PERSONAL DATA PROCESSING POLICY

SUBPROCESS
PRIVACY GOVERNANCE

Approvals	
Process Owner: Luz Patricia Chitiva Lozano	**Process Owner:** Helber Alonso Melo Hernández
Title: Cybersecurity, Information Security, Privacy and Continuity Manager	**Title:** Risk Vice President

Policies, Definitions or Guidelines "New Architecture" V6

TABLE OF CONTENTS

PERSONAL DATA PROCESSING POLICY

1. INTRODUCTION

BANCO POPULAR (hereinafter, "**THE BANK**"), in compliance with the provisions of Law 1581 of 2012, and in accordance with Article 2.2.2.25.3.1 of Decree 1074 of 2015 (Single Regulatory Decree of the Commerce, Industry and Tourism Sector), adopts this Personal Data Processing Policy (hereinafter, "**THE POLICY**").

The purpose of this **POLICY** is to inform Data Subjects (hereinafter, "**THE DATA SUBJECT**") about the guidelines, principles, and procedures that govern the processing of personal information carried out by **THE BANK** in its capacity as Data Controller, as well as the mechanisms established for the exercise of the fundamental right of habeas data.

Likewise, this document establishes the purposes of data processing, the security measures implemented for the protection of personal information, and other relevant aspects to ensure appropriate processing in accordance with applicable personal data protection regulations.

2. SCOPE

This **POLICY** applies to personal information contained in databases and/or files that include personal data and that, in accordance with applicable regulations, are subject to processing by **THE BANK** in its capacity as Data Controller.

3. RECIPIENTS

This policy is addressed to our clients, users, employees, suppliers, shareholders, and partners, who are our stakeholder groups on whom THE BANK carries out the processing of personal information.

4. IDENTIFICATION OF THE DATA CONTROLLER

THE BANK, as Data Controller of the data contained in its databases, provides its contact and location information as follows, in accordance with paragraph 1 of Article 2.2.2.25.3.1 of Decree 1074 of 2015:

- Corporate Name: BANCO POPULAR S.A.
- Tax Identification Number (NIT): 860.007.738–9
- Registered Address: Calle 17 No. 07–43, Bogotá D.C., Colombia
- Phone: +57 601 756 0000
- Website: www.bancopopular.com.co

5. APPLICATION AND REGULATORY FRAMEWORK

The main current regulations in Colombia on personal data protection are listed below. THE BANK is fully committed to compliance with these provisions, which have been considered for the development of this Policy and the Comprehensive Personal Data Protection Program:

- Article 15 of the Political Constitution of Colombia.
- Statutory Law 1266 of 2008, *"Which sets forth general provisions of habeas data and regulates the management of information contained in personal data databases, particularly financial, credit, commercial, and service information, as well as information from third countries, and issues other provisions."*
- Statutory Law 1581 of 2012, *"Which establishes general provisions for the protection of personal data."*
- Law 2300 of 2023, *"Which establishes measures to protect consumers' right to privacy."*
- Single Regulatory Decree 1074 of 2015, "*By which the Single Regulatory Decree of the Commerce, Industry and Tourism Sector is issued" (which consolidated and repealed Decree 1377 of 2013 "regulating Law 1581 of 2012 in part" and Decree 886 of 2014 "*regulating Article 25 of Law 1581 of 2012 regarding the National Database Registry").
- Constitutional Court Judgment C-748 of 2011, Reporting Justice (MP) Jorge Pretelt Chaljub.
- Chapter Three of Title V of the Superintendence of Industry and Commerce (SIC) External Circular "*PERSONAL DATA PROTECTION*".

THE BANK, as a financial institution, in addition to ensuring that the personal data it manages is processed in accordance with Statutory Law 1581 of 2012 and other regulations that supplement, regulate, or amend it, is also required to comply with the provisions applicable to its **CLIENTS** under the financial activity it performs, as well as those issued by the **Financial Superintendence of Colombia** (hereinafter "**SFC**").

In this regard, it declares that its **CLIENTS**' financial information is subject to banking confidentiality obligations. For this purpose, reference is made to the following regulations:

- Law 1328 of 2009, Article 7, literal i. *"Duty to maintain confidentiality of information provided by the financial consumer that is considered confidential under applicable regulations, without prejudice to its disclosure to competent authorities."*
- Basic Legal Circular of the SFC, Part I, Title IV, Chapter I – Special Obligations: *"(...) supervised entities [by the SFC] must protect the confidential information of their clients, adopting procedures and control mechanisms that must be incorporated into their corporate governance code or ethics code, in order to prevent the leakage of such information."*

6. DEFINITIONS

In accordance with the applicable legislation on the matter and with the purpose of ensuring that the recipients of this document have clarity regarding the terms used, the following definitions are established:

Authorization: Prior, express, and informed consent of **THE DATA SUBJECT** to carry out the Processing of personal data.

Area Responsible for Data Protection: The area within **THE BANK** whose function is the supervision and control of the implementation of the Personal Data Protection Policy and the execution of the Comprehensive Personal Data Protection Program. This area is led by the Cybersecurity, Information Security, Privacy and Business Continuity Management.

