

PERSONAL DATA PROCESSING AND PROTECTION POLICY

1. OBJECTIVE.

This Data Processing Policy, hereinafter referred to as the "Policy", aims to define the framework through which **Emergent Cold LatAm** manages and protects the personal data it processes during its operations in the region.

In this regard, this Policy establishes the principles, guidelines, and responsibilities that must be observed in the processing of personal data, with the objective of ensuring a uniform, adequate, and consistent level of protection in the countries where we operate. Its purpose is to ensure that the collection, use, storage, access, transfer, and deletion of personal data are carried out in a lawful, transparent, and secure manner, in accordance with applicable international standards, promoting an organizational culture oriented toward safeguarding individuals' rights.

Emergent Cold LatAm, hereinafter referred to as "**ECLA**" or the "**Company**", is the largest provider of cold chain logistics solutions for the food industry in Latin America, with operations distributed across multiple countries in the region.

In the development of its commercial, operational, and administrative activities, the Company processes personal data for various purposes necessary for the proper delivery of its services, the operation of its facilities, and the fulfillment of its contractual and corporate obligations.

ECLA recognizes the importance of protecting the personal information entrusted to it and, consequently, is committed to managing personal data in a responsible, ethical, and transparent manner. In all its operations, the Company complies with applicable privacy and personal data protection laws in each country where it operates, applying corporate standards that ensure an adequate and consistent level of protection across the region.

Likewise, the Company adopts principles and practices aligned with regulatory frameworks and internationally recognized privacy standards, which allow it to guarantee proper protection of personal data throughout the entire data lifecycle, from its collection to its secure deletion.

This regional regulatory framework provides the foundation for the management of personal data processing within **Emergent Cold LatAm** and establishes guidelines that must be followed by all employees, areas, and operations involved in such processing.

2. SCOPE OF APPLICATION

This Policy applies to all processing of personal data carried out by the Company, whether in physical or digital format, that is contained in its records or databases.

It applies to all its directors, managers, employees, and collaborators, hereinafter referred to as "Stakeholders", and to any third party who, by virtue of a mandate or contract, processes personal data on behalf of **Emergent Cold LatAm**.

3. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

- 3.1. Personal Data:** Any information related to or referring to an identified or identifiable natural person.
- 3.2. Sensitive Personal Data:** Personal data that refer to the physical or moral characteristics of individuals or to facts or circumstances of their private life or intimacy, revealing ethnic or racial origin, political, union or guild affiliation, socioeconomic status, ideological or philosophical beliefs, religious beliefs, data concerning health, human biological profile, biometric data, and information relating to sexual life, sexual orientation, and gender identity of a natural person.
- 3.3. Regional Data Protection Officer (RDPO):** A person designated within the Company responsible for ensuring compliance with personal data protection regulations in all countries where ECLA operates, overseeing proper data processing, managing subject requests, assessing risks, and notifying security incidents to authorities and affected individuals when applicable.
- 3.4. Local Data Protection Officer (LDPO):** A person responsible in each country for ensuring compliance with regional and country-specific requirements, overseeing proper data processing, managing requests, assessing risks, and notifying security incidents to the authorities of the country where they are located.
- 3.5. Data Subject:** The natural person to whom the personal data relates.
- 3.6. Data Controller:** ECLA, which determines the purposes and means of processing personal data.

- 3.7. Third-Party Processor or Processor:** A natural or legal person who processes personal data on behalf of **Emergent Cold LatAm**.
- 3.8. Data Processing:** Any operation or set of operations that allows the collection, storage, recording, organization, preparation, selection, extraction, communication, assignment, transfer, transmission, or deletion of personal data, or their use in any other way.
- 3.9. ARSOP Rights:** Refers to the rights of Access, Rectification, Erasure (Suppression), Objection, Blocking, and Portability of personal data, in accordance with Applicable Legislation.

4. RESPONSABILITIES

The entity responsible for the processing of personal data is **Emergent Cold LatAm**, within the scope of the development of its corporate purpose and the proper provision of its commercial and operational services.

The monitoring of compliance with this Policy and the verification of the effectiveness of associated controls will be the responsibility of the **Regional Compliance Team**, which acts as monitoring, evaluation, and follow-up body in matters of privacy and data protection. The role of **Regional Compliance Director** or **Regional Data Protection Officer** (RDPO) will hold responsibility for data processing in all countries.

