PO-181-0

PRIVACY POLICY

MANUAL

PRIVACY MANUAL

Approvals	
Process Owner: Jairo Francisco González Matallana	Dr. Yibran Ortegón Botello
Title: Privacy, Cybersecurity and Information Security Manager	Enterprise Risk Manager

TABLE OF CONTENTS

1. INTRODUCTION: POLICIES AND PROCEDURES MANUAL ON PERSONAL DATA PROTECTION – COMPREHENSIVE PERSONAL DATA MANAGEMENT PROGRAM (PIGDP)

The protection of citizens' personal data has been regulated under Colombian legislation through Law 1581 of 2012 and Chapter 25 of Decree 1074 of 2015 (Regulatory Decree 1377 of June 27, 2013), which regulates, develops, and complements the general standard and establishes mandatory compliance measures for entities that, in the course of their activities, process this type of personal data.

The main purpose of personal data protection regulations is to safeguard the right to honor, personal privacy, and one's own image of natural persons, assigning specific functions and obligations to all persons involved in the processing of databases where personal data is stored. The Law also establishes sanctions for entities that fail to comply with the obligations derived from the regulation, including the closure of databases, monetary fines, and even referral of the matter to judicial authorities for investigation and/or prosecution of the corresponding offense, with applicable custodial and financial penalties.

The main purpose of this document is to consolidate the set of policies, principles, measures, controls, procedures, and mechanisms that allow the Bank to guarantee the principle of privacy and the effective implementation of personal data regulations and the principle of demonstrated accountability.

This document identifies and details the roles, functions, and obligations of the Bank's employees and collaborators, including personnel hired through temporary employment agencies or the SENA, or under service provision contracts, who, in their capacity as users of the Bank's databases containing personal data of clients, employees, suppliers, shareholders, and other natural persons processed by the Bank, are required to know and comply with them.

Through this document, the Bank declares the importance of respect for and protection of personal data and considers personal data one of its most important assets. Therefore, it expresses its full commitment to the implementation, execution, monitoring, and continuous improvement of the Comprehensive Personal Data Management Program.

In accordance with the above and in line with Decree 1074 of 2015, the principle of demonstrated accountability is referred to under the following terms:

"The data controllers must be able to demonstrate, at the request of the Superintendence of Industry and Commerce, that they have implemented appropriate and effective measures to comply with the obligations established in Law 1581 of 2012 and this decree, in a manner that is proportional to the following:

1. The legal nature of the controller and, where applicable, its business size, considering whether it is a micro, small, medium, or large enterprise, in accordance with applicable regulations.

2. The nature of the personal data subject to processing.
3. The type of processing.
4. The potential risks that the aforementioned processing could cause to the rights of the data subjects."

The objective of the Comprehensive Personal Data Management Program is to ensure high standards of personal data protection and to enable Banco Popular to demonstrate to the Superintendence of Industry and Commerce its compliance with and commitment to the responsible use of personal information provided by all data subjects, as well as the proper implementation of Law 1581 of 2012 and other regulatory provisions.

1.1 PIGDP STRUCTURE

Comprehensive Personal Data Management Program

Organizational Commitment	**Program Controls**	**Continuous Evaluation and Review**	**Demonstrate Compliance**
Consists of fostering a culture of respect for personal data protection within the Bank.	Ensure compliance with the adopted policies.	Permanently ensure effectiveness through the "Demonstrated Accountability Principle".	Accredit compliance before data subjects and before the SIC.

1.2 SCOPE OF APPLICATION

This Policy shall apply to all types of processing of personal data under the responsibility of Banco Popular, including, but not limited to, databases, information systems, applications, physical media, servers, computers, and/or other mobile devices used for the processing of personal data that must be protected in accordance with current regulations. This section establishes the parameters, guidelines, and practices that Banco Popular must implement and oversee in order to demonstrate effective compliance with personal data regulations and the principle of demonstrated accountability.

1.3 OBJECTIVE

To define personal data governance through the establishment of guidelines, responsibilities, behaviors, general procedures, roles, functions, and obligations of those responsible for and users involved in the management and processing of personal data, focused on protecting the privacy of personal data belonging to clients, employees, suppliers, shareholders, and other natural persons processed by the Bank.

1.4 SCOPE

This Policy is mandatory for all Bank employees and collaborators, including personnel hired through temporary employment agencies, the SENA, or service provision contracts.

This Privacy Policy defines the basic framework that will guide the implementation of any directive, system, process, procedure, and/or action related to Personal Data Protection.

Additionally, this Policy applies to all personal data of natural persons that has been collected, created, processed, stored, or used by the Bank, regardless of the medium, format, presentation, or location in which it is found.

2. GLOSSARY

AUTHORIZATION: Prior, express, and informed consent of the Data Subject to carry out the processing of personal data. It should be noted that consent is the cornerstone of data protection, and this requires that, as a rule, data belonging to any individual cannot be processed without their consent, without prejudice to the fact that in some cases this obligation may be exempt. For example: when data is processed within the framework of a commercial, employment, or administrative relationship, or when, by legal provision, such authorization is not required.

DATABASE: An organized set of personal data subject to processing. Whenever there is a set of personal data organized according to any criteria, a database exists. For example, a payroll software application constitutes a database, but so does a data table in Word format. It should also be noted that this concept applies to non-automated data, such as a physical folder or A–Z file system.

TRANSFER (CESSION): Disclosure of data made to a person other than the data subject.

DATA COMMUNICATION: The result of any disclosure of personal data made to a person other than the data subject, during a transfer, transmission, or assignment of personal data.

PERSONAL DATA: Any information related to or that can be associated with one or more identified or identifiable natural persons. That is, any data that can be linked to a natural person or allows their identification.

INFORMATION DOMAIN: Information domains are a set of data logically grouped by business functions and constitute the basis for implementing the information governance and management model.

