PERSONAL DATA PROCESSING AND PROTECTION POLICY – MAERSK COLOMBIA GROUP

1. **INTRODUCTION:**

MAERSK COLOMBIA S.A.S., MAERSK LOGISTICS & SERVICES COLOMBIA LTDA., AGENCIA DE ADUANAS MAERSK S.A.S. NIVEL 1 (hereinafter, individually the "Company" and jointly the "Maersk Colombia Group", "Maersk" and/or the "Companies"), committed to the protection and proper processing of the personal data of those individuals with whom Maersk maintains any type of relationship, and in compliance with the provisions of Statutory Law 1581 of 2012, Decree 1377 of 2013, Decree 886 of 2014, Law 1266 of 2008, and other applicable regulations, hereby adopt this Personal Data Processing and Protection Policy (the "Policy").

2. **DEFINITIONS:**

For the development and implementation of this Policy, the definitions established in the current regulations on personal data protection are adopted, as well as additional definitions applicable herein. These definitions shall be interpreted in a systematic and comprehensive manner, considering the guiding principles of the fundamental right to habeas data, as well as technological developments and the principle of technological neutrality.

- **Authorization:** Prior, express, and informed consent granted by the Data Owner for the processing of their personal data.
- **Database:** An organized set of personal Data Owner to Processing.
- **Client:** A natural or legal person to whom MAERSK offers or provides any of its services.
- **Personal Data:** Information that identifies or may be associated with one or more identified or identifiable natural persons.
- **Private Data:** Information of a reserved or intimate nature, relevant only to its Data Owner.
- **Public Data:** Information that, by its nature, is not considered private, semi-private, or sensitive. Public data includes, among others, marital status, profession or occupation, and the status of merchant or public servant. This type of information may be found in official records, public documents, gazettes, official bulletins, and final judicial decisions that are not subject to confidentiality.
- **Semi-private Data:** Information that is not entirely reserved, private, or public, and whose access or disclosure may be of interest both to the Data Owner and to a specific group or to society in general, such as financial or credit information.
- **Sensitive Data:** Information that affects the privacy of the Data Owner or whose improper use may lead to discrimination. This category includes data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in labor unions, social organizations or human rights organizations, as well as information related to health, sexual life, and biometric data.
- **Data Processor:** A natural or legal person, public or private, who, by itself or jointly with others, carries out the Processing of personal data on behalf of Maersk, which acts as the Data Controller.
- **Processing Policy:** This document that establishes the guidelines for the management of personal data by MAERSK, in accordance with the applicable legislation on the matter.
- **Vendor:** A natural or legal person who, by virtue of a commercial relationship, provides a service to MAERSK.

- **Data Controller:** As indicated in this document.
- **Data Owner:** A natural person whose personal data is subject to Processing, whether as a client, Vendor, employee, or other third party who has provided personal information to Maersk within the framework of a commercial or legal relationship.
- **Employee:** A natural person who, under an employment contract, provides services to MAERSK.
- **Transfer:** An act through which the Data Controller or Data Processor of personal data in Colombia sends the information to a recipient who also acts as a Data Controller and may be located within or outside the country.
- **Transmission:** A procedure through which personal data is communicated within or outside Colombia so that a Data Processor may carry out its Processing on behalf of the Data Controller.
- **Processing:** Any action or set of actions performed on personal data, including its collection, storage, use, circulation, or deletion.

3. DATA CONTROLLERS RESPONSIBLE FOR THE PROCESSING OF PERSONAL DATA:

3.1. MAERSK COLOMBIA S.A.S

- **Tax ID (NIT):** 800235053 - 1
- **Address:** Calle 127A No. 53A-45, Torre 2 Oficina 401-B, 401-C and 401-D, Edificio Centro Empresarial Colpatria, Bogotá, Colombia
- **Contact e-mail:** dataprivacycolombia@maersk.com
- **Phone:** +(57) (601) 7940389 / (601) 7940390

3.2. AGENCIA DE ADUANAS MAERSK S.A.S NIVEL 1

- **Tax ID (NIT):** 900568476 – 5
- **Address:** Calle 127A No. 53A-45, Torre 2 Oficina 401-B, 401-C and 401-D, Edificio Centro Empresarial Colpatria, Bogotá, Colombia
- **Contact e-mail**: dataprivacycolombia@maersk.com
- **Phone:** +(57) (601) 7940389 / (601) 7940390

