Continental assist

Personal Data Processing Policy

2026

Table of Contents

1. OBJECTIVE

The purpose of this Personal Data Processing Policy is to establish the principles, purposes, guidelines, procedures, and control measures adopted by CONTINENTAL ASSIST, hereinafter THE ORGANIZATION, to ensure the protection, confidentiality, integrity, and availability of personal data that it collects, stores, uses, transmits, transfers, or deletes in the course of its operations.
This Policy aims to ensure compliance with the legal and regulatory provisions applicable to the protection of personal data in the jurisdictions where THE ORGANIZATION operates, including Colombia, Mexico, the United States, and when applicable the European Union, as well as international standards on privacy and information security. It guarantees the exercise of data subjects' rights and promotes an organizational culture of responsibility and data protection.

2. SCOPE

This Policy applies to THE ORGANIZATION, its subsidiaries, affiliates, branches, representative offices, and to all its managers, employees, contractors, suppliers, business partners, and third parties acting as data controllers or processors on behalf of THE ORGANIZATION.
The Policy applies to all personal data processed by THE ORGANIZATION, regardless of the medium or format in which it is stored, including physical, electronic, digital, automated, or manual databases, and to processing activities carried out inside or outside the territories of Colombia, Mexico, the United States, andwhen applicable the European Union, when such processing is related to operations of THE ORGANIZATION or to data subjects located in those jurisdictions.
This Policy also applies to all activities involving the processing of personal data, including collection, storage, use, circulation, transmission, transfer, updating, rectification, blocking, and deletion of personal data, in accordance with the applicable regulations.

3. TERMS AND DEFINITIONS

a. **Authorization:** Prior, express, and informed consent granted by the Data Subject for the Processing of their personal data, in accordance with applicable legislation.
b. **Database:** An organized set of personal data subject to Processing, regardless of its medium or format.
c. **Personal Data:** Any information related to or that can be associated with an identified or identifiable natural person.
d. **Sensitive Personal Data:** Information that affects the privacy of the Data Subject or that may lead to discrimination if misused, such as health data, biometric data, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, union membership, among others defined by applicable regulations.
e. **Public Data:** Personal data classified as public by law or the Constitution, or data that is not private or semi-private and whose access is not legally restricted.
f. **Private Data:** Personal data that, due to its intimate or reserved nature, is relevant only to the Data Subject and whose access is restricted.
g. **Semi-private Data:** Personal data that is not intimate, reserved, or public and whose knowledge may be of interest to the Data Subject, a specific group, or society in general, as defined by applicable law.
h. **Personal Data of Children and Adolescents:** Personal data concerning minors, whose processing is subject to special protection rules and the principle of the best interests of the child, in accordance with applicable regulations.
i. **Data Subject:** A natural person whose personal data is subject to Processing.

j. **Data Controller:** A natural or legal person, public or private, that decides on the collection, use, and other Processing of personal data, as well as the purposes and means of such Processing.
k. **Data Processor:** A natural or legal person, public or private, that processes personal data on behalf of the Controller, following their instructions and applicable law.
l. **Processing:** Any operation or set of operations performed on personal data, such as collection, storage, use, circulation, transmission, transfer, updating, rectification, or deletion.
m. **Data Transmission:** Processing involving the communication of personal data to a Processor, whether national or international, to process it on behalf of the Controller.
n. **Data Transfer:** Communication of personal data to a third party acting as a Controller, whether national or international, for its own or shared purposes.
o. **International Transfer of Personal Data:** Transfer of personal data to a recipient located in a country different from the one where the data or the Controller is located.
p. **Personal Data Security Breach (Security Incident):** Any event that causes the loss, destruction, alteration, unauthorized disclosure of, or improper access to personal data.

4. REGULATORY FRAMEWORK

This Policy is aligned with the following regulations and standards:

a) **Colombia:** Law 1581 of 2012 and regulatory decrees; Law 1266 of 2008.
b) **México:** Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP), its Regulation, and INAI Guidelines.
c) **United States:** California Consumer Privacy Act (CCPA) y CPRA, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Federal Trade Commission Act (FTC).
d) **European Union:** General Data Protection Regulation (GDPR).
e) **International Frameworks:** ISO/IEC 27701:2019 Privacy Information Management System (PIMS).

5. PRINCIPLES OF PROCESSING

The principles for the interpretation and application of this Policy are the following:

5.1 Legality: The Processing of Personal Data is a regulated activity subject to applicable laws.

5.2 Purpose: The Processing of Personal Data must adhere to a legitimate, specific, explicit, and informed purpose. Accordingly, THE ORGANIZATION will process personal data only for the purposes described in this Policy and/or those communicated to the Data Subject at the time of collection, as well as those necessary for carrying out its corporate purpose, providing its services, executing contractual relationships, and meeting legal and regulatory obligations, in accordance with applicable legislation.

5.3 Freedom: The Processing of personal data will be carried out based on a legitimate legal cause in accordance with applicable legislation in each jurisdiction. In Colombia and Mexico, when required, prior, express, and informed consent will be obtained from the Data Subject, except in cases expressly authorized by law.

5.4 Veracity: Information subject to Processing must be truthful, complete, accurate, up-to-date, verifiable, and understandable. Processing of partial, incomplete, misleading, or erroneous data is prohibited.

