested in exercising any of the rights, as well as the responses to such requests. This information will be treated in accordance with the rules applicable to ARGOS correspondence.

Before going to the competent authority in the exercise of the legal actions contemplated for the Data Holders or interested parties, the process of queries or claims described above must be previously complied.

IX. CENTRAL DATABASES REGISTRY

In the development of ARGOS businesses whenever acting as Data Responsible or Data Administrator, will have a central registry in which it will list each of the databases contained in its information systems. The central personal databases registry will allow:

1. Register personal database contained in ARGOS information systems. It will be assigned a registration number to each data base. The inscription of the database will indicate: (i) The type of PD it contains; (ii) The purpose and intended use of the database; (iii) Identification of the department that processes the database; (iv) The treatment system used (automated or manual) in the database; (v) The indication of the level and security measures that apply to the database by virtue of the type of personal data it contains; (vi) The location of the database in the information systems; (vii) The group of people or stakeholders whose data is contained in the database; (viii) The condition of ARGOS as Data Responsible or Data Administrator for the treatment of the databases; (ix) Authorization to communicate or transfer the database, if it exists; (x) Origin of the data and procedure in obtaining consent; (xi) ARGOS official custodian of the database; (xii) The other requirements that are applicable in accordance with the regulations of the law that will be issued.

2. The cancellation of the personal databases will be also registered indicating the reasons and the technical measures adopted by ARGOS to make the cancellation effective.

3. For compliance and auditing purposes, the changes made in the personal databases will be periodically updated in relation to the requirements stated above. If the databases have not undergone changes, this will be recorded.

4. The record of security incidents that arise against any of the personal databases guarded by ARGOS and the sanctions imposed or the measures taken by the violations, will be also documented.

X. PERSONAL DATA TREATMENT

The operations in which Argos acts as Data Responsible or Data Administrator, will be governed by the following guidelines.

1. **Treatment of PD related to labor Relations.** ARGOS will process PD of its employees, contractors and of candidates who apply for vacancies, at three times: before, during and after the employment or service relationship. When the Treatment is before the employment relationship, ARGOS will inform, in advance, to the people interested in participating in a selection process, the rules applicable to the treatment of PD provided and obtained during the selection process. Once the selection process is exhausted and the Data Holder is not selected, ARGOS will report the negative result and deliver the PD collected to the non-selected persons, unless the Data Holder authorize the conservation, destruction or other treatment of PD. The information obtained by ARGOS regarding those who were

not selected, the results of the psychotechnical tests and interviews, will be eliminated from their information systems, thus complying with the principle of purpose.

When ARGOS contracts personnel selection processes with third parties, will regulate in the contracts the treatment that must be given to the PD delivered by the candidates, as well as the destination of the personal information obtained from the respective process. The PD and information obtained from the selection process regarding the personnel selected to work at ARGOS, will be stored in the personal folder, applying high level security measures to this information, due to the potential that such information contains sensitive data. The purpose of the delivery of the data provided by those interested in the vacancies of ARGOS and the personal information obtained from the selection process, is limited to apply to vacancies, therefore, its use for different purposes is prohibited.

ARGOS will store the PD and information obtained from the employee selection process in a folder identified with his name during the contractual relationship. This physical or digital folder will only be accessed and processed by the Labor Relations Area and to manage the contractual relationship between ARGOS and the employee. The use of employee information for purposes other than managing the contractual relationship is prohibited at ARGOS. The different use of employees' PD will only proceed by order of the competent authority, provided that such authority lies. The Legal Vice Presidency will be responsible for evaluating the competence and effectiveness of the order of the competent authority to prevent an unauthorized transfer of PD.

For data treatment after the contractual or labor relationship has ended, whatever was the cause, ARGOS will proceed to store in a central file the PD obtained from the selection process and the personal information collected during development of the employment relationship. Considering that labor data may contain sensitive data, high levels of security and controls will be applied to this information. Transferring such information to non-authorized third parties is prohibited because it may configure a deviation in the purpose for which PD were collected.

2. **Shareholders PD treatment.** PD of natural persons who have the status of shareholder of ARGOS, will be considered reserved information, since it is registered in the books of commerce and has the character of reserve by legal provision. Consequently, access to such personal information will be made in accordance with the rules contained in the Commercial Code that regulate the subject. ARGOS will only use PD of the shareholders for the purposes derived from the existing statutory relationship.

3. **Suppliers PD Treatment.** ARGOS will only collect from its suppliers the data that is necessary, pertinent and not excessive for selection, evaluation and execution of the contract that may take place. When ARGOS is required by legal obligations to disclose the supplier's personal data because of a contracting process, transfer will be carried out according to the provisions of this policy.

   ARGOS will treat PD of the employees of its suppliers, which are necessary, pertinent and not excessive to analyze and evaluate, according to the characteristics of the services contracted with the supplier, the security aspects of their access to ARGOS operations, as well as moral suitability and competence. Once these aspects are verified, ARGOS must return the information to the supplier, except when it is necessary to preserve this data. In any case, upon receipt of this information, the provider will collect the consent of its employees for the processing of their personal data and its transfer to ARGOS.

When ARGOS delivers PD from its employees to its suppliers, they must protect the PD transferred, in accordance with the provisions of this policy. For this purpose, the respective audit clause will be included in the contract or document that legitimizes the delivery of PD. ARGOS will verify that the requested data is necessary, pertinent and not excessive with respect to the purpose of the transfer.

