PERSONAL DATA PROCESSING POLICY
ARQUIB GROUP

PERSONAL DATA PROCESSING POLICY

CHAPTER I
GENERAL ASPECTS

1.1 INTRODUCTION

GRUPO INVERSIONES ARQUIB S.A.S. (in its position as holding company) and its related companies, which are listed at the end of this document (the "Related Companies"), which together form the ARQUIB GROUP, recognizes the importance of the security, privacy and confidentiality of the personal information of its customers, employees, suppliers and all other Data Subjects whose Personal Data is processed.

For this reason, in compliance with Articles 15 and 20 of the Political Constitution of Colombia, Law 1581 of 2012, Decree 1377 of 2013, ARQUIB GROUP adopts this Personal Data Processing Policy (hereinafter the "Policy") in order to guarantee the constitutional right of *habeas data*, as well as the privacy, intimacy and good name of its customers, employees, suppliers and all other Data Subjects.

ARQUIB GROUP shall ensure at all times access to this Policy so that its customers, employees, suppliers and all other Data Subjects may request rectification, clarification, modification and/or deletion thereof at any time. In turn, ARQUIB GROUP shall make a special effort to update this Policy, in response to legislative, regulatory or jurisprudential developments or its internal policies, which shall be informed and made known by written document, publication on its website, verbal communication or by any other source of information suitable for communication to interested parties.

1.2 LEGAL FRAMEWORK

This Policy is developed based on the following legal framework:

- Political Constitution, Articles 15 and 20.
- Regulatory Decree 886 of 2014.
- Statutory Law 1582 of 2012.
- Sole Decree 1074 of 2015.
- Regulatory Decree 1727 of 2009.
- Decree 1759 of 2016.
- Regulatory Decree 2952 of 2010.
- Decree 1377 of 2013.
- Title V of the Unified Official Letter of the Superintendency of Industry and Commerce.

1.3 DEFINITIONS

For the purposes of the interpretation of this Policy, the following definitions shall be adopted:

- **Authorization:** A prior, express and informed consent given by the Data Subject so that the Data Controller may carry out the Processing of the Personal Data.

- **Privacy Notice:** A verbal or written communication, electronic, physical or in any other format known or to be known, generated by the Data Controller by means of which the Data Subject is informed about the existence of the Data Processing Policies applicable to Data Subjects, the way to access such policies and the characteristics and purposes of the intended Processing of the Personal Data.

- **Database:** An organized set of Personal Data that is subject to Processing.

- **Queries:** The Data Subjects or their successors may query the personal information of the Data Subject contained in any database, whether in the public or private sector. The Data Controller or Data Processor shall provide them with all the information contained in the individual record or that is linked to the identification of the Data Subject.

- **Personal Data:** Any information linked or that can be associated to one or several individuals, determined or determinable. In other words, the “personal data” should be understood as information related to an individual.

- **Public Data:** It is data that is not semi-private, private or sensitive according to the mandates of the law or the Political Constitution. Data related to the marital status of individuals, their profession or trade, and their capacity as merchants or public servants, among others, are considered Public Data. By their nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins, duly executed court rulings that are not subject to confidentiality.

- **Semi-private Data:** It is information that is not of an intimate, confidential or public nature and whose knowledge or disclosure may be of interest not only to its Data Subject but also to a certain sector or group of persons or to society in general, such as financial or credit data or commercial or service activities.

- **Private Data:** It is data that, due to its intimate or confidential nature, is only relevant to the Data Subject. Private Data is understood as the tastes or preferences of individuals.

- **Sensitive Data:** Sensitive data are understood as those that affect the privacy of the Data Subject or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership at union, social, human rights or other organizations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sex life, and biometric data.

- **Rights of Children and Adolescents:** Processing shall ensure respect for the prevailing rights of children and adolescents. Only data of a public nature may be processed.

- **Data Processor:** Individual or legal entity, whether public or private, that by themselves or in association with others, carries out the Personal Data Processing on behalf of the Data Controller.

- **Habeas Data:** It is right that every Data Subject has to know, update, rectify or oppose the information concerning their personal data.

- **Data Processing Policy or Policy:** It refers to this document as a policy for the processing of personal data applied by the Company in accordance with the guidelines of the legislation in force on the matter.

