Content

PRIVACY POLICY, PROCESSING AND PROTECTION OF PERSONAL DATA

INSURCOL SAS, a legal entity identified with Nit. 800.042.972-6, with registered office at Calle 41 No. 21-32, Bolívar neighborhood, Bucaramanga, Santander, and incorporated in accordance with the laws of the Republic of Colombia, establishes this personal data processing policy in compliance with Law 1581 of 2012 and its regulatory decrees, including Decree 1377 of 2013, Decree 886 of 2014, Resolution 2238 of 2024 of the Ministry of ICT, Circular 003 of 2024 of the SIC and the current provisions of the National Database Registry (RNBD).

1. OBJECTIVE

Establish the guidelines and procedures that regulate the collection, storage, use, circulation, transfer, and deletion of personal data managed by INSURCOL SAS, ensuring respect for the fundamental rights of data subjects and compliance with applicable regulations.

2. SCOPE

This policy applies to all databases and files containing personal information collected, stored, used, processed, or shared by INSURCOL SAS in the exercise of its corporate purpose.

INSURCOL SAS is committed to implementing technical, administrative and organizational measures that guarantee the security and confidentiality of personal data, in accordance with Law 1581 of 2012, Decree 1377 of 2013, Decree 886 of 2014 and Resolution 2238 of 2024 of the MinTIC. Likewise, in compliance with Circular 003 of 2024 of the SIC, the company will keep its databases updated in the RNBD and will facilitate the exercise of their rights by the owners.

By granting authorization for the processing of personal data, the data subject accepts the terms and conditions set forth in this policy.

INSURCOL SAS respects and protects the privacy of personal data provided by customers, employees, suppliers, and other stakeholders. This policy defines the purposes of processing, protection measures, and mechanisms for data subjects to access, update, rectify, delete their data, or revoke the authorization granted.

3. DATA CONTROLLER .

The party responsible for processing personal data is **INSURCOL SAS,** with Tax Identification Number 800042972-6, which acts as the controller for the management, storage, and protection of personal information collected in the course of its business:

a. Main address: Bucaramanga
b. Address: Calle 41 No. 21-32
c. Email: datospersonales@insurcol.com
d. Phone number: 300 2052430
e. Website: www.insurcol.com

4. RECIPIENTS OF THE DATA PROCESSING POLICY .

This policy is addressed to all natural persons whose personal data are in the databases of **INSURCOL SAS**, including, but not limited to, customers, employees, suppliers, contractors, business partners and any other person with whom the company has a commercial, employment or contractual relationship.

Likewise, this policy is mandatory for all employees, managers, and third parties who have access to personal information as managers, agents, or collaborators, ensuring compliance with legal provisions on data protection.

5. REGULATORY PROVISIONS.

This policy is developed within the framework of the personal data protection regime in Colombia, in accordance with the following provisions:

Article 15 of the Colombian Constitution protects the rights to privacy, good name, and habeas data. This constitutional provision informs the other rules governing data protection in Colombia.

Statutory Law 1581 of October 17, 2012, establishes the minimum conditions for legitimate processing of personal data of data subjects.

Decree 1074 of 2015, which incorporated Decrees 1377 of 2013 and 886 of 2014, among others, defined specific aspects regarding the collection of personal data, the content of the information processing policy, and the National Database Registry, among other points addressed.

External Circular 02 of November 3, 2015, from the Superintendency of Industry and Commerce.

Decree 1759 of 2016, which modifies article 2.2.2.26.3.1 of Decree 1074 of 2015, extending the deadlines for registering databases in the National Database Registry.

Resolution 2238 of 2024 of the Ministry of Information and Communications Technologies (MinTIC): This resolution updates the Ministry's personal data processing policy and repeals Resolution 924 of 2020. It establishes new guidelines for the management and protection of personal data in the institutional context.

Update of the National Database Registry (RNBD): In 2024, the obligation for companies and organizations to register and keep their databases updated with the RNBD was strengthened. This update is crucial to ensure transparency and the protection of citizens' rights regarding their personal data.

Circular 003 of 2024 From the Superintendency of Industry and Commerce (SIC): This circular reiterates the importance of complying with the obligations of registering and updating databases with the RNBD, and establishes specific measures to ensure the protection of personal data.

6. DEFINITIONS

For the purposes of interpreting and applying this policy, the following concepts must be considered:

- **AUTHORIZATION:** Prior, express and informed consent of the Data Subject to carry out the processing of personal data.
- **CONSULTATION :** Request from the Data Owner or persons authorized by the latter or by law, to know the information held about him in INSURCOL SAS databases or files.
- **COMPLAINT :** Request by the Data Subject or persons authorized by the Data Subject or by law to correct, update or delete their personal data or to revoke authorization in the cases established by law.
- **DATABASE :** Organized set of personal data that is the object of Processing.
- **PERSONAL DATA.** The information processed by **INSURCOL** , hereinafter referred to as "Personal Data", is that provided by the Owners when they access its goods and/or services, or in connection with them, such as: name, surname, identification, age, sex, telephone number, physical and electronic address, telephone number, country, city, financial and/or accounting information, profession, occupation, commercial and/or work experience, academic training, family data, and other necessary data requested in the registration process. Likewise, **INSURCOL** will process personal data obtained through its video surveillance systems. The collection of personal data through video surveillance systems at INSURCOL will be carried out through security cameras installed in each of its locations and on the premises where the company so requires for security purposes.
- **PRIVATE PERSONAL DATA** : Data that, due to its intimate or confidential nature, is only relevant to the data subject. Examples include information extracted from a home inspection, telephone number (if not found in public databases), or salary. This also includes data held in the Registry's files, referring to a person's identity, biographical details, affiliation, and fingerprint.
- **SENSITIVE PERSONAL DATA :** Information that affects a person's privacy or whose improper use may lead to discrimination, such as information that reveals racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organizations, human rights organizations, or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties, as well as data relating to health, sexual life, and biometric data (fingerprints, photos).
- **SEMI-PRIVATE PERSONAL DATA:** Semi-private data is data that is not of an intimate, reserved, or public nature and whose knowledge or disclosure may be of interest not only to its Owner but also to a certain sector or group of people or to society in general, such as, among others, data relating to the fulfillment or non-fulfillment of financial obligations or data relating to relationships with social security entities.
- **PUBLIC PERSONAL DATA:** Data classified as such by law or the Political Constitution, or data that is not private, semi-private, or sensitive. Public data includes, among others, the name, identification number, date and place of issue of the identification document, profession or trade, and status as a merchant or public servant, data contained in the National Single Transit Registry (RUNT), or data contained in the public commercial registry of the Chambers of Commerce, among others.

- **DATA CONTROLLER:** Person natural or legal entity, public or private, which by itself or in association with others, carries out the processing of personal data on behalf of the data controller .
- **DATA CONTROLLER: Natural or legal** person , public or private, who, by itself or in association with others, decides on the database and/or the processing of data.
- **SUBPROCESSOR:** Person who processes data on behalf of a Data Processor.
- **OWNER :** Natural person: clients, consumers , employees, former employees, suppliers, among others, whose personal data is subject to Processing.
- **TRANSFER :** activity in which the person responsible for and/or in charge of processing personal data, located in Colombia, sends the information or personal data to a recipient , who in turn is the person responsible for processing and is located inside or outside the country.
- **TRANSMISSION :** processing of Personal Data that involves communicating the same within or outside the territory of the Republic of Colombia when the purpose is to carry out Processing by the Data Controller on behalf of the controller;
- **SGPDP:** Personal data protection management system .
- **PDP:** Data Protection personal.
- **INCIDENTS:** These may be computer attacks or loss of databases due to internal reasons .
- **VIDEO SURVEILLANCE SYSTEM:** Video surveillance systems (CCTV) or security cameras implemented to ensure the safety of property or people in a given location have been increasingly used, as they are considered an ideal means of monitoring and observing activities in domestic, business, workplace, and public settings.
- **SAGRILAFT: Comprehensive Risk** Management and Self-Control System for Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction.
- **NNA:** Refers to those under 18 years of age, and corresponds to the acronym for Boys, Girls and Adolescents.
- **ICT:** Information and Communication Technologies
- **SUCCESSOR** In law, the successor in title is a natural or legal person who has succeeded or replaced another person, the deceased , by any legal title to the right of another. The succession or substitution may have occurred by an act inter vivos or by cause of death mortis causa.
- **ADEQUACY:** This means that personal data must be processed in a way that guarantees an adequate level of protection, in accordance with current regulations. This means that data can only be transferred to countries or entities that offer an adequate level of protection, recognized by the competent authorities.
- **RELEVANCE:** This principle establishes that the personal data collected and processed must be relevant and adequate in relation to the specific purposes for which they were obtained. That is, only the data necessary to fulfill the processing objectives should be collected and used.
- **PROPORTIONALITY.** This principle implies that the processing of personal data must be proportional to the purposes for which they are collected. This means that only data strictly necessary for the explicit, lawful, and legitimate purpose that justifies their processing should be processed, and for the time necessary to fulfill those purposes, avoiding any excess or misuse.

7. OBLIGATIONS.

This policy is **mandatory and must be strictly adhered to by INSURCOL SAS**, each and every one of its employees, contractors, strategic partners, and any third party that has access to personal data as a data **controller, processor, or subprocessor** . All parties involved in the processing of personal data must comply with the provisions set forth in this policy during the performance of their duties, activities, and contractual performance. This commitment remains in place even after the end of the employment, contractual, or commercial relationship with INSURCOL SAS.

Likewise, any person who accesses, manages or processes personal data by order of INSURCOL SAS is obliged to maintain **strict confidentiality and reserve.** regarding information, ensuring its adequate protection and preventing its unauthorized disclosure.
Failure to comply with these obligations constitutes a **very serious offense** and may give rise to disciplinary, contractual or legal sanctions as appropriate.

Any incident, irregularity, or non-compliance related to the processing of personal data must be reported immediately through the following channels:

- **Email:** personaldata@insurcol.com
- **Physical address:** Calle 41 No. 21-32, Barrio Bolívar, Bucaramanga, Santander, Colombia

INSURCOL SAS will take appropriate actions to ensure compliance with current regulations and the protection of the rights of data subjects.

8. ADMINISTRATIVE STRUCTURE ON DATA PROTECTION AND PROCESSING

INSURCOL SAS has defined the following governance structure for the **Personal Data Security Management System (SGSDP)** , with the purpose of guaranteeing the adequate protection and treatment of personal data in accordance with current regulations.