3.3. MAERSK LOGISTICS & SERVICES COLOMBIA LTDA

- **Tax ID (NIT):** 830080634 – 2
- **Address:** Calle 127A No. 53A-45, Torre 2 Oficina 401-B, 401-C and 401-D, Edificio Centro Empresarial Colpatria, Bogotá, Colombia
- **Contact e-mail:** dataprivacycolombia@maersk.com
- **Phone:** +(57) (601) 7940389 / (601) 7940390

4. OBJECTIVE:

The purpose of this Policy is to define the guidelines governing the processing and protection of personal data managed by MAERSK, specifying the purposes of the processing, the rights of the Data Owners, and the mechanisms available for them to exercise such rights, including consultation, updating, deletion of their information, or the revocation of the authorization granted, among other relevant aspects. In accordance with Article 15 of the Political Constitution of Colombia and the applicable regulations, MAERSK has adopted a policy based on principles of transparency for the

management of personal data. Consequently, it only collects information from natural persons with whom it maintains contractual or commercial relationships—such as Clients, Employees, Partners, or Vendors—when such information is provided freely, knowingly, and with prior authorization.

5. GUIDING PRINCIPLES APPLICABLE TO PERSONAL DATA

In the application of this Policy, the following principles shall apply:

a. **Principle of legality in data Processing**: The processing of personal data constitutes an activity regulated by the regulations on Habeas Data, which require that such processing be carried out in strict compliance with the provisions established by law and its complementary, modifying, or regulatory provisions. Consequently, any activity related to the handling of personal data must observe the principles, rights, and procedures set forth in the applicable legislation.

b. **Principle of purpose**: The processing of personal data must respond to a legitimate purpose, in accordance with the provisions of the Constitution and the law. Such purpose must be duly defined and clearly communicated to the Data Owner.

c. **Principle of freedom:** The processing of personal data may only be carried out when the Data Owner has granted prior, express, and informed consent. The collection, use, or disclosure of such information without such authorization shall not be permitted, unless there is a legal provision or a judicial order that exempts this requirement.

d. **Principle of accuracy or quality:** The information subject to processing must be characterized by its truthfulness, integrity, accuracy, timeliness, verifiability, and clarity. The processing of personal data that is partial, erroneous, incomplete, fragmented, or that may lead to misunderstanding or incorrect interpretations is prohibited.

e. **Principle of transparency:** During the processing of personal data, the Data Owner's right to freely access the information concerning them must be guaranteed at all times, including confirmation of the existence of their data. The Data Controller and/or the Data Processor are obliged to provide this information in a clear, precise, and timely manner whenever requested by the Data Owner.

f. **Principle of restricted access and circulation**: The processing of personal data must respect the limits defined by the nature of the information, as well as by the law and the Constitution. Consequently, it may only be carried out by persons expressly authorized by the Data Owner or those legally authorized to do so, in accordance with the applicable regulations.

g. **Principle of security**: The information subject to processing by the Data Controller or Data Processor must be managed in accordance with the Habeas Data Law, implementing appropriate technical, human, and administrative measures to ensure its protection.

These actions must be aimed at preventing the adulteration, loss, consultation, use, or unauthorized or fraudulent access to personal data.

h. **Principle of confidentiality:** Any person involved in the processing of non-public personal data has the duty to maintain the confidentiality of such information, an obligation that remains in force even after the termination of their relationship with the corresponding activities. The disclosure or delivery of such data may only be carried out within the framework of the purposes permitted by law and in accordance with the conditions established therein.

6. AUTHORIZATION FOR PROCESSING

MAERSK will request the Data Owner's authorization for the processing of their personal data through physical, digital, audiovisual means, or other available technological mechanisms. Such authorization shall be retained as documentary support so that it may be consulted subsequently if required. Consent must be obtained, at a minimum, at the time the personal data is collected.

7. CASES IN WHICH AUTHORIZATION IS NOT REQUIRED

MAERSK notifies that the authorization of the Data Owner shall not be required in the following cases:

- When a public entity or administrative authority requires the information in the exercise of its legal functions, or when there is a judicial order requiring it.
- When the information corresponds to public data.
- In cases of medical or health emergencies that make it necessary to process the information.
- When the law expressly authorizes the processing for historical, statistical, or scientific purposes.
- When the data is related to the Civil Registry of individuals.

