PERSONAL DATA PROCESSING POLICY

I. PURPOSE AND SCOPE

LUP TOOLS S.A.S., in order to strictly comply with current regulations on the protection of Personal Data, especially Law 1581 of 2012 and its Regulatory Decree 1377 of 2013, and other provisions that modify, add to, supplement, or repeal them, and committed to the privacy of the personal information of its clients, consumers, partners, suppliers, contractors, users, employees, collaborators, shareholders, and the general public, adopts this Personal Data Processing Policy (hereinafter the 'Policy').

This Policy is mandatory for LUP TOOLS S.A.S. (hereinafter 'LUP'), who will act as the Data Controller.

This Policy, applicable to Personal Data registered in its Databases, outlines the general corporate guidelines for the proper Processing of the Data Subjects' Personal Data, their rights, the department responsible for handling inquiries and complaints, and the procedures that must be followed to access, update, rectify, and delete Personal Data. Thus, LUP affirms that it guarantees the rights to privacy, intimacy, and good name in the Processing of Personal Data, and accordingly, all its actions will be governed by the principles of legality, purpose, freedom, truthfulness or quality, transparency, restricted access and circulation, security, and confidentiality.

All individuals who provide Personal Data to LUP may access, update, rectify, delete, or revoke the previously granted Authorization.

In compliance with the constitutional right to Habeas Data, as established in Article 15 of the Political Constitution of Colombia, LUP only collects Personal Data when it has been previously, expressly, and informedly authorized by its Data Subject or by virtue of Personal Data Transmission or Transfer contracts, implementing clear policies and procedures regarding the confidentiality, security, and privacy of Personal Data.

Likewise, in the course of its operations, LUP may carry out the Processing of Personal Data jointly with other companies that may belong to its corporate group or with those who represent its rights or in the future hold the status of creditor, assignee, or any other role in relation to the Data Subjects.

II. DEFINITIONS

Authorization: Prior, express, and informed consent of the Data Subject for the Processing of Personal Data.
Privacy Notice: Verbal or written communication aimed at informing the Data Subject about LUP's data protection policy.
Database: Organized set of Personal Data subject to Processing.
Successor: The person who has succeeded another due to their death (e.g., heirs).

Companies: Refers to LUP or any of its Affiliates.
Affiliated Companies: Any company directly or indirectly controlled by LUP, including those under unified control and direction.
Personal Data: Any information linked or that can be associated with one or more identified or identifiable natural persons.
Public Data: Data determined as such by law or the Constitution, and those not classified as private or semi-private.
Private Data: Data of intimate or reserved nature relevant only to the Data Subject.
Semi-private Data: Not intimate, reserved, or public, and may be of interest to a certain sector or group.
Sensitive Data: Data affecting the Data Subject's intimacy or misuse of which may lead to discrimination, such as racial or ethnic origin, political orientation, religious or philosophical beliefs, union memberships, health, sexual life, and biometric data.
Processor: Individual or legal entity that processes Personal Data on behalf of the Controller.
LUP: A company that offers a Software as a Service (SaaS) platform for managing OKRs, experimentation, knowledge capture, and use of generative AI for strategic decisions.
Habeas Data: The right of the Data Subject to demand access, inclusion, exclusion, correction, addition, update, and certification of Personal Data, and to limit its disclosure.
Controller: The individual or entity that alone or jointly with others decides on the Processing of Personal Data.
Data Subject: Natural person whose Personal Data is being processed. This includes clients, users, employees, contractors, visitors, candidates, etc.
Data Transfer: The Controller/Processor sends Personal Data to another Controller in or outside Colombia.
Data Transmission: The communication of Personal Data inside or outside Colombia for processing by a Processor.
Processing: Any operation on Personal Data such as collection, storage, use, circulation, or deletion.

III. GUIDING PRINCIPLES OF PERSONAL DATA PROCESSING

LUP is committed to processing Personal Data according to the following principles:

Legality: Processing is governed by law and relevant regulations.
Purpose: Data will be processed for legitimate purposes as informed to the Data Subject.
Freedom: Data will only be processed with the Data Subject's prior, express, and informed consent.
Truthfulness or Quality: Data must be truthful, complete, updated, verifiable, and understandable.
Transparency: Data Subjects have the right to obtain information at any time about the existence of data concerning them.
Restricted Access and Circulation: Processing is limited based on the data's nature, ensuring it is only accessed by authorized persons.
Security: Data is handled using technical, human, and administrative measures to prevent

unauthorized access or fraud.
Confidentiality: All individuals involved in Processing non-public data must guarantee its confidentiality even after their relationship ends, disclosing data only when allowed by law.