- **Supplier:** Any individual or legal entity that provides any service to the Company by virtue of a contractual or mandatory relationship.

- **Claim:** The Data Subject or their assignees who consider that the information contained in a database should be corrected, updated or deleted, or when they notice the alleged breach of any of the duties contained in the law, may file a claim with the Data Controller or the Data Processor.

- **Data Controller:** It is the individual or legal entity, whether public or private, who by themselves or in association with others, decides on the Database and/or the Personal Data Processing.

- **Data Subject:** It is the individual to whom the information contained in a database refers. This person is subject to the right of *habeas data*.

- **Transfer:** It takes place when the Data Controller and/or Data Processor, located in Colombia, sends the Personal Data to a recipient, which in turn is a Data Controller and is located inside or outside the country.

- **Transmission:** Personal Data Processing that involves the communication to a third party inside or outside the territory of the Republic of Colombia, when such communication is intended for Processing by the Data Processor in the name and on behalf of the Data Controller, in order to comply with the purposes of the latter.

- **Processing:** Any operation or set of operations on Personal Data, such as collection, storage, use, circulation or deletion.

"For understanding the terms not included within the above list, you should refer to the legislation in force, especially Law 1581 of 2012 and Chapters 25 and 26 of Decree 1074 of 2015, giving the meaning used in said regulation to the terms whose definition is in doubt."

1.4 PURPOSE

The purpose of this document is to establish the criteria for the collection, storage, use, circulation, transfer, transmission, suppression and compliance with the purposes indicated below, which will be processed by each of the Related Companies, who will act as Data Controller of the Personal Data, respectively.

The purpose of the Data Processing Policy is to comply with Colombian legislation on personal data protection, that is, Article 15 of the Constitution, the Statutory Law 1581 of 2012 and its regulatory decrees and other regulations that add, supplement or amend them and inform Data Subjects of the purposes associated with the personal data processing to be carried out by the Related Companies as Data Controller who –in the exercise of its activities– hereinafter collects, processes, stores and disposes of Personal Data obtained and/or received from its customers, employees, suppliers and third parties, as well as to inform the rights to which they are entitled as a Data Subjects, the person or area responsible for addressing requests, queries and complaints and customer channels made available by the Related Companies to ensure the exercise of the right of habeas data.

Our Policy applies to all collection, storage, use, transfer, transmission, and suppression of information that may be associated or related to determined or determinable individuals within the territory of the Republic of Colombia, as well as the processing made by those third parties with whom the Data Controller agrees to carry out any activity related to, or associated with, the Personal Data Processing for which the Related Companies is responsible.

ARQUIB GROUP may also process the data of its former employees, visitors, guests and persons who request information about the services it provides, in accordance with the terms set forth in this policy.

The Personal Data collected shall be used to initiate, advance and maintain the contractual, commercial or labor relationship, and/or to receive advertising or information on which the Data Subjects have authorized its Processing, as well as responding to petitions and requests filed by Data Subjects.

Likewise, Personal Data shall be processed and/or transferred when a legal duty so requires and to comply with a competent authority's request when formally required.

1.5 SCOPE

Complying with the requirements of current regulations on Personal Data Protection, providing due protection to the interests and needs of the Data Subjects' information processed by ARQUIB GROUP. This Policy applies to all Data Subjects' information processed in any way by ARQUIB GROUP**.**

CHAPTER II
PRINCIPLES

2.1 PRINCIPLES

In the development of its commercial activities, ARQUIB GROUP shall collect, use, transmit, transfer and generally process the Data Subjects' information, in accordance with the purposes set forth in this Policy. To this end, ARQUIB GROUP is committed –regarding the development, interpretation and enforcement of law, regulations and standards in force– to apply the following principles in a harmonious and integral manner:

2.2 PRINCIPLE OF LEGALITY

Processing is a regulated activity that must be subject to the provisions of Law 1581 of October 17, 2012, regulatory decrees and other provisions that develop them.

2.3 PRINCIPLE OF PURPOSE

The Personal Data Processing made by ARQUIB GROUP shall comply with a legitimate purpose in accordance with the Constitution and the law, which in any case shall be informed to the Data Subject.

2.4 PRINCIPLE OF FREEDOM

Processing can only be carried out with the prior, express and informed consent of the Data Subject. Personal Data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that relieves consent.