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 Data Controller. The data processor is a third party (usually a company, but not necessarily) that provides a service to the data

controller and, for that purpose, requires access to the controller's personal data. Examples include companies contracted by the Bank to perform collections management, call centers, courier services, hardware or software maintenance companies, etc. The relationship between the controller and the processor must be governed by a personal data processing agreement.

DOMAIN LEADER: A business leader and/or recognized subject-matter expert designated as responsible for all aspects associated with the governance and management of information for their information domain, through coordination with the various stakeholders related to the assigned domain, representing information interests for stakeholders and the Bank.

PERSONAL DATA PROTECTION OFFICER: The person or area designated by the Bank, whose main role is to ensure the effective implementation of the policies and procedures adopted by the Bank for compliance with personal data protection regulations, as well as the implementation of good personal data management practices within the organization.

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 Policy, the Data Controller is Banco Popular S.A.

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

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

Transfer occurs when the controller shares personal data with a third party so that the third-party processes it on its own behalf and for the purposes defined in the authorization granted by the Data Subject.

TRANSMISSION: Processing of personal data that involves the communication of such data within or outside the territory of the Republic of Colombia when its purpose is the processing of data by a Data Processor on behalf of the Data Controller. Transmission occurs when the party sharing the personal data limits its processing to one or more specific purposes defined by the controller within the contract and by the data subject in their authorization. This third-party acts on behalf of the controller and assumes the role of "data processor."

PROCESSING: Any operation or set of operations performed on personal data, such as collection, storage, use, circulation, or deletion.

USERS: An authorized subject or process with access to data or resources. Typically, a user is a person who accesses personal data processed by the Bank. A user may have different access profiles and may be an internal or external user (for example, a user from another organization accessing our system to provide a service, such as technical support).

3. DATA RISK LEVELS

The risk in the processing of data has been classified into three levels, according to the typology and sensitivity of the data contained in the databases: basic level, medium level, and high level.
Personal Data Classification by Sensitivity Level

Level	TYPE / DESCRIPTION
Low	**Public data.** Data classified as such under the provisions of the law or the Political Constitution, and all data that is neither semi-private nor private. Public data includes, among others, data contained in public documents, duly enforceable judicial rulings not subject to confidentiality, and data relating to a person's civil status. This definition does not imply disregard for the Bank's principles and obligations in the processing of public personal data. Examples: Name, civil status, identification number, date of birth, profession or occupation.
Medium	**Data subject to Law 1266 of 2008:** financial, credit, commercial and service-related data. Examples: Credit histories, financial data, credit bureau reports. **Semi-private data:** data that is neither intimate, confidential, nor public in 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. **Private data:** data that, due to its intimate or confidential nature, is only relevant to the data subject. Examples: Email address, contact phone number, personal address, employment and academic data.
High	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 trade unions, social or human rights organizations, or organizations that promote the interests of any political party or guarantee the rights of opposition political parties, as well as data relating to health, sexual life and biometric data. Examples: Ideological, political and religious data, sexual preferences, trade union membership, ethnic data, health data, fingerprints, photographs, videos and lifestyle information.

4 DATABASE INVENTORY

4.1 IDENTIFICATION OF PERSONAL DATABASES

Within the process of identifying, inventorying, and updating its databases, the Bank has established the following general criteria:

4.1.1 Purposes

The Bank has identified databases according to their purpose. This is understood in the sense that a central registered database may be segmented into other decentralized databases that respond to the same content and purpose but are subject to different forms of processing or may be located in repositories different from the central database.

4.1.2 Processing Method

- **Automated database**
  The Bank identifies as an automated database one that is stored and managed with the help of computer tools or automated information systems.

- **Physical (paper) database**
  The Bank identifies a physical or manual database when it contains files whose information is organized and stored in physical form.

The inventory of personal databases registered with the Superintendence of Industry and Commerce is presented according to electronic form F.1.10.4.0101 Database Updates – Substantial Changes, considering its proper completion in accordance with A-181-00101 Annex: Completion Guide for Database Update Form – Substantial Changes.

5. GOVERNANCE FOR PRIVACY MANAGEMENT

Banco Popular must structure the functions and responsibilities regarding Privacy Risk and the management of Privacy risks. This framework defines the three lines of defense scheme, considering business line management, an independent Privacy risk management function, and independent review.

First Line (Operations)

- Identify, assess, manage and mitigate privacy-related risks.
- Guide the development and implementation of internal policies and procedures to ensure that activities carried out are consistent with the requirements of Law 1581 of 2012 and its regulatory decrees, as well as internal policies and guidelines.
- Implement corrective actions to address deficiencies in their processes and controls.

Second Line (Governance)

- Establish guidelines, policies, standards, roles and responsibilities for privacy management.
- Perform continuous monitoring and follow-up on the implementation of effective risk management practices by the First Line.
- Alert the First Line of emerging issues and changes in risk scenarios.

Third Line (Control)

- Evaluate compliance with privacy-related policies, guidelines and procedures in accordance with its work plan.

6. ROLES AND RESPONSIBILITIES

To comply with the objectives of this Privacy Policy, the following specific functions and obligations have been defined within the Bank, in accordance with the provisions set forth in Annexes A-181-00102 Report Generation as Part of the PIGPD and A-181-00103 Contracting Requirements for Personal Data Processors, when applicable:

6.1 SENIOR MANAGEMENT

The Bank's senior management is responsible for ensuring the processes and procedures necessary for the operation of the Comprehensive Personal Data Protection and Demonstrated Accountability Management Program, as well as for ensuring that the processes and procedures are established, implemented, executed, maintained, and continuously improved.

The Bank shall carry out the necessary management to maintain effective data protection beyond the minimum legal obligations it may have.

