Personal Data Treatment Policy

1. Introduction

DHL SUPPLY CHAIN (Suppla S.A., Suppla Cargo S.A.S., Serviceuticos Ltda and DHL Supply Chain Colombia S.A.S.), hereafter the Company, are committed to the protection of the fundamental right to HABEAS DATA that all individuals have to know, update and rectify any and all of their information or personal data that has been collected in databases or files, where the Company acts as the party responsible or Administrator of the treatment, according to the constitutional rights, freedoms and guarantees referred to in articles 15 and 20 of the Constitution, for which the Company has implemented both the Personal Data Treatment Policy and the Comprehensive Personal Data Protection Program.

2. Legal Framework

2.1 Political Constitution of Colombia, Article 15.
2.2 Law 1266 of 2008
2.3 Law 1581 of 2012
2.4 Regulatory Decrees 1727 of 2009 and 2952 of 2010
2.5 Partial Regulatory Decree No. 1377 of 2013
2.6 Single Decree 1074 of 2015
2.7 Constitutional Court of Colombia Sentence C – 1011 of 2008, and C – 748 of 2011
2.8 Decree 1377 of 2013.

3. Definitions

For this policy, the following definitions should be considered in the application of the Personal Data Treatment Policy. The definitions here will be applied and implemented considering the interpretation criteria that guarantee a systematic and comprehensive application and, in line with technological advances, technological neutrality; and all other principles and standards governing the fundamental rights related to the right to habeas data and to the protection of personal data.

3.1 **Authorization:** The Owner's previous, express, and informed consent to handle the personal data.
3.2 **Databases**: An organized set of personal data subject to treatment.
3.3 **Personal Data:** Any information related to, or that may be associated with, one or more individuals or determinable individuals.
3.4 **Sensitive Data:** Sensitive data means any data affecting the Owner's privacy or that which misuse may lead to discrimination, such as revealing racial or ethnic origin, political orientation, religious or philosophical convictions, participation in trade unions, social, human rights or other organizations promoting the interests of any political party or advocating for the rights and guarantees of opposition political parties; any data on health, sexual activity, and biometric data.
3.5 **Administrator:** A person or legal entity, public or private, who by themselves or in conjunction with others, handles the personal data on behalf of the Party Responsible.
3.6 **Responsible Party:** A person or entity, public or private, who makes decisions about the database and/or the processing of the data on their own or in conjunction with others.
3.7 **Owner:** An individual whose personal data is subject to treatment.
3.8 **Treatment:** Any operation or set of operations on personal data, such as collection, storage, usage, release, or withholding.

3.9 **Habeas Data:** The fundamental right of everyone to know, update, rectify and/or cancel information and personal data that have been collected and/or processed in public or private databases, in accordance with the provisions of the applicable law and regulations.

3.10 **Privacy Notice** A written physical, electronic, digital, or sound recording containing verbal communication created by the RESPONSIBLE party, addressed to the Owner, for the processing of their personal data, used to notify the Owner about the existence of the information treatment policies that will be applicable to their data, the way to access them and the purposes of the treatment intended for the personal data.

3.11 **Transfer:** A data transfer means any type of data communication that occurs when the Responsible Party and/or the Administrator, located in Colombia, sends the personal information or data to a receiver, who is in turn also a Responsible Party of the treatment and is located in or outside the country.

3.12 **Transmission:** A treatment of personal data involving the communication of personal data within or outside the territory of the Republic of Colombia when it is intended for the treatment of information by an Administrator on behalf of the Responsible Party.

3.13 **Data Protection Officer:** Refers to the person in SUPPLA whose role consists of monitoring and controlling the application of the Personal Data Protection Policy. The Data Protection Officer will be appointed by the legal representative and/or the executive committee of the Company.

4. Party Responsible for the Treatment of Personal Data

DHL SUPPLY CHAIN and its subsidiaries operating on behalf of the DHL brand, Suppla S.A., Suppla Cargo S.A.S., Serviceuticos Ltda and DHL Supply Chain Colombia S.A.S brand; holders of TINs 890.903.295-0, 811.023.952-8, 830.009.622-3 and 901.003.044-6, respectively, and with offices in Bogota at the address for legal notifications and business address AC 22 No. 56 - 40 and CR 60 NO. 22 – 50, Hotline: 3183385132, are responsible for the processing of personal data and sensitive data of their employees, suppliers and customers. The Company's data protection policy can be accessed on the website www.dhl.com

5. Guiding Principles for the Treatment of Personal Data

The Company will harmoniously and comprehensively apply the following principles when processing personal data:

5.1 **Principle of Legality in Data Processing:** As a minimum, the processing of personal data must be subject to the provisions of all current laws governing the matter and provisions that establish it.

