PERSONAL DATA PROCESSING POLICY
Linio Colombia S.A.S

PERSONAL DATA PROCESSING POLICY.

The protection of your Personal Data matters a lot to us, please read this Policy carefully and find out, among other things, how, when and for what we process your Personal Data, as well as how you can exercise the rights that you have as data subject.

1. Personal Data Controller:

Linio Colombia S.A.S.; ABC de Servicios S.A.S.; Agencia de Seguros Falabella Ltda.; Banco Falabella S.A.; Digital Payments S.A.S.; Falabella de Colombia S.A. and Mallplaza Servicios S.A.S., individually the "**Company**" and together the "**Companies**", will act as Controller, for the collection, storage, use, processing, updating, circulation, deletion, transfer, transmission and, in general, any operation or set of operations in and on your Personal Data, understood as any information linked or that may be associated with you as the Subject.

Below, each of the Companies that act as Data Controllers are identified, as well as the link to the Personal Data Processing Policies and channels enabled for the exercise of rights:

Trade Name	NIT	Address	Phone	Consultation of the Policy for the Processing of Personal Data	Channels to exercise rights
Linio Colombia S.A.S.	900.499.362-8	Calle 99 # 14 – 49 Piso 9°. Bogotá	(571) 4842222	www.linio.com.co	datos.personales@falabella.com
ABC de Servicios S.A.S.	830.514.755-1	Avenida 19 120 - 71 Piso 3°. Bogotá	(571) 5878000	www.cmrpuntos.com.co	datospersonales@cmrpuntos.com.co
Agencia de Seguros Falabella LTDA	900.074.589-8	Avenida 19 120 - 71 Piso 2°. Bogotá	(571) 5878000	www.segurosfalabella.com.co	protecciondedatosasf@falabella.cl
Banco Falabella S.A.	900.047.981-8	Avenida 19 120 - 71 Piso 3°. Bogotá	(571) 5878000	www.bancofalabella.com.co	datospersonales@bancofalabella.com.co
Digital Payments S.A.S.	901.476.442-3	Avenida 19 120 - 71. Bogotá	(571) 5878787	www.fpay.com.co	datospersonales@fpay.com.co
Falabella de Colombia S.A.	900.017.447-8	Calle 99 # 11A – 32. Bogotá	(571) 5878002	www.falabella.com.co	habeasdataclientes@falabella.com.co
Mallplaza Servicios S.A.S.	901.120.943-3	Avenida Calle 19 No. 28-80. Piso 6, oficinas administrativas. Bogotá	(571) 7458787	www.mallplaza.co	datos.personales@mallplaza.com

2. Definitions

The words and terms will have the meanings indicated below, for your proper understanding of this Personal Data Policy:

2.1. Agreement of Assignment and Transmission of Personal Data: Refers to the agreement signed by ABC de Servicios S.A.S.; Agencia de Seguros Falabella Ltda.; Banco Falabella

S.A., Digital Payments S.A.S.; Falabella de Colombia S.A.; Linio Colombia S.A.S.; Mallplaza Servicios S.A.S. and Sodimac Colombia S.A., under which the Company (as Processor) may collect personal data and authorizations for the processing of the data of Subjects on behalf of the aforementioned companies.

2.2. **Authorization:** Means the prior, express and informed consent of the Data Subject to carry out the Processing. This can be i) written; ii) verbal or; iii) through unequivocal conduct that allows reasonable conclusion that the Subject accepted the Processing of their data.

2.3. **Authorized: Mea**ns all persons who, under the responsibility of the Companies or their Processors, may carry out Processing of Personal Data by virtue of the Authorization granted by the Subject.

2.4. **Privacy Notice.** Verbal or written communication generated by the Controller, addressed to the Subject for the Processing of their personal data, through which they are informed about the existence of the Information Processing policies that will be applicable to them, the way to access them and the purposes of the Processing that is intended to give to the personal data.

2.5. **Database**: Means the organized set of Personal Data that are subject to Processing.

2.6. **Service Channels**: Means through which the Subject can exercise their rights.

2.7. **Customer**: Natural person who makes purchases through physical retail establishments and/or digital channels provided by the Companies.

2.8. **Potential Customer(s):** Natural Person(s) who could become a buyer(s) or consumer(s) of the products or services offered through physical retail establishments and/or digital channels provided by the Companies.