Governing Bodies of the SGSDP.

8.1 Higher Body of the SGSDP

- It will be the **General Manager** of INSURCOL SAS or the governing body designated by the company.
- You will be responsible for overseeing the implementation, compliance and continuous improvement of the SGSDP.
- It will rely on the **SGSDP Committee** and other assigned officials to ensure the proper functioning of the system.

The Systems Engineer will assume the role of president of the SGSDP and will be responsible for Technical Support. For administrative and documentary tasks, he or she will be supported by the Computer Engineer.

- It will act as **a communication channel** between the different bodies and members of the SGSDP.
- He will be responsible for coordinating the handling of **queries, complaints, and claims** submitted by personal data holders.

Area coordinators and/or sub-coordinators will make up the Personal Data Security Management System Committee (SGSDP).

- It will be the **body responsible for the implementation, maintenance and improvement** of the SGSDP.
- He will coordinate data protection strategies and oversee the implementation of policies and protocols.

8.2 SGSDP Key Area Managers :

8.2.1 Documentary Database Manager is the worker who manages and/or administers databases.

- Appointed by the **General Manager** through the job manual **.**
- Responsible for ensuring the implementation, compliance, and updating of policies and protocols related to **document management** and the secure storage of personal data.

8.2.2 Officer , INSURCOL legal advisor and/or INSURCOL lawyer:

- Appointed by the **General Manager** , through the job role and/or Function Manual.
- Ensures that INSURCOL SAS complies with current regulations on personal data protection and keeps legal protocols up to date.

8.3 Responsible for ICT, will be the Systems Engineer, for administrative and documentary tasks, will have the support of the Computer Engineer .

- Appointed by the **General Manager** .
- It guarantees the **digital security** of personal data, ensuring the correct implementation of cybersecurity, access, and protection policies in electronic media.

8.4 Manager /Systems Engineer:

- Appointed by the **General Manager,** through the job role and/or Function Manual.
- Oversees security in **physical spaces** , ensuring the proper protection of documents and information in non-digital media.

9 PROCESSING AND PURPOSE OF DATABASES.

INSURCOL SAS will collect, store, use, circulate, and delete personal data in accordance with this policy, limiting it to data that is relevant and appropriate for the specific purpose of its processing, in accordance with current regulations.

The information required from clients, suppliers, employees, shareholders, contractors, job applicants, and visitors will depend on the purpose for which it is requested.

In order to fulfill its mission, organizational commitments, and acquired obligations, INSURCOL SAS processes personal data for the following purposes:

9.1 Processing of Customer Data

INSURCOL SAS will collect and process its customers' personal data for the following purposes:

A. Commercial and Contractual Relationship

- Manage commercial and contractual relationships established with clients.
- Validate information on restrictive lists and carry out preventive monitoring in compliance with the **SAGRILAFT** and **Business Transparency and Ethics Program (PTEE)** .
- Maintain documentary evidence of document delivery, inductions, training, talks, meetings, and other company activities.
- Send invoices and communications related to contracts entered into between the parties.

B. Communication and Contact.

- Inform about the products and services offered by the organization.
- Establish communication with customers through calls, text messages, emails, physical documents, and corporate applications.
- Send information about events, organizational changes, policies and projects of INSURCOL SAS.
- Contacting customers for satisfaction surveys, market research, and customer segmentation.

C. Administrative and Operational Management.

- Conduct audits, analyses, and data studies to design, implement, and develop programs, projects, and events.
- Manage requests, complaints and claims submitted by customers.
- Contacting data subjects via telephone or electronic means for surveys and confirmation of personal data.
- Send account statements, invoices, and other information related to contractual obligations.
- Provide the services offered by INSURCOL SAS and accepted in the signed contracts.

D. Protection and Regulatory Compliance.

- Comply with laws, regulations, or legal processes requiring the disclosure of information.
- Implement measures to prevent fraud, security attacks or technical problems that affect INSURCOL SAS or third parties.
- Provide contact information to third parties with whom INSURCOL SAS has contractual relationships, when necessary for the fulfillment of its obligations.

E. Other Legal and Business Uses

- Offer additional products and services.
- Evaluate consumer habits, analyze trends, and conduct statistical studies.
- Request feedback on products and services.
- Other uses described in this policy or permitted by law.

9.2 Supplier Data Processing

INSURCOL SAS will collect and process information from its suppliers to efficiently manage the commercial and contractual relationship, ensuring regulatory compliance and security in the processing of personal data.

A. Commercial and Contractual Relationship

- Select, evaluate and re-evaluate suppliers, as well as manage invitations to quote and
- make purchases of goods and services.
- Make payments arising from contractual obligations.
- Send correspondence related to contracts and other business matters.
- Ensure the traceability and compliance of contracts entered into.

B. Communication and Contact

- Maintain contact with suppliers through calls, text messages, emails, and physical documents to manage quotes and develop business.
- Establish communication with suppliers on any aspect related to the purposes of this policy.
- Contact suppliers to conduct surveys, studies, or confirm personal data necessary for the execution of a contractual relationship.

