

L & M L A W Y E R S A S S O C I A T E D S . A . S

PERSONAL DATA PROTECTION POLICY

Legal to grow, protect and transcend.

Last updated: **September 20, 2021**

— 01

Objective and Scope of Application

L&M LAWYERS ASSOCIATED S.A.S (hereinafter, the "Firm"), in compliance with Law 1581 of 2012, Decree 1377 of 2013, and any regulation that may replace or amend them, hereby informs Data Subjects of this Personal Data Protection Policy.

The purpose of this Policy is to inform Data Subjects of their rights and the mechanisms established by the Firm for their exercise, the department responsible for handling complaints and claims, and the procedures established for accessing, updating, rectifying, and deleting information, as well as the scope and purpose of the Processing to which Personal Data will be subjected.

SCOPE OF APPLICATION

This Personal Data Protection Policy shall apply to all Data Subjects whose Personal Data is collected and processed by the Firm within the territory of the Republic of Colombia.

— 02

Definitions

- ◆ **Authorization:** Prior, express and informed consent from the Data Subject to carry out the Processing of Personal Data.
- ◆ **Privacy Notice:** Verbal or written communication generated by the Data Controller, directed to the Data Subject, informing them of the existence of the applicable Data Processing Policies, how to access them, and the purposes of the Processing.
- ◆ **Database:** An organized collection of Personal Data that is subject to Processing.
- ◆ **Personal Data:** Any piece of information linked to one or more identified or identifiable individuals, or that can be associated with a natural person.
- ◆ **Public Data:** Data classified as such by law. Data that is not semi-private, private, or sensitive.
- ◆ **Semi-Private Data:** Data that is not intimate or reserved in nature, nor public, the knowledge of which is of interest to the Data Subject and to certain groups or sectors of society.
- ◆ **Private Data:** Data that is only relevant to its Data Subject.
- ◆ **Sensitive Data:** Data that affects the privacy of the Data Subject or whose improper use may generate discrimination: data related to racial or ethnic origin, political orientation, religious or philosophical convictions, trade union membership, health, sexual life, and biometric data.
- ◆ **Data Processor:** A natural or legal person, public or private, that — alone or in association with others — processes Personal Data on behalf of the Data Controller.

- ◆ **Data Controller:** A natural or legal person, public or private, that — alone or in association with others — decides on the Database and/or the Processing of data.
- ◆ **Claim:** A request from the Data Subject or persons authorized by them or by Law to correct, update, or delete their personal data, or to revoke authorization.
- ◆ **Data Subject:** A natural person whose Personal Data is subject to Processing.
- ◆ **Transfer:** Occurs when the Data Controller and/or Data Processor, located in Colombia, sends information or personal data to a recipient who is also a Data Controller, whether within or outside the country.
- ◆ **Transmission:** Processing of Personal Data that involves communicating such data within or outside the territory of the Republic of Colombia for the purpose of Processing by a Data Processor on behalf of the Data Controller.
- ◆ **Processing:** Any operation or set of operations on Personal Data, such as collection, storage, use, circulation, or deletion.

— 03

Principles

In accordance with Law 1581 of 2012, all Processing carried out by the Firm shall comply with the following principles:

- ◆ **Lawfulness:** The Processing of personal data shall be carried out in accordance with applicable legal provisions.
- ◆ **Purpose:** The Processing must be based on a legitimate purpose consistent with the Constitution and the Law, which must be disclosed to the Data Subject.
- ◆ **Freedom:** The Processing of Personal Data may only be carried out with the prior, express, and informed authorization of the Data Subject. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that waives consent.
- ◆ **Accuracy or Quality:** Information subject to Personal Data Processing must be truthful, complete, accurate, up-to-date, verifiable, and comprehensible.
- ◆ **Transparency:** The Data Subject's right to obtain, at any time and without restrictions, information about data concerning them, must be guaranteed throughout the Processing.
- ◆ **Restricted Access and Circulation:** The Processing of personal data may only be carried out by persons authorized by the Data Subject and/or by those provided for by Law.
- ◆ **Security:** Personal Data subject to Processing shall be handled by adopting all necessary technical, human, and administrative security measures to prevent its loss, alteration, unauthorized or fraudulent consultation, use, or access.
- ◆ **Confidentiality:** All parties involved in the Processing are obligated to maintain confidentiality over personal data that is not of a public nature, even after their relationship with any Processing activities has ended.