2.9. **Candidates**: Natural Person who applies for any of the vacancies of the Company or Related Companies.

2.10. **Collaborators / Workers / Employees**: Natural Person who is engaged by the Company by means of an Employment Contract.

2.11. **Consultation**: It means the request of the Owner of the Personal Data, of the persons authorized by it, or those authorized by law, to know the information on the Subject in the Databases of one or more Companies.

2.12. **Personal Data**: Means any information linked or that can be associated with one or more natural persons, determined or determinable.

2.13. **Private Personal Data:** Means Personal Data that by its intimate or reserved nature is only relevant to the Subject.

2.14. **Public Personal Data:** Means Personal Data deemed as such according to the mandates of the law or the Political Constitution and all those that are not semi-private, private or sensitive. For example: data contained in public documents, public records, gazettes, official gazettes and duly enforceable court rulings that are not subject to confidentiality, those

relating to the marital status of persons, their profession or trade and their status as a merchant or public servant.

2.15. **Semi-Private Personal Data:** Means Personal Data that is not intimate, reserved, or public and whose knowledge or disclosure may interest not only its Subject but a certain sector or group of persons, or society in general. For example: data relating to compliance with and non-compliance with financial obligations or data relating to relations with social security institutions.

2.16. **Sensitive Personal Data:** Means Personal Data that affects the privacy of the person or whose improper use may generate discrimination. For example: those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of trade unions, social or human rights organizations or organizations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, data relating to health, sex life and biometric data (fingerprints, photographs, recordings on security cameras).

2.17. **Habeas Data Right**: Means the right that all persons have to know, update and rectify the information that has been collected about them in databases and in files of public and private entities, in accordance with article 15 of the Political Constitution of Colombia.

2.18. **Data Processor:** Means the natural or legal person who carries out the Processing of Personal Data on behalf of the Data Controller.

2.19. **Financial Information**: Means the information referring to the birth, execution and extinction of monetary obligations, regardless of the nature of the agreement that gives rise to them.

2.20. **Suppliers:** Natural or Legal Person that supplies or provides products, goods or services to the Company(ies).

2.21. **Claim:** Means the request of the Subject or the persons authorized by them or by law to correct, update or delete their Personal Data or when they notice that there is an alleged breach of the data protection regime, according to article 15 of Law 1581/2012.

2.22. **Data Controller:** Means the natural or legal person, whether public or private, that by itself or in association with others, decides on the database and/or the Processing of Personal Data.

In this case, the following Companies are the Data Controllers: ABC de Servicios S.A.S.; Agencia de Seguros Falabella Ltda.; Banco Falabella S.A.; Digital Payments S.A.S.; Falabella de Colombia S.A.; Linio de Colombia S.A.S.; and Mallplaza Servicios S.A.S.

2.23. **Subject:** Means the natural person whose Personal Data are subject to Processing.

2.24. **Assigned Worker**: Natural person engaged by employment agreement to a Temporary Services Company duly authorized by the Ministry of Labor that provides services to a Company.

2.25. **Processing or Processing of Personal Data:** Means any operation or set of operations on Personal Data such as the collection, storage, use, circulation, transfer, transmission,

updating or deletion of Personal Data, among others. The Processing may be national (within the Republic of Colombia) or international (outside the Republic of Colombia).

2.26. Transmission: Means the Processing of Personal Data that implies the communication thereof inside or outside the territory of the Republic of Colombia when its purpose is the performance of Processing by the Processor acting on behalf of the Controller.

2.27. Transfer: Means the Processing of Personal Data that takes place when the Controller and/or Processor for the Processing of Personal Data sends the Personal Data to a recipient, who in turn will be Data Controller and is inside or outside the Republic of Colombia.

2.28. Sellers/Tenants: Means all natural and/or legal persons who offer their goods and/or services through physical retail establishments and/or digital channels provided by the Companies to be acquired by Customers or Consumers.

2.29. Visitors: Means such natural person who accesses the retail establishments, whether physical or digital or the administrative facilities of any of the Companies.

3. Purpose and Scope

The purpose of this Personal Data Processing Policy (the "**Policy**") is, together with the technical, human and administrative measures implemented, to ensure adequate compliance with the applicable Personal Data Protection Law, as well as the definition of the guidelines for the attention of queries and claims of the Subjects of Personal Data regarding which the Companies carry out some type of Processing.