5.5 Transparency: Data Subjects shall have the right to access their Personal Data at any time and without restrictions.

5.6 Restricted Access and Circulation: Only authorized personnel of THE ORGANIZATION may process Personal Data.

5.7 Security: THE ORGANIZATION guarantees that it has implemented the necessary administrative, technical, and human measures to prevent Personal Data under its Processing from being altered, lost, consulted, used, or accessed without authorization or fraudulently.

5.8 Confidentiality: As a general rule, all Personal Data processed by THE ORGANIZATION is confidential. It will only disclose such information in cases expressly provided by law, including judicial or administrative orders, medical or health emergencies, or for statistical or historical purposes.

5.9 Integral Interpretation: Processing carried out by THE ORGANIZATION will consider current legal provisions, high court rulings, and instructions and guidelines issued by administrative authorities, such as the Superintendence of Industry and Commerce in Colombia.

6. DEVELOPMENT

6.1. Identification of Databases

THE ORGANIZATION manages and administers personal databases in the context of its commercial, operational, administrative, contractual, and labor activities.

Databases consist of organized sets of personal information that allow THE ORGANIZATION to meet contractual, legal, and operational obligations and to carry out its corporate purpose.

Databases may be stored in physical or digital formats, including information systems, cloud platforms, electronic files, manual records, and any other storage medium.

Below are the main types of databases:

Databases of Clients and Users: These databases contain personal information about individuals or legal entities that acquire, use, or interact with the products or services offered by THE ORGANIZATION.

They include identification data, contact information, contractual information, transactional data, commercial data, and any other information necessary for service provision.

a. **Third-party databases (corporate clients):** These correspond to databases owned by corporate clients or business partners who share information with THE ORGANIZATION for the provision of services to their users, affiliates, or end customers.
   In these cases, THE ORGANIZATION generally acts as the Data Processor, handling the information in accordance with the instructions of the Data Controller and the contracts signed between the parties.
b. **Databases of suppliers and contractors:** These include personal information of suppliers, contractors, and service providers, including natural persons or legal representatives of legal entities.

c. **Databases of employees, former employees, and candidates:** These databases contain personal information of job applicants, current employees, and former employees, including employment, academic, performance, payroll, and social security data.

6.2. Purposes of the processing of personal data

The personal data contained in the databases managed by THE ORGANIZATION shall be processed exclusively for the purposes described below, according to the nature of each database and in compliance with the applicable legislation on personal data protection.

1) Purposes of processing – Customer and user databases

The personal data of customers and users shall be processed for the following purposes:

a. Execute, develop, maintain, and manage contractual relationships with customers and users.
b. Provide the services offered by THE ORGANIZATION, ensuring their proper operation, continuity, and quality.
c. Manage customer service processes, support, requests, complaints, claims, and inquiries.
d. Carry out billing, collection, payment recovery, and reconciliation processes.
e. Establish and maintain communication channels with data subjects for the delivery of information related to services, account statements, operational and contractual notifications.
f. Send information about products, services, promotions, campaigns, events, or updates, when authorized by the data subject or permitted by applicable regulations.
g. Implement loyalty programs, benefits, satisfaction surveys, and service quality assessments.
h. Conduct internal analyses, statistical and technical studies, and continuous improvement of services, products, and processes.
i. Comply with legal, contractual, administrative, and regulatory obligations applicable to THE ORGANIZATION.
j. Respond to requests from competent judicial or administrative authorities.
k. Prevent, detect, and manage fraud, operational, commercial, or financial risks.
l. Ensure the security of individuals, facilities, technological platforms, and information systems.

2) Purposes of processing – Corporate client (third-party) databases

When THE ORGANIZATION acts as the Data Processor on behalf of corporate clients or business partners, personal data shall be processed for the following purposes:

a. Verify the identity of end users or individuals associated with corporate clients.
b. Coordinate, execute, and manage the delivery of contracted services.
c. Comply with the instructions provided by the Data Controller.
d. Execute and fulfill the contractual agreements signed between the parties.
e. Prepare reports, operational records, and information related to the execution of the service.
f. Respond to operational, contractual, or legal requirements associated with the provision of the service.
g. The processing of such data shall be carried out exclusively within the framework defined by the Data Controller and in accordance with the contracts signed.

3) Purposes of processing – Supplier and contractor databases

The personal data of suppliers, contractors, subcontractors, legal representatives, employees, or individuals associated with them shall be processed for the following purposes:

a. Carry out evaluation, verification, and contractual engagement processes.
b. Verify commercial, financial, reputational, and regulatory compliance backgrounds, including controls aimed at preventing money laundering, terrorist financing, and other legal or reputational risks.
c. Manage the execution, supervision, modification, and termination of contracts.
d. Administer accounting, financial, and payment processes, including invoicing, withholdings, tax obligations, and reporting to competent authorities.
e. Conduct internal or external audits, quality controls, performance evaluations, and risk management.
f. Manage physical or logical access to facilities, technological platforms, information systems, or corporate networks, when necessary for contractual execution.
g. Maintain operational, contractual, and administrative communication with suppliers and contractors.
h. Respond to requests from judicial, administrative, or regulatory authorities.
i. Comply with legal obligations in tax, accounting, commercial, and corporate compliance matters.
j. Retain contractual and documentary information for the periods required by applicable legislation.