Additionally, each local operation may designate, when required by national legislation or when deemed appropriate by the Company, a **Local Data Protection Officer (LDPO)** or a **specialized officer**. These roles will be responsible for ensuring compliance with applicable obligations in their jurisdiction and for coordinating their functions with the Regional Compliance Team, guaranteeing consistent management aligned with corporate guidelines.

Inquiries, requests, or the exercise of rights related to personal data protection may be submitted through the following official channels provided by **Emergent Cold LatAm**:

- **Corporate email:** datospersonales@emergentcold.com
- **Whistleblowing Channel:** <https://emergentcoldlatam.com/etica-y-cumplimiento/>

5. GUIDELINES FOR PERSONAL DATA PROCESSING

5.1. GUIDING PRINCIPLES FOR PERSONAL DATA PROCESSING

These principles guide how personal data are collected, used, stored, and protected, ensuring that such processing is carried out with respect for the rights and freedoms of data subjects, under minimum criteria.

- 5.1.1. **Lawfulness:** All processing of personal data must be based on an explicit legal basis, in accordance with one or more of the lawful grounds established by Applicable Legislation, such as the data subject's consent, compliance with a legal or contractual obligation, the legitimate interest of the controller, among other enabling grounds. The principle of lawfulness ensures that no processing is carried out arbitrarily or without legal basis.
- 5.1.2. **Purpose Limitation:** Personal data must be collected for specific, explicit, and legitimate purposes and may not be further processed in a manner incompatible with the original purpose declared to the data subject. This principle seeks to clearly define the objectives of processing, ensuring consistency with the information provided to the data subject.
- 5.1.3. **Proportionality:** This principle aims to limit the collection and processing of personal data to those strictly necessary and relevant to achieve the declared purpose.
- 5.1.4. **Data Quality:** The Company shall ensure that personal data are accurate, complete, and up to date, adopting reasonable measures for their correction or update when applicable.
- 5.1.5. **Security:** Personal data shall be protected through the implementation of appropriate technical and organizational measures designed to preserve their confidentiality, integrity, and availability, and to protect them against unauthorized access, destruction, loss, alteration, or unlawful disclosure. The level of security applied shall be proportional to the nature of the data and the risks associated with processing.
- 5.1.6. **Transparency and Information:** The Company shall provide the data subject, in a clear, accessible, and understandable manner, following internal procedures and protocols, with all relevant information regarding the processing of their data, including the identity of the controller, the legal basis, the purpose, recipients, the rights available to them, and the channels to exercise them.

5.1.7. **Accountability:** The Company and its employees must be able to demonstrate, when applicable, that they effectively comply with the principles and obligations established by Applicable Legislation. This translates into having policies, controls, audits, procedures, and documentation that allow demonstrating due diligence in the protection of personal data.

5.2. DATA SUBJECT RIGHTS.

Every data subject may exercise the following rights:

- **Access:** Request information about data relating to them, their origin, recipients, purpose of storage, and the identification of people or entities to whom their data are regularly transmitted.
- **Rectification:** Request the modification of their data when it is erroneous, inaccurate, ambiguous, or incomplete, and must prove such circumstance.
- **Erasure:** Request the deletion of their data under specific grounds, such as when they are no longer necessary for the purposes for which they were collected or when the data subject has withdrawn their consent.
- **Objection:** Object to the processing of their data for specific purposes, for example, for direct marketing purposes.
- **Restriction and/or Blocking:** Request the temporary suspension of any data processing operation when the data subject submits a request for rectification, erasure, or objection, while such request is being resolved.
- **Portability:** Request and receive a copy of their data in a structured, generic, and commonly used electronic format to transfer it to another controller.

The exercise of rights is regulated in the Procedure for exercising ARSOP rights of ECLA.

5.3. PROCESSING PERSONAL DATA

In accordance with Applicable Legislation on personal data protection, **Emergent Cold LatAm** may process, as applicable, the following categories of personal data:

- **Identification Data:** first name, last name, identification document number, passport, or other similar official identifiers.