5.2 **Principle of Purpose:** The treatment must be for a legitimate purpose in accordance with the Constitution and the Law, which must be notified to the Owner.

5.3 **Principle of Freedom:** All treatment may only be conducted with the previous, express, and informed consent of the Owner. Personal data may not be obtained or disclosed without previous authorization, or in the absence of a legal or judicial order to waive consent.

5.4 **Principle of Accuracy or Quality:** The information subject to treatment must be truthful, complete, accurate, up-to-date, verifiable, and understandable. No treatment of partial, incomplete, partial, or error-inducing data must occur.

5.5 **Principle of Transparency:** The right of the Owner to obtain information about the existence of their personal data from the Party Responsible or the Administrator, at any time and without restrictions, must be guaranteed.

5.6 **Principle of Restricted Access and Release:** The treatment will be subject to the limits derived from the nature of the personal data, the provisions of the Constitution, and the law. In this sense,

the treatment may only be conducted by persons authorized by the Owner and/or by persons authorized by law or through a court order.

5.7 **Principle of Security:** All data subject to treatment must be managed with the necessary technical, human, and administrative measures to secure the records, preventing their modification, loss, inquiry, use or unauthorized or fraudulent access by third parties.

5.8 **Principle of Confidentiality:** Any individuals involved in the treatment of personal data that I not public in nature, shall be required to ensure the data's confidentiality, even after the end of their participation in any of the tasks involved in the treatment, only being authorized to provide or release personal data when in line with the performance of authorized activities, as authorized by law and under the terms provided by law.

5.9 **Principle of Timelessness:** Personal data will only be kept for as long as doing so is reasonable and necessary to fulfill the purposes justifying the treatment, in accordance with any provisions applicable to the subject matter and the information's administrative, accounting, fiscal, legal, and historical aspects. Data will be kept when doing so is necessary for the fulfillment of a legal or contractual obligation. Once the purpose of the treatment and the terms established above have been fulfilled, the data will be deleted.

5.10 **Comprehensive Interpretation of Constitutional Rights:** Rights will be construed in harmony and at the same level of the right to information provided for in article 20 of the Constitution and any other applicable constitutional rights**.**

5.11 **Principle of Necessity:** Treatment of personal data must be that which is strictly necessary to comply with the purpose of the database.

6. Treatment of Personal Data

The Company protects the privacy of sensitive data.

6.1 Treatment of Sensitive Data:

a) When the Owner has given their express authorization to such treatment, except in cases where such authorization is not required by law.

b) When the treatment is necessary to safeguard the vital interest of the Owner and they are physically or legally disabled. In such cases, legal representatives must grant authorization on the Owner's behalf.

c) When the treatment is conducted by a foundation, NGO, association, or any other non-profit organization whose purpose is political, philosophical, religious or that of a trade union within the legitimate scope of its activities and has all due guarantees, provided that the treatment pertains exclusively to their members or to persons who maintain regular contacts for its purpose. In such cases, the data may not be provided to third parties without authorization by the owner.

d) When the treatment pertains to data that is necessary to recognize, exercise or defend a right in a legal procedure.

e) When the treatment has a historical, statistical, or scientific purpose. In such cases, measures must be taken to suppress the identity of the owners.

6.2 Treatment of Personal Data of Children and Adolescents.

The treatment of this type of personal data requires special respect to the rights or children and adolescents.

The use of children and adolescents' personal data will be conducted as long as there is express authorization by their legal representatives, and when such treatment meets the parameters and requirements of safeguarding and pursuing the best interests of the children and adolescents, as well as respecting their fundamental rights.

Once the above requirements have been met, the legal representative of the child or minor shall give the authorization, this after the child or adolescent has been given a chance to exercise their right to be heard, opinion that will be assessed considering their maturity, autonomy, and ability to understand the matter.