4) Purposes of processing – Databases of employees, former employees, and candidates

1. Candidates and applicants

The personal data of applicants or candidates shall be processed for the following purposes:

a. Carry out recruitment, selection, evaluation, and verification of academic and employment references.
b. Conduct technical tests, psychometric assessments, or competency evaluations.
c. Retain résumés/CVs for future recruitment processes.

2. Active employees

The personal data of active employees shall be processed for the following purposes:

a. Formalize and manage the employment or contractual relationship.
b. Manage payroll, payments, social benefits, affiliations, and reporting to the social security system.
c. Comply with applicable labor, tax, and regulatory obligations.
d. Administer performance evaluations, disciplinary processes, and internal monitoring.
e. Manage training programs, welfare initiatives, professional development, and employment benefits.
f. Ensure the physical and technological security of THE ORGANIZATION's facilities, assets, information, and systems.
g. Manage physical and logical access to facilities, technological platforms, and corporate resources, including the processing of sensitive personal data such as fingerprints, facial recognition, or other biometric data, for entry and exit control, attendance registration, and monitoring of schedules and working hours.

h. Fulfill legal obligations regarding occupational health and safety, including, when necessary and permitted by law, the processing of sensitive personal data related to the employee's health.
i. Respond to requests from judicial, administrative, or regulatory authorities.

3. Former employees

The personal data of former employees shall be processed for the following purposes:

a. Retain employment information in accordance with applicable legal terms and deadlines.
b. Issue employment certifications and respond to requests made after the termination of the employment relationship.
c. Address judicial, administrative, or legal proceedings related to the terminated employment relationship.

6.3. Types of personal data processing

THE ORGANIZATION may carry out the following processing activities on personal data, in accordance with applicable laws:

a. **Collection:** Collection consists of obtaining personal data directly from the data subject or authorized third parties, through physical or digital forms, contracts, electronic platforms, phone calls, emails, cookies, administrative records, or other lawful mechanisms. Collection shall be conducted lawfully, transparently, and proportionally to the purpose of processing.
b. **Recording:** Recording consists of incorporating personal data into organized databases, information systems, or structured files, in order to enable their management, consultation, and control.
c. **Organization and storage:** Storage involves the preservation of personal data in physical or electronic media, ensuring their availability, integrity, and confidentiality through appropriate technical and administrative controls.
d. Use: Use consists of applying or utilizing personal data to fulfill the purposes informed to the data subject, including service provision, contractual management, customer service, internal analysis, and other legitimate activities.
e. **Analysis and processing:** Includes automated or manual processing of personal data to generate statistics, profiles, segmentations, reports, or improvements to products and services, always respecting the rights of the data subject and legal limitations. When processing involves decisions based solely on automated processing that produce legal effects or significantly affect the data subject, THE ORGANIZATION shall guarantee the right to request human intervention, express their point of view, and contest the decision, in accordance with Article 22 of the GDPR when applicable.
f. **Circulation or communication**: Circulation consists of the delivery or disclosure of personal data to authorized third parties, internal or external, when necessary to fulfill contractual, legal, or operational purposes.
g. **Transmission:** Transmission refers to the processing of personal data carried out by a third party acting as Data Processor on behalf of THE ORGANIZATION, under a contract that defines confidentiality and security obligations.
h. **Transfer:** Transfer occurs when personal data are sent to a third party acting as Data Controller, whether domestic or international, for its own or shared purposes, in accordance with applicable legislation.

i. **Updating and rectification:** Consists of modifying personal data to ensure their accuracy, truthfulness, and validity, in response to requests from the data subject or legal requirements.
j. **Blocking and deletion**: Blocking involves temporarily restricting the processing of personal data, while deletion consists of the permanent elimination of personal data when they are no longer necessary or when the data subject exercises their right under the law.

6.4. Authorization and legal basis for the processing of personal data

THE ORGANIZATION declares that, in accordance with applicable regulations in Colombia, Mexico, the United States, and, where applicable, the European Union, it shall obtain a valid legal basis for the processing of the personal data of data subjects contained in its databases. Such legal basis may consist of the data subject's consent, the execution of a contract, compliance with legal obligations, or legitimate interest, as appropriate.

Where required by applicable law, THE ORGANIZATION shall obtain the prior, express, and informed authorization of the data subject for the processing of their personal data.

For obtaining authorization, THE ORGANIZATION shall take into account the following:

a. THE ORGANIZATION shall adopt procedures to obtain the data subject's authorization no later than at the time of data collection, through physical, electronic, digital, or any other means permitted by law.
b. The data subject shall be clearly and previously informed of the data to be collected, the purposes of processing, the rights available to them, and the mechanisms to exercise such rights.
c. Authorization may be granted in writing, electronically, verbally, or through any unequivocal conduct of the data subject that reasonably allows concluding that consent has been given, in accordance with applicable legislation.
d. Consent, when serving as the legal basis for processing, must be expressed through a clear affirmative action. Silence, pre-checked boxes, or inactivity shall not constitute valid consent where the GDPR or other regulations requiring unequivocal manifestation apply.
e. THE ORGANIZATION shall retain evidence of the authorization granted by the data subject, in the terms required by law.
f. If the purpose of processing is substantially modified, the data subject shall be informed and, where required by applicable regulations, new authorization shall be obtained.
g. In the processing of sensitive data, the data subject shall be informed of which sensitive data will be processed, the purposes of such processing, and shall be advised that they are not obliged to authorize such processing, except in cases permitted by law.
h. THE ORGANIZATION shall not condition the provision of services on the authorization for the processing of sensitive data, unless such data are strictly necessary for service provision or required by law.
i. THE ORGANIZATION shall make available to the data subject free, accessible, and effective mechanisms to request the deletion of personal data, the revocation of consent, or the restriction of processing, in accordance with applicable legislation.
j. In jurisdictions where applicable, the data subject may exercise the right to opt out of the sale, sharing, or use of their personal data for targeted advertising or marketing, in accordance with applicable privacy laws (e.g., CCPA/CPRA in the United States).

6.5. Classification of personal data

THE ORGANIZATION may process the following categories of data:

a. **General personal data:** Identification, contact, employment, commercial, and financial information.
b. **Sensitive data:** Health data, biometric data, racial or ethnic origin, beliefs, trade union membership, or other protected data. These shall only be processed with explicit consent or legal mandate.
c. **Children's data:** Such data shall only be processed with the authorization of the legal representative and under the principle of the best interests of the child.
d. **Health information (HIPAA):** When THE ORGANIZATION acts as a Business Associate of a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), it shall comply with applicable contractual and regulatory obligations, including the execution of a Business Associate Agreement (BAA) and the implementation of administrative, technical, and physical safeguards in accordance with such regulation.

6.6. Duties and rights

6.6.1. Duties of THE ORGANIZATION as Data Controller

When THE ORGANIZATION acts as the Data Controller of personal data, it shall comply with the following obligations, without prejudice to those established under applicable regulations in Colombia, Mexico, the United States, and, where applicable, the European Union, as well as in this Policy:

a. Guarantee the data subject, at all times, the full and effective exercise of their rights in relation to personal data protection, including the rights of access, rectification, cancellation, deletion, objection, portability, and restriction of processing, as applicable under the relevant legislation.
b. Obtain and retain evidence of the legal basis for processing, including the data subject's consent when required by applicable regulations.
c. Clearly and previously inform the data subject about the purpose of data collection, the use of their personal data, the rights available to them, and the mechanisms to exercise such rights.
d. Implement and maintain reasonable and appropriate technical, administrative, and physical measures to protect personal data against loss, unauthorized access, misuse, disclosure, alteration, or destruction.
e. Ensure that the information provided to Data Processors or authorized third parties is truthful, complete, accurate, up-to-date, and relevant.
f. Adopt mechanisms for the timely updating of information and communicate necessary modifications to Data Processors to keep data current.
g. Rectify incorrect or incomplete information and communicate corrections to Data Processors and third parties who have received the data, where applicable.
h. Share only personal data whose processing has a valid legal basis under applicable regulations.
i. Require Data Processors to comply with confidentiality, security, and privacy obligations, including contractual data protection agreements (DPAs).
j. Address and process inquiries, requests, and claims submitted by data subjects within the timeframes established by applicable legislation.
k. Inform Data Processors when data are subject to requests, disputes, or verification processes, until the data subject's request is resolved.

l. Inform the data subject, upon request, about the use made of their personal data.
m. Notify competent authorities and, where required, data subjects, of security incidents or personal data breaches that pose risks to the rights and freedoms of data subjects, in accordance with applicable regulations.
n. When processing may involve a high risk to the rights and freedoms of data subjects, particularly in cases of large-scale processing of sensitive data, profiling, or the use of new technologies, THE ORGANIZATION shall conduct a Data Protection Impact Assessment (DPIA) in accordance with Article 35 of the GDPR, where applicable.
o. When the processing of personal data is subject to Regulation (EU) 2016/679 and THE ORGANIZATION is not established in the European Union but offers goods or services to individuals located in that territory or monitors their behavior, it shall designate a representative in the European Union in accordance with Article 27 of the GDPR.
p. Comply with the instructions and requirements of competent data protection authorities in the jurisdictions where THE ORGANIZATION operates (for example, the Superintendence of Industry and Commerce in Colombia, INAI in Mexico, and state authorities in the United States).

6.6.2. Duties of THE ORGANIZATION as Data Processor

When THE ORGANIZATION acts as the Data Processor on behalf of a Data Controller, it shall comply with the following obligations, without prejudice to those established under applicable regulations and contractual agreements:

a. Process personal data solely in accordance with the documented instructions of the Data Controller and applicable legislation.
b. Implement reasonable technical, administrative, and physical measures to ensure the security, confidentiality, and integrity of personal data.
c. Support the Data Controller in responding to data subject requests related to the exercise of their rights.
d. Update, rectify, block, or delete personal data when instructed by the Data Controller or when required by applicable legislation.
e. Restrict access to personal data exclusively to authorized personnel subject to confidentiality obligations.
f. Inform the Data Controller of security incidents or personal data breaches without undue delay.
g. Not disclose or transfer personal data to third parties without the authorization of the Data Controller, except where legally required.
h. Maintain records of processing activities when required by applicable legislation.
i. Where THE ORGANIZATION acts simultaneously as both Data Controller and Data Processor, it shall comply with the obligations applicable to each role.