IV. GENERAL PROVISIONS

LUP commits to:
• Include in every employment contract a clause indicating compliance with Law 1581 of 2012 and Decree 1377 of 2013.
• Include in the internal work regulations an obligation to comply with the aforementioned laws.
• Require third parties needing access to Personal Databases to sign a contractual clause indicating awareness and responsibility regarding these laws, and to obtain prior Authorization from the Data Subject.
• Require all providers, clients, consumers, volunteers, or any persons whose data is processed by LUP to provide written Authorization for unrestricted data processing, covering all operational purposes.
• Ensure all Databases managed by departments or companies have backup guarantees.
• Maintain restricted access to Databases. When sent via mass media, these will be password-protected.
• Avoid publishing Databases on intranet or internet without access restrictions.
• Require all departments processing Databases to have a written procedure ensuring compliance with this Policy, Law 1581 of 2012, and Decree 1377 of 2013.

V. AUTHORIZATION FOR PERSONAL DATA PROCESSING

Personal Data included in LUP's Databases are obtained through commercial, contractual, labor, or other types of relations related to its corporate purpose.
Upon collection, LUP will request prior, express, and informed Authorization from the Data Subjects, specifying:
(i) the Processing to be carried out and its specific purposes;
(ii) the right to refrain from answering questions about children or Sensitive Data;
(iii) the rights of the Data Subjects and how to exercise them;
(iv) the identity of LUP as the Data Controller;
(v) the location of this Policy.
Data may be stored in physical or digital media, owned or managed by specialized third parties, ensuring confidentiality and security.
Authorization may also be obtained through unequivocal conduct that clearly indicates the Data Subject's consent.
Consent can be given via written, verbal, virtual communication, or unequivocal conduct and must be properly recorded.
If Authorization is not obtained, the Company must refrain from processing the data, except in specific cases such as contractual performance, judicial or administrative requests, historical/statistical/scientific use, or public data.

VI. PURPOSES OF PERSONAL DATA PROCESSING

Personal Data collected will be processed for various purposes according to the role of the Data Subject:

Clients:
• Update and verify client information.
• Authenticate identity for service offers and market engagement.
• Conduct analytics and use of AI to support company indicators.
• Manage contracts and service delivery.
• Send commercial campaigns and promotions via various channels (calls, SMS, email, social media, etc.).
• Share commercial, legal, security, and service information.
• Locate the client for service provision and security communications.
• Perform market research, risk assessments, and statistical analysis.
• Prevent fraud, money laundering, terrorism financing.
• Validate transactions, including the use of biometric and sensitive data.
• Respond to judicial or administrative requests with relevant information only.
• Implement biosecurity and health measures.
• Maintain communication about events and programs.
• Conduct satisfaction surveys, advertising campaigns, and loyalty programs.
• Provide customer service and manage purchase orders and electronic payments.
• Share information with health authorities regarding outbreaks.
• Carry out video surveillance.
• Handle health-related data to offer tailored products and services.
• Use cloud services to process biometric or sensitive data.
• Share Personal Data with Affiliates and nonprofit entities for product/service offers.

Suppliers, Contractors, and Partners:
• Collect data about the individual or legal entity, including employees involved with LUP.
• Manage selection and onboarding procedures, contracts, finance, logistics, etc.
• Perform background checks, anti-money laundering controls, and fraud prevention.
• Execute contracts and partnerships ensuring obligation compliance.
• Offer services via various channels, conduct financial and market analysis.
• Respond to authority requests, use clinical data when necessary, share with Affiliates.

Applicants and Employees:
• Evaluate candidates and manage recruitment.
• Fulfill obligations under employment or service contracts.
• Identify personnel, manage academic/professional records.
• Prevent fraud and enforce workplace security.
• Promote employee welfare and institutional programs.
• Issue employment certifications and monitor health conditions related to pandemics.
• Share with consultants and Affiliates for operational purposes.

VII. PERSONAL DATA PROCESSING

a) Personal Data Processing

The Processing carried out by the Database Controllers will comply with Law 1581 of 2012, Decree 1377 of 2013, and any additional or modified regulations, as well as this Policy and corresponding authorizations.

b) Time Limit for Personal Data Processing

LUP will process Personal Data for the reasonable and necessary duration, which shall not be shorter than the existence of the Company or the term of the contractual, legal, or commercial relationship with the Data Subject. Once the purpose ceases, the data will be deleted or archived under adequate security conditions and only disclosed if legally required.

c) Types of Personal Data Processed

LUP may process identification, contact, location, birth data, socioeconomic, marital status, gender, age, biometrics, judicial records, work and academic data, health, images, videos, and sensitive data.

In the case of children and adolescents, the superior interest of the minor and fundamental rights will be respected. Authorization will be requested from their legal representative.