6.2 INTEGRATED RISK MANAGEMENT DEPARTMENT

- Designate the person or area that will assume the role of Personal Data Protection Officer within the organization.
- Approve and monitor the Comprehensive Personal Data Management Program.
- Report to the Board of Directors on the execution of the Comprehensive Personal Data Management Program.
- Establish, together with the Personal Data Protection Officer, the specific responsibilities of other Bank areas regarding the collection, storage, use, circulation, deletion, or final disposal of the data being processed.

6.3 PERSONAL DATA PROTECTION OFFICER

Banco Popular has decided to appoint the Privacy, Cybersecurity and Information Security Manager to assume the role of Personal Data Protection Officer.

The functions assigned to the Personal Data Protection Officer, in addition to all those generally established under applicable personal data protection laws, are as follows:

- Ensure the effective implementation of the policies and procedures adopted to comply with applicable laws and regulations, as well as the implementation of good personal data management practices within the Bank.
- Establish the guidelines required to ensure proper administration and protection of the information contained in databases.
- Structure, design, and manage the program that enables the Bank to comply with personal data protection regulations, and establish program controls, evaluation, and ongoing review.
- Promote the implementation of a system that allows the management of personal data processing risks.
- Serve as liaison and coordinator with the other areas of the organization to ensure transversal implementation of the Comprehensive Personal Data Management Program.
- Promote a data protection culture within the organization.
- Register the organization's databases in the National Database Registry and update the report based on the information provided by the different responsible areas and data domain leaders, always following the instructions issued by the Superintendence of Industry and Commerce (SIC).
- Review the content of national and international data transmission agreements entered into with data processors resident and non-resident in Colombia.
- Ensure the implementation of monitoring plans to verify compliance with personal data processing policies.
- Support and assist the Bank in attending inspections and responding to requests made by the Superintendence of Industry and Commerce.
- Carry out follow-up on the Comprehensive Personal Data Management Program.
- Periodically review and update the policies to be implemented at Banco Popular for the protection of personal data, which must be approved by the Integrated Risk Management Department.
- Assess information security incidents related to personal data to establish corrective measures as required and, where deemed necessary, report them to the Superintendence of Industry and Commerce.
- Monitor compliance with the policies and guidelines established in this Privacy Policy, ensuring they are aligned with current regulations.
- Participate in the development of new processes, products, or services to verify compliance with applicable personal data protection regulations.

6.4 FUNCTIONS ASSIGNED TO THE PRIVACY, CYBERSECURITY AND INFORMATION SECURITY MANAGEMENT AREA

- Define and maintain information security policies, which are stored in the entity's electronic and physical media.

- Adopt the necessary measures to ensure that Banco Popular users are aware of the information security policies, as well as the consequences they may face in the event of non-compliance.
- Establish information security and cybersecurity controls, both at a technical and physical security level, that must be considered by third parties when personal data is stored and/or processed under outsourced services.
- Monitor that the security guidelines established for the protection of data privacy in information systems are properly implemented.
- Consolidate an inventory of personal databases held by the organization and classify them according to their type (automated or physical), to be reported to the Superintendence of Industry and Commerce.
- Recommend a training program on personal data protection for Bank employees.
- Implement best practices related to information security management.

6.5 BANK PROCESS OWNERS

- Incorporate compliance with data protection policies into the activities of the processes under their responsibility Annexes A-181-00102 Report Generation as Part of the PIGDP.
- Ensure that, within product flows through the different channels, the prior, express, and informed authorization for the processing of personal data is requested from data subjects whenever personal information is collected.
- Ensure that there is authorization for the processing of personal data from data subjects in cases where data consultation is performed and prior to data upload, when such data is obtained from external sources.
- Maintain evidence (physical and/or digital) of the authorization for the processing of personal data granted by data subjects through the different channels.
- Ensure that all information related to individual clients that must be managed is extracted from the only official source that contains customer personal data within the Bank.
- Collaborate with the Privacy, Cybersecurity and Information Security Management area in the execution of activities related to personal data processing within their areas of responsibility.
- Promote the implementation, within the Bank's processes, of all necessary personal data protection mechanisms issued by the supervisory and control authority, as well as by the Privacy, Cybersecurity and Information Security Management area.
- Request support from the Privacy, Cybersecurity and Information Security Management area from the very beginning of projects and/or requirements, or when changes occur in processes or programs involving personal data processing, so that they meet the necessary data protection requirements before going live.
- Document the report generation process as part of the Comprehensive Personal Data Management Program.
- Ensure that, prior to the implementation or modification of information systems, testing is not performed using real data, unless the appropriate level of security corresponding to the type of database being processed is guaranteed.

- Implement all measures required by personal data protection regulations in the applications and databases under their responsibility to ensure compliance with data protection regulations.
- Verify that transfers of documentation to external document management companies are carried out under appropriate security and confidentiality measures.
- Protect the Bank's information assets that contain personal data by complying with the information security and cybersecurity policy, including reporting incidents that may compromise personal information.
- Define the value and criticality of personal information that is stored, processed, or transported through information assets; and based on this, define usage privileges and establish mechanisms to ensure minimum security conditions and mitigation of associated risks.
- Ensure that any sensitive information that may be stored locally on devices is deleted or stored in folders or servers once the purpose for which it was processed on those devices has been completed.
- Request support from the Privacy, Cybersecurity and Information Security Management area when entering into contracts or service orders in which any type of personal data processing is to be carried out, such as transmissions or transfers of data-to-data processors or data controllers.
- Provide, within the timeframes established by Law 1581 of 2012, the necessary information to the Customer Service Operations Management area – PQR, when requests for the exercise of data subject rights are submitted by data subjects and must be processed and responded to. Likewise, provide appropriate support in the event of special requirements from the Superintendence of Industry and Commerce.
- Identify all third parties, suppliers, or partners acting as personal data processors, to report them to the Privacy, Cybersecurity and Information Security Management area.
- Verify that third parties have implemented security conditions and measures that ensure the privacy and confidentiality of automated and physical information related to the personal data provided by the Bank and ensure that these are included within the established contracts.
- Report to the Privacy, Cybersecurity and Information Security Management area any substantial changes or updates to databases or to the data of the processors under their responsibility, in relation to the information registered in the National Database Registry.
- Ensure that, prior to the start of activities by third-party processors, a data transmission or transfer agreement has been signed, as applicable.
- Provide recommendations to the Personal Data Protection Officer aimed at improving internal processes related to this matter within the entity.