4. **PD treatment in contracting processes.** The third parties that, in contracting processes, alliances and cooperation agreements with ARGOS, access, use, process or store, for the development of the contract with ARGOS, PD of ARGOS employees or ARGOS third parties, will comply this policy, as well as the security measures indicated by ARGOS according to the type of PD treated. For this purpose, the respective audit clause will be included in the contract or document that legitimizes the delivery of PD. ARGOS will verify that the requested data is necessary, pertinent and not excessive with respect to the purpose of the transfer.

5. **Communities' PD Treatment.** The collection of data from natural persons that ARGOS treats in the development of actions related to the community, either because of corporate social responsibility or any other social activity, shall be subject to the provisions of this regulation. For this purpose, ARGOS will previously inform and obtain the authorization of the Data Holders in the documents and instruments that it uses related to these activities.

In each of the cases described above, ARGOS departments that carry out the business processes in which PD is involved must consider the formulation of rules and procedures that allow compliance and the implementation of the standard adopted in this policy.

XI. PROHIBITIONS

1. ARGOS prohibits the access, use, management, transfer, communication, storage, and any other treatment of Sensitive Personal Data except when Data Holder consent its treatment or law authorizes ARGOS treating personal sensitive data without consent. Failure to comply with this prohibition by ARGOS employees will be considered a serious breach of labor obligations, which may lead to the termination of the employment relationship and even legal actions. The breach of this prohibition by the suppliers that contract with ARGOS will be considered as serious breach of contracts that may cause termination of the contract and even legal actions

2. ARGOS prohibits the transfer, communication or circulation of PD, without the prior, written and express consent of the Data Holder, except in cases when law authorizes ARGOS to transfer PD without Data Holder consent.

3. In application of the rule on the adequate use of ARGOS computer resources or other associated regulations, ARGOS prohibits the access, use, transfer, communication, storage and any other treatment of PD of a sensitive nature that can be identified in an audit process. The identification

of sensitive data will be reported to the Data Holder for deletion. If the deletion by the Data Holder is not possible, ARGOS will proceed to delete them safely.

4. ARGOS prohibits the recipients of this rule any PD treatment that may give rise to any of the conduct classified as cybercrimes.

5. ARGOS prohibits the treatment of minor's PD, unless is expressly authorized by their legal representatives, except in cases where the law authorizes ARGOS to process it without prior consent. In all treatment of minor's PD, the rights recognized in the Political Constitution or the law must be guaranteed.

XII. INTERNATIONAL DATA TRANSFER

The transfer of PD to countries that do not provide adequate levels of data protection is prohibited. Safe countries are understood as those that meet the standards set by the competent authority. Exceptionally, international data transfers may be made by ARGOS when:

1. Data Holder has granted his prior, express and unequivocal authorization to carry out the transfer.

2. The transfer is necessary for the execution of a contract between the Data Holder and ARGOS as Data Responsible or Data Administrator.

3. The transfer is associated to bank or stock transaction and is executed in accordance to the legislation applicable to such transactions.

4. The transfer is done in the framework of international treaties that are applicable.

5. The transfer is legally required to safeguard a public interest.

At the moment of an international transfer of PD, prior sending or reception of data, ARGOS will sign agreements that regulate in detail the obligations, burdens and duties that arise for the intervening parties.

The agreements or contracts that are concluded must comply with the provisions of this policy, as well as in the legislation and jurisprudence that may be applicable to PD protection.

The Legal department will be responsible for approving the agreements or contracts that entail an international transfer of PD, considering the principles contained in this regulation.

XIII. ROLS AND RESPONSIBILITIES

The responsibility for the proper treatment of PD within ARGOS corresponds to all its employees and administrators. Consequently, each ARGOS department that treats PD, given their condition of Database Guards, must adopt rules and procedures for the application and compliance of this policy, In case of doubt regarding the treatment of PD, the area responsible for information security or the Legal Department should be contacted to indicate the guidelines to be followed.

XIV. DATA TEMPORALITY

During the PD treatment done by ARGOS, the permanence of the data in its information systems will be determined by the purpose of data collection. Consequently, once the purpose for which the data was collected has been exhausted, ARGOS will proceed to its destruction or return or to conserve it according to the provisions of the law, adopting technical measures that prevent inappropriate treatment.

XV. SECURITY MEASURES

During PD treatment subject to regulations of this policy, ARGOS will adopt physical, logical and administrative security measures, which are classified as high, medium and low level, according to the risk that may arise from the criticality of the PD treated.

Recipients of this policy are obligated to inform ARGOS any violation to the security measures adopted by ARGOS to protect the PD as well as any inappropriate information treatment. In these cases, ARGOS will communicate the situation to the supervisory authority and will proceed to manage the respective security incident related to PD, to establish the criminal, labor, disciplinary or civil repercussions.

XVI. SANCTIONS

Failure to comply with this policy will constitute a violation of the employment or commercial contract with Argos and will entail the application of sanctions that may even imply the termination of the labor or commercial relationship. Additionally, it may imply sanctions imposed by the competent authorities.

The notification of any investigation initiated by any authority related to the treatment of PD, must be communicated immediately to the Legal Vice Presidency of ARGOS, in order to take the measures aimed to defend the company and to avoid the imposition of the sanctions established in the applicable law.

XVII. DELIVERY OF PERSONAL DATA TO AUTHORITIES

When the State authorities request ARGOS access or delivery of the PD contained in any of its databases, the legality of the request, the relevance of the data requested in relation to the purpose expressed by the authority, will be verified. The delivery of the requested of personal information will be documented, foreseeing that it complies with all its attributes (authenticity, reliability and integrity), and advising the duty of protection on these data, both to the official who makes the request, who receives it, and as the entity for which they work. The authority that requires personal information will be prevented about the security measures that apply to the PD delivered and the risks that their improper use and inappropriate treatment entail.