6.6.3. Rights of data subjects

The data subjects whose personal data are processed by THE ORGANIZATION shall have the following rights, in accordance with applicable legislation in Colombia, Mexico, the United States, and, where applicable, the European Union:

a. **Right of access:** To know which personal data are processed, their origin, the purposes, and any transfers made.
b. **Right of rectification:** To request the correction of inaccurate, incomplete, or outdated data.

c. **Right of erasure or cancellation:** To request the deletion of personal data when they are no longer necessary, consent has been withdrawn, or processing is unlawful, except where legal retention obligations apply.
d. **Right to object or restrict processing:** To object to or limit the processing of personal data for certain purposes, including direct marketing, where permitted by law.
e. **Right to data portability:** To request the delivery of their personal data in a structured, commonly used, and machine-readable format, where applicable.
f. **Right to withdraw consent:** To revoke the authorization granted for the processing of personal data, when processing is based on consent.
g. **Right to opt out of the sale or sharing of personal data:** In jurisdictions where applicable (e.g., CCPA/CPRA in the United States), to request that their data not be sold or shared for targeted advertising.
h. **Right not to be subject to automated decisions:** To request human intervention when decisions are based solely on automated processing, where applicable.
i. **Right to file complaints or claims:** With THE ORGANIZATION or with the competent data protection authorities in each jurisdiction.
j. **Right to obtain a copy of the legal basis for processing:** To request proof of consent or other legal basis, where applicable.
k. **Right to free access:** To access their personal data processed by THE ORGANIZATION free of charge through the channels provided.

6.7. Procedures

The procedures established by THE ORGANIZATION to guarantee the rights of data subjects may be exercised by:

a. The data subject, who must prove their identity through reasonable means made available by THE ORGANIZATION.
b. Their successors, heirs, or assignees, who must prove such status in accordance with applicable legislation.
c. Their legal representative and/or attorney-in-fact, upon proof of representation or power of attorney through the relevant documents.
d. A person authorized by the data subject, when the data subject has granted authorization to act on their behalf, in accordance with applicable regulations.
e. In the case of children and adolescents (or minors), by the persons legally empowered to represent them.

The procedures, deadlines, and terms established in this chapter constitute the general rule applicable to the handling of inquiries, complaints, and claims related to the processing of personal data, as they correspond to strict standards designed to protect the rights of data subjects.

When the processing of personal data is subject to the legislation of a different jurisdiction, and such regulations establish longer deadlines or specific conditions for handling requests, THE ORGANIZATION may apply those terms to the extent they are mandatory, while ensuring in all cases timely, diligent, and rights-compliant attention to the data subject.

6.7.1. Procedure for handling inquiries

An inquiry is a request for information regarding the personal data processed by THE ORGANIZATION, for example:

a. Confirm whether THE ORGANIZATION holds personal data of the requester.

b. Request access to or a copy of the personal data being processed.
c. Ask how or for what purposes personal data are being used.
d. Request proof of the authorization granted, where applicable.

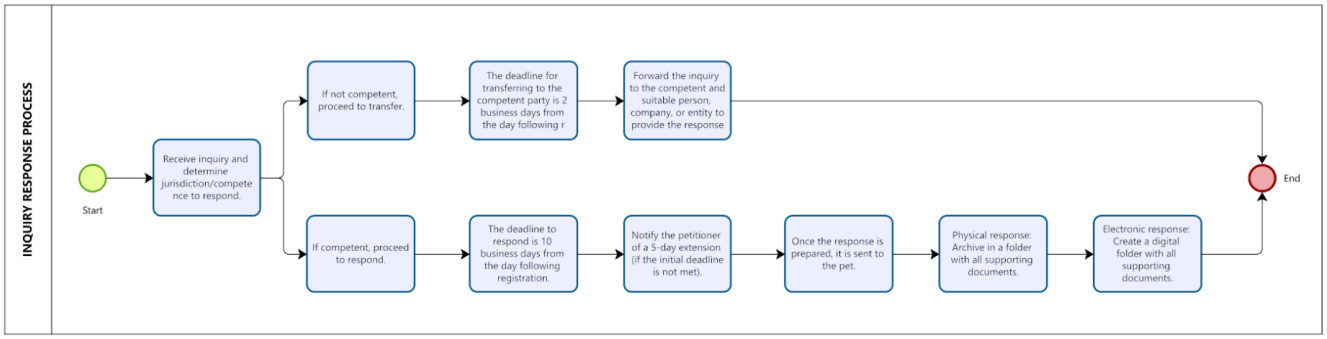
Important: If the data subject is unsure whether their request qualifies as an inquiry or a claim, they may submit it as a "data protection request," and THE ORGANIZATION will internally classify it to ensure proper handling.

Any data subject may inquire about the information contained in the databases managed by THE ORGANIZATION.

Data subjects may submit their inquiries via telephone communication or email, as detailed in this Policy.

THE ORGANIZATION shall respond within a maximum period of ten (10) business days, counted from the day following receipt of the inquiry.

If the initial period is insufficient to provide a response, THE ORGANIZATION may extend the deadline by an additional five (5) business days, in which case the data subject shall be informed along with an explanation of the reasons for the delay.