Area responsible for handling petitions, complaints, claims, and inquiries: Petitions, complaints, claims, and inquiries submitted by data subjects through the different channels provided by THE BANK shall be handled by the Support and Customer Service Management for PQRs. For their proper handling, active participation is required from the business areas involved in the processing of personal data, in accordance with their role within the data life cycle.

Privacy Notice: Verbal or written communication issued by **THE BANK**, addressed to **THE DATA SUBJECT** for the Processing of their personal data, through which the existence of the applicable information processing policies is informed, as well as how to access them and the purposes of the Processing intended for personal data.

Database: Any organized set of Personal Data that is subject to Processing (manual or automated).

Personal Data: Any information linked to or that may be associated with one or more identified or identifiable natural persons (hereinafter "**Personal Data**" or "**Personal Information**"). The term "personal data" must therefore be understood as information related to a natural person (an individual considered as such).

Public Data: Data that is not semi-private, private, or sensitive. Public data includes, among others, data related to a person's marital status, profession or occupation, and their status as a merchant or public servant, data contained in public documents, and duly final judicial rulings that are not subject to legal reserve.

Private Data: Data that, by its intimate or reserved nature, is only relevant to **THE DATA SUBJECT**. Data Processor: A natural or legal person, public or private, who, alone or jointly with others, carries out the Processing of Personal Data on behalf of **THE BANK**.

Semi-private data: Semi-private data is data that is not of an intimate, reserved, or public nature, and whose knowledge or disclosure may be of interest not only to THE DATA SUBJECT but also to a certain sector or group of people or to society in general, such as financial and credit data related to commercial or service activities.

Sensitive data: Data that affects the privacy of the data subject or whose improper use may lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organizations, human rights organizations, or organizations that promote the interests of any political party or guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sexual life, and biometric data.

Data processor: A natural or legal person, public or private, who, alone or jointly with others, processes personal data on behalf of the data controller.

Authorized entities: For the purposes of this **POLICY** of **THE BANK**, this refers to the entities that make up the Aval Financial Conglomerate, listed in Resolution 0155 of 2019 issued by the Financial Superintendence of Colombia, or any other rule that modifies, supplements, or replaces it, as well as the entities that form part of the Sarmiento Angulo Business Group, listed in the Certificate of Legal Existence and Representation of **THE BANK** issued by the Bogotá Chamber of Commerce.

National Database Registry: The public directory of databases subject to processing operating in the country. The registry is administered by the Superintendence of Industry and Commerce and is freely accessible to citizens.

Data controller: A natural or legal person, public or private, who, alone or jointly with others, decides on the database and/or the processing of data. For the purposes of this document and in accordance with what has been previously referenced in different sections, **THE BANK** shall be understood as the Data Controller.

Immediate Low-Value Payment Systems (SPBVI): A set of organized policies, rules, agreements, payment instruments, entities, and technological components, such as equipment, software, and communication systems, that enable transfers or payments between accounts or deposits of financial institutions in an instantaneous manner.

Data subject: A natural person whose personal data is subject to processing.

Processing: Any operation or set of operations on personal data, including but not limited to collection, storage, use, circulation, or deletion.

Data Transfer: Data transfer occurs when the Data Controller and/or Data Processor, located in Colombia, sends information or personal data to a recipient who, in turn, acts as a Data Controller and is located within or outside the country.

Data Transmission: Processing of personal data that involves the communication thereof within or outside the territory of the Republic of Colombia when its purpose is the performance of processing by the Data Processor on behalf of the Data Controller.

7. GUIDING PRINCIPLES

THE BANK is committed to **DATA SUBJECTS** to process their personal data in accordance with the following principles:

Lawfulness in data processing: THE BANK is aware that processing activities referred to in Law 1581 of 2012 are regulated activities that must comply with the provisions established therein and in other applicable regulations that develop it.

Restricted access and circulation: Processing may only be carried out by people authorized by the **DATA SUBJECT** and/or by people provided for in the applicable regulations. Personal data, except for public information, shall not be made available by **THE BANK** on the Internet or other mass dissemination or communication media, unless access is technically controllable to ensure restricted knowledge only to the data subjects or third parties authorized under the law.

Confidentiality: All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after the termination of their relationship with any of the activities involved in the processing, and may only provide or communicate personal data when this corresponds to the development of the activities authorized under this law and under its terms.

Purpose: Processing must serve a legitimate purpose in accordance with the Constitution and the Law, which must be informed of the **DATA SUBJECT**.

Freedom: Processing may only be carried out with the prior, express, and informed consent 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 exempts consent.

Privacy by design and by default: Personal data protection must be incorporated from the outset into the design of systems, products, or processes, and ensure that, by default, only the data strictly necessary for each purpose is processed, to safeguard confidentiality and privacy throughout the entire lifecycle of personal data.

Security: Information subject to processing by the Data Controller or Data Processor referred to in this law must be handled with the technical, human, and administrative measures necessary to ensure the security of records, preventing their alteration, loss, consultation, use, or unauthorized or fraudulent access.