This Policy is of mandatory and strict compliance by the Companies, their directors, administrators, Collaborators and other third parties who represent or act for them, or with whom the Companies have any type of legal, commercial or contractual relationship.

All Collaborators of the Companies are required to observe, respect, comply with and enforce this Policy in the performance of their duties.

4. Principles for the Processing of Personal Data

In the development, interpretation and application of this Policy, the following principles will be applied in a harmonious and comprehensive manner:

4.1. Principle of Freedom: Unless otherwise legally required, the Processing of data may only be exercised with the prior, express and informed authorization of the Subject. Personal Data may not be obtained or disclosed without the prior consent of the Subject, or in the absence of a legal or judicial mandate that relieves consent. The data Subject will be informed in a clear, sufficient and prior manner about the purposes of the Processing.

4.2. Principle of Purpose: The Processing will obey to a legitimate purpose in accordance with the Constitution and the Law, which will be informed to the Subject in a prior, clear and sufficient manner. Personal Data may not be collected without a specific purpose.

4.3. Principle of Legality in terms of Data Processing: The Processing referred to in the Law is a regulated activity that will be subject to the provisions of the Law applicable in the Republic of Colombia and the other provisions that develop it.

4.4. Principle of Truth or Quality: The information subject to Processing will be truthful, complete, accurate, updated, verifiable and understandable. The Processing of partial, incomplete, fractional or misleading data is prohibited. Reasonable measures will be taken to ensure that the data are accurate and sufficient and, when requested by the Subject or when the Company(ies) determine so, they are updated, rectified or deleted if appropriate.

4.5. Principle of Security: Each Company will comply with the technical, human and administrative measures to ensure the security of the Personal Data avoiding its adulteration, loss, consultation, use or unauthorized or fraudulent access.

4.6. Principle of Transparency: In the Processing, the right of the Subject to obtain at any time and without restrictions information about the existence of Personal Data that concerns them will be guaranteed.

4.7. Principle of Access and Restricted Circulation: Access to Personal Data will only be allowed to the following persons: (i) the Subject; (ii) to persons authorized by the Subject; and (iii) to persons who by legal mandate or court order are authorized to know the information of the Subject.

4.8. Principle of Confidentiality: All persons involved in the Processing of Personal Data that are not public in nature are required to guarantee the reservation of the information, even after the end of their relationship with any of the tasks that comprise the Processing, being able only to make provision or communication of Personal Data when this corresponds to the development of the activities authorized by law.

5. Authorization

At the time of Processing Personal Data, the Companies, in their capacity as Controllers, will obtain the consent of the Subject, which in any case will be prior, express and informed.

The Authorization may be obtained by any means that guarantees its reproduction.

In the following events no Authorization by the Subject is required:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- Data of a public nature.
- Cases of medical or health emergency.
- Processing of information authorized by law for historical, statistical or scientific purposes.
- Data related to the Civil Records of Persons.

In the event of collection of Sensitive Data, the Authorization will be explicit as to the fact that the Personal Data subject to Processing are sensitive and the purposes of the Processing. In this case, the Subject is not required to authorize the Processing of such information.

PARAGRAPH: In cases where it is not possible to make the Personal Data Processing Policy available to the Subject, the Company will inform by means of a Privacy Notice to the Subject about the existence of the Policies and the way to access it, in a timely manner and in any case at the latest at the time of collection of Personal Data. The Privacy Notice may be provided in physical documents in the commercial premises, by electronic means in virtual channels, by data message in chat, telephone channel, among other means that are provided by the Company.

6. Personal Data Subject to Processing

The Personal Data that will be subject to Processing by each Company are: identification data, contact information, location and geolocation information, navigation data, data classified as sensitive (Example: Data related to health, fingerprint, photos, video recordings, among other biometric data), financial information, goods, socioeconomic data, labor and academic information, preferences, tastes and consumption behaviors, data inferred or not from information observed or delivered directly by the Subject or by third parties and demographic and transactional information. Personal Data will be collected through the different channels provided by the Companies.

7. Processing and Purposes for which Personal Data may be Processed

Each Company will carry out the Processing of Personal Data in accordance with the conditions established by the Subject, the law or public entities, through physical, automated or digital means in accordance with the type and form of collection of information.