- **Contact Data:** address, domicile, landline and/or mobile phone number, personal or professional email addresses, and other contact information maintained with us.
- **Sensitive Personal Data:** personal data referring to the physical or moral characteristics of individuals or to facts or circumstances of their private life or intimacy, revealing ethnic or racial origin, political, union or guild affiliation, socioeconomic status, ideological or philosophical beliefs, religious beliefs, among others that form part of the most intimate sphere of the data subject.
- **Signature:** handwritten, digital, and/or electronic signature used in contracts, forms, access records, or other documents related to our operations.
- **Credentials and Electronic Identifiers:** usernames, passwords, codes, tokens, device identifiers, or other means of authentication and access control to systems, applications, facilities, or services of ECLA.
- **Banking Data and Data Derived from the Commercial Relationship:** account numbers, payment method details, commercial background, information on coverage, contracted services, claims history, payment behavior, solvency, or other data necessary for managing the contractual relationship and associated risks.
- **Sensitive Health Data, when strictly necessary and permitted by law:** clinical information relevant to work fitness, medical restrictions associated with service provision, medical certificates, records of occupational accidents or illnesses, and, in general, data relating to physical or mental health status required for safety, risk prevention, or compliance with legal or contractual obligations.
- **Biometric Data:** if identification or authentication systems based on physical or behavioral characteristics are implemented (e.g., fingerprints, facial recognition, or other equivalent methods), which will be processed exclusively for access control, security, or authentication purposes, with restricted access and enhanced safeguards, being considered sensitive data under applicable regulations.
- **Browsing and Use of Digital Channels Data:** activity logs on websites, portals, applications, and other platforms enabled by **Emergent Cold LatAm** or by third parties with whom agreements are maintained (access logs, IP address, device identifiers, date and time of connection, clicks, or interaction with content), to the extent necessary for operation, security, service improvement, and compliance with legal obligations.

- **Geolocation Data:** when you use applications, devices, vehicles, or services that allow determining your approximate or precise location (e.g., through GPS, mobile network antennas, IP addresses, or similar technologies). These data may be linked to drivers, route personnel, or other employees or collaborators and will be processed only when strictly necessary for logistics operations, personal safety, cargo traceability, fleet management, or compliance with contractual or regulatory obligations, under criteria of proportionality and enhanced transparency.

In all cases, the processing of the above categories, and especially sensitive, biometric, and geolocation data, will be subject to the principles of lawfulness, purpose limitation, minimization, proportionality, security, and accountability, and will be carried out only to the extent that an adequate legal basis exists.

5.4. DATA RETENTION GUIDELINES

Emergent Cold LatAm shall retain personal data only for as long as necessary to fulfill the purposes for which they were collected, comply with applicable legal or contractual obligations, and address any potential liabilities arising from processing. Once these purposes have been fulfilled, the data shall be deleted, anonymized, or archived in accordance with the internal procedures defined for this purpose.

If you want, I can also format this into a polished Word/PDF policy or continue translating the remaining sections.

5.4.1. DATA RETENTION CRITERIA

Retention periods shall be determined considering:

- Applicable legal and regulatory requirements in each country.
- Essential operational and commercial purposes for the Company's activities.
- Legitimate interests documented and proportionate.
- Contractual periods with clients, suppliers, and employees.

Considering that regulatory frameworks regarding data protection and information retention vary among different countries, **Emergent Cold LatAm** shall maintain a retention matrix that will serve as a regional reference and may be supplemented with country-specific annexes integrating the corresponding local obligations and requirements.

5.4.2. MANAGEMENT OF RETENTION PERIODS

The Company shall maintain specific retention schedules according to the nature of the data and the type of process, which shall be defined, approved, and updated by the **Regional Data Protection Officer (RDPO)**, in coordination with the departments responsible and the legal and compliance areas, to ensure alignment with:

- ✓ Regulatory developments regarding data protection and records management.
- ✓ Operational, technological, or regulatory changes that modify retention periods.
- ✓ Internal procedures and compliance with the regional PDP program.

Data that have exceeded their retention period shall be securely deleted or subject to an alternative permitted treatment (anonymization, restricted archiving, etc.), following the procedures established in the **Data Retention Policy**.