2.5 PRINCIPLE OF VERACITY OR QUALITY

The information subject to Processing must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fractioned or misleading data is prohibited.

2.6 PRINCIPLE OF TRANSPARENCY

During Personal Data Processing, Data Subjects shall be guaranteed the right to obtain information about the existence of data concerning them from ARQUIB GROUP or the Data Processor, at any time and without restrictions.

2.7 PRINCIPLE OF RESTRICTED ACCESS AND CIRCULATION

The Processing is subject to the limits deriving from the nature of the Personal Data, the provisions of the law and the Constitution. In this sense, the Processing may only be carried out by persons authorized by the Data Subject and/or by the persons provided for by law. Personal Data, except for public information, may not be made available on the Internet or other means of mass dissemination or communication, unless access is technically controllable in order to provide restricted knowledge only to Data Subjects or authorized third parties.

2.8 PRINCIPLE OF SECURITY

The information subject to be processed by ARQUIB GROUP as Data Controller or Data Processor, or by a third party as Data Processor, shall be handled with the technical, human

and administrative measures that are necessary to provide security to the records avoiding their adulteration, loss, query, use or unauthorized or fraudulent access.

2.9 PRINCIPLE OF CONFIDENTIALITY

All persons involved in the Processing of Personal Data that are not of a public nature are bound to ensure the confidentiality of the information, even after the end of their relationship with any of the tasks comprising the Processing, and may only provide or communicate Personal Data, when applicable, for the development of the activities authorized in the regulations in force.

2.10 PRINCIPLE OF TEMPORALITY

Personal Data shall be kept only for the reasonable and necessary time to fulfill the purposes that justified the Processing, taking into account the provisions applicable to the matter in question and the administrative, accounting, fiscal, legal and historical aspects of the information. When necessary, Data shall be kept complying with a legal or contractual obligation. Once the purpose of the Processing and the terms established above have been fulfilled, the Data shall be deleted.

2.11 PRINCIPLE OF COMPREHENSIVE INTERPRETATION OF CONSTITUTIONAL RIGHTS

Law 1581 of 2012 shall be interpreted in the sense that constitutional rights, such as *habeas data*, the right to a good name, the right to honor, the right to privacy and the right to information are adequately protected. Rights shall be interpreted in harmony and balance with the right to information provided for in Article 20 of the Constitution and with the applicable constitutional rights.

2.12 PRINCIPLE OF NECESSITY

The Personal Data recorded in a Database must be strictly necessary for the fulfillment of the Processing purposes informed to the Data Subject. In this sense, they must be adequate, pertinent and in accordance with the purposes for which they were collected.

2.13 PRINCIPLE OF INTEGRITY

Partial, incomplete, fractioned or misleading personal data may not be processed, and the Data Controller shall be responsible for maintaining the integrity of the data.

CHAPTER III
DATA CATEGORIES

3.1 SENSITIVE DATA

According to the Definitions section, Sensitive Data is understood as: “Those that affect the privacy of the Data Subject or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions, social organizations, human rights or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sex life, and biometric data.”

3.1.1 Processing of Sensitive Data:

In accordance with the above, ARQUIB GROUP shall only be able to process this type of data in the following cases:

- When Data Subjects have given their explicit authorization to such Processing, except in those cases where the granting of such authorization is not required by law.

- When the Processing is necessary to safeguard the vital interest of Data Subjects and they are physically or legally incapacitated. In these events, the legal representatives must give their authorization.

- When the Processing refers to data that are necessary for the recognition, exercise or defense of a right in a judicial process.

- When the Processing is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit organization, whose purpose is political, philosophical, religious or union, provided that they exclusively relate to their members or persons who maintain regular contacts by reason of their purpose. In these events, Data may not be provided to third parties without the Data Subject's authorization.

- The processing has a historical, statistical or scientific purpose. In this event, the measures leading to the suppression of the Data Subject's identity shall be adopted.

In any case, and given the nature of such type of data, in compliance with Law 1581 of 2012 and regulations, ARQUIB GROUP must be subject to compliance with the following obligations:

- Inform Data Subjects that, since it is Sensitive Data, they are not obliged to authorize its processing.