6.3 Database Purpose:

The Company, as the Party Responsible for the information, guarantees to its Owners that the information will be used strictly in accordance with the purpose it holds in the company:

a) Process the information of each of the applicants and employees that enables managing the company's labor relationship, maintaining confidentiality in the treatment of the data.

b) Dispensation of labor certifications.

c) Storing any personal data and information provided to the Company in the employees' files, during and after the term of the contractual relationship, while applying all necessary data security measures.

d) Administrating all the information necessary to fulfill any tax, commercial, corporate and accounting requirement of the parties.

e) Complying with internal procedures to manage customers, suppliers, contractors and employees.

f) Conducting the activities necessary to manage employee related requests, claims and complaints. Creating and updating the Company's databases.

g) Consulting disciplinary, court and criminal records with any public or private entity, if required.

h) Conducting home visits and all the procedures related to it.

i) Performing reliability assessments as established by the company.

j) Providing information to third parties to assess and classify suppliers and/or customer.

k) Send invoices and/or payments to customers, suppliers, contractors and/or employees.

l) Transmitting and/or transferring personal data to third parties with whom contracts have been signed for this end, for commercial, administrative and/or operational purposes.

m) Conducting the activities necessary to manage the requests, complaints and claims submitted by customers, suppliers, contractors and/or employees, and send them to the departments responsible for issuing the corresponding responses.

n) Conducting an analysis to control and prevent fraud and money laundering, including but not limited to consulting and reporting to restrictive lists and financial risk information centers.

o) Inquiring and reporting to credit and data bureaus.

p) Creating and updating customer, supplier, contractor, and employee databases.

q) Conducting an analysis to control and prevent fraud and money laundering, including but not limited to consulting and reporting to restrictive lists and financial risk information centers.

r) Updating the personal data and image (photographs) for the different programs, platforms, tools or portals that have direct relation to the employee's role, or updates of the company.

s) Consulting the different national and international sources that contain relevant information for risk prevention.

t) Conducting the necessary activities in the Company's ERP to manage response times and effectiveness in personnel daily activities for statistical and continuous improvement purposes.

u) The purposes authorized here are outlined without any geographical or territorial limitation.

7. Owner's Rights:

The Company will respect the rights of the data Owners when treating all personal data, at all. For the purposes of this policy, the Personal Data Owner's Rights will be as follows:

a) The right to know, update and rectify their personal data with the Party Responsible or the Administrator. This right may be exercised, among others, regarding any partial, inaccurate, incomplete, partial, or misleading data, or such data which treatment is expressly prohibited or has not been authorized.

b) The right to request proof of the authorization granted to the Administrator, except when authorization is expressly waived by law.

c) The right to be notified by the Party Responsible or the Administrator, upon request, regarding the use given to the Owner's personal data.

d) The right to file complaints before the Superintendence of Industry and Commerce, for the infringement of any law governing the protection of personal data and other rules that modify, add, or complement them, after inquiring with the Party Responsible for the treatment.

e) The right to revoke the authorization and/or request the deletion of the data when treatment does not adhere to the principles, rights, and constitutional and legal guarantees. Such revocation and/or deletion will be effective when the Superintendence of Industry and Commerce, or the competent authority, has determined that the Party Responsible or Administrator have committed conduct against the Constitution or the law in the treatment of the personal data.

f) The right to free access to their personal data subject to treatment.

7.1 Authorization by the Owner

Any treatment of personal data that the Company performs requires prior and informed authorization by the Owner, which must be obtained in any form as long as it can be subsequently retrieved and consulted.

Despite the exceptions provided by law, treatment requires prior and informed authorization by the Owner, which must be obtained in any form so long as it may be subsequently retrieved and searched. Such authorization will be deemed in compliance with these requirements when it is provided (i) in writing, (ii) verbally, or (iii) through unequivocal actions by the holder making it possible to reasonably conclude that the Owner granted authorization, such as when, for example, a resume is sent to the Company to participate in selection processes, or when entering Company facilities while aware of the existence of video surveillance systems.

The authorization shall not be necessary in the exceptions provided by law, by way of example and without prejudice to the rules that modify, add, or complement them, the authorization shall not be necessary in the following cases:

Information is required by a public or administrative entity while exercising their lawful duties or by a court order.

a) When the data is public in nature.

b) In the event of a medical or public health emergency.

c) When the treatment of the information is authorized by law for historical, statistical, or scientific purposes.

d) When it is data related to the vital statistics records of individuals.

7.2 Duty to Notify the Owner: The Party Responsible for the treatment, at the time of requesting authorization by the owner, must clearly and expressly notify them of the following:

a. The scope of the treatment to which their personal data will be submitted and the purpose thereof;
b. The voluntary nature of the response to the questions that they are asked, when such questions pertain to sensitive data or the data of children and adolescents;
c. The rights granted to them as Owner;
d. The identification and the physical or electronic address of the Party Responsible for the treatment.