Temporality: The retention period of personal data shall be the time necessary to achieve the purpose for which it was collected and/or while the Data Subject has pending obligations or direct or indirect liability, for any additional time required by special regulations or by applicable statutes of limitation.

Transparency: Processing must guarantee the Data Subject's right to obtain from the Data Controller or Data Processor, at any time and without restrictions, information regarding the existence of data concerning them.

Accuracy or quality: THE BANK shall ensure that personal data collected is truthful, complete, accurate, updated, verifiable, and understandable.

8. AUTHORIZATION

The processing of personal data by **THE BANK** requires the free, prior, express, and informed consent of the **DATA SUBJECT**.

8.1 METHOD OF OBTAINING AUTHORIZATION:

In order to guarantee the rights of the **DATA SUBJECT**, **THE BANK**, in its capacity as Data Controller, may obtain authorization through the means established for this purpose, ensuring that the data subject grants prior, express, and informed consent for the processing of their personal data, preserving evidence in physical and/or digital media, and ensuring in all cases that it is possible to verify the granting of such authorization.

By virtue of its nature and corporate purpose, **THE BANK** collects, consults, receives, records, stores, preserves, modifies, reports, delivers, transmits, transfers, shares, and deletes personal information, for which it obtains prior authorization from the data subject.

It shall be understood that the **DATA SUBJECT** has granted authorization when it is expressed:

- In writing;
- Virtually;
- Orally; or
- Through unequivocal conduct of the DATA SUBJECT that reasonably allows the conclusion that authorization was granted. Such conduct must be unequivocal so that it leaves no doubt about the will to authorize processing. Under no circumstances may silence of the DATA SUBJECT be considered unequivocal conduct.

The submission of personal data attached to THE BANK's corporate emails, or the entry or uploading thereof through the platforms or applications established for such purpose, shall be deemed unequivocal conduct.

8.2 CASES IN WHICH AUTHORIZATION IS NOT REQUIRED:

Authorization from the **DATA SUBJECT** shall not be required for the processing of their personal data when it involves:

1. Provision of information required by a public or administrative authority in the exercise of its legal functions or by judicial order.
2. Cases of medical or health emergency.
3. Processing information for historical, statistical, or scientific purposes in which the information is not linked to a specific individual.
4. Data related to the Civil Registry of Persons.

9. PURPOSES AND PROCESSING OF PERSONAL DATA

All personal data processing activities must comply with the purposes mentioned in the Authorization granted by the **DATA SUBJECT**, or in the specific documents where each type or processing process of Personal Data is regulated.

The specific purpose of the processing of personal data shall be informed to the **DATA SUBJECT** at the time of obtaining their Authorization.

The following are generally listed, without limitation, the main purposes of personal data processing by **THE BANK**:

9.1 CUSTOMERS AND/OR USERS

a. To promote, commercialize, or offer, individually or jointly, its own products and/or services or those offered in commercial alliance, through channels authorized by law or contract, or to complement, optimize, or deepen the portfolio of products and/or services currently offered.
b. As an element of analysis in pre-contractual, contractual, and post-contractual stages in order to establish and/or maintain contractual relationships, including as part of this, the following purposes:
    i. Evaluate risks derived from the potential, current, or terminated contractual relationship.
    ii. Carry out, validate, authorize, or verify transactions, including, when required, the consultation and reproduction of sensitive data such as fingerprint, image, or voice.
    iii. Obtain knowledge of my commercial or transactional profile.
    iv. Become aware of the origin, modification, execution, termination, updates, payment habits, credit behavior, or compliance with direct, contingent, or indirect obligations, current, active or passive obligations, or those that I may enter into in the future, including information related to the management, status, and compliance with my payment obligations arising from relationships, contracts, and

services, payment habits, including contributions to the social security system, obligations and outstanding debts, overdue and unpaid obligations, processes, or the improper use of financial services, in databases managed directly by the contracting parties, by financial information operators, authorities or state entities, information operators and/or entities that are part of the Comprehensive Social Security System, public utility service providers and mobile telephony companies, or database administrators or similar entities that may in the future be established and that have as their purpose any of the foregoing activities.

v. To exercise its rights, including those related to judicial and extrajudicial collection activities and related procedures to obtain payment of obligations owed by the DATA SUBJECT or their employer.

vi. vi. To collect and provide information to foreign authorities with jurisdiction over THE BANK, THE AUTHORIZED ENTITIES, or their activities, products, and/or services, when required to comply with legal or regulatory duties, including those related to the prevention of tax evasion, money laundering, terrorist financing, or other similar purposes.

c. To carry out the national or international transfer of my personal data to commercial, contractual, or related partners and their third parties, which are linked to THE BANK in the development of its corporate purpose, and in order to provide me with benefits regarding the products or services acquired, contact me by telephone or by any means of communication, to inform me about responses to my inquiries, advertising, communications, services, rates, offers, among others.