- Inform Data Subjects, explicitly and in advance, in addition to the general authorization requirements for the collection of any type of Personal Data, which of the data to be processed are sensitive and the purpose of the processing, as well as obtaining their express consent.

3.2 PUBLIC DATA

According to the Definitions section, Public Data are those "that are not semi-private, private or sensitive. Data related to the marital status of individuals, their profession or trade, and their capacity as merchants or public servants, among others, are considered Public Data. By their nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins, duly executed court rulings that are not subject to confidentiality."

3.2.1 Processing of Public Data:

With respect to this type of data, ARQUIB GROUP shall be able to carry out their Processing according to the legal provisions in force.

3.3 SEMI-PRIVATE DATA AND PRIVATE DATA

Semi-private Data corresponds to "information that is not of an intimate, confidential or public nature and whose knowledge or disclosure may be of interest not only to its Data Subject but also to a certain sector or group of persons or to society in general, such as financial or credit data or commercial or service activities." While Private Data is "data that, due to its intimate or confidential nature, is only relevant to the Data Subject."

3.3.1 Processing of Semi-Private Data and Private Data:

For the processing of this type of data, ARQUIB GROUP must have the corresponding Data Subject's authorization. This authorization shall be based on the provisions of the Constitution and current regulations.

3.4 CHILDREN AND ADOLESCENTS' DATA:

ARQUIB GROUP shall ensure that the processing of this type of data is carried out in accordance with the rights of children and adolescents. In this sense, their special character shall be protected and their fundamental rights shall be respected, in accordance with the provisions of the law.

In this sense, ARQUIB GROUP shall comply with the following requirements and shall be subject to the following parameters:

- Processing shall respond to and respect the best interests of children and adolescents.

- To carry out any form of Processing, ARQUIB GROUP must have the authorization of the minor's legal representative.

- ARQUIB GROUP shall listen to the minor, respecting in any case their opinion, which shall be assessed taking into account their maturity, autonomy and capacity to understand the matter.

- ARQUIB GROUP must inform the optional nature of answering questions about the children or adolescents' data and also inform explicitly and in advance what the data and the purpose of processing are.

CHAPTER IV
AUTHORIZATION

4.1 AUTHORIZATION

Without prejudice to the exceptions provided for by law, the Processing requires the Data Subject's express, prior, free and informed authorization, which must be obtained by any means that may be subject to query and subsequent verification, such as a physical or electronic document, a data message, telephone calls, text messages or any technical or technological mechanism, known or to be known, that allows expressing or obtaining consent via click or double click.

The Data Subject's authorization shall not be necessary when:

- The information is required by a public or administrative entity in the exercise of its legal functions or by court order.

- The data is public.

- In cases of medical or sanitary emergency.

- The data processing has been authorized by law for historical, statistical or scientific purposes.

- It is data related to the Civil Registry of Persons.

The authorization may also be obtained from the Data Subjects' unequivocal conduct, which allow to reasonably conclude that they gave their consent for the Processing of their information. Such conduct must clearly externalize the will to authorize the Processing. The Data Subject's consent may be obtained by any means that may be subject to subsequent query, such as written, verbal, digital communication or by unequivocal conduct.

By virtue of its nature and corporate purpose, ARQUIB GROUP receives, collects, records, preserves, stores, modifies, reports, queries, delivers, transmits, transfers, shares and deletes personal information, for which it obtains the Data Subject's prior, express and informed authorization.

ARQUIB GROUP shall keep proof of such authorizations in an appropriate manner, ensuring and respecting the principles of privacy and confidentiality of information.

4.2 PROCESSING AND PURPOSES

The purposes for which each Related Company, in the development of its purpose, perform the Processing of Personal Information shall be regulated in each particular annex applicable to each of the Related Companies.