— 04

Data Controller

Company Name	L&M LAWYERS ASSOCIATED S.A.S
Address	Calle 25B N° 69B-71, Office 502 · Bogotá D.C., Colombia
Phone	(+57) 302 530 5490
Email	info@lymlawyers.com
Website	www.lymlawyers.com

— 05

Processing of Personal Data

The Firm, acting as Data Controller, in order to properly develop its business activities and strengthen its relationships with third parties, shall collect, store, use, transmit, transfer, update, rectify, and delete Personal Data of Data Subjects, for which it shall request prior authorization and inform Data Subjects of the specific Processing purposes.

The information collected may only be used by the Firm, its employees, consultants, advisors, group subsidiaries, and commercial and strategic partners expressly authorized by the Firm.

5.1. Authorization

At the time of collecting Personal Data, the Firm shall request prior, express, and informed authorization from Data Subjects, unless one of the exceptions under Article 10 of Law 1581 of 2012 applies.

Authorization may be given: (i) in writing, (ii) verbally, or (iii) through unequivocal conduct from which reasonable consent can be inferred. Under no circumstances will the Firm interpret the Data Subject's silence as unequivocal conduct.

IMPORTANT: *The Firm shall maintain proof of authorizations in an appropriate manner, respecting the principles of confidentiality and privacy of information.*

5.2. Purposes of Personal Data Processing

The Firm shall process Personal Data for the purposes set out below. Data Processors or third parties with access to Personal Data must align their Processing with these same purposes or with those disclosed at the time of collection.

5.2.1. Clients and Prospective Clients

- Managing the contractual and/or pre-contractual relationship, including the provision of legal services, legal advice, and judicial and extrajudicial representation.
- Collecting, storing, and processing all information provided by Data Subjects in databases.
- Sending information related to services offered, regulatory updates, events, publications, and material of interest.
- Billing, accounting management, and compliance with tax obligations.
- Handling inquiries, requests, complaints, and claims.
- Complying with legal obligations regarding the prevention of money laundering and terrorist financing (AML/CTF).
- Complying with requirements from administrative or judicial authorities.
- Collecting information for commercial research and marketing purposes.
- Handling contact requests and inquiries received through the Firm's digital channels.
- Analyzing metrics and browsing preferences to improve user experience.
- Reporting and consulting on current or overdue obligations with credit risk bureaus.
- Consulting databases administered by credit bureaus to evaluate the Data Subject's credit history, financial solvency, and the feasibility of establishing or maintaining a contractual relationship.

5.2.2. Employees and Job Applicants

- Managing the employment relationship, including social security system enrollment, payroll, benefits, training, and employee wellness.
- Evaluating and selecting personnel for hiring and/or promotion processes.
- Access control and physical and digital security at the Firm's premises.
- Managing employment references, subject to prior authorization from the Data Subject.
- Developing training programs and internal campaigns.
- Verifying, corroborating, validating, researching, or comparing information provided by Data Subjects.
- Complying with legal requirements and information requests from administrative authorities and social security entities.

5.2.3. Shareholders

- Recognition, protection, and exercise of the rights of the Firm's shareholders.
- Fulfilling legal and contractual obligations, including dividend payments.
- Carrying out procedures related to the sale, transfer, or disposal of shares.
- Filing registrations with the Chamber of Commerce's mercantile registry.