Fowchart No. 1 – Procedure for handling inquiries

6.7.2. Procedure for handling claims

A claim is a request to correct, update, delete personal data, revoke authorization, or report possible misuse. For example:

a. Correct inaccurate or outdated data.
b. Request the updating of information.
c. Request the deletion (erasure) of personal data where applicable.
d. Request the revocation of authorization, where applicable.
e. Report that unauthorized or unlawful processing is being carried out, contrary to the law or to this Policy.

Note: Requests for deletion or revocation of authorization shall not proceed where there is a current legal or contractual obligation requiring the retention or processing of the information.

Any data subject may submit claims related to the information contained in the databases managed by THE ORGANIZATION.

Data subjects may submit their claims via telephone communication or email.

THE ORGANIZATION shall respond within a maximum period of fifteen (15) business days, counted from the day following receipt of the claim.

If the initial period is insufficient to provide a response, THE ORGANIZATION may extend the deadline by an additional eight (8) business days, in which case the data subject shall be informed along with an explanation of the reasons for the delay.

The claim must include the identification of the data subject, a description of the facts giving rise to the claim, the address, and any supporting documents the claimant wishes to submit.

If the claim is incomplete, the claimant shall be required, within five (5) business days following receipt of the claim, to correct the deficiencies.

If two (2) months elapse from the date of the request without the claimant providing the required information, it shall be understood that they have withdrawn the claim.

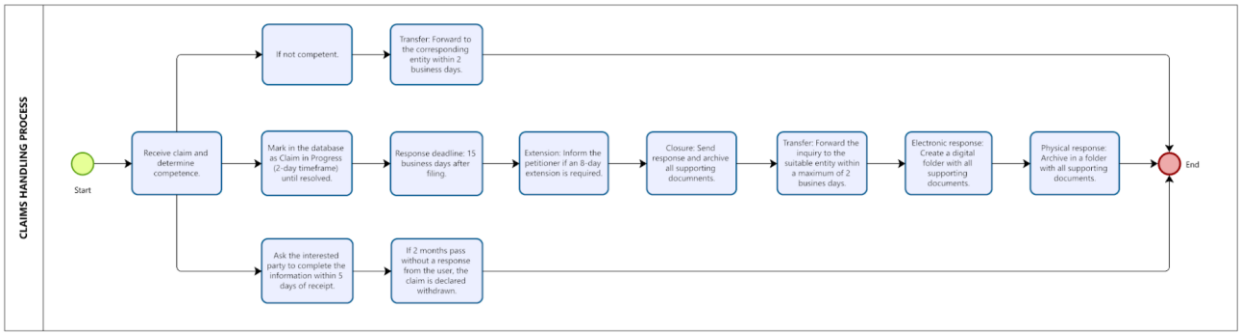
Once the complete claim has been received, a note shall be included in the database stating “claim in process” and the reason for it, within no more than two (2) business days. This note shall remain until the claim is resolved.

6.7.3. Forwarding of inquiries or claims due to lack of competence

In the event that THE ORGANIZATION is not competent to respond to the inquiry or claim submitted by the data subject, it shall forward the inquiry or claim to the competent party within two (2) business days following the date of receipt, and shall notify the data subject accordingly.

6.7.4. Updates by successors, legal representatives, and attorneys-in-fact

Requests may also be submitted on behalf of the data subject by their attorneys-in-fact, legal representatives, or successors, who must prove their status through a birth certificate, a duly granted general or special power of attorney, a document evidencing the initiation of succession proceedings, or, in general, any document that meets the legal requirements to demonstrate that they are acting on behalf of the data subject.



Flowchart No. 2 – Procedure for handling claims

6.8. Transfer of personal data to third countries

6.8.1. International transfer of personal data to third countries

THE ORGANIZATION may transfer personal data to recipients located in other countries when necessary for the development of its activities, the provision of services, contractual compliance, operation of technological platforms, support, customer service, legal compliance, or any other informed and permitted purpose.

In all cases, international transfers shall be carried out in accordance with the requirements, authorizations, exceptions, and/or mechanisms applicable in each jurisdiction where the data subjects are located, where THE ORGANIZATION operates, or where processing takes place, implementing reasonable contractual, technical, and organizational safeguards to protect personal data.
To ensure an adequate level of protection, THE ORGANIZATION may implement, among others, the following mechanisms:

a. Data Transfer Agreements (DTA).
b. Standard contractual clauses or model contractual clauses for data protection.
c. Binding Corporate Rules (BCR).
d. Data Processing Agreements (DPA) with third parties.
e. International transfer risk assessments and mitigation measures.
f. Transfer Impact Assessments (TIA), when the destination country does not have an adequacy decision issued by the European Commission.

6.8.2. Exceptions to the restriction on international transfer

The restriction on transferring personal data to third countries shall not apply in the following cases, in accordance with applicable regulations:

a. Transfers necessary for the execution of financial, banking, or securities transactions, in accordance with applicable legislation.
b. Transfers carried out within the framework of international treaties or agreements entered into by the States where THE ORGANIZATION operates, under the principle of reciprocity or international cooperation.
c. When the data subject has granted prior, express, and informed consent for the international transfer of their personal data, where such consent is required by applicable regulations.
d. Exchange of medical or health-related data, when necessary for the protection of the life, health, or integrity of the data subject or other persons.
e. Transfers necessary for the execution of a contract between the data subject and THE ORGANIZATION, or for the implementation of pre-contractual measures requested by the data subject.
f. Transfers required for the safeguarding of public interest, or for the recognition, exercise, or defense of a right in judicial, administrative, or arbitral proceedings.
g. Transfers made to service providers or Data Processors acting on behalf of THE ORGANIZATION, provided that there is a contract ensuring confidentiality, security, and processing limitations.