8. PURPOSE OF THE PROCESSING OF PERSONAL DATA.

This Policy establishes specific purposes for the processing of personal data, determined according to the nature of the relationship that each counterparty maintains with the Company. Accordingly, the following specific purposes are established:

8.1. **Processing of personal data of Employees:** The personal data of employees will be used for the following purposes:

a. To comply with the obligations imposed by Colombian Labor Law on employers or with the orders issued by the competent authorities.
b. Payroll management aimed at fulfilling labor and tax payment obligations arising from the employment relationship.
c. Employee information: including general, academic, contractual, and family data of employees.

d. Control of employees' working hours.

e. Human talent management: to carry out recruitment, hiring, training, retention, and termination processes. This includes the verification of degrees, licenses, and certifications necessary for the performance of duties, compliance with labor and contractual obligations, payroll payment, training or education in any modality, as well as the granting and administration of permits, leaves, and other labor authorizations.

f. Compliance with the obligations imposed and/or commitments assumed by the Company regarding the implementation of labor welfare policies, risk prevention, emergency response, compliance with the Occupational Health and Safety Management System (SG-SST), and other legal obligations in matters of occupational health.

g. Social security and labor benefits: related to the affiliation, administration, and control of contributions to the social security system, pensions, subsidies, economic benefits, and voluntary or mandatory benefits.

h. Compliance with legal and corporate duties: to respond to requests from administrative, judicial, or supervisory authorities, as well as to support internal procedures, internal investigations, disciplinary processes, audits, and document management associated with regulatory and corporate compliance.

i. Promotion of institutional activities and organizational well-being: to organize and record participation in integration activities, organizational culture initiatives, training, recreation, institutional events, or spaces for physical and mental health.

j. Institutional communication and information updates: for contact purposes, sending internal communications, notifications regarding regulatory or policy changes, and requests for updating or verifying personal information, as well as establishing communication in emergency situations.

k. Preparation of internal statistics and continuous improvement: data analysis to generate indicators, diagnostics, and internal reports on matters related to organizational performance, health, safety, work environment, productivity, and other strategic aspects.

l. Attention to the exercise of the Data Owner's rights: to address petitions, consultations, complaints, requests for access, correction, deletion, or opposition, as well as for the exercise of constitutional, legal, and contractual rights.

m. National and international transfer of data to members of the Maersk Group or allied third parties.

n. To manage the functions carried out by employees.

o. To verify, compare, and evaluate the labor and personal competencies of employees.

p. To issue certifications related to the Data Owner's relationship with the Company.

q. To provide employment references to potential employers of a former employee.

r. To capture images, photographs, and fingerprints necessary for employee identification, compliance control, and the collection of evidence of services performed.

s. To conduct security background checks on employees in accordance with the Company's AML/CFT prevention system.

t. Any others specifically established in the authorizations granted by the respective Data Owner.

8.2. **Processing of personal data of Vendors:** The personal data of Vendors and Contractors will be used for the following purposes:

a. Accounting, tax, and administrative management: to comply with legal and contractual obligations with Vendors and contractors.

b. Monitoring and management of the pre-contractual, contractual, and post-contractual stages, including carrying out selection processes, onboarding procedures, and the creation of the Vendor in the Company's information systems.

c. Payment management and information verification: to process payments and validate tax, banking, and contact information, and to comply with processes associated with the invoicing cycle, as well as to comply with legal provisions regarding taxes, withholdings, and other obligations applicable to the commercial relationship maintained with the Vendor.

d. Document management and communication traceability: for the registration, control, and traceability of incoming and outgoing correspondence, including the sending of commercial, advertising, or any other type of information to the Vendor.

e. Security and access control: to ensure security at the Company's facilities through the registration of entry and exit.

f. Handling of rights and legal requests: to respond to requests from Data Owners and requirements from authorities.

g. Internal analysis and process improvement: to generate internal reports.

h. Execution of administrative procedures: for audits, internal controls, and administrative processes.

i. Updating of information and institutional communications: to keep information updated and notify changes in the processing of data.

j. Management of institutional events and activities: to organize, record, and control participation in activities carried out and/or attended by the Company.

k. Conduct security background checks on Vendors in accordance with the Company's AML/CFT prevention system.

l. National and international transfer of data to members of the Maersk Group or allied third parties.

m. Management of accounts receivable collection at both the pre-legal and legal stages, carried out directly and/or through third parties designated by the Company.

n. Any others specifically established in the authorizations granted by the respective Vendor.