5.2.4. Suppliers and Prospective Suppliers

- Fulfilling legal and contractual obligations.
- Verifying legal, technical, and financial requirements.
- Verifying commercial and reputational background.
- Billing, accounting management, and compliance with tax obligations.
- Reporting and consulting on current or overdue obligations with credit risk bureaus.
- Consulting credit bureau databases to evaluate credit history and financial solvency.
- Attending to judicial or administrative requirements and complying with judicial or legal orders.
- Complying with legal obligations regarding the prevention of money laundering and terrorist financing (AML/CTF).

SECURITY AND TRANSFER

In keeping with the security principle, the Firm has adopted reasonable technical, administrative, and human measures to protect Personal Data and prevent its alteration, loss, unauthorized consultation, use, or access. The Firm may transmit and/or transfer Personal Data to third parties located in Colombia or abroad, provided that prior and express authorization from the Data Subject has been obtained.

5.3. Rights of Data Subjects

In accordance with the Law, Data Subjects have the following rights:

- a. To access, update, and rectify their Personal Data held by Data Controllers or Data Processors. This right may be exercised with respect to partial, inaccurate, incomplete, fragmented, misleading data, or data whose Processing is expressly prohibited or has not been authorized.
- b. To request proof of the authorization granted to the Data Controller, unless expressly exempted as a Processing requirement under Article 10 of Law 1581 of 2012.
- c. To be informed by the Data Controller, upon request, about the use made of their Personal Data.
- d. To file complaints with the Superintendency of Industry and Commerce (SIC) for violations of Law 1581 of 2012 and other regulations that amend, add to, or complement it.
- e. To revoke authorization and/or request deletion of data, provided there is no legal or contractual obligation requiring the Data Subject to remain in the database.
- f. To access their personal data that has been subject to Processing free of charge, at least once per calendar month and whenever there are material changes to the processing policies.

PERSONS ENTITLED TO EXERCISE THESE RIGHTS

The Data Subject (upon proving their identity), their heirs (upon proving such status), and the Data Subject's representative and/or attorney (upon proving representation or power of attorney).

5.4. Obligations of the Data Controller

In accordance with the Law, the Data Controller shall fulfill the following obligations:

- a. Guarantee the Data Subject, at all times, the full and effective exercise of the right to habeas data.
- b. Request and retain a copy of the respective authorization granted by the Data Subject.
- c. Properly inform the Data Subject of the purpose of the collection and the rights they hold by virtue of the authorization granted.
- d. Maintain information under the necessary security conditions to prevent its alteration, loss, unauthorized or fraudulent consultation, use, or access.
- e. Ensure that the information provided to the Data Processor is truthful, complete, accurate, up-to-date, verifiable, and comprehensible.
- f. Update information, timely notifying the Data Processor of any changes to data previously provided, and taking all necessary measures to keep such information current.
- g. Rectify information when incorrect and communicate the relevant changes to the Data Processor.
- h. Provide the Data Processor only with data whose Processing has been previously authorized.
- i. Require the Data Processor to comply at all times with the security and privacy conditions applicable to the Data Subject's information.
- j. Process inquiries and claims within the timeframes set out in this Policy.
- k. Adopt an internal policy and procedure manual to ensure proper compliance with Personal Data protection regulations.
- l. Inform the Data Processor when certain information is under dispute by the Data Subject, once a claim has been submitted and its processing has not yet concluded.
- m. Inform the Data Subject, upon request, about the use made of their data.
- n. Notify the data protection authority when security code violations occur or when risks arise in the management of Data Subject information.
- o. Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

5.5. Special Provisions for Processing Sensitive Data

The Firm may request Sensitive Data at any time, informing the Data Subject — no later than at the time of collection — that the requested data is of this nature and which type of Sensitive Data will be collected. The Firm may process sensitive data if:

- The Data Subject provides explicit and voluntary consent for specific purposes.
- Processing is necessary to comply with legal obligations.
- Processing is necessary to protect the vital interests of the Data Subject or another natural person.
- Processing relates to Personal Data that the Data Subject has made public.
- Processing is necessary for the establishment, exercise, or defense of legal claims, or when courts or tribunals act in the exercise of their judicial function.
- Processing is necessary for reasons of substantial public interest.