However, the main purposes of the Processing of Information with respect to employees, candidates and suppliers shall be those set forth below:

4.2.1 Employees

The following are the purposes of the Processing to be applied by ARQUIB GROUP to its employees:

a) Comply with laws, among others, on labor, social security, pensions, professional risks, family compensation funds (Integrated Social Security System) and taxes, and to develop the pre-contractual, contractual and post-contractual relationship.

b) Manage information internally, in the development of the existing labor relationship and in compliance with the legal obligations arising therefrom.

c) Comply with the requirements made by the competent judicial and/or administrative authorities.

d) Send information to participate in wellness and related activities developed by ARQUIB GROUP.

e) Send information to third parties, permitted by law, in order to perform wellness and related activities offered by ARQUIB GROUP.

f) Identify and secure biometric data captured through video surveillance or recording systems and to prevent internal and external fraud in this regard.

g) Process the minors' Personal Data in order to comply with legal obligations.

h) Manage the ARQUIB GROUP budget chain: payments, issuance of income and withholding certificates (individuals and legal entities) and payment reports.

i) Manage the Accounting process of ARQUIB GROUP.

j) Request and access my data for the purpose of training the staff in the development of the functions they perform as employees of ARQUIB GROUP.

k) Accomplish other purposes determined in processes for obtaining Personal Data for processing, and in any case in accordance with the law and within the framework of the functions of ARQUIB GROUP.

4.2.3 Candidates

The following are the purposes of the Processing to be applied by ARQUIB GROUP to its candidates:

a) Use, in the case of participants in selection processes, the processed Personal Data for carrying out the selection processes and managing the resumes, guaranteeing the principle of restricted access.

b) Adopt measures aimed at preventing illicit activities, including activities related to money laundering and terrorism financing.

c) Evaluate, corroborate and determine the candidate's compliance with the requirements of the position and ARQUIB GROUP, in accordance with the company's recruitment & selection policy and procedure.

d) Share the candidate information with third parties for reliability validation, i.e., home visit, medical examination, security study, integrity tests and any other required within the selection process.

e) Corroborate the correctness of the information provided by the applicant.

f) Perform other activities related to recruitment and selection of personnel.

g) Accomplish other purposes determined in processes for obtaining Personal Data for processing, and in any case in accordance with the law and within the framework of the functions of ARQUIB GROUP.

4.2.4 Suppliers

The following are the purposes of the Processing to be applied by ARQUIB GROUP to its suppliers:

a) Develop the corporate purpose of ARQUIB GROUP.

b) Collect the necessary information of any kind, permitted by law, for the participation and performance of wellness and related activities developed by ARQUIB GROUP.

c) Compile accounting records.

d) Manage billing.

e) Adopt measures aimed at preventing illicit activities, including activities related to money laundering and terrorism financing.

f) Accomplish other purposes determined in processes for obtaining Personal Data for processing, and in any case in accordance with the law and within the framework of the functions of ARQUIB GROUP.

4.3 DURATION OF THE PERSONAL DATA PROCESSING

Personal Data shall be subject to Processing by ARQUIB GROUP during the contractual term in which the Data Subject has the product, service, contract or relationship, plus the term

established by law. Additionally, they shall be kept in accordance with the principles of necessity and reasonableness.

CHAPTER V
DATA SUBJECTS' RIGHTS

5.1 DATA SUBJECT'S RIGHTS

The Data Subjects of the Information stored in the databases of ARQUIB GROUP may exercise the following rights at any time:

- Request proof of the authorization granted to ARQUIB GROUP, except when expressly exempted by law such authorization as a requirement for the Processing.

- Contact ARQUIB GROUP, through the channels established in this Policy, in order to know, update and rectify the Personal Data free of charge.

- Be informed by ARQUIB GROUP, upon request, regarding the use of the Data.

- File before the Superintendency of Industry and Commerce (SIC) complaints for violations of the provisions of the Data Protection Law as amended, substituted or added.

- File complaints before the Superintendency of Industry and Commerce for violations of the provisions of regulations in force.

- Access the Personal Data subject to Processing, free of charge.

- Know, update and rectify their information in case of partial, inaccurate, incomplete, fractioned, misleading data or the Processing of which is prohibited or has not been authorized.

Pursuant to Article 20 of Decree 1377 of 2013, the following persons may make the exercise of the aforementioned rights:

a) By the Data Subjects, who must prove their identity sufficiently by the different means made available for them by the Data Controller.

b) By their successors, who must prove their status as such.

c) By the Data Subjects' proxy and/or attorney-in-fact, upon accreditation of the proxy or power of attorney.

d) By stipulation in favor of or for another person.

e) The children or adolescents' rights shall be exercised by the persons who are empowered to represent them.

According to chapter XIII of this Policy, ARQUIB GROUP shall inform about the channels and procedures provided for the Data Subject to exercise their rights effectively.