   For the purposes set forth in paragraph b above, THE BANK, where applicable, may process my personal data before consultation entities that manage or administer databases for legally defined purposes, domiciled in Colombia or abroad, whether natural or legal persons, Colombian or foreign.

d. To carry out cross-selling of products and/or services offered by THE BANK or by any of THE AUTHORIZED ENTITIES or their commercial partners, including the execution of co-branding agreements.

e. To prepare and report information contained in satisfaction surveys, studies, and market analysis, for which I authorize the possibility of being contacted for such purposes.

f. To send messages through physical or digital means regarding promotions, commercial campaigns, advertising, marketing, raffles, events, or other benefits, as well as to provide information about other services and/or products offered by THE BANK, THE AUTHORIZED ENTITIES, or their commercial partners.

g. To send notifications through physical or digital means, in order to deliver account statements, institutional campaigns or financial education campaigns, and to inform about the innovations or modifications made to its products and/or services, and to make known improvements or changes in its service channels.

h. For their Personal Data to be used as evidence.

i. To incorporate, update, consult, modify, enable, share, or transfer my name, identification document, mobile phone number, email address, alphanumeric key, financial product numbers, and any other data associated with my payment methods, for the purpose of populating federated and centralized directories of immediate low-value payment systems, including the Banco de la República (Bank of the Republic), in order to carry out all processes related to the operation of Immediate Low-Value Payment Systems (SPBVI).

j. To comply with legal obligations, especially the regulations issued by the Superintendencia Financiera de Colombia (Financial Superintendence of Colombia).

Your Personal Data may be consulted, circulated, transmitted, and/or transferred to all areas of THE BANK, as well as to service providers, public entities or entities providing public services such as notaries, the National Civil Registry (Registraduría Nacional del Estado Civil), the Comptroller General's Office, the Inspector General's Office (Procuraduría), DIAN (National Tax and Customs Directorate), registry offices, compensation funds, pension and severance fund administrators, information operators through which severance payments, social security contributions, and parafiscal contributions are settled (such as Aportes en Línea, SOI, SIMPLE), network users, distribution networks, and persons who carry out the promotion of its products and services, including call centers, located in Colombia or abroad, whether natural or legal persons, Colombian or foreign, to its commercial force, telemarketing teams and/or data processors working on behalf of THE BANK, including contractors, delegates, outsourcing providers, third-party service providers, branch networks or partners, for the purpose of providing system hosting services, maintenance services, analysis services, email or physical mail messaging services, delivery services, payment and collection transaction management services, software implementation or technological services (hereinafter the "Third Parties"), who are obliged to guarantee the confidentiality of the information in accordance with Law 1581 of 2012.
Suppliers (Natural Persons):

THE BANK, in the development of its corporate purpose, is authorized to enter contracts of various nature with suppliers that ensure the supply or delivery of goods, services, civil works, among others. Accordingly, when suppliers are natural people, they will use the personal data provided by them for the following purposes:

a. To serve as support for structuring possible commercial and/or service relationships with such entities.
b. To carry out due diligence processes, verification of commercial and reputational background, and potential risks of relationship associated with money laundering and terrorist financing, and to exercise the right to sufficiently know the supplier.

c. To assess the present or future risk of the contractual relationship, as well as to administer, manage, and monitor the contractual relationship.
d. To comply with operational, legal, and/or security processes, such as registration in supplier systems, updates, and evaluation visits.
e. The information may also be used for statistical purposes.

9.2 CANDIDATES FOR EMPLOYMENT AT THE BANK

THE BANK requires, for the development of its corporate purpose, the hiring of personnel to perform the various activities carried out by the organization. In view of this, **THE BANK** receives résumés, conducts psychotechnical tests, or other necessary assessments to ensure the recruitment of the best talent.

Therefore, the personal data contained in documents shall be processed for the following purposes:

a. Direct contact between the **DATA SUBJECT** (job applicant) and **THE BANK**.
b. To evaluate suitability in accordance with the characteristics of the position to be filled.
c. Verification of the information contained in the résumé, either directly or through the recruitment company contracted by THE BANK, which is also subject to personal data protection policies.
d. Conducting selection tests, interviews, home visits, medical entrance examinations, and security background checks, either directly or through the recruitment company contracted by THE BANK.
e. Sending institutional information from THE BANK.
f. Sending text messages (SMS) and email communications.
g. Retaining personal data for future recruitment processes.

9.3 EMPLOYEES OF THE BANK:

Accordingly, when **THE BANK** hires individuals as employees, it shall process their personal data for the following purposes:

a. To carry out the activities required by THE BANK, or by any party designated by it for such purposes, related to personnel administration, human resources activities, social welfare, implementation of programs and workshops, training, and Occupational Health and Safety (OHS).
b. To share and provide my personal information to suppliers contracted by THE BANK to support the activities carried out, so that they may send information, contact me if necessary through any enabled communication channel, and perform any action required for the proper functioning and improvement of the activities proposed by THE BANK.
c. To send me satisfaction surveys or any other type of surveys that allow the measurement of my perception regarding quality-of-life programs, culture, public health emergencies

or any other serious or sudden situation that may arise, work environment and organizational climate, among other topics.