8.3. **Processing of personal data of Clients:** The personal data of clients will be used for the following purposes:

a. Administrative management for the execution of the pre-contractual, contractual, and post-contractual stages, and for all matters related to the monitoring of the commercial agreement entered into with the Data Owner.

b. Documentary and administrative management: To register, control, and ensure the traceability of documents associated with contractual or operational relationships, as well as to carry out internal processes, audits, procedures, and administrative processes required for organizational operation.

c. Accounting, tax, and legal management: To comply with accounting, tax, fiscal, and legal obligations, as well as to respond to requests from judicial, administrative, or supervisory authorities, including requests from authorities.

d. Customer service and management of complaints and claims: Data is processed to receive, manage, and respond to petitions, complaints, claims, suggestions, and requests for services or information, as well as to facilitate the exercise of rights by the Data Owners.

e. Commercial relationships and customer loyalty: Personal information is processed to establish, maintain, and strengthen contractual or commercial relationships, carry out loyalty activities, monitoring, and improvement of the customer experience.

f. Internal analysis and process improvement: To prepare management reports and analyses.

g. Execution of administrative procedures: For the development of controls, audits, and internal procedures.

h. Updating information and institutional communications: To keep contact information updated and inform about changes in the data processing policy.

i. Management of events, activities, and communications: To manage participation in institutional activities or events carried out by the Company. Sending communications, emails, telephone contact, or correspondence with the Data Owner for the development of advertising, promotional, and marketing activities, offering products and/or services, issuing invitations to events, and all those associated with the commercial relationship or existing link with the Company.

j. Consultation and reporting to information bureaus.

k. National and international transfer of data to members of the Maersk Group or allied third parties.

l. Conduct security background checks on clients in accordance with the Company's AML/CFT prevention system.

m. Management of accounts receivable collection at both the pre-legal and legal stages, carried out directly and/or through third parties designated by the Company.

n. Any others specifically established in the authorizations granted by the respective client.

9. **DUTIES OF MAERSK AS DATA CONTROLLER.** MAERSK shall comply with the following duties:

a. Allow the effective exercise of the right to habeas data by the Data Owner, guaranteeing full access to the rights established by law.
b. Obtain and retain proof of the authorization granted by the Data Owner for the processing of their data, under the conditions defined by the applicable regulations.
c. Inform the Data Owner, in a prior and express manner, about the purpose of the processing of their personal data, as well as the rights granted to them by virtue of the authorization provided.
d. Protect personal data through administrative, technical, and physical security measures that prevent its alteration, loss, unauthorized or fraudulent access, use, or consultation.
e. Provide the Data Processor with data that is truthful, complete, accurate, updated, verifiable, and understandable, complying with the legally required quality standards.
f. Update the information provided, informing the Data Processor of any changes regarding the data previously delivered.
g. Immediately correct inaccurate information and communicate the corresponding update to the Data Processor for adjustment.
h. Provide only personal data authorized by the Data Owner, in accordance with the terms required by law.
i. Require the Data Processor to guarantee security and confidentiality conditions at all times in the management of personal data.
j. Timely address consultations and claims submitted by Data Owners, within the timeframes and requirements established by law.
k. Adopt an internal manual of policies and procedures to ensure effective compliance with the applicable regulations, particularly in the management of claims and requests.
l. Inform the Data Processor when a claim is pending, indicating that the relevant information must not be processed while the dispute is being resolved.
m. Properly respond to the Data Owner's requests regarding the use and processing that has been given to their personal data.
n. Report to the data protection authority any security incident that compromises the confidentiality, integrity, or availability of personal data.
o. Comply with the instructions and requirements of the Superintendence of Industry and Commerce regarding the processing of personal data.

10. **SENSITIVE DATA**

Sensitive data shall be understood as those linked to the most intimate sphere of the Data Owner and which, by their nature, could give rise to situations of discrimination if used improperly. This category includes, among others, data related to racial or ethnic origin, religious or philosophical beliefs, political orientation, membership in trade unions, social organizations, human rights organizations, or political parties — including opposition parties. Health-related data, information regarding sexual life, and biometric data such as photographs, fingerprints, video images, facial

patterns, voice patterns, iris patterns, or palm prints, which allow the unique identification of a person, are also considered sensitive.