CHAPTER VI
DUTIES OF ARQUIB GROUP AS DATA CONTROLLER AND DATA PROCESSOR

6.1 ARQUIB GROUP AS DATA CONTROLLER

Whenever each Related Company, as Data Controller of the Data Subject's Data, has information that may be subject to modification, verification, rectification, consultation and/or deletion, it shall:

- Guarantee the Data Subject, at all times, the full and effective exercise of the right of *habeas data*.

- Observe the principles relating to the Processing of Personal Data mentioned in this Policy.

- Request and keep a copy of the respective authorization granted by the Data Subject.

- Duly inform Data Subjects about the purpose of the collection and about the rights they are entitled to by virtue of the authorization granted.

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

- Ensure that the information eventually provided to the Data Processor is truthful, complete, accurate, updated, verifiable and understandable.

- Update the information, taking into consideration all new developments with respect to the Data previously provided and to adopt the other necessary measures so that the information provided is kept up to date.

- The rights of the Data Subject will be included in the Data Privacy Notice that will be published in each web page of the Related Companies and will be indicated at the time of obtaining the consent of the Data Subject.

- Rectify the information when it is incorrect and communicate the pertinent rectification to the Data Processor.

- Provide the Data Processor only with the data that it is authorized to provide to third parties.

- Require the Data Processor to respect the security and privacy conditions of the Data Subject's information at all times.

- Process the queries and claims formulated by the Data Subject in the terms indicated in this Policy.

- Inform the Data Processor when certain information is under discussion by the Data Subject once the claim has been filed and the respective process has not been completed.

- Inform, upon request of the Data Subject, about the use given to their data.

- Inform the Superintendency of Industry and Commerce of violations of security codes and risks in the management of the Data Subject’s information.

- Inform the Data Subject of the changes, additions and/or modifications to these policies regarding the use of information contained in their databases.

6.2 ARQUIB GROUP AS DATA PROCESSOR

In the cases in which any of the Related Companies acts as Data Processor, it shall comply with the obligations established and that coincide with those indicated in the capacity of Data Controller, only those that were not listed in section 6.1 of this Policy shall be expressly referred to in this section.

- Update, rectify or delete data on a timely basis.

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

- Allow access only to persons authorized by the Data Subject or empowered by law for that purpose.

- Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

6.3 EMPLOYEE DATA

The majority of employees' Personal Data is held in the Human Resources' main computer system. Human Resources is responsible for the general maintenance of employee data files.

Employees' Personal Data may also be disclosed, where the employee has consented, in response to requests from third parties –such as banks, mortgage lenders, prospective employers and organizations– seconded by employees.

In addition, employees' Personal Data may also be disclosed to outsourcing service providers or other agencies and/or companies providing services to ARQUIB GROUP, which are subject to a duty of confidentiality.

Automatically collected biometric data that can recognize each employee is considered sensitive data, therefore, it shall be processed accordingly.

From time to time, ARQUIB GROUP may disclose or be required to disclose employees' Personal Data in response to requests from a regulatory body, law enforcement or government agencies, or otherwise as part of an investigation or litigation process.

CHAPTER VII
GENERAL ACTIONS FOR THE PROTECTION OF PERSONAL DATA

7.1 DATA PROCESSING

All ARQUIB GROUP members, when performing the activities inherent to their position, shall assume the responsibilities and obligations inherent to personal information management, from its collection, storage, use, circulation and until its final disposal.

7.2 USE OF DATA

The personal information contained in databases must be used and processed in accordance with the purposes described in this Policy.

Likewise, the following assumptions should be taken into consideration:

a) If an area other than the one that initially collected the Personal Data requires to use it, it may do so as long as its use is in accordance with the nature of the services offered by ARQUIB GROUP and is in line with the purposes set forth in this Personal Data Processing Policy.

b) Each area must ensure that no confidential information or Personal Data is disclosed in the recycling practices of physical documents. Therefore, it shall not be possible to recycle resumes, academic degrees, academic or labor certificates, medical examination results or any document containing information that could identify a person.

c) In the event that a data controller has provided Personal Data or Databases to any area for a specific purpose, the area that requested Personal Data must not use such

information for a purpose other than that related to this Policy. At the end of the activity, the area that requested the information must eliminate the Database or the Personal Data used, avoiding the risk of outdated information or cases in which during that time a Data Subject has filed a claim.

d) Officers may not make decisions that have a significant impact on personal information, or that have legal implications, based solely on the information provided by the information system, so they must validate the information through other physical instruments or manually, and, if necessary, directly with the Data Subject, in cases where it is necessary.