For sensitive data, LUP will comply strictly with legal principles and guarantees. No activity will be conditioned upon the provision of sensitive data, unless legally required.

d) LUP as Data Processor

LUP may act as a Processor of Personal Data provided by third parties under contract and will comply with Article 18 of Law 1581 of 2012.

e) Transmission and Transfer of Personal Data

LUP may transmit or transfer Personal Data to third parties inside or outside Colombia, including Affiliates, for the authorized purposes. LUP will ensure security and confidentiality, and require third parties to comply with legal obligations.

f) Use of Cookies

LUP may use cookies to enhance websites and browsing experience, and to tailor ads and content. Users can change cookie preferences. Data collected via cookies is encrypted and does not include financial data.

g) Payment Processes

Payments may be made through external financial entities' websites, and in such cases, those entities are responsible for data handling. If LUP collects the data directly, it will do so under this Policy. Data will not be shared unless necessary and authorized.

VIII. RIGHTS OF THE DATA SUBJECT

According to Article 8 of Law 1581 of 2012, the Data Subject has the following rights:

- Free access to their Personal Data being processed.
- Request proof of authorization, except when exempted under Article 10 of the Law.

• Be informed about the use of their data upon request.
• Know, update, and rectify data, especially if inaccurate, incomplete, or unauthorized.
• Submit requests and complaints regarding Personal Data protection.
• Revoke consent and request deletion of data, provided no legal or contractual duty prevents it.
• File complaints with the Superintendency of Industry and Commerce.
• Refrain from answering questions about Sensitive Data or children's data.
• Free access to their data under Processing.

IX. PROCEDURES FOR HANDLING REQUESTS AND COMPLAINTS

i) Who may exercise rights:
• The Data Subject, proving their identity.
• Their successors, with proof.
• Legal representatives or attorneys, with accreditation.
• Stipulations in favor of or for another person.
• Legal representatives of children and adolescents.

ii) Procedure for handling inquiries:
Requests may be submitted to:
• Learn about data usage.
• Request proof of authorization.
• Access data held by LUP.
Requests must state 'Exercise of access right or inquiry' and will be answered within ten (10) business days. If incomplete, LUP will notify the requester within five (5) days. If no reply is received within two (2) months, the request will be considered withdrawn. The deadline may be extended for five (5) more days if necessary.

iii) Procedure for handling complaints:
Complaints may be submitted to:
• Report improper data Processing.
• Correct, update, or delete data.
• Revoke authorization.
Complaints will be answered within fifteen (15) business days. If incomplete, LUP will request more info within five (5) days. If no response is received in two (2) months, the complaint is considered withdrawn. The response period may be extended eight (8) days. If LUP is not competent, the complaint will be forwarded within two (2) business days.

X. CHANNELS FOR HANDLING INQUIRIES AND COMPLAINTS

To submit inquiries, complaints, request information, consult, modify, update, rectify or delete Personal Data, or revoke the Authorization, you may contact:

➢ LUP TOOLS S.A.S.
NIT: 901.803.834-0

Address: Calle 5 SUR No. 43 C 80 PISO 8, Medellín, Colombia
Email: hello@lup.com.co

Requests must include:
(i) Full name of the Data Subject
(ii) Contact details (physical address, email, phone number)
(iii) Copy of ID or authorization documents
(iv) Facts of the request or complaint
(v) Specific request
(vi) Supporting documents
(vii) ID number and signature

XI. INFORMATION ABOUT THE DATA CONTROLLER

The company responsible for data processing is:

➢ LUP TOOLS S.A.S.
NIT: 901.803.834-0
Address: Calle 5 SUR No. 43 C 80 PISO 8, Medellín, Colombia
Email: hello@lup.com.co

XII. TRAINING PROGRAMS

LUP is committed to providing training to employees involved in Personal Data Processing so they understand this Policy, their responsibilities, and the procedures to ensure proper handling of Personal Data.

XIII. RETENTION PERIOD OF THE DATABASES

Databases will remain active for as long as necessary to fulfill the authorized purpose, in accordance with special laws governing the matter or laws governing the company's legal functions.

XIV. VALIDITY AND MODIFICATION OF THE PERSONAL DATA PROCESSING POLICY

This Policy is effective from the date of its publication.

It may be modified at any time to adapt it to legislative or jurisprudential developments or best practices for Personal Data protection. If there are substantial changes regarding the Data Controller's identity or the purposes of Processing that affect the Authorization, the Controller will inform the Data Subject before or at the time of implementing such changes, via the official website (https://www.lup.com.co/), where the updated Policy and its effective date will be available.

If the purpose of Processing changes, a new Authorization must be obtained from the Data Subject.