11. PROCESSING OF SENSITIVE DATA

The processing of sensitive data shall only be permitted under the following circumstances:

a. When the Data Owner has granted explicit authorization for the processing, except in cases where such authorization is not required by law.
b. When the processing is necessary to protect a vital interest of the Data Owner, and the Data Owner is physically or legally incapable. In such cases, authorization must be granted by the corresponding legal representative.
c. When the processing is carried out by a foundation, non-governmental organization, association, or any non-profit entity, within the framework of its legitimate activities and with the appropriate safeguards, provided that it is limited to the management of data of its members or of persons with whom it maintains regular contact by reason of its corporate purpose. In no case may such data be provided to third parties without the authorization of the Data Owner.
d. When the processing is necessary for the recognition, exercise, or defense of a right in a judicial proceeding.
e. When the processing is carried out for historical, statistical, or scientific purposes, in which case measures must be adopted to ensure the dissociation of personal data, suppressing the identity of the Data Owners.

12. DATA OF CHILDREN AND ADOLESCENTS

Maersk Colombia Group does not directly process the personal data of minors in general commercial or contractual activities. However, specifically, the Company may collect and process the personal data of the minor children of its employees, solely for the purpose of complying with legal obligations in labor matters, particularly those related to affiliation with the social security system and parafiscal contributions, as well as to ensure the effective exercise of the fundamental rights of minors, such as access to health services and recreational activities.

In any case, the corresponding authorization for the processing of such data will be obtained when applicable, ensuring at all times respect for the best interests of the minor and the protection of their prevailing rights, in accordance with the provisions of the Political Constitution and the applicable regulations.

13. RIGHTS OF THE PERSONAL DATA OWNERS

In accordance with the provisions of Article 8 of Law 1581 of 2012, the Data Owner of personal data has the following rights:

a. To know, update, and rectify their personal data before the Data Controller or Data Processor.
b. To request proof of the authorization granted to MAERSK for the processing of their data, except in cases where the law establishes an exception.
c. To be informed, upon request, about the use that MAERSK has made of their personal data.

d. To file complaints before the Superintendence of Industry and Commerce in the event of possible violations of the provisions of Law 1581 of 2012, provided that the consultation or claim procedure with MAERSK has been previously exhausted.
e. To revoke the authorization granted and/or request the deletion of their personal data when the principles, rights, and guarantees established in the Constitution and the law are not respected. This right shall not apply in cases where the Data Owner has a legal or contractual duty to remain in the Company's database due to ongoing contractual relationships.
f. To access, free of charge, their personal data that has been subject to Processing.

14. PROCEDURE TO EXERCISE YOUR RIGHTS

The Data Owner of personal data, duly accredited in accordance with the law, may submit a claim or inquiry before the Data Controller in the following cases:

- When they consider that the information contained in a database under the responsibility of MAERSK requires correction, updating, or deletion.
- If they identify a possible breach of the duties established in Law 1581 of 2012 or other applicable regulations.
- When they have questions or claims related to this Policy.
- If they wish to consult the information that MAERSK holds about them.

The request must comply with the requirements established in Article 15 of Law 1581 of 2012 and follow the procedure described below. The Data Owner must submit the request through the following channels:

- **E-mail:** dataprivacycolombia@maersk.com
- **Physical address:** Calle 127A No. 53A-45, Torre 2 Oficina 401-B, 401-C and 401-D, Edificio Centro Empresarial Colpatria, Bogotá, Colombia
- **Phone:** (+57) 6017940389 / 6017940390.

14.1. **INQUIRIES:** The Data Owners of personal data, as well as their successors, have the right to consult the information contained in any database under the responsibility of the Company. MAERSK shall provide all the information contained in the individual record or any data associated with the identification of the Data Owner.

Inquiries shall be addressed within a maximum period of ten (10) business days counted from the date of receipt. If it is not possible to respond within this period, the requester will be notified, indicating the reasons for the delay and the date on which the response will be provided. In any case, this new period may not exceed five (5) additional business days following the expiration of the initial term.