d. To enroll me and my immediate family group in applicable activities referred to in section (a), whether in person or virtually.
e. To provide details and/or recognitions through any means.
f. To contact me through the different available communication channels to receive information about institutional celebrations, outplacement programs or employees close to retirement, and any type of communications or campaigns led by THE BANK's Human Resources areas.
g. To consult my financial and commercial information with financial information operators, credit bureaus, and/or databases.
h. To carry out all necessary actions to complete the recruitment processes in which I participate and, in turn, to complete all related stages.
i. To design and implement, either virtually and/or in person, programs, courses, workshops, and other activities that promote my personal and professional development.
j. To use my image in photographs and audiovisual productions or corporate videos disclosed on social networks such as Twitter® (now X Corp), Instagram®, YouTube®, Facebook®, TikTok®, LinkedIn® or others known or to be known, the institutional website of **THE BANK**, and even for publication in printed and/or advertising media, assigning any rights over the documents and images obtained for such purposes.
k. To consult and request information related to my health status and medical history, directly or before competent health and sanitary authorities, and to keep a record thereof, the data of which, being classified as sensitive, shall be managed by the Occupational Health and Safety Department or whoever acts in its place, as applicable.

9.4 SHAREHOLDERS

The information and personal data of shareholders, including personal and contact information, as well as information and documentation provided through virtual channels, telephone channels, email, and information updates, shall be collected, consulted, updated, modified, and processed directly by **THE BANK** and/or by third parties designated by it, for the following purposes:

a. To comply with the obligations and rights derived from their status as Issuer and Depository, respectively.
b. To carry out the comprehensive administration activities of the shareholders' registry book.
c. To provide information related to procedures, complaints, and requests from shareholders.
d. To grant access to information to judicial or administrative authorities that request such data in the exercise of their functions.
e. To manage the risk of Money Laundering and Terrorist Financing and corruption.
f. To comply with the activities and purposes necessary for the issuer–shareholder relationship.

9.5 ACCESS CONTROL AND VIDEO SURVEILLANCE

THE BANK, for visitors, video surveillance recordings, and security of its facilities, may process personal data for the following purposes:

a. To identify and maintain control over persons entering the facilities in order to ensure both their safety and that of users.
b. To carry out statistical processing for the control of people flow and thus provide better service.
c. Entry, stay, and exit registration of the facilities.
d. Administrative procedures.

9.6 PROCESSING OF DATA IN ARTIFICIAL INTELLIGENCE SYSTEMS

THE BANK may use artificial intelligence tools in the processing of personal data. The use of artificial intelligence tools shall be subject to corporate principles and the principles set forth in this **POLICY**, highlighting the principles of privacy by design and by default, security, and demonstrated accountability in the design, use, and management of these tools.

The use of Artificial Intelligence tools for the handling of personal data shall be carried out in accordance with the authorization granted by the **DATA SUBJECT**. For these purposes, in accordance with External Circular 002 of 2024 of the Superintendencia de Industria y Comercio (SIC), the processing of personal data in artificial intelligence systems shall be subject to the following guidelines:

- Weighing of the principles of the Personal Data Protection Regime (Statutory Law 1581 of 2012).
- Preventive approach.
- Risk identification and mitigation.
- Data accuracy and currency.
- Security.
- Restricted access and circulation.

9.7 SPECIAL CATEGORIES

9.7.1 SENSITIVE DATA

Sensitive personal data are those that affect the privacy of the **DATA SUBJECT** or whose improper use may lead to discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, the membership in trade unions, social or human rights organizations, or organizations that promote the interests of any political party or that guarantee the rights and protections of opposition political parties, as well as data relating to health, sexual life, and biometric data.

Additionally, sensitive data includes, among others, data collected and processed through psychotechnical tests, home visits, and security background checks, which are intended to determine the level of alignment between the profile and competencies of the candidate for a vacancy. It also includes images and recordings obtained through different means, whose purpose is to provide security for people, assets, and facilities, and to monitor activities inherent to the financial sector, which may be used as evidence in any type of proceeding before any authority.

In accordance with Article 6 of Statutory Law 1581 of 2012 and its regulatory provisions, the processing of sensitive data is prohibited and shall only proceed when the following requirements are met:

1. The Data Subject has given explicit authorization for such processing, except in cases where, by law, such authorization is not required.
2. The processing is necessary to safeguard the vital interest of the Data Subject and the Data Subject is physically or legally incapacitated. In such cases, legal representatives must grant authorization.
3. The processing relates to data necessary for the recognition, exercise, or defense of a right in a judicial proceeding.
4. The processing has a historical, statistical, or scientific purpose. In this case, measures must be adopted to remove the identity of the Data Subjects.

If **THE BANK** requires the collection of Sensitive Data and the performance of any processing activity on such data, it shall inform the **DATA SUBJECT** or their legal representative or guardian and shall obtain prior authorization, as well as inform the Data Subject of their right not to provide such data.