C. Regulatory Compliance and Safety

- Conduct validations on restrictive lists and preventive monitoring in compliance with the SAGRILAFT and Business Transparency and Ethics Program (PTEE).
- Respond to requests from public, administrative and/or judicial entities.
- Ensure the correct linking of suppliers in compliance with current regulations.
- Implement control, follow-up, monitoring, and surveillance measures in the procurement of goods and services.
- Comply with laws, regulations, or legal processes requiring the disclosure of information.
- Prevent fraud, security attacks, technical problems or any situation that may affect INSURCOL SAS or third parties.

D. Administrative and Operational Management

- Audit, study, analyze, and use information from the database to design, implement, and develop programs, projects, and events.
- Socialize policies, projects, programs, results and organizational changes.
- Manage administrative procedures, requests, complaints and claims.
- Provide information to the sales force and/or distribution network, telemarketing, market research, and any third party with which INSURCOL SAS has a contractual relationship.
- Contact suppliers via SMS, chat, or email to send information about service improvement campaigns.
- Send account statements, invoices, and other information related to contractual obligations.
- Manage the delivery of documents, records of inductions, training sessions, talks, and meetings as evidence of contractual compliance.

E. Confidentiality and Data Protection

- The information provided by INSURCOL SAS to suppliers is confidential and must be protected in accordance with the provisions of Law 1581 of 2012 and the regulations that govern it.
- INSURCOL SAS suppliers must implement appropriate measures to guarantee the security and protection of the personal data processed.

9.3 Processing of Employee Data

INSURCOL SAS will store each employee's documents and personal data, both digitally and physically, in individual folders accessible only by the Human Resources, HSE&RSE, Payroll, and Quality Departments. This information is processed solely for the purpose of fulfilling and executing the employment relationship between the employee and INSURCOL SAS.

A. Contractual relationship and legal obligations

- Formalize the employment contract.
- Execute the object of the contract.
- Comply with legal obligations, such as affiliations with the General Comprehensive Social Security System (EPS, Pension Fund, ARL, Family Compensation Fund).
- Make payments for salaries, benefits, and extra-legal benefits not constituting salary through electronic transfers.
- Keep track of the terms of the contract and those arising from it.
- Determine the health conditions of the worker for his/her entry and exit.
- Issue employment certifications.
- Confirm employment references.
- Maintain a history of workers.

B. Administrative and operational management

- Manage the preparation of the identification card.
- Manage the opening of payroll accounts.
- Manage severance pay withdrawals, the acquisition of drafts, and discounts to AFC accounts.
- Manage the acquisition of airline tickets.
- Manage travel expense advances.
- Make reports on new developments in group policies.
- Manage user assignment for different technology platforms.

C. Control and monitoring of contractual compliance

- Provide information requested by clients, agencies, and/or auditors to verify the employee's professional profile and skills necessary for the execution of the contract.
- Provide information to INSURCOL SAS clients to control, monitor, and oversee compliance with local labor recruitment, respond to requests from public, administrative, and/or judicial entities, validate restricted lists of public entities or conduct preventive monitoring of counterpart knowledge, and perform statistical analyses of the hiring of skilled and unskilled labor.

D. Safety and health at work

- Record, track and control the worker's occupational medical history.
- Address issues related to occupational health and safety in the workplace, as well as the obligations, rights, and duties of both the employee and the company.

E. Regulatory compliance and audits

- Attend internal and external audits.
- Respond to requests and/or judicial and extrajudicial actions.
- Attend to administrative, judicial and extrajudicial matters.

F. Record and evidence of activities

- Serve as proof of document delivery, record of inductions, training sessions, talks, meetings, and various company activities.
- Provide evidence of any type of procedure, process and/or certificate required by the Company.

Additionally, INSURCOL SAS may:

A. Worker information management

- Obtain contact information, training, and other relevant information needed during the selection process and potential employment relationships.

- Carry out the relevant procedures for the development of the company's corporate purpose, in compliance with the contract entered into with the Data Subject.
- Manage administrative procedures such as applications, complaints, and claims.

B. Communication and notifications

- Contact the Owner by telephone to conduct surveys, studies and/or confirm personal data necessary for the execution of a contractual relationship.
- Contact the Data Controller via electronic means – SMS, corporate phone applications, or chat – to send news related to service improvement campaigns.
- Contact the Data Subject via email or corporate phone applications to send any type of information, account statements, or invoices related to the obligations arising from the contract entered into between the parties.

C. Compliance with obligations and benefits

- To comply with the obligations contracted by INSURCOL SAS with the Data Subject, in relation to the payment of salaries, social benefits and other remunerations established in the employment contract or as provided by law.
- Offer corporate wellness programs and plan business activities for the Holder and his or her beneficiaries (children, spouse, permanent partner).

D. Security and legal compliance

- Disclose information when necessary to comply with laws, regulations, or legal processes, ensure compliance with terms and conditions, stop or prevent fraud, attacks on the security of INSURCOL SAS or third parties, prevent technical problems, or protect the rights of third parties as required by law.
- The other purposes described in this policy or in the Law.

9.4 Processing of Shareholder Data

INSURCOL SAS will use the personal data of shareholders exclusively for purposes related to their status as partners of the company, ensuring compliance with applicable regulations and the confidentiality of the information.

A. Financial and administrative management

- Make the payment of utilities.
- Maintain a record of meetings held and validate the attendance of its members.

B. Calls and communication

- Convene the Shareholders' Meeting.
- Call meetings of the General Shareholders' Meeting.
- Send correspondence to shareholders.