7.3 STORAGE OF INFORMATION

Digital and physical information is storage in media or environments that have adequate controls for data protection. This involves physical and IT security controls, technological controls and environmental controls in restricted areas, in our own facilities and/or computer centers or document centers managed by third parties.

7.4 DESTRUCTION

The destruction of physical and electronic media is carried out through mechanisms that do not allow their reconstruction. It is carried out only in those cases in which it does not constitute the disregard of any legal regulation, always leaving the respective traceability of the action. Destruction includes information held by third parties as well as in our own facilities.

CHAPTER VIII
PROCEDURE FOR RESPONDING TO QUERIES, CLAIMS AND/OR COMPLAINTS

ARQUIB GROUP has an administrative infrastructure designed, among other functions, to ensure that requirements, requests, queries, complaints and claims related to data protection are duly managed, in order to guarantee the exercise of the rights contained in the Constitution and the law, especially the right to know, update, rectify and delete personal data, as well as the right to revoke the consent granted for the personal data processing.

For queries, claims, complaints or to exercise the rights you have as a data subject, you may contact ARQUIB GROUP as follows:

8.1 PROCEDURE TO RAISE QUERIES

The Data Subjects, their assignees or representatives may consult the personal information of the Data Subject contained in any Database owned by GRUPO ARQUIB. Thus, the Related Companies and/or the Data Processor shall provide them with all the information contained in the individual record or that is linked to the identification of the Data Subject.

a) Data Subjects may query their Personal Data at any time. For such purpose, you may submit a request indicating the information you wish to know, through any of the mechanisms indicated in section No. 8.3.

b) Data Subjects must prove their identity, that of their representatives, the representation or stipulation in favor of another or for another. When a person makes a request other than the Data Subject and it is not accredited that such person is acting on behalf of the Data Subject, it shall be deemed not filed.

c) The query must contain at least:

- The full name and surname(s) and address and/or e-mail address of the Data Subject or any other means to receive the response.

- Documents proving the identity of the applicant and, if applicable, that of their representative with the respective authorization.

- The clear and precise description of the Personal Data with respect to which the Data Subject seeks to exercise any of the rights and the specific request.

  If the query made by the Data Subject is incomplete, ARQUIB PLUS shall require the interested party within five (5) business days following the receipt of the query to correct the faults.

  If the applicant has not submitted the required information after two (2) calendar months from the date of the request, the request shall be deemed withdrawn.

- The queries shall be addressed by ARQUIB PLUS in a maximum term of ten (10) working days as from the date of receipt thereof.

  When it is not possible to respond to a query within said term, the applicant shall be informed about it, stating the reasons for the delay and indicating the date on which the query shall be responded, which in no case may exceed five (5) working days following the expiration of the term.

8.2 PROCEDURE FOR FILING COMPLAINTS AND CLAIMS

In accordance with the provisions of Article 14 of Law 1581 of 2012, when Data Subjects considers that the information processed by ARQUIB GROUP should be subject to correction, updating or deletion, or when it should be revoked by noticing the alleged breach of any of the duties contained in the Law, they may file a complaint or claim with ARQUIB GROUP, which shall be processed under the following rules:

a) Data Subjects or their representatives must prove their identity, that of their representatives, the representation or stipulation in favor of or for another person. When a person makes a request other than the Data Subject and it is not accredited that such person is acting on behalf of the Data Subject, it shall be deemed not filed.

b) The request for rectification, update, deletion or revocation must be submitted through the means made available by ARQUIB GROUP and indicated in this document and must contain, at least, the following information:

   - The name and address or e-mail address of the Data Subject or any other means to receive the response.

   - Documents proving the identity of the applicant and, if applicable, that of their representative with the respective authorization.

   - The clear and precise description of the Personal Data with respect to which the Data Subject seeks to exercise any of the rights and the specific request.

c) If the application is incomplete, ARQUIB GROUP shall require the interested party within five (5) business days of receipt to correct the faults.