6.8.3. Transfers to the United States and other countries without comprehensive privacy laws

In jurisdictions that do not have a comprehensive personal data protection law, THE ORGANIZATION shall implement contractual, technical, and organizational safeguards to ensure an adequate level of protection, including confidentiality obligations, usage restrictions, security measures, and audit mechanisms.

6.8.4. Information to the data subject

The data subject shall be informed, under the terms required by applicable regulations, about the international transfers of their personal data, the purposes of such transfers, and the protection mechanisms implemented.

6.9. Registration of databases

To the extent applicable under current regulations in each jurisdiction, THE ORGANIZATION shall carry out the registration, enrollment, or notification of its personal data databases before the competent data protection authorities, providing the required information regarding the identification of the databases and the Personal Data Processing Policies.
In Colombia, where applicable, THE ORGANIZATION shall register its databases in the National Database Registry administered by the competent data protection authority.
In Mexico and the United States, where required by applicable legislation, THE ORGANIZATION shall comply with obligations of registration, notification, internal documentation, or regulatory reporting as required by competent authorities or applicable regulatory frameworks.

6.9.1. Obligations to update the registry

Where applicable, THE ORGANIZATION shall comply with the following obligations:

a. Periodic updates: Update the information registered in the corresponding regulatory registries within the deadlines established by applicable legislation in each jurisdiction.
b. Substantial changes: When substantial modifications are made to the registered information, THE ORGANIZATION shall update such information within the deadlines established by applicable legislation.
c. Creation of new databases: When new databases subject to registration are created, THE ORGANIZATION shall carry out their registration or documentation within the deadlines established by applicable legislation.

6.10. Security incident reporting

In the event of security incidents, understood as any violation of security codes, loss, destruction, alteration, disclosure, or unauthorized access to personal data stored in a database, THE ORGANIZATION shall implement internal procedures for the detection, analysis, containment, and mitigation of the incident.
Where applicable under current regulations, THE ORGANIZATION shall notify security incidents to the competent authorities and, where required, to the data subjects, within the deadlines established by applicable legislation in each jurisdiction.

In particular:

a. Colombia: Security incidents shall be reported to the competent data protection authority within fifteen (15) business days following identification of the incident.
b. Mexico: Data subjects shall be informed when the incident significantly affects their patrimonial or moral rights, in accordance with applicable legislation.
c. United States: Data subjects and competent state authorities shall be notified in accordance with applicable state data breach notification laws.
d. European Union (GDPR): Where processing is subject to the GDPR, THE ORGANIZATION shall notify the competent supervisory authority without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the incident, where required. The

incident shall also be communicated to data subjects when it is likely to result in a high risk to their rights and freedoms, in accordance with applicable regulations.

7. FINAL PROVISIONS

7.1. Service channels

THE ORGANIZATION has established the following channels for handling inquiries, claims, and complaints from data subjects whose personal data have been processed by THE ORGANIZATION through the management and administration of databases:

United States

Phone:	+1 786 800 2764
Email:	info@continentalassist.com

Colombia

Phone:	+ 57 5086267
Email:	smartinez@continentalassist.com

Mexico

Phone:	+52 1 55 30987684 - +52 1 55 79281978
Email:	info@continentalassist.com

Likewise, within its organizational structure, THE ORGANIZATION has designated an officer responsible for Personal Data Protection and for handling inquiries, claims, and complaints from data subjects whose personal data have been processed by THE ORGANIZATION.

The responsible officer shall be the Administrative Manager, who may be contacted through the channels described in this document.

7.2. Data Controller

THE ORGANIZATION processes personal data of clients, users, employees, candidates, suppliers, business partners, and other third parties, who shall hereinafter be generally referred to as data subjects.

For the purposes of this Personal Data Processing Policy, any reference to “THE ORGANIZATION” shall be understood to include the different companies that make up the Continental Assist corporate group and that operate in various jurisdictions, including, but not limited to:
(i) Continental Assist Colombia S.A.S., incorporated under the laws of the Republic of Colombia;
(ii) Continas Mex, S. de R.L. de C.V., incorporated under the laws of the United Mexican States;
(iii) Continental Assist LLC, incorporated under the laws of the corresponding State in the United States of America.

Each company shall act as the data controller with respect to the personal data it collects, processes, or manages within the scope of its own operations and under the applicable legislation

in its respective jurisdiction, without prejudice to the existence of joint processing or intra-group transfers in accordance with applicable data protection contracts and agreements.
In compliance with applicable personal data protection regulations in Colombia, Mexico, the United States, and, where applicable, the European Union, THE ORGANIZATION is identified as the data controller of the personal data it collects, uses, stores, shares, transmits, or transfers in the course of its commercial, operational, administrative, and labor activities.