C. Regulatory and legal compliance

- Attend to administrative, judicial and extrajudicial matters.
- Provide information to clients and/or third parties with whom we intend to initiate contractual and/or legal relationships, to certify the shareholding structure of INSURCOL SAS.
- Provide information to clients and/or their designated contractors for validation against restrictive lists or preventive monitoring of counterparty knowledge within the SAGRILAFT and Business Ethics and Transparency (PTEE) programs.

D. Record and evidence of activities

- Serve as proof of document delivery, record of inductions, training sessions, talks, meetings, and various company activities.
- Provide evidence of any type of procedure, process and/or certificate required by the Company.

9.5 Contractor Data Processing

INSURCOL SAS will collect and process the personal data of contractors for the purpose of properly managing the commercial and contractual relationships established, ensuring compliance with applicable regulations and the protection of information.

A. Contractual and administrative management

- Execute the purpose of the contract or order and comply with the other assumed services.
- Control and supervise the conditions of the contract and those derived from it.
- Make payments of obligations through electronic transfers.
- Issue certifications at the request of the owner.

B. Assessments and audits

- Attention to internal and external audits.
- Evaluate the performance of the Company's contractors.

C. Communication and correspondence

- Sending correspondence or communications related to the subject matter of the contract.
- Presentation and authorizations to the Company's contractors.

D. Regulatory and legal compliance

- Attention to administrative, judicial and extrajudicial matters.

E. Record and evidence of activities

- Serve as proof of document delivery, record of inductions, training sessions, talks, meetings, and various company activities.
- Provide evidence of any type of procedure, process and/or certificate required by the Company.

9.6 Processing of Data of Applicant Workers

INSURCOL SAS will collect and store the personal data of applicants during the selection process, both in physical and digital format. This data will be managed exclusively by the Human Resources Department, ensuring the implementation of appropriate security measures to protect its confidentiality.

A. Candidate Verification and Evaluation

- Verify the holder's information with companies, training and development centers, and authorities to check for criminal, disciplinary, and tax records, as well as traffic violations.
- Ensure that the candidate's profile is appropriate for the position being applied for, in terms of training, experience, and skills.
- Carry out psycho-technical evaluations.

B. Registration and Monitoring

- Maintain a historical record of applicants to be linked to the Company.
- Validate against restrictive lists of public entities or perform preventive monitoring of counterpart knowledge.

C. Regulatory Compliance and Evidence

- Attend to administrative, judicial and extrajudicial matters.
- Serve as proof of document delivery, record of inductions, training sessions, talks, meetings, and various company activities.
- Provide evidence of any type of procedure, process and/or certificate required by the Company.

9.7 Processing of Visitor Data

INSURCOL SAS will collect and store visitors' personal data for the purpose of managing their access to the facilities and ensuring the security of INSURCOL's personnel, assets, and infrastructure.

A. Access Control and Security

- Allow and manage access to the facilities.
- Maintain a visitor log for protection and control of entry and exit.
- Ensure the safety of INSURCOL's personnel, assets, and infrastructure.

B. Use of Surveillance Systems

Capture images and videos using the surveillance system to:

- Protect personnel, assets, and infrastructure from potential threats or incidents.
- Monitor and record who enters and leaves the premises, ensuring that only authorized persons have access.
- Deter criminal activities and facilitate the identification of persons involved in the incident.
- Provide visual evidence in the event of administrative, judicial, or extrajudicial investigations.
- Comply with safety and protection regulations established by law.

The data collected by INSURCOL's video surveillance systems at each of its locations is used for the following purposes:

a) Ensure the safety of assets and people who are part of the organization.
b) Ensure compliance with the labor obligations of visitors and INSURCOL employees.
c) Keep a temporary record of images for use in disciplinary investigations.
d) To be used in any judicial and/or extrajudicial proceedings in which INSURCOL is involved.

As proof of document delivery, records of inductions, training sessions, talks, meetings, and various company activities, as well as to demonstrate any type of procedure, process, and/or certification required by the Company.

9.8 Community Data Processing

INSURCOL SAS, in the development of its corporate purpose and within the framework of its Corporate Social Responsibility actions, may collect and process personal data of community members for the purpose of managing requests and ensuring regulatory compliance:

A. Attention to Requests and Management of PQRS

- Respond to requests, complaints and claims (PQRS) submitted by community members.
- Ensure effective communication with the community to resolve concerns and facilitate the management of procedures.

B. Validations and Regulatory Compliance

- Conduct validations on restrictive lists of public entities or carry out preventive monitoring of counterparty knowledge, if applicable.
- Attend to administrative, judicial and extrajudicial matters related to the community.

C. Record and Evidence of Activities

- Maintain a record of document delivery, inductions, training sessions, talks, meetings, and other company activities.
- Provide evidence of any type of formality, procedure, or certification that the company requires in its relations with the community.

9.9 Processing of Data of Former Employees

INSURCOL SAS will store and process the personal information of all individuals with whom it has signed employment contracts, for the purpose of ensuring compliance with legal, administrative, and labor obligations following the termination of the contractual relationship.

A. Registration and Certification

- Maintain a historical record of former employees, including the conditions of their employment and retirement.
- Issue certifications regarding the employment relationship that existed.