6.6 HUMAN TALENT MANAGEMENT AND DEVELOPMENT AND HUMAN TALENT SERVICE MANAGEMENT

- Obtain from employees and candidates the relevant authorizations for the processing of their personal information before and during the employment relationship.

- Timely handle inquiries and complaints regarding personal data submitted or made by employees currently or formerly linked to the Bank.
- Establish transversal training plans for all employees and positions within Banco Popular.

- Carry out the necessary training for new employees who, due to the conditions of their position and functions, have access to personal data managed by the Bank.
- Measure participation and evaluate performance in data protection training programs.
- Promote training for the Bank's employees and third parties regarding the importance of compliance with personal data protection.
- Communicate efficiently to the Technology area the termination of employees no later than the day of their departure.
- Ensure that in all welfare processes where data of minors is collected or may be collected, the proper authorization for its processing is obtained from parents and guardians.
- Establish appropriate controls to ensure that only authorized personnel within the area have access to sensitive information.
- Verify that transfers of sensitive documentation to external archiving companies are carried out under appropriate security and confidentiality measures.
- Verify that transmissions and transfers of personal data are carried out in accordance with the guidelines of the Privacy, Cybersecurity and Information Security Management area.

6.7 STRATEGIC PROCUREMENT MANAGEMENT AND INFRASTRUCTURE DIRECTORATE

- Timely handle inquiries and complaints regarding personal data submitted or made by suppliers, lessors, and individual contractors of the Bank.
- Obtain from individual suppliers, lessors, and legal representatives the relevant authorizations for the processing of their personal information before and during the contractual relationship with the Bank.
- Obtain authorization for the processing of sensitive information (video recordings) of contractors performing work within the Bank's facilities, before and during the employment relationship.
- Request from suppliers the Personal Data Processing Policy and the Personal Data Processing Security Manual, when the Privacy, Cybersecurity and Information Security Management area deems it necessary.
- Inform all Bank areas requesting the contracting of a service that involves any type of personal data processing that they must obtain an opinion issued by the Privacy, Cybersecurity and Information Security Management area from the very beginning of the initiative, containing the personal data protection guidelines.
- Ensure compliance with what is established in A-181-00103 Contracting Requirements for Personal Data Processors, which must be considered for the contracting of personal data processors.

6.8 LEGAL VICE PRESIDENCY

- Provide advisory support to process owners in understanding personal data protection regulations, as well as in the drafting and review of legal documents and clauses.
- Prepare and send to the relevant areas the Personal Data Transmission or Transfer Agreement, as applicable, under the guidelines established in current personal data protection regulations.
- Include the personal data protection clause in service contracts when the third party, supplier, or partner being contracted processes personal data.
- Support the Customer Service Operations Management area – PQRs in validating responses provided to data subjects who submit inquiries or complaints to the Bank.
- Monitor and follow up on legislation and regulations issued regarding personal data protection and provide recommendations for internal adjustments within the entity.

6.9 TECHNOLOGY AND PRODUCTIVITY MANAGEMENT

- Implement technical aspects in applications and databases to ensure compliance with regulations, in accordance with requests and requirements from process owners.
- Timely deliver the information required by the Customer Service Operations Management – PQR, to respond to inquiries and complaints from Data Subjects or competent authorities.

6.10 COMMERCIAL AND MARKETING AREA LEADERS

- Ensure that commercial flows or future initiatives involving the collection and processing of personal data include the authorization for data processing from data subjects.
- Verify that in all potential marketing processes, the necessary mechanisms are implemented to obtain prior authorization from potential customers for subsequent processing activities.
- Verify that in all customer onboarding processes, the appropriate authorizations from data subjects are in place for all intended purposes.
- Verify that the commercial force (especially external staff) has been properly trained in personal data protection, implemented organizational procedures, responsibilities, and the consequences of non-compliance.
- Verify that prior to the execution of commercial campaigns, authorization for data processing from the data subject is in place and that the data subject has not requested exclusion from commercial campaign interactions via SMS, email, or telephone calls. If so, they must be excluded from these processes.
- Verify that no decentralized databases are created by internal or external commercial staff that could violate the principle of data quality.

6.11 CUSTOMER SERVICE OPERATIONS MANAGEMENT – PQR

- Send, request support, and follow up with the different areas and domain owners of the Bank for the corresponding investigation of inquiries and complaints submitted by data subjects, which may arise from the exercise of personal data protection rights. This includes validating information related to products, channels, or any type of interaction with the data subject or processing of personal data stored in the Bank, in order to process data subject requests.
- Report on the information required by the Privacy, Cybersecurity and Information Security Management area, related to requests for handling complaints regarding personal data protection received by the Bank, as well as the updating of entities acting as personal data processors and the databases registered by the Bank with the Superintendence of Industry and Commerce (SIC).
- Respond to all requests submitted through the different channels enabled by Banco Popular that may arise from the exercise of data subjects' rights in relation to Personal Data Protection, within the timeframes established by Law 1581 of 2012, regulatory decrees, and other binding regulations.
- When requested, request support from the Institutional Legal Studies Directorate of the Legal Vice Presidency for the preparation of responses to requirements issued by the Superintendence of Industry and Commerce regarding Personal Data Protection.
- When legal support is required, request assistance from the Banking Business Management area of the Legal Vice Presidency for the preparation of responses to complaints, petitions, or claims submitted by data subjects regarding Personal Data Protection.
- Implement a typology for the proper categorization when registering inquiries and complaints related to personal data, following the guidelines provided by the Privacy, Cybersecurity and Information Security Management area of the Bank.
- Submit a monthly report on the management of personal data protection requests to the Privacy, Cybersecurity and Information Security Management area.