The Personal Data may be Processed by such Collaborator of each Company that has Authorization for it, or those whose functions include being in charge of carrying out such activities. Likewise, the Processing will be carried out by the third-party Processors commissioned by the Company(ies) for the fulfillment and execution of the purposes authorized by the Subject. Public or administrative entities, in the exercise of their legal functions or by court order, may request access to information.

Each Company may process Personal Data for the following purposes:

7.1. Purposes of data Processing common to the Parties listed in this Policy.

In the event that it applies, the Company may process, with prior authorization, personal information in accordance with the following purposes common to **Potential Customers, Customers, Candidates, Collaborators, Assigned Workers and Employees, Sellers/Tenants and/or Suppliers, and Visitors**:

- Validation of the information in order to comply with the regulations on Money Laundering and Terrorism Financing by the Company or with third parties contracted for such purpose.
- For e-commerce purposes.
- Storage of information on own or third-party servers, located in the Republic of Colombia or abroad.
- Disclose, Transfer and/or Transmit Personal Data nationally and internationally, to parents, affiliates or subsidiaries of the Companies or to third parties, to fulfill the purposes described in

this Policy, as a result of an agreement, law or lawful link that so orders, or to implement cloud computing services.
- Meet requirements of external, internal and/or competent authorities audits.
- Compliance with the Policies that the Companies have according to the contractual and/or commercial relationship, including the Personal Data Processing Policy.
- Manage compliance with legal, pre-contractual, contractual, post-contractual, tax, financial and/or accounting obligations.
- Manage queries, requests, petitions, complaints and claims related to the subjects of the information.
- Implement artificial intelligence programs or any other that technology and the law allow.
- Guarantee physical and digital security, improvement of service and experience in commercial establishments or in the facilities of the Companies.
- Send information by the Companies, via physical and/or electronic mail, text messages (SMS and/or MMS), through social media such as Facebook, Instagram or WhatsApp or other similar platforms, push notifications, telephone means or any other means of communication that technology and the Law allow.

7.2. Purposes of Processing the data of Customers or Potential Customers

The personal information of Customers or Potential Customers may be processed in accordance with the following purposes:

i) Commercial Purposes:

- Develop commercial and marketing activities, such as: consumer analysis; profiling, brand traceability; sending news, advertising, promotions, offers and benefits; customer loyalty programs; market research; generation of campaigns and events of the Companies' brands.
- Offer means of financing, for which they may verify and analyze current and historical credit behavior, estimate income levels, validate identity and perform credit checks, among others.

ii) Service Purposes

- Notify orders, deliveries or events related to the products or services purchased or contracted by the Companies.
- Carry out data update campaigns, for the purposes indicated in this Policy.
- Conduct Satisfaction Surveys.

iii) Analysis and Operational Purposes

- Develop studies of the Subject's knowledge, for the different purposes indicated in this Policy.
- Carry out statistical analysis, billing, offering and/or recognition of benefits, telemarketing and collections related to the Companies.
- If required by the nature of the activities, compare, contrast, consult and complement the Personal Data with financial, commercial, credit and service information available in credit information centers and/or financial information database operators ("Information Centers").
- Manage browsing information to maintain access, remember preferences and offer relevant content, as well as those provided by the use of cookies.

iv) Security, Information and Prevention Purposes

- Study credit and financial product applications.
- Perform credit scoring, apply income validation tools, income predictive tools and tools to prevent fraud and, in general, perform adequate risk management.
- In case that due to the nature of the activities it is required, report to the Information Centers about compliance or non-compliance of obligations acquired with the Companies.
- If required by the nature of the activities, provide the Information Centers with data related to credit applications, as well as other data related to commercial, financial and, in general, socioeconomic relations, among others.