B. Compliance with Legal Requirements

- Respond to requests from judicial, public and administrative entities.

C. Occupational Medical History Management

- Record, track and control the worker's occupational medical history.
- Address issues related to occupational health and safety within the framework of the rights, duties, and obligations of both the employee and the company.
- Respond to requests and/or judicial and extrajudicial actions and administrative investigations that require the use of the employee's occupational medical history for the Company's defense.

D. Evidence and Control of Activities

- Attend to administrative, judicial and extrajudicial matters.
- Maintain records as proof of document delivery, inductions, training, talks, meetings, and other activities carried out within the company.
- Provide evidence of any procedure, process or certificate required by the Company.

10 ATTENTION TO QUERIES, COMPLAINTS AND CLAIMS FROM THE INFORMATION HOLDER

INSURCOL SAS, in compliance with Law 1581 of 2012 and Decrees 1377 of 2013 and 1074 of 2015, will address any query, complaint, or claim related to the handling of personal data through the Systems area.
Information holders may submit their requests at:

- **Administrative Headquarters** : Calle 41 No. 21-32, Barrio Bolívar, Bucaramanga - Colombia., **Systems Engineer, the support of the Computer Engineer may also be counted on .**
- **Email** : datospersonales@insurcol.com

10.1 Procedures for receiving and resolving queries and complaints

The Data Subject, their successors in title, representatives, and/or attorneys-in-fact may submit inquiries in person, in writing, or digitally, ensuring the protection and confidentiality of personal data.

10.1.1 Options for submitting the query:

10.1.1.1 In person:

- Go to the INSURCOL SAS administrative headquarters with identification.
- If submitted by a representative or attorney, a duly signed written Power of Attorney must be submitted, attaching a copy of the identification document of the owner and the attorney.
- Request to speak with the Systems Engineer, who will address your query or complaint.
- Once you have met with the systems engineer, he or she will record the inquiry using the **INSURCOL - established forms** within the comprehensive management system and continue with the customer service process.

10.1.1.2 Written:

- Presentation of the account of the request or claim to be made, this document must include the correspondence address or means to receive a response.
- Attach a copy of the identification document of the Holder or the attorney (in this case, include the authenticated power of attorney).

10.1.1.3 Digital:

- Go to the website www.insurcol.com in the PQR section and fill out the form.
- Send an email to datospersonales@insurcol.com.

10.1.2 Response Time:

- INSURCOL SAS will respond to the query within **a maximum of ten (10) business days** from its receipt.
- If it is not possible to respond within this period, the applicant will be notified of the delay, explaining the reasons and indicating the date on which the request will be resolved, in accordance with the **Habeas Data regulations.**

10.2 Procedures for claims

The owner of the information, his/her successors in title, representative and/or attorney who consider that the personal data in a Database should be **corrected, updated or deleted**, or who notice the alleged **non-compliance** with the duties established in Law 1581 of 2012, may submit a written complaint to the responsible area, following these parameters:

10.2.1 Claim Requirements :

The claim must be submitted by written request to the Systems Engineer area (see section 10 of this policy) and must contain:

a. The identification of the Holder.
b. The description and evidence of the facts that support the claim.
c. The correspondence address or means to receive a response

10.2.2 Claim Process :

1. **If the claim is incomplete,** the interested party will be asked to correct the information within five (5) business days following receipt of the claim.
2. If the applicant does not respond within two (2) months, it will be understood that he has withdrawn the claim.
3. Once the complete claim has been received, within a maximum period of five **(5) business days** , a legend will be included in the Claims Database with the indication " **claim in process** " and its reason. This legend will remain in effect until the claim is resolved.
4. INSURCOL SAS will attend to the claim in a maximum period of fifteen (15) business days, counted from the day following the date of receipt.
5. **If it is not possible to address the claim within this period** , the interested party will be informed of the delay, indicating the reasons and the resolution date, which may not exceed eight (8) business days after the expiration of the first period.

10.3 Procedure for Deleting the Storage of Personal Data in Physical Formats:

Personal data stored physically by INSURCOL SAS must be deleted according to the document control described in the **PERSONAL DATABASE MANAGEMENT MANUAL.**
This applies only to the following purposes:

1. According to the validity established in the manual
2. When the data subject so requests.

11 REQUIREMENT OF ADMISSIBILITY

The owner of the information or his successor in title only will be able to submit a complaint in view of the **Superintendence of Industry and Commerce** , once you have exhausted the consultation or claim process with INSURCOL SAS, in accordance with the provisions of current regulations.

12 CASES IN WHICH AUTHORIZATION IS NOT NECESSARY FOR THE PROCESSING OF PERSONAL DATA

In accordance with the provisions of Article 10 of Law 1581 of 2012, the Data Subject's authorization will NOT be required for the processing of his or her personal data in the following cases:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- Data of a public nature, as established by law
- Cases of medical or health emergencies, in which the processing of personal data is required to protect the health and life of the Data Subject.
- Processing of information authorized by law for historical, statistical or scientific purposes.
- Data related to the Civil Registry of persons.

13 AUTHORIZATION FOR PROCESSING SENSITIVE DATA:

For the collection and processing of sensitive data, the following requirements must be met

- Obtain explicit authorization, prior to or concomitant with the collection.
- Inform the Owner that he is not obliged to provide this data
- Implement special security measures such as database encryption, access control, and backups to secure locations.