   If the applicant has not submitted the required information after two (2) calendar months from the date of the request, the request shall be deemed withdrawn.

d) The maximum time to respond to this request shall be fifteen (15) business days from the day following the date of its receipt. When it is not possible to respond to it within said term, the interested party shall be informed of the reasons for the delay and the date on which the claim shall be responded, which in no case may exceed eight (8) business days following the expiration of the first term.

8.3 CHANNELS FOR ANSWERING QUERIES AND/OR COMPLAINTS

ARQUIB GROUP has made the following customer channels available for Data Subjects to exercise their rights, such as knowing, updating, rectifying and/or suppressing their personal data.

- WhatsApp chat: +57 (310) 810 9242
- Location: Km 2 vía Chía-Cajicá, Edificio Quantum Centro de Convergencia. Of. 405.
- Office Hours: Monday to Friday, from 8:00 am to 5:30 pm.
- E-mail: contacto@grupoarquib.com

8.4 COMPLAINTS FILED WITH THE SUPERINTENDENCY OF INDUSTRY AND COMMERCE

Data Subjects, assignees or any other person with legitimate interest, may only file complaints with the Superintendency of Industry and Commerce, upon exhausting the query, complaint and/or claim procedure before ARQUIB GROUP mentioned in this Policy, in accordance with the provisions of Article 16 of Law 1581 of 2012.

CHAPTER IX
VIDEO SURVEILLANCE

In the development of its corporate purpose and its relations with third parties, understood as users, employees, suppliers, customers, visitors, guests, and others, ARQUIB GROUP

captures images and sounds through its Video Surveillance System for the following purposes:

- Evidence risk factors and/or threats that may occur in the environment subject to the video surveillance system on a timely basis, in order to ensure the safety and peace of mind of users, employees, suppliers, customers, visitors, guests and others.

- Ensure effective monitoring of access controls to the different services and areas of the Institution, within its facilities and perimeter zones.

- Support the verification of internal and investigative procedures that may be necessary in the event of any contingency that may arise, either internally or at the request of a competent authority.

- Verify the quality of service in all areas subject to video surveillance and/or to respond to any internal query/complaint/claim filed.

The above applies to areas that have security cameras owned by each of the Related Companies as Data Controller has adopted procedures in order to inform the Holders that at the time of accessing their facilities, they are accessing a video surveillance area and that they will be recorded and monitored by the Video Surveillance System that is available, This procedure is informed through a privacy notice located at the gates and places with the greatest number of personnel, being understood that at the moment of accessing the facilities by means of unequivocal conduct, the Data Subject is authorizing the Processing of his/her Personal Data.

CHAPTER X
TRANSFER AND TRANSMISSION OF PERSONAL DATA

Each Related Company, as Data Controller of the personal data stored in its databases, may nationally or internationally transfer or transmit data in the development of the purposes described in this Policy.

Related Company shall verify that the recipient of the Personal Data offers an adequate level of data protection, as indicated by the Superintendency of Industry and Commerce, to

determine whether it has the appropriate conditions to ensure adequate levels of security for the information subject to transmission or transfer.

Additionally, Related Company shall enter into a transmission and/or transfer agreement or other legal instrument that guarantees the protection of the Personal Data subject to transmission and/or transfer and, in the applicable cases, Related Company shall request the declaration of conformity.

CHAPTER XI
VALIDITY OF AND AMENDMENT TO THE POLICY

This policy may be amended at any time in order to adapt it to new practices developed or legislative or jurisprudential developments in the field.

Each Related Company shall pertinently inform the Holders of any update or modification, in their respective web pages or in any other means deemed pertinent, indicating the effective date of the corresponding modification or update, as the case may be.

The present Personal Data Processing Policy of ARQUIB GROUP, is effective as of February 7, 2025.

GRUPO INVERSIONES ARQUIB S.A.S.
NIT. 900.809.925 – 6

ARQUIB PLUS FINTECH S.A.S.
NIT. 901.795.042-9

MAJ CARGO S.A.S.
NIT. 901.144.782-8

ARQUIB CONSULTING SERVICES S.A.S.
NIT. 901.772.275 - 9

ARQUIB CONTABILIDAD Y AUDITORIA S.A.S.
NIT. 901.797.954 – 1