7.3. Purposes of Processing of Candidates, Collaborators, Assigned Workers and Employees' Data

In the event that a Company carries out a selection and/or hiring process; or there is an employment agreement with the Subject, each Company may process the Personal Data collected, with the prior authorization of the Subject, for the following purposes:

i) Purposes of processing within selection and/or hiring processes

- Comply with the purposes of the Company's selection and/or hiring process, evaluate their suitability and/or eventual hiring.
- Verify and confirm the accuracy of the information included in the resume and any other document or information provided to the Company.
- Conduct security studies of the candidate, which includes consulting or obtaining judicial records, conducting home visits and consulting data in information centers, among others.
- Be part of the database of applicants for future hiring.
- Sending communications of selection processes similar to those in which the subject has participated.
- Comply with the Company's hiring policies.
- Verify their background in accordance with the provisions of binding compliance programs such as, for example, crime prevention, ethics and free competition.
- Request supports corresponding to the résumé, medical examinations, psycho-technical tests and any other that may be necessary.
- Manage the human resources of the Companies in accordance with the applicable legal and contractual terms.
- Comply with the legal obligations of the Companies in its capacity as employer, including among others the management of payroll, fringe benefits, comprehensive social security system, prevention of occupational hazards, pensions, taxes, among others.
- Manage labor welfare activities, talent and promotion of Collaborators. As part of the management of the welfare of its Workers, the Employer Company may contact the Employee and offer products and services through financial, credit, educational or any other entity with which it has commercial ties. To do so, it may require communicating Personal Data of the Collaborator to such third parties with due compliance with the corresponding legal requirements.
- Make use of personal information and images generated in the framework of the activities, processes and events of the Companies, to socialize them internally and externally through digital channels, social media, WhatsApp, YouTube, or any other communication media; as well as the creation and distribution of physical, digital or audiovisual advertising material.

- Carry out physical and digital security risk management activities of the employing Company through the video surveillance and biometric registration devices provided.
- Carry out due diligence and disciplinary investigation procedures in matters of legal or reputational risk management, such as fraud, possible commission of crimes, infringements of free competition, information leaks, or any other defined by the Company.
- Register, process and store the information provided in the complaints and/or inquiries filed in the Integrity Channel of the Company.

7.4. Purposes of data processing of Vendors/ Sellers/ Tenants and/or Suppliers

Where applicable, the Company may process personal information of Vendors/Sellers/Tenants and/or suppliers, in accordance with the following purposes:

i) Purposes of commercial relationship with third parties

- Perform analytical and data mining activities in order to understand the behavior of vendors, sellers and/or suppliers and their projections in terms of sales, products, and other relevant figures, within the permitted legal framework.
- Involve vendors, sellers and/or suppliers in marketing initiatives on the products, goods and services of the Companies, which may include, among others and without limitation: invitations to events, offering products and financing solutions, call to activities associated with the business relationship or existing link with the Companies, among others.
- Implement relationship strategies with customers, suppliers, shareholders and other third parties with which the Companies have commercial, contractual or legal ties.
- Consult in credit bureaus or credit information centers, all relevant information for the Companies to know its performance as a debtor and the financial situation in which it finds itself, in order to determine its viability to enter into or maintain a contractual relationship with the Companies.
- Report to the credit bureaus or credit information centers, the non-compliance of the commitments acquired with the Companies as part of the contractual relationships or obligations acquired with the latter.
- Sending information related to matters associated with the operation, commercial, accounting, financial, among others, that may be necessary for the normal course of the Company's business.

7.5. Purposes of Visitor Data Processing

- For statistical purposes.
- Perform Video Surveillance in order to ensure the safety of our Potential Clients, Candidates, Collaborators, Assigned Workers and Employees, Vendors/Sellers and/or Suppliers, facilities, goods and assets.
- Improve our service, as well as the experience in our facilities.

The validity of the database will be the reasonable and necessary time to fulfill the purposes of the Processing in each case, taking into account the provisions of Article 2.2.2.25.2.8 of Decree 1074/2015.

8. Rights of the Data Subjects

The Personal Data Subject, has the right to:

8.1. Know, update and rectify the Personal Data with the Data Controllers or Data Processors. This right may be exercised, among others, against partial, inaccurate, incomplete, fractioned, misleading data or data whose processing is expressly prohibited or has not been authorized. For this purpose, it is necessary to previously establish the identification of the person in order to prevent unauthorized third parties from accessing the Subject's data.

8.2. Request proof of the Authorization granted to the Company, unless it is one of the cases in which authorization is not required, in accordance with the law.

8.3. Be informed by the Company, upon request, regarding the use it has made of its Personal Data.

8.4. File before the Superintendence of Industry and Commerce complaints for violations of the provisions of the law in force and other rules that modify, add to or complement it.