13.1 Authorization for the processing of data of children and adolescents (NNA):

To collect and process data from children and adolescents, the following requirements must be met:

- Obtain authorization from their legal representatives, guaranteeing the minor's right to be heard according to their level of maturity.
- Please note that providing this data is optional.

INSURCOL SAS does not use, store, or process personal data of minors. If data of minors is detected in its databases, it will be deleted immediately.

14 PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA:

In the development, interpretation and application of this policy, the following principles shall be applied in a harmonious and comprehensive manner:

14.1 PRINCIPLES RELATED TO THE COLLECTION OF PERSONAL DATA.

The collection and processing of personal data must be carried out for lawful purposes and in compliance with current regulations. Personal data may only be collected and processed when it is adequate, relevant and not excessive in relation to the specific, explicit and legitimate purposes for which it was obtained .

Personal data will be processed fairly, legally, and transparently. They may not be used for purposes incompatible with those for which they were collected, except for historical, statistical, or scientific purposes, provided that appropriate security measures are adopted.

Personal data will be accurate and up-to-date. If it is determined to be inaccurate or incomplete, it will be updated, corrected, or deleted at the request of the data subject or at the initiative of the organization. Only the personal data strictly necessary to fulfill the purposes of processing will be collected, and the recording and disclosure of irrelevant data is prohibited. The data minimization principle will be applied to ensure that information processing is the minimum necessary to fulfill the intended purposes .

14.2 PRINCIPLES FOR DATA COLLECTION:

The Organization will take into account the following principles for data collection:

- **Adequacy**: The data must be suitable for the intended purposes.
- **Relevance:** The data must be relevant to the purposes of the processing.
- **Proportionality**: The data must be consistent with the purposes for which they were intended.

14.2.1 PRINCIPLE OF DIGNITY:

Any action or omission related to the processing of personal data must always be carried out while safeguarding the dignity of the Data Subject and respecting their constitutional rights. This includes, in particular, the right to a good name, honor, privacy, and the right to information. Protecting the Data Subject's dignity implies that any handling of their personal data must be carried out with respect and consideration, avoiding any form of abuse or mistreatment.

14.3 PRINCIPLES RELATED TO THE USE OF PERSONAL DATA.

- **PURPOSE:** Data must be processed for explicit, informed and legitimate purposes .
- **TEMPORALITY:** It They will retain it only for the time necessary to fulfill their purposes and legal obligations.
- **NON-DISCRIMINATION:** This It is prohibited to carry out discriminatory acts based on the information collected.

14.3.1 PRINCIPLE OF LEGALITY:

The processing of personal data is a regulated activity that must strictly comply with all applicable legal and regulatory provisions. According to Law 1581 of 2012, this activity must be governed by the principles of legality, purpose, freedom, truthfulness, transparency, restricted access and circulation, security, and confidentiality.

14.3.2 PRINCIPLE OF LIBERTY:

The processing of personal data may only be carried out with the prior, express, and informed consent of the Data Subject. This means that the Data Subject must be clearly informed about the specific purposes for which their data will be collected and used, and must freely and consciously grant their consent.

14.4 PRINCIPLES RELATED TO INFORMATION QUALITY.

- **TRUTHFULNESS OR QUALITY:** The information must be accurate, complete, up-to-date, and verifiable. The processing of partial, inaccurate, or misleading data is prohibited .

14.4.1 PRINCIPLE OF INTEGRITY:

When processing personal data, the Data Subject's right to obtain information from the Controller or the Data Processor about the existence of data concerning him or her, at any time and without restrictions, must be guaranteed.

14.5 PRINCIPLES RELATED TO THE PROTECTION, ACCESS AND CIRCULATION OF PERSONAL DATA.

- **SECURITY:** Technical and administrative measures will be implemented to prevent unauthorized access, loss or misuse of information .
- **TRANSPARENCY** : The owner has the right to obtain information about his or her data at any time .
- **RESTRICTED ACCESS:** Only the following may access the data:

  - ✓ Data subject.
  - ✓ Persons authorized by the Owner.
  - ✓ Authorities by legal mandate

- **RESTRICTED CIRCULATION:** Information will only be provided to :

  ✓ Data owner, their successors in title or their legal representatives.
  ✓ Persons authorized by law or by the Owner
  ✓ Public entities in the exercise of their functions, under appropriate protection measures.

- **CONFIDENTIALITY:** All persons involved in the processing of personal data must guarantee the confidentiality of the information, even after their relationship with the Organization has ended.

14.6 PRINCIPLES RELATED TO DATA TRANSFER AND TRANSMISSION

- **International transfer: Personal data** may only be transferred to countries that guarantee an adequate level of protection .
- **Transmission contract:** When data is transferred to data processors, a contract will be signed to guarantee its protection.

These principles ensure that personal data is processed in accordance with best practices and in compliance with current regulations.

15 STORAGE OF PERSONAL DATA.

The Data Subject expressly consents to INSURCOL storing their personal data in the manner it deems most appropriate, provided that the necessary security measures are in place to protect said information. INSURCOL is committed to implementing and maintaining robust and up-to-date security protocols, including both technical and organizational measures, to ensure the confidentiality, integrity, and availability of personal data. These security measures are designed to prevent unauthorized access, loss, alteration, or improper disclosure of information. Furthermore, INSURCOL will ensure that data storage complies with all applicable legal standards and regulations, thus providing comprehensive and effective protection of the Data Subject's personal data.