7 GENERAL OBLIGATIONS

Personnel who, for the proper performance of their duties, are authorized to access personal data, including personnel of data processors, have the following obligations:

- All staff in general, area leaders, managers, or directors responsible for supervising compliance with service contracts or alliances with third parties or suppliers that involve any type of processing of personal data of clients, users, or employees, must periodically report the information required to update the information related to processors, such as processing activities, purposes, types of data, and data protection policy, as well as all information related to databases containing personal information, in accordance with what is established in process P-181-00101 Management of Updates to Databases Registered with the SIC V2.

- Maintain confidentiality regarding any type of personal information known in the course of work activities, even after the employment relationship with Banco Popular has ended.
- Keep all physical records and/or documents containing personal data stored in a secure place when not in use, particularly outside working hours.
- It is prohibited to remove any medium containing sensitive personal data in which Bank-owned information is stored from the Bank's facilities without prior validation by the Privacy, Cybersecurity and Information Security Management area. In the event of transfer or distribution of sensitive or high-risk documents or media, this must be carried out using mechanisms that prevent access, use, or manipulation of the information by unauthorized third parties.
- Temporary databases or copies of documents containing personal data may be created when required for a specific need or for occasional and auxiliary tasks, provided that their existence does not exceed one month. These temporary databases or document copies must comply with appropriate security levels based on the type or risk of the data and must be deleted or destroyed once they are no longer required for the purposes for which they were created.
- Only authorized people may enter, modify, or delete personal data through applications into the databases. Direct entry into the database is not permitted; if required, the provisions established in the Information Security model guidelines must be followed to adopt appropriate measures.
- User access permissions are granted by the technology area in accordance with role-based profiles.
- Report to the Privacy, Cybersecurity and Information Security Management area any security incidents that become known and that may affect databases, media, or documents containing personal information.

7.1 REGARDING AUTOMATED DATABASES

- Change administrator users' passwords periodically.
- Close or lock all sessions at the end of the working day or in the event of temporarily leaving the workstation, to prevent unauthorized access.
- Do not copy the information contained in databases where personal data is stored (especially sensitive data) onto personal computers, CDs, external drives, USB devices, or any other storage medium.
- Users are prohibited from sending sensitive personal information or information classified as high risk. In any case, such transmission may only be carried out if the necessary mechanisms are adopted to ensure that the information cannot be read or manipulated by third parties.
- Users may not install any type of software programs or devices either on central servers or on the workstation computer.
- It is prohibited to:

    - Use other users' usernames and passwords to access the system.

- Violate the security measures established in information systems by attempting to access databases or programs to which access has not been granted.
- In general, use the corporate network, information systems, and any means made available to the user in a way that violates the rights of third parties or of the organization itself, or to carry out acts that may be considered unlawful.

7.2 REGARDING PHYSICAL – NON-AUTOMATED DATABASES

- Maintain the necessary confidentiality regarding any type of personal information known in the course of work activities, even after termination of the employment relationship with the entity.
- Keep properly safeguarded the document that identifies you as an employee of the Bank, as well as access keys to offices and to desks, filing cabinets, or other items that contain physical (non-automated) databases with personal data. Any fact that may compromise such custody must be reported to your Manager or leader.
- Lock desks and office doors at the end of the working day or when temporarily leaving the area, in order to prevent unauthorized access.
- Report to the Privacy, Cybersecurity and Information Security Management area any security incidents you become aware of that are related to physical databases.
- It is prohibited to remove any list or similar document containing personal data in which Bank-owned information is stored from the Bank's premises without the corresponding authorization.
- Keep all physical records or documents containing personal data stored in a secure place when not in use, particularly outside working hours.
- Ensure that no printed documents containing protected data are left in the printer output tray.

8. PRIVACY AND PERSONAL DATA PROTECTION POLICY

This section refers to the Policy published on the internet, which came into force on October 10, 2015 and is made available to customers and users through the website **www.bancopopular.com.co.** Its main purpose is to make known the internal regulations adopted by the Bank in this matter.

The privacy and personal data protection policies shall apply to all "automated and physical" databases containing personal data that are subject to processing by THE BANK, including all information obtained or collected prior to Law 1581 of 2012, and any other data that may be processed by the Bank in the development of its corporate purpose or in connection with any type of civil, labor, or commercial relationship that may arise as part of its activities, whether related or inherent to its corporate nature.

The policies and/or their amendments are designed by the Privacy, Cybersecurity and Information Security Management area and are approved by the Integrated Risk Management area.

These are made known to the data subjects through the entity's website www.bancopopular.com.co.

The main content of the policies establishes:

- Identification of the data processing controller.
- Name or legal name of the entity.
- Scope, application, and regulatory framework.
- Purposes and processing of personal data.
- Authorization.
- Rights held by the data subjects.
- Person or area responsible for handling petitions, inquiries, and complaints.
- Service channels.
- Duties of Banco Popular as Controller and Processor.
- International transfer of personal data.

8.1 INFORMATION COLLECTION

For the purposes of complying with Article 9 of Law 1581 of 2012, the areas responsible for the channels through which personal data is requested must establish mechanisms to obtain authorization from data subjects or from whoever is legally authorized in accordance with Article 2.2.2.25.4.1 of Chapter 25 of Decree 1074 of 2015, ensuring that such authorization can be verified and consulted.

If the data is collected through a physical medium, the authorization must include the signature of the data subject. If a technological or verbal method is used, efficient mechanisms must be implemented that allow the entity to retain evidence of acceptance of data processing and to consult it when required.

In cases where Banco Popular acts as the data controller and regardless of the collection method, authorization from the data subject must be obtained and proof of such authorization must be retained.