8.5. Revoke the authorization and/or request the deletion of the data at any time. The request for deletion of the information and the revocation of the authorization shall not apply when the Data Subject has a legal or contractual duty to remain in the database of the Data Controller or Data Processor.

8.6. Access free of charge to the Personal Data that have been subject to Processing.

8.7. Answer, optionally, the questions related to Sensitive Personal Data or Personal Data of minors. Since the Personal Data is Sensitive Personal Data, the Subject is not obliged to authorize its Processing.

The Subjects may exercise before the Company the rights established by law, in this Policy or in the Authorization granted, at any time.

9. Duties of the Company when acting as Controller.

Each Controller is obliged to comply with the following duties:

9.1. Regarding the Data Subject.

a. Guarantee the Data Subject, at all times, the full and effective exercise of the rights set forth in paragraph 8 of this Policy.

b. Request and keep, under the conditions set forth in this Policy, a copy of the Authorization granted by the Data Subject.

c. Clearly and sufficiently inform the Data Subject about the purpose of the Processing and the rights it has by virtue of the Authorization granted.

d. Inform, at the request of the Data Subject, about the use given to its Personal Data.

e. Process the queries and claims formulated in the terms set forth in this Policy.

9.2. Regarding the quality, security and confidentiality of the Personal Data.

a. Observe the principles of accuracy, quality, security and confidentiality under the terms set forth in this Policy.

b. Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, unauthorized or fraudulent use or access.

c. Update the information when necessary.

d. Rectify the Personal Data when appropriate.

9.3. Regarding Processing through a Processor.

a. Provide to the Processor only the Personal Data whose Transmission is previously authorized by the Data Subject or by the regulation in force.

b. Ensure that the information provided to the Processor is truthful, complete, accurate, updated, verifiable and understandable.

c. Communicate in a timely manner to the Processor, all developments with respect to the data previously provided and take other necessary measures to ensure that the information provided to it is kept up to date.

d. Inform in a timely manner to the Processor the rectifications made on the Personal Data so that it proceeds to make the necessary adjustments.

e. Require the Processor at all times, to respect the security and privacy conditions of the Data Subject's information.

f. Inform the Processor when certain information is under discussion by the Data Subject once the claim has been filed and the respective process has not been completed.

9.4. Regarding the Superintendence of Industry and Commerce.

a. Inform the Superintendence when violations to the security codes occur and there are risks in the administration of the Personal Data of the Data Subject.

b. Comply with the instructions and requirements given by the Superintendence of Industry and Commerce.

10. Duties of the Company when acting as Processor.

On the occasion of the Personal Data Assignment and Transmission Agreement, the Company may collect personal data and authorizations for the processing of data on behalf of the Companies

identified in paragraph 1 of this Policy and of Sodimac Colombia S.A., and to that extent, the Company, when acting as Processor, shall be obliged to comply with the following duties:

10.1. Regarding the Data Subject.

a. Guarantee the Data Subject, at all times, the full and effective exercise of the right of habeas data.

b. Carry out the Processing for the purposes that are the object of the Assignment, respecting the purposes authorized by the Data Subject.

c. Process the queries and claims made by the Data Subjects under the terms set forth in this Policy.

10.2 Regarding the quality, security and confidentiality of the Personal Data.

a) Preserve the integrity and accuracy of the Personal Data under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

b) Update, rectify or delete the data in a timely manner.

c) Update the information within five (5) business days from the date of receipt thereof.

d) Refrain from circulating information that is being disputed by the Data Subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.

e) Allow access to the information only to the persons authorized by the Data Subject or empowered by law for such purpose.

10.3 Regarding the Superintendence of Industry and Commerce

a. Inform the Superintendence of Industry and Commerce when there are violations to the security codes and there are risks in the administration of the Data Subject's information

b. Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

11. Authorization

Those obliged to comply with this Policy shall obtain from the Data Subject his/her prior, express and informed Authorization to process his/her Personal Data. This obligation is not necessary in the case of Public Personal Data.

The Authorization of the Data Subject must be obtained through any means that may be subject to subsequent consultation, such as the website, invoices or serialized coupons, forms, formats,

activities in social media, Petition, Claim Complaint formats, data messages or Apps, emails, text messages, dispatch guides, among others.

The Authorization may also be obtained from unequivocal conduct of the Personal Data Subject that allows to reasonably conclude that he/she gave his/her consent for the Processing. Such conduct(s) must be very clear so as not to admit any doubt or mistake about the will to authorize the Processing.