In cases of joint processing of personal data among the companies of the group, they may act as joint controllers or as independent controllers, depending on the nature of the operation and the actual distribution of decisions regarding the purposes and means of processing. For this purpose, they may enter into internal agreements clearly defining their respective responsibilities in personal data protection, in accordance with applicable legislation in each jurisdiction, including, where relevant, Article 26 of Regulation (EU) 2016/679 (GDPR), Law 1581 of 2012 and its regulatory decrees in Colombia, the Federal Law on the Protection of Personal Data Held by Private Parties in Mexico, as well as applicable federal or state regulations in the United States.

The foregoing does not imply the creation of a single global legal entity responsible for data processing, but rather a corporate coordination under common compliance standards, respecting the legal and regulatory independence of each company.

Within the framework of this Policy, the following are identified as data controllers:

United States

Name:	Continental Assist LLC
Tax ID (CN):	46-1966662
Type:	Limited Liability Company.
Registered Office:	Aventura, Florida, United States
Address:	20803 Biscayne Boulevard, suite 370
Phone:	+1 786 800 2764
Email:	info@continentalassist.com

Colombia

Name:	Continental Assist Colombia S.A.S.
Tax ID (NIT):	900.808.800-1
Legal Entity Type:	Juridical
Type:	Simplified Joint Stock Company
Registered Office:	Bogotá, Colombia
Address:	Autopista Norte No. 114 – 44
Phone:	+ 57 5086267
Email:	smartinez@continentalassist.com

Mexico

Name:	Continas Mex, S. de R.L. de C.V.
Tax ID (RFC):	CME1501213A6
Type:	Legal entity under the general law regime
Registered Office:	Mexico city, Mexico
Address:	Avenida Insurgentes 662, 7th floor, suit A
Phone:	+52 1 55 30987684 - +52 1 55 79281978
Email:	info@continentalassist.com

7.3. Role of Data Controller and Data Processor

THE ORGANIZATION may act as a data controller when it determines the purposes and means of personal data processing and manages its own databases. In this role, THE ORGANIZATION decides which data are collected, for what purposes they are used, and how they are managed.

Likewise, THE ORGANIZATION may act as a data processor when it processes personal data on behalf of a third party acting as the data controller, in accordance with the documented instructions of such third party and the contracts entered into between the parties.

When acting as a data controller, THE ORGANIZATION shall comply with this Personal Data Processing Policy and with applicable regulations.

When acting as a data processor, THE ORGANIZATION shall comply with the policy and instructions of the data controller that provided the database, without prejudice to its own legal obligations that may apply.

7.3.1. Databases not managed by THE ORGANIZATION

THE ORGANIZATION declares that, within the scope of its ordinary operations, it does not manage or administer the following types of databases or files, unless otherwise required by legal or contractual provisions:

a. Databases or files maintained exclusively for personal or domestic purposes, not forming part of commercial or business activities.
b. Databases intended for national security and defense, as well as those related to the prevention, detection, monitoring, and control of money laundering, terrorist financing, or other public security activities, when administered directly by competent authorities.
c. Databases containing intelligence or counterintelligence information, administered by competent authorities or entities.
d. Databases or files containing journalistic, editorial, or expressive information, insofar as they are protected by freedom of the press and applicable laws.
e. Databases regulated under special regimes of financial, credit, or commercial information, where processing is subject to specific sectoral laws distinct from general personal data protection laws.
f. Databases regulated under special regimes applicable to the solidarity, cooperative, or similar sectors, where particular sectoral regulation applies.

7.4. Reserved rights

This document is the exclusive property of THE ORGANIZATION; therefore, its use, copying, distribution, reproduction, commercialization, exploitation, or adoption by any natural or legal person, public or private, national or foreign, is strictly prohibited. THE ORGANIZATION reserves the right to initiate any legal actions as may be appropriate.

7.5. Availability

This Policy shall be physically available at THE ORGANIZATION's administrative offices and on the website: www.continentalassist.com

7.6. Retention of databases

Personal data shall be retained only for the time necessary to fulfill the purposes for which they were collected and for as long as legal, contractual, or liability obligations arising from the processing remain in effect. Where it is not possible to establish a specific retention period, THE ORGANIZATION shall apply objective conservation criteria based on the nature of the data, the type of legal relationship, and the applicable statute of limitations in each jurisdiction.

7.7. Final statements

THE ORGANIZATION reiterates its commitment to the protection of personal data and respect for the rights of data subjects, acting in accordance with applicable legislation in the jurisdictions where it operates and with the principles of legality, transparency, purpose, necessity, security, and confidentiality. Information shall be processed solely for the informed purposes and through the implementation of appropriate technical, administrative, and organizational measures to prevent misuse, loss, alteration, or unauthorized access.
Likewise, THE ORGANIZATION promotes an organizational culture oriented toward information protection, training its personnel and requiring employees, contractors, and partners to comply with confidentiality and data protection obligations. This Policy may be updated when necessary to reflect regulatory, operational, or technological changes. THE ORGANIZATION maintains internal records and controls that allow it to demonstrate compliance with data protection obligations where required by applicable regulations. In Mexico and the United States, there is no general mandatory registry of personal data databases; however, THE ORGANIZATION shall maintain internal documentation to demonstrate compliance with privacy obligations in accordance with applicable regulations.

Continental assist

www.continentalassist.com