THE BANK shall process sensitive data for various purposes; the following are provided by way of example:

a. To update databases and process the opening and/or linking of products and/or services at **THE BANK**.
b. To store them in a database for verification and authentication at the cashier level and on the platform used, and in general to access special services within **THE BANK's** branches.
c. To validate identity in the use of products and/or services.
d. So that identity verification through biometric data may be used as evidence.
e. To allow identity verification through a certified biometric operator or directly, by validating identity against the database produced and managed by the National Civil Registry Office (Registraduría Nacional del Estado Civil – "RNEC").
f. To preserve the safety of individuals who visit THE BANK's facilities.

THE BANK shall not condition access to its products or services on the failure to provide this authorization, unless such data is necessary for the establishment and/or proper maintenance of the relationship or for compliance with obligations borne by THE BANK and/or the Data Subject.

9.7.2 PROCESSING OF PERSONAL DATA OF CHILDREN AND ADOLESCENTS

The processing of personal data of children and adolescents is prohibited, except when it concerns data of public nature, and when such processing complies with the following parameters and/or requirements:

a. That it responds to and respects the best interests of children and adolescents.
b. That the fundamental rights of children and adolescents are ensured.

Once the above requirements are met, the legal representative of the child or adolescent shall grant authorization, after the minor has exercised their right to be heard, whose opinion shall be assessed considering their maturity, autonomy, and capacity to understand the matter.

10. TRANSFER AND TRANSMISSION OF PERSONAL DATA

THE BANK may transfer (as Data Controller to another Data Controller) and transmit personal data to third parties (as Data Controller to third parties acting as Data Processors) with whom it maintains an operational relationship that provides services necessary for its proper operation or in accordance with the functions assigned under applicable regulations.

THE BANK, in its capacity as Data Controller of the personal data stored in its databases and in accordance with the purposes established in this POLICY, may carry out the transmission and/or transfer of such information, considering the conditions set forth in applicable regulations and under the following terms:

- The transmission and/or transfer must be carried out for a legitimate purpose.
- Prior, express, and informed authorization of the Data Subject must be obtained.
- Personal data to be transmitted or transferred must be relevant, necessary, and not excessive in relation to the purpose for which it is being transmitted or transferred.
- When there is an administrative or judicial order requiring it.
- When there is an agreement that regulates in detail the obligations and duties regarding the exchange of information, or, where applicable, data protection clauses within broader contracts, as well as confidentiality and information security clauses in comprehensive agreements.

In such cases, the necessary measures shall be adopted to ensure that persons who have access to your personal data comply with this Policy and with the principles of personal data protection and the obligations established by law.

In the event that data is sent, transferred, or transmitted to another country, the authorization of the **DATA SUBJECT** whose information is being transferred or transmitted must always be obtained. Unless otherwise provided by law, such authorization is a necessary requirement for the international circulation of data. In this regard, prior to sending personal data to another country, THE BANK must verify that it has the prior, express, and unequivocal authorization of the DATA SUBJECT allowing the transfer or transmission of their personal data.

11. TEMPORALITY OF PERSONAL DATA PROCESSING

Personal data shall be subject to processing by THE BANK for the duration of the contractual term during which the data subject maintains the product, service, contract, or relationship, plus the period established by law.

12. RIGHTS OF THE DATA SUBJECT

In the processing of personal data, **THE BANK** shall recognize in favor of the **DATA SUBJECT** the following rights, in accordance with the legal terms established by Law 1581 of 2012 and its regulatory decrees:

1. To access free of charge the data provided that have been subject to processing.
2. To know, update, and correct their personal information free of charge.
3. To request proof of the authorization granted to THE BANK.
4. To be informed by THE BANK, upon request, regarding the use that has been made of their personal information.
5. To revoke authorization and request deletion of the data when it is not used in accordance with the authorized purposes and uses; revocation and/or deletion shall proceed when the Superintendence of Industry and Commerce (SIC) has determined that THE BANK has engaged in conduct contrary to the law and the Constitution in the processing. Revocation shall proceed provided that there is no legal or contractual obligation to retain the personal data.
6. To submit inquiries and complaints regarding personal information.
7. File complaints before the SIC, as the competent authority, for violations of the provisions set forth in the law and other regulations that amend, replace, or supplement it. For this right, in all cases, the Data Subject must have previously exhausted the consultation or claim procedure before THE BANK, in accordance with Article 16 of Statutory Law 1581 of 2012.

12.1 PEOPLE TO WHOM INFORMATION MAY BE DISCLOSED

The exercise of the rights and those established by law may be exercised by the following people, in accordance with Article 13 of Statutory Law 1581 of 2012 and Article 2.2.2.25.4.1 of the Single Regulatory Decree 1074 of 2015:

a. By the Data Subject, who must sufficiently prove their identity through the different means made available by the Data Controller.
b. By their successors in title, who must prove such status.
c. By the representative and/or attorney-in-fact of the Data Subject, upon prior proof of representation or authorization.

d. By stipulation in favor of another or for another.
e. The rights of children, girls, and adolescents shall be exercised by the people who are legally authorized to represent them.