7.3 Persons to Whom the Information can be Provided

The Company may provide the information to the following individuals:

a) Owners, their successors or their legal representatives;

b) Public or administrative entities while exercising their lawful duties or by a court order

c) Third parties authorized by the Owner or by law.

8 Duties of the Party Responsible for the Treatment and the Administrator

All parties responsible for the treatment of data will comply with the following duties, notwithstanding any other provisions provided for in this policy and the regulations governing their activities:

8.1. Duties of the Party Responsible for the Treatment:

a) To always guarantee full and effective exercise of the Owner's right to *habeas data*.

b) To request and keep a copy of the authorization granted by the Owner.

c) To notify the Owner about the purpose of the collection and the rights they are entitled to under the authorization granted.

d) Keeping the data under the necessary security conditions to prevent tampering, loss, inquiry, and unauthorized or fraudulent use or access.

e) To ensure that the information provided to the Administrator is true, complete, accurate, up-to-date, verifiable, and understandable.

f) To update the information, notifying the Administrator in a timely manner of all added information previously provided to them, and take any other necessary actions to keep the information provided to them up to date.

g) To rectify the information when it is incorrect. and notifying the Administrator when appropriate.

h) To only provide the Administrator of the treatment with data which treatment is previously authorized in accordance with the provisions of any governing laws.

i) To require the Administrator to observe the Owner's information conditions of security and privacy.

j) To process inquiries and complaints submitted under the terms set in this policy and the law governing the matter.

k) To notify the Administrator when certain information is contested by the Owner, whenever a claim has been filed and the respective process has not been completed.

l) Notify the request of the owner about the use of their data.

m) To notify the Data Protection Authority when security code violations and risks exist in the management of the Owner's data.

n) To comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

8.2. Duties of the Administrator

The Administrators of the treatment of data will comply the following duties, notwithstanding any other provisions provided for in this manual and the regulations governing their activities:

a) Guaranteeing full and effective exercise of the Owner's right to *habeas data*, at all times.

b) Keeping the data under the necessary security conditions to prevent tampering, loss, inquiry, or unauthorized or fraudulent use or access.

c) Timely updating, rectifying, or deleting the data, under the terms of this manual.

d) Updating any information reported by the Responsible Party within five (5) business days of the request.

e) Processing any inquiries and claims made by Owners in the terms set by Law.

f) Implementing a policy and procedures manual with the purpose of ensuring proper compliance with the provisions of Law 1581 of 2012 and specially to process inquiries and complaints.

g) Recording the status of “Complaint in Process" in the database, as stablished by the governing law.

h) Recording the status "Information in Judicial Dispute" in the database once notified by the competent authority on judicial proceedings related to the quality of personal data.

i) Refraining from releasing information being contested by the Owner, and for which a block has been ordered by the Superintendency of Industry and Commerce.

j) Only allowing access to the data to people authorized to do so.

k) Notifying the Superintendency of Industry and Commerce when there are security code violations and risks in the administration of the Owner's data.

l) Complying with the instructions and requirements issued by the Superintendency of Industry and Commerce.

m) Verifying that the Data Administrator has the Owner’s authorization for the treatment of their personal data.

9. Party Responsible for the Processing Requests, Inquiries and Complaints

THE COMPANY as an institution, and in the terms established in the current regulations, will act as the RESPONSIBLE FOR THE TREATMENT of personal data; and its different commercial, financial, and administrative units will act as the ADMINISTRATORS OF THE TREATMENT of personal data.

Notwithstanding the foregoing, THE COMPANY has appointed a PRIVACY OFFICER, or an agency acting as the party that will receive, process and route any requests received, and forward them to the previously mentioned respective unit, responsible, agencies that once they receive these communications, will comply with their personal data protection duties, and must process Owner requests related to the exercise of the Owner’s rights to access, consult, rectify, update, delete and revoke referred to in the terms, time and conditions established in the current personal data protection regulations.

If you believe that THE COMPANY has inappropriately or unlawfully used your personal data, you may contact us by email at protecciondedatos@dhl.com, at the hotline 318 3385132, or at the offices located in the judicial notifications and business addresses AC 22 NO. 56 - 40 and CR 60 NO. 22 – 50, and submit your requests, queries and/or claims via a Form for the Exercise of Rights FA-CM-R-PL1-1, which you can request at the email protecciondedatos@dhl.com

If you want to learn more about our data treatment guidelines, you can check our Comprehensive Personal Data Program, which you can request at our email protecciondedatos@dhl.com or at our hotline 3183385132.