- Processing is mandatory by virtue of Law.

IMPORTANT: *The Firm shall not make any activity conditional upon the provision of Sensitive Data. Sensitive Data will be handled with the utmost diligence and the highest security standards. Only authorized personnel shall have access to such information.*

5.6. Processing of Personal Data of Children and Adolescents

In compliance with the Law, the Firm guarantees that the Processing of Personal Data of children and adolescents shall be carried out with strict respect for their fundamental rights and only with the prior and express consent of their parents or legal guardians. In all cases, the Processing shall respond to and respect the best interests of children and adolescents.

— 06

Department Responsible for Handling Requests, Inquiries, and Claims

The Firm has designated its Customer Service Department as the department responsible for receiving and handling requests, complaints, claims, and inquiries related to Personal Data.

CONTACT CHANNELS

Email: info@lymlawyers.com Phone: (+57) 302 530 5490

6.1. Procedures for Exercising Data Subject Rights

6.1.1. Inquiries

The Data Subject, as well as their heirs, representatives, and/or attorneys, may submit inquiries regarding their Personal Data held in the Firm's Databases, in accordance with the following:

- a. The request shall be analyzed to verify the identity of the Data Subject. If submitted by a third party who fails to demonstrate proper representation under applicable law, the request shall be rejected. The Firm may request the Data Subject's identification document and any powers of attorney, general or special, or other documents it deems necessary in each case.
- b. All inquiries shall be resolved within a maximum of ten (10) business days from the date of receipt. If it is not possible to process the inquiry within this period, the interested party shall be notified of the reasons for the delay and the date on which a response will be provided, which may not exceed five (5) additional business days beyond the initial deadline.

6.1.2. Claims

The Data Subject, as well as their heirs, representatives, and/or attorneys, may submit claims regarding Personal Data they believe should be corrected, updated, deleted, or for which they wish to revoke Authorization, in accordance with the following:

- A. The request shall be analyzed to verify the identity of the Data Subject. If submitted by a third party who fails to demonstrate proper representation, the request shall be rejected.
- B. The claim must include: (i) the Data Subject's identification; (ii) contact information; (iii) documents proving identity or representation; (iv) a clear description of the Personal Data in question; (v) a description of the facts giving rise to the claim and its objective; (vi) supporting documents; (vii) signature and identification number.
- C. If the claim is incomplete, the Firm shall notify the claimant within five (5) days of receipt, requesting they remedy the deficiencies. If two (2) months pass from the date of notification without the required information being submitted, the claim shall be deemed withdrawn.
- D. If the department receiving the claim is not competent to resolve it, it shall refer the matter to the appropriate department within a maximum of two (2) business days and notify the claimant of such referral.
- E. The maximum period for resolving a claim is fifteen (15) business days from the day following receipt. If it is not possible to resolve the claim within this period, the interested party shall be informed of the reasons for the delay and the expected resolution date, which may not exceed eight (8) business days beyond the initial deadline.
- F. The Data Subject has the right to request the deletion of their information from the Databases at any time, in full or in part. However, this right is not absolute and may be denied when: (i) a legal or contractual obligation requires the Data Subject to remain in the Database; (ii) deletion would obstruct judicial or administrative proceedings; (iii) the Personal Data is necessary to protect the legally protected interests of the Data Subject or to fulfill a legally acquired obligation.

— 07

Effective Date

EFFECTIVE DATE AND RETENTION

This Personal Data Protection Policy is effective as of September 20, 2021. Personal Data stored in the Databases shall be retained and processed in accordance with the principle of temporality. Its retention shall be determined by the duration of the contract associated with the product or service, extending throughout the period in which the purpose that motivated its collection persists, and for any additional period required by applicable regulations.

L&M LAWYERS ASSOCIATED S.A.S

Legal to grow, protect and transcend.