13 DUTIES OF THE BANK

13.1 When THE BANK acts as Data Controller

Without prejudice to the provisions contained in the law, the duties of **THE BANK** as Data Controller are the following:

1. To guarantee THE DATA SUBJECT the full and effective exercise of the right to personal data protection;
2. To request and/or retain the corresponding authorization granted by THE DATA SUBJECT;
3. To properly inform THE DATA SUBJECT about the purpose of the collection and the rights that arise by virtue of the authorization granted;
4. To store the information under the necessary security conditions to prevent its alteration, loss, consultation, use, or unauthorized or fraudulent access;
5. To ensure that the information being processed is truthful, complete, accurate, updated, verifiable, and understandable. To rectify it if applicable;
6. To require the Data Processor at all times to respect the security and privacy conditions of THE DATA SUBJECT's information;
7. To process the consultations and claims submitted under the terms set forth in this law;
8. To inform the Data Processor when certain information is under dispute by THE DATA SUBJECT, once a claim has been filed and the respective procedure has not yet been completed;
9. To inform, upon request of THE DATA SUBJECT, about the use given to their data;
10. To inform the data protection authority when security code breaches occur and when there are risks in the administration of THE DATA SUBJECT's information.

13.2 When THE BANK acts as Data Processor

Without prejudice to the provisions of the law, the duties of THE BANK as Data Processor are as follows:

1. To guarantee to THE DATA SUBJECT, at all times, the full and effective exercise of the right to personal data protection;
2. To store the information under the necessary security conditions to prevent its alteration, loss, consultation, use, or unauthorized or fraudulent access;
3. To promptly carry out the updating, correction, or deletion of data under the terms of this law;
4. To update the information reported by the Data Controllers within five (5) business days counted from its receipt;

5. To process consultations and claims submitted by THE DATA SUBJECT under the terms established in this law;
6. To record in the database the label “claim in process” in the manner regulated in this law;
7. To insert in the database the label “information under judicial dispute” once notified by the competent authority about judicial proceedings related to the quality of the personal data;
8. To 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;
9. To allow access to the information only to people who are authorized to access it;
10. To verify the existence of the authorization and its scope.

13.3 National Database Registry (RNBD)

THE BANK must register its databases together with this **POLICY** in the National Database Registry administered by the Superintendence of Industry and Commerce, in accordance with the applicable regulations.

14. PROCEDURE FOR ADDRESSING DATA SUBJECT RIGHTS

The area responsible for handling consultations, claims, and in general any request from the Data Subject regarding the processing of their personal data, within the framework of Statutory Law 1581 of 2012 and its regulatory decrees, is the Customer Support and PQRs Service Management of **THE BANK**. In these cases, the corresponding areas of **THE BANK** may participate depending on the request.

To process the request, the Data Subject must prove their identity according to **THE BANK’s** procedures; if the inquiry or claim is not submitted by the Data Subject, a document proving the status of representative, successor in title, or attorney-in-fact must be attached.

For the filing and handling of inquiries and/or claims, the Data Subject must provide the following information:

- **Inquiry: THE BANK** guarantees the right of inquiry by providing people exercising this right with all information contained in their individual record or linked to the identification of the **DATA SUBJECT**. The **DATA SUBJECT** must provide the following information:

    - First and last name of THE DATA SUBJECT and their representatives, if applicable.
    - Type and identification number.
    - Description of the inquiry.
    - Supporting documents for the request, if applicable.
    - Contact details (physical address and/or email address and telephone numbers).
    - Notification channel or address to receive the response to the request.
    - Signature, identification number, and fingerprint (branches).
    - The request must be submitted through the channels enabled by THE BANK.

- **Claim:** When the **DATA SUBJECT** or their successors in title consider that their information must be corrected, updated, deleted, authorization revoked, or when they notice a possible non-compliance by **THE BANK** with its duties regarding Personal Data Protection as set forth in applicable law and in this **POLICY**, the **DATA SUBJECT** must provide the following information:

  - First and last name of the **DATA SUBJECT** and their representatives, if applicable.
  - Type and identification number.
  - Reason(s)/fact(s) giving rise to the claim, with a brief description of the right they wish to exercise (know, update, rectify, request proof of authorization, revoke it, delete, access information).
  - Contact details (physical address and/or email address and telephone numbers).
  - Notification channel or address to receive the response to the claim.
  - Signature, identification number, and fingerprint (branches).
  - The request must be submitted through the channels enabled by THE BANK.

In any case, the request for deletion of information and the revocation of authorization shall not proceed when the Data Subject has a legal or contractual duty to remain in the database.

14.1 Timeframes for responding to Habeas Data rights

- **Processing of Inquiries**: If it is an inquiry submitted by the **DATA SUBJECT** regarding data contained in **THE BANK's** database, its legitimacy will be verified and the inquiry will be addressed within a period not exceeding **ten (10) business days** counted from the day following its receipt.

  If it is not possible to resolve the inquiry within this timeframe, the **DATA SUBJECT** shall be informed of this situation using the email address or notification address provided in the respective inquiry. In any case, the response period may be extended by up to **five (5) additional business days** counted from the expiration of the initial term.

- **Processing of Claims: THE BANK** shall resolve the claim within a maximum term of **fifteen (15) business days** counted from the day following its receipt.