8.2 AUTHORIZATIONS

In accordance with current regulations, the consent of the subject must meet the following characteristics:

- **Be prior**: authorization must be provided at a stage prior to the incorporation of the data into the database and its use for commercial purposes.
- **Be express**: it must be granted in an unequivocal, explicit, and specific manner for the required purpose.
- Authorization must be unequivocal; therefore, under Colombian law, tacit consent is not considered valid.

- **Be informed**: the data subject must know the purpose of the database and the processing that will be given to their data, as well as be fully aware of the effects of their authorization. Specifically, it is mandatory to inform the data subject of: (i) the processing that will be carried out on their data and its purpose; (ii) the optional nature of answering questions regarding sensitive data; (iii) the rights they have; (iv) the identification, physical or email address of the data controller.

To obtain authorization, the following instructions are followed:

First, before the person grants authorization, they must be clearly and expressly informed of the following:

- The processing to which their personal data will be subjected and its purpose.
- The optional nature of responses to questions asked when these relate to sensitive data or data of children and adolescents.
- The rights they have as data subjects, as provided in Article 8 of Law 1581 of 2012.
- The identification, address, and telephone number of Banco Popular.
- The Bank's service channels for personal data processing matters.

Second, consent from the data subject is obtained through any means that can be subsequently verified. The mechanisms may be predefined through technical means that facilitate the data subject's automated expression of consent. It is understood, as previously indicated, that authorization complies with these requirements when it is expressed through:

- **In writing:** Evidence is left of compliance with the obligation to inform and of consent. If the data subject requires a copy, it must be provided.
- **Verbally:** through telephone calls in which the data subject is informed of their rights and the purposes of the data processing, subsequently being given the opportunity to express their acceptance. From such communications, evidence shall be retained through recordings stored in a manner that allows subsequent consultation.
- **Digital:** through applications and/or internet portals in which the data subject is informed of their rights and the purposes of the data processing, subsequently being given the opportunity to express their acceptance. Evidence of such acceptance shall be retained through logs, stored in a manner that allows subsequent consultation.
- **Unequivocal conduct of the data subject:** authorization may also be obtained from unequivocal conduct of the data subject that reasonably allows the conclusion that they granted consent for the processing of their information.

When personal data is sensitive, authorization for the processing of such data must be explicit. In no case may silence from the data subject be considered unequivocal conduct.

8.2.1 CASES IN WHICH AUTHORIZATION FOR PERSONAL DATA PROCESSING IS NOT REQUIRED

Authorization from the data subject shall not be required when it concerns:

a) Information required by a public or administrative entity in the exercise of its legal functions or by judicial order;
b) Data of a public nature;
c) Cases of medical or health emergency;
d) Processing of information authorized by law for historical, statistical, or scientific purposes;
e) Data related to the Civil Registry of Persons.

Any person who accesses personal data without prior authorization must in any case comply with the provisions contained in Law 1581 of 2012.

8.2.2 AUTHORIZATION FOR THE PROCESSING OF SENSITIVE DATA

Banco Popular may only carry out operations or processing of sensitive data with prior and express authorization from the data subject of such personal data, provided that the data subject has been informed:

When sensitive data is collected, the following requirements must be met:

- The authorization must be explicit.
- The data subject must be informed that they are not obliged to authorize the processing of such information.
- The data subject must be explicitly and previously informed which of the data to be processed are sensitive and the purpose of such processing.

8.2.3 AUTHORIZATION FOR THE PROCESSING OF DATA OF CHILDREN AND ADOLESCENTS

When collecting and processing data of children and adolescents, the following requirements must be met:

- Authorization must be granted by people legally authorized to represent the children and adolescents (NNA). The representative of the NNA must guarantee their right to be heard and must consider their opinion regarding the processing, considering the maturity, autonomy, and capacity of the NNA to understand the matter.
- It must be informed that answering questions regarding the data on children and adolescents is optional.
- The process must respect the best interests of children and adolescents and ensure respect for their fundamental rights.
- Banco Popular will only use, store, and process personal data of minors that are children, descendants, or dependents of employees or contractors, and only when such data is of a public nature. The purpose of such processing will be exclusively to plan and carry out activities related to the personal and family welfare of employees and minors.

8.3 PRIVACY NOTICE

Banco Popular makes available to data subjects the privacy notice for the processing of personal data. This notice is a verbal or written communication addressed to the Data Subject through

physical or electronic means. Through this document, the Data Subject is informed of the existence of the personal data processing policies applicable to them, the way to access such policies, and the characteristics of the processing intended to be given to personal data at the time of collection.

The privacy notice must include at least:

1. Name or corporate name and contact details of the Data Controller.
2. The processing to which the data will be subjected and its purpose.
3. The rights of the Data Subject.
4. The mechanisms provided by the Data Controller so that the Data Subject may become aware of the data processing policy and any substantial changes made to it or to the corresponding Privacy Notice. In all cases, it must inform the Data Subject how to access or consult the data processing policy.

8.4 PROOF OF AUTHORIZATION

In order to later be able to consult the authorization obtained in physical, digital, or magnetic (telephone call) form, the Bank shall retain proof of such authorization while the client remains active and subsequently for 10 years after they cease to be a client of the Bank, as support in possible events that may arise against the Bank.

Data Processors acting in such capacity by virtue of a data transmission contract signed with the Bank are required to retain evidence of the personal data processing authorizations granted by the data subjects and collected through the different existing mechanisms. The Bank shall include these obligations in personal data protection contracts.

8.5 AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA

For updating the authorization for the processing of personal data, the following must be considered:

- The legal team of Grupo Aval is responsible for defining and delivering the authorization for the processing of personal data to the Institutional Legal Studies Directorate of the Bank, which must analyze it, issue an opinion on the document, and communicate it to the Privacy, Cybersecurity and Information Security Management.
- The customization of the authorization for the processing of personal data for use within the Bank is carried out by the areas of the Institutional Legal Studies Directorate and Privacy, Cybersecurity and Information Security Management.
- The Bank's own channels enabled for the exercise of data subjects' rights are included in the authorization for the processing of personal data once they are reported by the Business Intelligence, Customer Experience and Care, Segments and Channels Management; the Payment Methods Operations Management; the Talent Care

Management in the case of employees; and the Strategic Supply Management for cases involving natural person suppliers or lessors.