5.5. LAWFULNESS OF DATA PROCESSING

Emergent Cold LatAm shall process personal data only when there is an appropriate legal basis, in accordance with Applicable Legislation and its Legal Bases Policy. Processing activities may be based on:

- **Performance of a contract or implementation of pre-contractual measures:** for example, the processing of customer and supplier data necessary for the provision of transportation, logistics, and cold chain services, or the processing of employee and candidate data arising from employment relationships or recruitment processes.
- **Compliance with legal obligations:** such as retaining certain data after the end of the contractual relationship to comply with tax, labor, social security, risk prevention, operational safety, or other obligations imposed by applicable legislation.
- **Legitimate interest of Emergent Cold, duly balanced:** for example, the management and security of logistics operations, fleet and cargo monitoring and traceability, provided that the data subject has not objected and that their rights and reasonable expectations are respected.

- **Consent of the data subject:** in cases where legislation requires it or where it is considered the most appropriate basis. As a general rule, **Emergent Cold LatAm** shall seek to ensure that the processing of personal data is based on free, specific, informed, unequivocal, and verifiable consent, especially when sensitive data are involved or when the purposes are not strictly necessary for the provision of the service (for example, certain marketing actions or the use of additional functionalities). Consent may be withdrawn at any time, without retroactive effects, through the channels made available, without such withdrawal affecting the lawfulness of processing carried out previously.

In all cases, **Emergent Cold LatAm** shall document the legal basis applicable to each relevant processing activity and shall periodically review its adequacy, in accordance with the provisions established in the Legal Bases Policy and the remainder of its compliance system regarding personal data protection.

5.6. PURPOSE OF PERSONAL DATA PROCESSING

We also process personal data for various operational and legal purposes, including, without limitation:

- **Employee Management and Internal Operations**
 - Employee data (drivers, warehouse operators, administrative personnel).
 - Information necessary for access control, shifts, food handling training, internal traceability, etc.
 - Compliance with labor and social security obligations.
- **Coordination with B2B Clients**
 - Contact details of our clients.
 - Use for coordinating deliveries, incidents, returns, or administrative matters.
- **Security and Regulatory Compliance**
 - Visitor logs, security cameras (which may capture images of individuals).
 - Compliance in food safety audits or traceability processes, which may involve personal information of responsible parties or witnesses to processes.
- **Supplier Management**

- Data of individuals linked to transportation, maintenance, supplies, or service providers.
- **Handling Complaints or Inquiries**
 - Addressing, managing, and responding to inquiries, requests, or petitions made by different users.
- **Ensuring the proper technical functioning of the website** and, where applicable, using the cookies you have authorized, in accordance with the provisions of our Cookies Policy.
- **To comply with applicable legal obligations** or to carry out any additional processing for which you have provided your express consent.

5.7. DATA PROCESSING BY THIRD PARTIES AND DATA SHARING

Depending on the purposes for which personal data are collected, the following people may have access to such information, as applicable:

- Authorized personnel of the Company or its representatives acting on behalf of the entity, all subject to applicable data protection laws.
- Regulatory authorities or other competent bodies, when required by applicable legal provisions.
- Third parties or data processors, such as service providers that process personal data on behalf of and under the instructions of the controller.

All the above are only after adopting the necessary measures to ensure that such information may be shared and after executing the corresponding data processing agreement, in accordance with data protection legislation.

Furthermore, whenever personal data is processed by service providers or external collaborators on behalf of **Emergent Cold LatAm**, appropriate technical, organizational, and contractual measures shall be adopted to ensure their protection and confidentiality throughout the entire processing operation, in accordance with the Supplier Management Policy.

5.8. SECURITY MEASURES AND INCIDENT REPORTING.

ECLA shall implement appropriate technical and organizational measures to ensure a level of security proportionate to the risk associated with the processing

of personal data. Such measures may include, among others, access controls, encryption, pseudonymization, vulnerability management, security monitoring, and any other actions aimed at protecting confidentiality, integrity, and availability of information and systems used for processing.

The Company shall maintain a preventive and continuous improvement approach regarding information security, adopting practices aligned with internationally recognized standards and adapting its controls to the operational characteristics of each country within the region.