14.2. **CLAIMS:** The Data Owner of personal data, or their successors, who consider that the information recorded in a database should be corrected, updated, or deleted, or who identify a possible breach of the legal obligations by the Data Controller or Data Processor, may submit the corresponding claim before them. The processing of such request shall be subject to the following procedural rules:

a. **Minimum requirements of the request:** To ensure a clear response consistent with what is requested, the request must include:
   - **Addressed to:** MAERSK.
   - **Identification of the Data Owner:** Full name and identification number.
   - **Description of the facts:** Reasons supporting the inquiry or claim.
   - **Purpose of the request:** Indicate whether correction, updating, deletion, or another action regarding the data is requested.
   - **Notification address:** Physical and/or electronic address of the Data Owner.
   - **Supporting documents:** Attach any relevant document supporting the request.

b. **Submission of identification document**
   The request must be submitted together with a copy of the Data Owner's identification document.

c. **Correction of incomplete requests**
   If the request does not meet the minimum requirements, MAERSK will notify the interested party within five (5) business days following its receipt so that the deficiencies may be corrected.

d. **Withdrawal of the request:**
   If two (2) months have elapsed from the date of the request for additional information without the applicant providing the required information, MAERSK will understand that the request has been withdrawn.

e. **Response timeframes**
   - **Standard term:** MAERSK will resolve the request within a maximum period of fifteen (15) business days counted from the day following its receipt or from the date on which the Data Owner completes the request.
   - **Exceptional extension:** If MAERSK cannot address the request within the initial term, it will inform the interested party of the reasons for the delay and the new response date, which may not exceed eight (8) additional business days.

f. **Referral to the competent entity**
   If MAERSK is not competent to address the request, it will forward it to the corresponding entity within a maximum period of **two (2) business days** and will inform the Data Owner of this action, thereby being released from any responsibility regarding the request.

15. REQUIREMENT OF PRIOR PROCEDURE

The Data Owner or their successor may only file a complaint before the Superintendence of Industry and Commerce once they have previously exhausted the consultation or claim procedure before the Company, in accordance with the provisions established in the applicable regulations.

16. RESTRICTIONS FOR THE EXERCISE OF THE RIGHT

In accordance with the provisions of the Law, MAERSK may deny access to personal data, the revocation of authorization, or the request for deletion of information in the following cases:

a. When there are no records of the applicant's personal data in MAERSK's database.
b. When the applicant is not the Data Owner of the personal data or, in the event of acting on their behalf (such as a successor or attorney-in-fact), is not duly accredited.
c. When the rectification, cancellation, or objection has already been previously processed.
d. When there is a legal prohibition or a decision issued by a competent authority that restricts access to personal data or prevents its rectification, cancellation, or objection.
e. When the request may affect or violate the rights of a third party.
f. When the applicant is not a public or administrative entity acting within the scope of its legal functions, or there is no judicial order supporting the request.
g. When the Data Owner has a legal or contractual duty to remain in MAERSK's database.

17. MAERSK SECURITY MEASURES

We have implemented appropriate technical and organizational security measures for the protection of your personal information. Any data provided will be treated strictly as confidential and will only be used for the purposes for which it was collected. We store personal data on servers with limited access located in protected facilities, and our security measures are regularly evaluated. The servers are protected by antivirus software, among other measures, with the purpose of preventing the destruction, loss, alteration, misuse or any unlawful processing that may compromise the confidentiality, integrity or availability of the information.

Access to personal information will be restricted only to employees who require it for the performance of specific functions, such as Human Resources, Billing or Customer Service personnel. However, MAERSK shall not be responsible for unauthorized access by third parties, technical failures in information systems or any consequence that may arise from such events beyond its control.

18. MODIFICATIONS TO THE PROCESSING POLICY

We reserve the right, at our sole discretion, to modify and/or update this Policy at any time without prior notice. We will publish the updated version of this Policy at any time. The Policy is available at https://www.maersk.com/local-information/latin-america/colombia. If the changes introduced affect substantial aspects of the Policy, they will be duly communicated to the Data Owner, either prior to or at the time of their implementation.

19. EFFECTIVE DATE

This Policy shall be effective as of March 4, 2025.

The databases containing personal information will remain active during the period in which such information is necessary for the fulfillment of the purposes established in this Policy, or while the relationship that gave rise to the processing remains in force.