- Privacy, Cybersecurity and Information Security Management communicates the updated version of the authorization for the processing of personal data to the different **product areas, channels, and subsidiaries** of the Bank, so that they may update it in the channels, formats, and documents where it is included.
- It must be considered that the timeframe to update the authorization for the processing of personal data is a maximum of 45 calendar days, from the notification sent by Privacy, Cybersecurity and Information Security Management.
- The areas responsible for products and channels where the authorization for the processing of personal data is presented to clients, in onboarding, creation, and updating processes, must notify Privacy, Cybersecurity and Information Security Management of the date on which the authorization was effectively implemented in the different channels and formats.
- The areas owning digital formats in which the clause for authorization for the processing of personal data is included must request from the Process and Automation Management: the adjustment of the formats, the updating in electronic forms and the dissemination of these updates through a bulletin.
- The areas that own printed electronic forms must immediately report the change so that previous blank formats are collected and destroyed.
- The areas responsible for products and channels, as well as subsidiaries, must always ensure the use of the latest version of the authorization for the processing of personal data approved by the Institutional Legal Studies Directorate and Privacy, Cybersecurity and Information Security Management.

9. INFORMATION TRANSMISSION

The exchange or electronic or physical transmission of personal data is carried out in accordance with the Security and Information Security Policies and guidelines implemented at Banco Popular. As a general guideline, the following are established:

- Sensitive, confidential, or private information transmitted through telecommunications networks, both internal and external, must be protected.
- The areas responsible for information assets containing sensitive, confidential, or private information must define which security, and privacy controls must be implemented for network services.
- For the transmission of sensitive personal information of high-risk level, reinforced security measures must be adopted.
- Prior to the transmission of data to third-party Data Processors, the personal data transmission contract must be signed between the parties in advance.

10. TRANSFER AND TRANSMISSION OF DATA TO THIRD COUNTRIES

Unless there is express authorization from the Data Subject and the other exceptions provided for in Law 1581 of 2012, the transfer of data to third countries that do not provide adequate levels of data protection is prohibited.

10.1 DATA TRANSMISSION TO A PROCESSOR FOR THE PROCESSING OF PERSONAL DATA

Banco Popular may transmit or deliver personal data from its databases to a third party in Colombia or abroad so that this third party, acting as a Processor, carries out the processing of personal data. For these purposes and in accordance with the law, a data transmission contract must be executed with such third party, in which:

- The scope of processing, the activities that the Processor will carry out for the processing of personal data, the conditions for the use of the data, and the obligations of the Processor towards the Data Subject and the Data Controller shall be specified.
- The Processor undertakes to comply with the obligations under the Data Processing Policy and to process personal data in accordance with the purpose authorized by the Data Subjects and applicable laws.
- The Vice Presidency of Legal Affairs – General Secretariat shall draft the transmission or transfer agreements, as applicable, and the Privacy, Cybersecurity and Information Security Management shall review them; the document shall be jointly approved.

11 ACCESS TO AND CONTROL OF PERSONAL INFORMATION

The Vice Presidency of Corporate Innovation and Technology Management shall implement technological and monitoring controls that allow traceability and control of users who access the information.

At the level of physical facilities and access to non-automated physical documentation, each area shall be responsible for the access and control of the information maintained in its management files.

11.1 USE OF INFORMATION

Personal data contained in the different databases shall be used and processed solely for the purpose established in the Data Subject's authorizations.

Any use of information different from the previously established purpose must be included within the authorization for the processing of personal data, which shall require renewed authorization from the Data Subject with additional purposes.

The new purposes to be incorporated into the processing authorization must be validated by the Vice Presidency of Legal Affairs – General Secretariat of the Bank.

The introduction of personal data into databases, modification, or deletion of personal data may only be performed by authorized employees through the applications. Direct entry into the database is not permitted. Where required, the provisions established in the Information Security model guidelines must be followed to adopt appropriate measures in this regard.

11.2 INFORMATION STORAGE

The storage of automated and physical information must be carried out in media or environments that have adequate controls for the protection of data. This includes security controls, technological controls, and environmental controls in restricted areas, in own facilities and/or in computing centers or document centers managed by third parties.

Custody of information must be carried out under conditions that do not cause deterioration of information assets.

11.3 DESTRUCTION

The destruction of information containing personal data in physical or electronic media is carried out through mechanisms that do not allow its reconstruction, in accordance with what is defined in Directive AVBP.DISI.GA.055 Destruction of Restricted Information, of the Information Security Guidelines document.

The destruction of information held by third parties must be carried out in accordance with what is defined contractually in the Clause Procedures and controls for the delivery and destruction of information.

12. MANAGEMENT OF INCIDENTS RELATED TO DATABASES CONTAINING PERSONAL INFORMATION

The Bank has established a Privacy Incident Management procedure to respond if an incident may affect or has affected databases containing personal data; such incidents must be reported to Privacy, Cybersecurity and Information Security Management.

The Bank shall allocate the necessary resources to provide appropriate monitoring, detection, and management of Privacy incidents, establishing procedures for incident management.

The responsibility of each employee, contractor, collaborator, or third party is to promptly report any suspicious event, weakness, or violation of policies that may affect the privacy of data subjects.

All incidents and suspicious events must be reported as soon as possible through the internal channels established by Banco Popular under the RRI11 Information Security and Cybersecurity

Incident Management process. The escalation levels for communication in the event of a privacy incident are those established in the procedure.