In the case of the collection of Sensitive Personal Data, the Authorization must be explicit as to the fact that the data to be processed are of such quality as well as the purposes. In this case, the Data Subject is not obliged to authorize the Processing of such information.

12. Cookies

The Companies may use cookies or similar technologies for the collection of Personal Data.

The Companies may use their own- or third-party cookies to (i) improve their services and their operation, as well as to optimize the experience of their users; (ii) prepare statistical information; and, (iii) personalize the content offered to their users based on an analysis of their browsing habits.

12.1. What are cookies?

Cookies are files that are stored in the terminal or device of the user browsing the Internet and that, in particular, contain a number that allows the user's device to be identified, even if the user's location or IP address changes.

Cookies are installed while browsing the Internet, either by the websites visited by the user or by third parties with which the website is related, and allow the latter to know their activity on the same site or others with which it is related. For example: the place from which you access, the time of connection, the device from which you access (fixed or mobile), the operating system and browser used, the most visited pages, the number of clicks made and data regarding the user's behavior on the Internet.

The Companies' websites are accessible without the need for cookies to be enabled. However, their deactivation may prevent them from functioning correctly.

12.2. What may cookies be used for?

Necessary and essential cookies will be used to ensure the use of the website and mobile applications in order to allow the user to navigate freely, use secure areas and personalized options.

In addition, cookies will be used to collect data relating to the analysis of the use of the website. These are used to help improve customer service, measuring the use and performance of the site in order to optimize and customize it.

The Companies' websites may also have links to social media (such as Facebook or Twitter). The Companies do not control the cookies used by these external websites. For more information about

cookies from social media or other third-party websites, you are advised to review the respective cookie policies.

12.3. What types of cookies may be used and how may they be used?

a. Session cookies: Session cookies are those that last the time the user is browsing the website and are deleted at the end of navigation. They are used to store information for the provision of the service requested by the user on a single occasion.

b. Persistent cookies: These cookies remain stored in the user's terminal for a longer time, thus facilitating the control of the chosen preferences without having to repeat certain parameters each time the website is visited.

c. First-party cookies: These cookies are created for the website and can only be read by the website itself. On the Companies' website, persistent cookies are installed for the following purposes:

- **Technical:** These cookies are used to control the loading of the images that appear in the home page, depending on the parameters that have been programmed (time, number of times viewed, etc.). They also serve to allow access to certain parts of the website and to locate the user.

- **Personalization:** These cookies allow the user to access the service with some predefined general characteristics, depending on a series of criteria in the user's terminal (for example, the language, the type of browser through which he/she accesses the service, the regional configuration from where he/she accesses the service, etc.).

- **Analytics:** These cookies allow tracking of incoming traffic to the website and analysis of user behavior on the site. These cookies generate an anonymous user identifier (id) that is used to measure how many times a user visits the site. They also record when you first and last visited the site, when a session has ended and your navigation. This allows improvements to be made to the website based on analysis of user usage data.

c. **Third-party cookies:** These are cookies created by third parties. These cookies consist of:

- **Social media cookies:** The Companies may use cookies from Facebook, Twitter, LinkedIn, among other social media, so that the user can share content from the website or mobile application on those social media; or, to facilitate registration on the sites, so that with the data that users have provided to social media can directly complete the fields of the registration form.

- **Advertising cookies:** The Companies use cookies stored by third parties that manage the spaces that display advertising of the Companies and to which users have access. These cookies make it possible to measure the effectiveness of online campaigns, provide information of interest and offer advertising content of the user's preference. Through the cookie policies of these third parties more information can be obtained about how they work and how they are used.

By accepting the use of cookies, the user allows to improve the Companies' websites, to offer an optimal access and to provide a more efficient and personalized service.

In any case, the user can disable the use of cookies when he/she considers it appropriate through the configuration/adjustment options of the browser. Cookies can be blocked, restricted or disabled. However, in the event that the user decides to change the configuration of cookies, the service provided through the different websites could be partially or totally affected.

13. National or International Transfers of Personal Data

The Companies may transfer data to other Controllers when authorized by the Data Subject, by law or by administrative or judicial order.