  If it is not possible to resolve the claim within this term, the **DATA SUBJECT** shall be informed of the delay, indicating the reasons and the expected response date, using the email address or notification address provided in the respective claim. In any case, the response term shall not exceed **eight (8) business days** following the expiration of the initial term.

  If the claim is incomplete, **THE BANK** shall request the **DATA SUBJECT** within **five (5) business days** following receipt of the request to complete and correct it. If **two (2)**

months elapses from the date of the request without a response from THE DATA SUBJECT, the request shall be deemed withdrawn.

If the recipient of the claim is not determined to resolve it, it shall be forwarded to the competent authority within a maximum of **two (2) business days** and the **DATA SUBJECT** shall be informed of this fact.

If the claim is received in a complete form or is later completed, a "note" must be included in the database within **two (2) business days** stating: "***CLAIM UNDER PROCESS***".

Once the terms established by Statutory Law 1581 of 2012 and other regulations that supplement or amend it have been fulfilled, if the exercise of rights of access, updating, or rectification is denied, in whole or in part, the Data Subject may bring the case to the attention of the Superintendence of Industry and Commerce – Data Protection Delegation when the request for deletion or revocation is denied.

14.2 Special rules for the exercise of Data Subject rights

Requests for rectification, updating, or deletion must be submitted through the channels enabled by **THE BANK** as set forth in this **POLICY**, subject to prior validation and authentication of the **DATA SUBJECT's** identity according to **THE BANK's** procedures, and must contain, at a minimum, the required information.

Regarding deletion of data, the **DATA SUBJECT** has the right to request **THE BANK** to delete (remove) their personal data when it is appropriate, or when it is no longer necessary or relevant for the purpose for which it was collected, or when the period required for fulfilling such purposes has been exceeded.

- The deletion of data shall not proceed when:
  - The **DATA SUBJECT** has a legal or contractual duty to remain in the database.
  - The deletion of data would hinder judicial or administrative actions related to tax obligations, investigation and prosecution of crimes, or enforcement of administrative sanctions.
  - The data is necessary to protect the legally protected interests of THE DATA SUBJECT; to carry out an action in the public interest; or to comply with a legally acquired obligation by THE DATA SUBJECT.

14.3 Guideline regarding data deletion

When the Data Subject requests the deletion of their personal data, it shall apply only to the <u>active processing</u> of such data, but it shall not necessarily imply its total deletion, especially if it must be retained as part of historical records required by law.

It must be considered that, in some cases, certain information must be retained in **THE BANK's** records as part of compliance with legal obligations.

14.4 Channels

THE BANK provides its **DATA SUBJECTS** with the following channels to exercise their rights, in accordance with the provisions of the regulations:

- **National Branch Network**: which can be consulted on the website www.bancopopular.com.co
- **Green Line:**
  - Bogotá: 601 743 4646.
  - National line for the rest of the country: 01 8000 184646.
- **Contact Us – Virtual Desk**: www.bancopopular.com.co

15. SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

THE BANK has adopted all possible and necessary technical, technological, legal, human, and administrative measures for the protection of data belonging to Data Subjects, to guarantee the attributes of confidentiality, availability, integrity, and privacy of information. Therefore, **THE BANK** stores it under the necessary security conditions to prevent alteration, loss, consultation, use, or unauthorized or fraudulent access, as well as to ensure respect for THE DATA SUBJECT's rights, as established by law.

THE BANK is exempt from liability, with respect to the obligations assumed under this **POLICY**, when due to any circumstance a competent authority requests that Personal Information be disclosed for judicial or administrative proceedings related to any type of obligation, process, investigation, prosecution, or data update, matters of public interest, or submission of tax reports, among others.

This **POLICY** shall apply if the data remains in **THE BANK's** databases and is not in the public domain.

16. DATA PROTECTION OFFICER

THE BANCK, in compliance with its duty of demonstrated responsibility under Articles 2.2.2.25.6.1 and following of the Single Regulatory Decree 1074 of 2015, THE BANK has designated the Information Security, Cybersecurity, Privacy, and Business Continuity Management as the area responsible for the personal data protection function.

The role of the Information Security, Cybersecurity, Privacy, and Business Continuity Management area within the organization is to ensure the effective implementation of the policies and procedures adopted by THE BANK to comply with regulations, as well as the implementation of good personal data management practices within THE BANK.

17. RETENTION PERIOD OF DATABASES

The retention period of databases will depend on the purposes of the processing established in this POLICY, and on the special regulations governing the matter, and shall remain in force for as long as **THE BANK** carries out activities inherent or related to its corporate purpose.

18. POLICY VALIDITY AND UPDATES

This policy came into effect on October 10, 2015 and shall be made available to Data Subjects through the website: www.bancopopular.com.co. Any substantial change to the **POLICY** will be duly communicated to Data Subjects through the usual contact channels and/or through **THE BANK's** website: www.bancopopular.com.co and/or the Data Subjects' email addresses.

19. CHANGE LOG

Version History		
Version #	**Publication date**	**Description of change**