Employees must report to their direct supervisor and to Privacy, Cybersecurity and Information Security Management any damage or loss of their computers or any other device containing information of employees, clients, or suppliers who are natural people.

Unless there is a request from the competent authority under an administrative or judicial requirement, no employee may disclose information about computer systems and networks that have been affected by cybercrime or system abuse. For the delivery of information or data pursuant to an order from an authority, the Judicial Support Directorate of the Vice Presidency of Legal Affairs must intervene to provide appropriate guidance.

13. GUIDELINES FOR THE PROCEDURE FOR THE EXERCISE OF DATA SUBJECT RIGHTS

The Customer Service Operations Management – PQR must include in its procedures the actions required to timely address, and in accordance with the guidelines established in the applicable personal data protection regulations, inquiries and complaints.

The Data Subject of the personal information provided to Banco Popular shall have the following rights:

- To know, update, and rectify their personal information free of charge.
- To request proof of the existence of the authorization granted to Banco Popular.
- To be informed regarding the use given to their personal information.
- To revoke authorization and request deletion of the data when it is not being used in accordance with the authorized purposes and uses.
- To submit inquiries and complaints regarding personal information.
- The other rights established by law.

13.1 PROVISIONS FOR REQUESTS AND COMPLAINTS PROCEDURES

Requests for rectification, updating, or deletion must be submitted through the channels enabled by Banco Popular as indicated in this document, and must contain at least the following information:

- The name, address of the data subject, and contact method to receive the response, such as telephone number, email address, or residential address.
- Documents proving identity or representation of the representative.
- A clear and precise description of the personal data for which the data subject seeks to exercise any of their rights.
- Where applicable, other elements or documents that facilitate the location of the personal data.

- Evidence of the complaint such as text messages, emails, and any other supporting documents.

13.1.1 INQUIRIES

Banco Popular guarantees the right of inquiry by providing individuals exercising this right with all information contained in their individual record or linked to the identification of the data subject. Inquiries and requests must be submitted by the data subject through any means and to any of the contacts indicated below and will be addressed within a maximum period of ten (10) business days, counted from the date of receipt through any communication channel. If it is not possible to resolve the inquiry within this period, the data subject will be informed of such situation at the notification address provided in the inquiry, and the response period may be extended for up to five (5) additional business days. The response to inquiries or complaints submitted by the data subject may be delivered by any physical or electronic means.

13.1.2 COMPLAINTS

When data subjects or their successors consider that their information should be corrected, updated, deleted, or that authorization should be revoked, or when they detect a presumed breach by Banco Popular of its duties regarding Personal Data Protection as set forth in applicable legislation and in the Privacy and Personal Data Protection Policy, they may submit a complaint as follows:

- Submit a written request regarding the specific issue.
- If the complaint is incomplete, Banco Popular will 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 abandoned.
- If the person receiving the complaint is not determined to resolve it, they shall forward it to the competent party to resolve it within a maximum term of two (2) business days and inform the data subject of this fact.
- If the complaint is received in full or has been subsequently completed, a “legend” must be included in the database within two (2) business days indicating: “COMPLAINT UNDER PROCESS”.
- Banco Popular shall resolve the complaint within a maximum term of fifteen (15) business days counted from the day following its receipt. If it is not possible to resolve the inquiry within this term, the data subject will be informed of the delay, the reasons, and the expected response date at the notification address provided in the complaint. In any case, the response time shall not exceed eight (8) additional business days following the expiration of the first term. The response to the complaint may be provided by any physical or electronic means.

13.1.3 DATA DELETION

The data subject has the right, at any time, to request from Banco Popular the deletion (suppression) of their personal data when:

- They consider that the data is not being processed in compliance with the principles, duties, and obligations established in Law 1581 of 2012.
- The data is no longer necessary or relevant for the purpose for which it was collected.
- The period necessary to fulfill the purposes for which the data was collected has expired.
- Data deletion does not proceed when:
- The data subject has a legal or contractual duty to remain in the database.
- Deletion of the data obstructs judicial or administrative actions related to tax obligations, investigation and prosecution of crimes, or updating 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.

It must also be considered that in some cases certain information must remain in historical records due to compliance with the organization's legal duties; therefore, deletion will apply to the active processing of such data in accordance with the data subject's request.

14. CHANNELS

The channels enabled data subjects and users to exercise their rights to know, update, rectify, delete data, and revoke authorization are:

- Banking offices nationwide
- Calling our Call Center in Bogotá D.C. at 60-1-743-4646, and from the rest of the country at 01-8000-184646.
- Regarding inquiries or complaints from Bank employees, these must be directed to the Talent Care and Services Management via email at **geratencionsth@bancopopular.com.co**.
- Inquiries or complaints from natural person suppliers will be handled by the Strategic Supply Management.

CHANGE LOG

History		
Version #	**Publication date**	**Description of change**
1	06/26/2020	The Policy is created with the purpose of regulating the guidelines for personal data governance, responsibilities, conduct and general provisions, focused on protecting the privacy of personal data of clients, employees, suppliers, shareholders and other natural persons with whom the Bank has a relationship.
2	10/06/2020	The policy is updated to include item 7.4 Personal Data Processing Clause, and the name of the Non-Financial Risk and Compliance Management is changed to Chief Risk Officer (CRO), and the position of Non-Financial Risk Manager to Chief Risk Officer (CRO). Additionally, the service channels for data subjects are adjusted to align with those defined in the Privacy and Personal Data Protection Policy on the Bank's website.
3	12/10/2021	The policy is updated: In item 4.1.2 Form of processing, guidance is added on how to register the personal database inventory with the Superintendence of Industry and Commerce. In item 5 Governance for privacy management, the reference framework defined in the three lines of defense scheme is included.
4	03/28/2023	Sections 1 and 7 are updated, and sections 6.1 and 8.2.1 are incorporated into the present policy, with the purpose of regulating the Comprehensive Data Protection Management Program.