16 SECURITY MEASURES: INSURCOL

INSURCOL SAS is committed to the proper use and processing of personal data, preventing unauthorized access by third parties that could lead to the disclosure, violation, modification, disclosure, and/or destruction of the information stored in its databases. For this reason, INSURCOL has security and access protocols for its information, storage, and processing systems, including physical measures to control security risks.

17 RIGHTS OF THE HOLDERS. INSURCOL

INSURCOL SAS informs data subjects that, in accordance with current legislation, they have the right to access, update, and rectify their information, and/or revoke authorization for its processing. Specifically, the following rights apply to data subjects, as established in Article 8 of Law 1581 of 2012:

a) Know, update, and rectify your information if it contains partial, inaccurate, incomplete, fragmented, misleading data, or data whose processing is prohibited or unauthorized.
b) Request proof of the authorization granted for the processing of your data.
c) Be informed, upon request, regarding the use that has been given to your personal data,
d) Submit complaints to the Superintendency of Industry and Commerce for violations of the provisions of the law.
e) Revoke authorization and/or request deletion of the data, provided there is no legal or contractual obligation that prevents its deletion.
f) Access your personal data that has been processed free of charge.
g) Please refrain from answering questions about sensitive data. Answers that address sensitive data or data about children and adolescents are optional.

18 PREVENTION MEASURES TO GUARANTEE THE BASIC PRINCIPLES OF INFORMATION

- Inform and train company personnel to ensure the proper collection, handling, use, processing, storage, and sharing of personal information.
- Include confidentiality agreements for all company employees in their employment contracts.

19 INFORMATION SECURITY INCIDENT TREATMENT

cyberattack that puts the protection of personal data collected in the Company's databases at risk is known , the Company's compliance officer will promptly inform the Superintendency of Industry and Commerce and the information holders about what happened.

Once the incident has been reported and its cause established, an action plan will be implemented to prevent the situation from recurring.

20 PROCEDURE FOR THE EXERCISE OF THE RIGHT TO HABEAS DATA

a. In case you wish to exercise your rights, the owner must send an email or physical to the following contact addresses

Address: Calle 41 No. 21-32
Email: datospersonales@insurcol.com

b. **Requests and Queries Regarding Personal Data.** When the data owner or their successors in title wish to consult the information stored in the database, **INSURCOL** will respond to the request within a maximum period of ten (10) days. In compliance with the provisions of Law 1581 of 2012, when it is not possible to respond to the query within this period, the user will be informed, the reasons for the delay will be explained, and the date on which their query will be responded to will be indicated, which may not exceed five (5) business days following the expiration of the first term.

c. **Revocation of authorization, withdrawal, or deletion of the Database and claims regarding personal data.** When the data subject or their successors in title consider that the information contained in the databases should be corrected, updated, or deleted, or when they become aware of a presumed breach of any of the obligations contained in Law 1581 of 2012, they may file a claim with **INSURCOL** , which will be processed under the following rules:

d. The claim must be submitted by means of a request addressed to **INSURCOL.** To file and process your request, please provide the following information:

I. Full name and surname
II. Contact information (physical and/or electronic address and contact telephone numbers),
III. Means to receive a response to your request,
IV. Reason(s)/fact(s) giving rise to the claim with a brief description of the right you wish to exercise (know, update, rectify, request proof of the authorization granted, revoke it, delete it, access the information)
V. Signature (if applicable) and ID number.
VI. Annexes of the documents to be asserted.

If the claim is incomplete, INSURCOL may require the interested party to correct the deficiencies within five (5) days of receiving it. After two (2) months from the date of the request, if the applicant does not submit the required information, it will be understood that the claim has been withdrawn. If **INSURCOL** is not competent to resolve the claim, it will forward it to the appropriate party within a maximum period of two (2) business days and inform the Data Subject of the situation, thereby releasing it from any claim or liability for the use, rectification or deletion of the data.

Once the complete claim has been received, a legend stating "claim in process" and the reason for the claim will be added to the database within a period of no more than two (2) business days. This legend must remain in effect until the claim is decided.

The maximum term for addressing the claim will be fifteen (15) business days counted from the day following the date of receipt. When it is not possible to address the claim within this term, the Holder will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

21 VALIDITY

The personal data incorporated into the Database will be valid for the period necessary to fulfill its purposes.

The databases in which personal data will be stored will be valid for the same period as the information is maintained and used for the purposes described in this policy. Once these purposes have been fulfilled, and provided there is no legal or contractual obligation to retain your information, your data will be deleted from our databases.

22 CHANGES IN THE PRIVACY POLICY.

Any substantial changes to the Processing policies will be promptly communicated to Data Subjects by publication on our web portals.

23 CURRENT LEGISLATION.

The current national legislation on personal data protection is contained in Law 1581 of 2012, Decree 1377 of 2013, and Law 1266 of 2008, as well as any regulations that modify or supplement them.

OMAIRA CARDENAS RODRIGUEZ
General manager

revised : April 1, 2025
Current Review Date : June 27, 2025
Updated on the website: YES X NO ___
Website update date : June 27, 2025