In the event of a breach of security measures that may compromise personal data or generate significant risks to the rights and freedoms of data subjects, Emergent Cold LATAM shall manage and report such incident in accordance with the applicable legislation in each jurisdiction.

Additionally, the Company shall follow up on each incident through internal investigation, containment, mitigation, and remediation procedures, maintaining close coordination between regional areas and local teams to ensure a consistent, efficient, and timely response throughout the region.

5.9. CROSS-BORDER DATA TRANSFERS

Any transfer of personal data to a country or international organization shall only be carried out if such country or organization provides an adequate level of data protection, determined by the standards of the corresponding countries, or if appropriate contractual safeguards are provided, in accordance with Applicable Legislation and the International Personal Data Transfer guidelines corresponding to each country where ECLA operates.

5.10. VERIFICATION OF ADEQUATE COUNTRY STATUS AND AUTHORITY DECISIONS

Before carrying out an international transfer, Emergent Cold LatAm shall verify, when applicable, whether the destination country, international organization, or applicable sectoral regime has an adequacy decision or declaration issued by the Personal Data Protection Authority.

Where such decision exists, the Company may rely on it as the basis for the transfer and shall comply with the conditions and instructions established by the authority.

5.11. TRANSFER RECORDS AND TRACEABILITY

Emergent Cold LatAm will maintain a reasonably updated record of relevant international personal data transfers, which shall include, at a minimum:

- a. The destination country and the identification of the main supplier or recipient;
- b. The categories of data and data subjects involved;
- c. The main purpose of the transfer and the associated legal basis; and
- d. The adequacy mechanism or safeguard used (adequate country, contractual clauses, other safeguards).

This record shall serve accountability and periodic risk review purposes and may be integrated into the Record of Processing Activities or the inventory systems maintained by the Company.

5.12. EFFECTIVENESS AND AMENDMENT OF THE POLICY

This Policy shall enter into force upon its publication and dissemination through official channels. The Company reserves the right to amend it to adapt it to regulatory, jurisprudential, or new institutional practices. Any amendment shall be duly communicated to data subjects through the usual communication channels.

5.13. INTEGRATION WITH THE CORPORATE COMPLIANCE PROGRAM

This Personal Data Processing Policy forms part of the **Corporate Compliance Program of Emergent Cold LATAM** and contributes to strengthening its governance structure and regulatory risk management framework regarding privacy and personal data protection. In this context, this Policy fulfills, among others, the following objective:

- **Establishing the regional compliance** framework applicable to the processing of personal data, defining principles, legal bases, purposes, categories of data, data subject rights, and internal responsibilities that guide the implementation of associated procedures and controls.
- **Serving as a mandatory reference** for the design, implementation, and evaluation of activities, processes, systems, and projects involving personal

data processing in any Company operation, ensuring that they are developed in accordance with this Policy and applicable legislation in each jurisdiction.

- **Aligning and articulating regional management with local compliance mechanisms**, so that each country may adopt or supplement the specific instruments required by its legislation, while always maintaining operational and regulatory consistency throughout the organization.
- **Integrating with internal privacy and data protection procedures**, including those that each country may define or require due to regulatory requirements, thereby contributing to organizational accountability and the proper processing of personal data throughout the region.

5.14. DATA SUBJECT REQUEST CHANNELS

The Company has the following official communication channels for submitting requests, inquiries, or exercising rights:

- **Corporate email:** datospersonales@emergentcold.com
- **Whistleblowing channel:** <https://emergentcoldlatam.com/etica-y-cumplimiento/>

These channels are intended to ensure timely, transparent management aligned with the data protection principles established in this Policy.

Emergent Cold LatAm reaffirms its commitment to the protection of personal data and to the implementation of responsible, consistent, and secure practices across all its operations in the countries where it operates. To this end, it shall continue strengthening its compliance framework, promoting processes aligned with international standards, and fostering an organizational culture based on transparency, integrity, and accountability.

Recognizing that each country has specific regulatory requirements regarding privacy, this Regional Policy shall be supplemented, when necessary, by **country-specific parameters, procedures and annexes** detailing local obligations, particular procedures, and additional controls that ensure effective compliance in each jurisdiction.

This Policy shall be periodically reviewed and updated whenever regulatory, technological, or operational changes so require, remaining the guiding framework for the processing of personal data.