10 Procedures

10.1 Inquiries

Owners or their representatives may review the Owner's personal data contained in any database of the Company. The Privacy Officer must provide the Owners, or their representatives, with all

information contained in the individual record or that are associated to the Owner's identification document.

Inquiries will be done using the means authorized by the Company for this purpose if proof of the inquiry is available.

Requests will be processed within ten (10) business days from the date of receipt. When it is not possible to process the inquiry within that period, the interested party will be notified of the reasons for the delay and a date on which the consultation will be processed, which may never exceed five (5) business days after the expiration of the first period.

10.2 Claims

An Owner or their representatives who believe that the information contained in a database must be corrected, updated, or deleted, or when they notice an alleged failure to perform any of the duties contained in Constitution and the Law, may file a claim with the Privacy Officer (the person appointed by the Company), which will be processed under the following rules:

a) The claim must be filed by filing the Form to Exercise the Rights FA-CM-R-PL1-1 and the Superintendency of Industry and Commerce Report Form FA-CM-R-PL1-5, which can be found on the website www.dhl.com, along with the identification document of the Owner of the data, a description of the facts that gave rise to the claim, an address, and any supporting documents. If the claim is incomplete, the interested party will be required to remedy any errors within five (5) days of receipt of the claim. if the applicant has not submitted the required information after two (2) months from the date of the request, it will be understood that the interested party has waived the claim.

b) If the person receiving the claim is not competent to fulfil the request, they will forward the claim to a competent person within two (2) business days and notify the interested party of the situation.

c) Once the complete claim has been received, the status "Claim in progress" and the reason, will be added to the database within a period not exceeding two (2) business days. Such status shall be maintained until the claim has been settled.

d) The maximum period to process the claim shall be fifteen (15) business days from the day after the date of receipt. When it is not possible to process the claim within that period, the interested party will be notified of the reasons for the delay and the date by which their claim will be processed, which may never exceed eight (8) business days after the expiration of the first period.

10.3 Destruction

The destruction of physical and electronic media will be done using means that do not allow it to be restored. It will be done only in cases when doing so does not constitute the infringement of any legal provision, while ensuring that traceability of the actions taken remains intact. Destruction includes all information in the possession of third parties, as well as in their own facilities**.**

11. International Use and Transfer of Data

Depending on the nature of any permanent or occasional relationship that any owner of personal data may have with THE COMPANY, all their information may be transferred abroad, subject to any applicable legal requirements. When agreeing to this policy you expressly authorize the transfer of personal data. Information for all such third-party relationships with THE COMPANY will be transferred. Notwithstanding the obligation

to observe and maintain the confidentiality of the data, THE COMPANY, will take all necessary measures to notify such third parties and require them to adhere to this Policy, under the understanding that any personal data that they receive may only be used for matters directly related to their relationship with THE COMPANY, and only for the duration of the relationship, and may not be used for any different purposes.

THE COMPANY may also transfer personal data to government or other public authorities (including, but not limited to legal or administrative authorities, tax authorities, criminal, civil, administrative, disciplinary, and tax investigation entities), and third parties involved in civil legal proceedings and their accountants, auditors, attorneys and other advisers and representatives, if it is necessary or appropriate: (a) to comply with any applicable laws, including laws other than those of your country of residence; (b) to comply in legal procedures; (c) to respond to requests from public and government authorities and to respond to requests from public and government authorities other than those of your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations; (f) to protect our, your or third-party rights, privacy, safety or property; and (g) to obtain any applicable indemnities or limit any damages that we may suffer.

The transfer of personal data from and to any country that does not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it meets the standards set by the Superintendence of Industry and Commerce on the matter.

This prohibition does not apply:

a) To information where the Owner has granted their express and unequivocal authorization to transfer it.

b) When transferring medical information when the treatment of the Owner requires it for personal or public health reasons.

c) To bank or stock transfers, in accordance with applicable law.

d) To transfers agreed in the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.

e) To transfers needed to execute a contract between the Owner and the Administrator, or for the execution of pre-contractual measures provided that the Owner has granted authorization.

f) To transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defense of a right in a legal proceeding.

12. Term:

This policy has an issuance date of July 27, 2013; however, it has an update effective from January 1, 2016, and will remain in effect until the end of the treatment of the personal data by the Company. Updated October 09, 2019. Updated February 02, 2021. Updated November 24, 2021. Updated December 20, 2023. Last updated February 1, 2024.

Miguel Paredes
President