14. National or International Transmissions of Personal Data

The Companies may transfer Personal Data to one or more of the Companies or to third parties located within or outside the territory of the Republic of Colombia in the following cases: (i) When authorized by the Data Subject; or (ii) When without the Authorization of the Data Subject, there is a Data Transfer Agreement or the document that takes its place between the Controller and the Processor.

15. Procedure for Data Subjects to exercise their rights

For the full and effective exercise of the rights granted to the Personal Data Subjects, or to the persons legitimized by law for such purpose, the Subject may contact the Companies through each of the e-mail addresses indicated in the Table of numeral 1 of this Policy. Through this means, all queries, complaints and/or claims associated with the right of Habeas Data may be submitted with respect to each Company. Requests shall state the date of receipt of the consultation and the identity of the applicant.

The claim must be addressed to the Company(ies) and contain at least the following information:

1. Name and identification of the Data Subject or the legitimated person.

2. Precise and complete description of the facts that give rise to the consultation, complaint and/or claim.

3. Physical or electronic address to send the response and report on the status of the process.

4. Documents and other relevant evidence that you want to assert.

Once the request is received by the Company, it shall proceed with the verification of the identity of the applicant or the legitimacy of the applicant for such purpose. The answer to the consultation shall be communicated to the applicant within a maximum term of ten (10) business days from the date of receipt thereof. When it is not possible to answer the consultation within such term, the Company

shall inform the interested party the reasons for the delay and the date on which the consultation will be answered, which in no case may exceed five (5) business days following the expiration of the first term.

If the consultation, complaint or claim is incomplete, the Company shall require the interested party within five (5) business days following its receipt to correct the faults. After two (2) months from the date of the requirement, without the applicant submitting the required information, it shall be understood that the inquiry, complaint and/or claim has been withdrawn.

The maximum term to address the claim shall be fifteen (15) business days from the day following the date of receipt. When it is not possible to address the claim within such term, the interested party shall be informed of the reasons for the delay and the date on which the claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

16. Person or area responsible for the protection of Personal Data

The Personal Data Protection Officer is the person in charge of the data protection function, who can be contacted through the channels indicated in the Table of numeral 1, column Channels to exercise the Rights of this Policy.

17. Procedure for the processing of children and adolescents' data

When dealing with the Processing of Personal Data of children and adolescents, the following requirements must be met: i) That the best interests of the children and adolescents are met and respected. ii) That respect for their fundamental rights is ensured. iii) That the authorization is granted by persons who are authorized to represent the children and adolescents. The representative of the children and adolescents shall guarantee them the right to be heard and to value their opinion of the Processing, taking into account the maturity, autonomy and capacity of the children and adolescents to understand the matter. iv) It shall be informed that it is optional to answer questions about the children and adolescents' data.

18. Video surveillance

The Companies may use video surveillance means installed in different internal and external sites of their retail establishments, facilities or offices. For this reason, they inform the general public about the existence of these mechanisms by posting video surveillance notices in visible places.

The information collected through these mechanisms is used for security purposes, the improvement of services and the experience of the visitors of each Company, also, as evidence in any type of process before any type of authority or organization.

The Companies will not disclose video recordings obtained to any third party, except by court order or competent authority or as permitted by law.

19.Information Security Policies

The Companies shall adopt the necessary technical, administrative and human measures to ensure the security of the Personal Data to which it processes, protecting the confidentiality, integrity, use, unauthorized and/or fraudulent access to them. To this end, they have implemented security protocols of mandatory compliance for all personnel who have access to Personal Data and / or information systems.

The internal security policies under which the information of the Data Subject is kept in order to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access are included in the internal policies of each Company.

The Processing of Personal Data shall be from the time the Authorization is obtained by a Company and until it is dissolved and/or liquidated or, until the purpose for which the Personal Data was collected is terminated, or when so required for compliance with a legal or contractual obligation, unless the Data Subject requests the deletion or revocation of the Authorization.

20. Adjustments to the Personal Data Processing Policy

This Personal Data Processing Policy is effective as of March 10, 2022. In order to maintain the validity of the Policy, each of the Companies may adjust and modify it, indicating the date of the update on the web page or through the use of other means such as data messages, physical materials at the points of sale, etc.

EDITION	EFFECTIVE DATE	DESCRIPTION
1.0	07/27/2013	Initial Version
2.0	12/15/2018	Second Version
3.0	03/10/2022	Third Version