Corporate Information on Privacy and Data Processin

Introduction

This document has been prepared by Banco de Occidente to consolidate, in a single source, information related to its practices on privacy, personal data processing, and regulatory compliance. Its content includes methodologies, internal procedures, organizational structure, control mechanisms, and designated channels, demonstrating the Bank's commitment to the protection of personal data belonging to clients, users, employees, and other stakeholders, in compliance with Law 1581 of 2012, its regulatory decrees, and other applicable legal provisions in Colombia.

Unit Responsible for Data Protection and Risk Mitigation in Data Processing

Banco de Occidente has a Personal Data Protection Unit within the Compliance Management area, responsible for designing, implementing, and administering the Comprehensive Personal Data Management Program, in accordance with Law 1581 of 2012 and related regulations. This unit, led by the Data Protection Officer, has specific duties including implementing the data processing policy and privacy notice, identifying data collection sources and authorization mechanisms, promoting risk management in data processing, coordinating technological control development, registering and updating databases with the Superintendence of Industry and Commerce, supporting the Bank during regulatory visits, fostering a data protection culture, managing the attention process for requests and complaints, and overseeing internal audits, among others.

Risk Management and Internal Audit in Data Protection

Banco de Occidente has developed and implemented a privacy policy system integrated into the group's overall risk/compliance management framework, through the Comprehensive Personal Data Management Program outlined in Manual MAN-APY-268. This system enables the identification, assessment, control, and monitoring of risks associated with personal data processing, including legal, reputational, and operational impacts. The methodology includes the three lines of

defense model: operational processes as the first line, supervisory functions such as the Data Protection Unit as the second, and internal audit as the third line, which conducts periodic audits to verify compliance with the privacy policy. This structure safeguards the confidentiality, integrity, and availability of information, in alignment with national and international standards. Furthermore, non-compliance in this area may result in sanctions imposed by the Superintendence of Industry and Commerce, including fines, activity suspension, or permanent closure of data-sensitive operations.

Nature of Captured Information

The nature of the information captured by Banco de Occidente includes a broad set of personal data from the data subject, such as financial, credit, commercial, professional, sensitive (including fingerprints, voice, and image), technical, administrative, private, and semi-private data, collected through physical, digital, or electronic means. This information may be related to past, present, or future and is processed through activities such as collection, verification, storage, analysis, circulation, transmission, and use for contractual, legal, commercial, and operational purposes.

The authorization provided by the data subject allows the Bank and authorized third parties to use this information in accordance with legal parameters for security, confidentiality, and purpose.

Use of Collected Information

Banco de Occidente uses personal data from its clients to fulfill the purposes associated with the efficient provision of its financial services, such as account management, transaction execution, administration of credit products, and other banking operations. This information is also treated as a strategic resource within the Bank's organizational structure, provided to responsible executives to support the achievement of commercial and operational objectives. Every set of information used for business purposes must have an "information owner" who oversees its

correct use, makes protection decisions, and determines access and usage privileges, in line with internal and legal information security policies.

Data Subject Control over Processing

Banco de Occidente recognizes the data subject's right to decide how their personal data is collected, used, retained, and processed. Therefore, the Bank requests explicit authorization for data processing no later than at the time of collection, clearly indicating which data is being gathered and the intended purposes of use. Authorization is not required in cases involving public data, judicial or administrative requests, medical emergencies, historical, statistical, or scientific use, or data excluded under Law 1581 of 2012.

In the case of minors, the Bank ensures their fundamental rights are respected and requires the authorization of their legal representative as established by law. Sensitive data will only be processed with the data subject's explicit consent unless legal exceptions apply. Personal data may also be transferred or transmitted to entities within the Bank's economic group, subsidiaries, affiliates, and legally authorized third parties, in accordance with the purposes previously agreed to by the data subject.

Data Subject Rights

Opt-Out Option

An opt-out option is available to all personal data holders. They may revoke the authorization for data processing or request the deletion of their information from the databases of Banco de Occidente and authorized entities. This right may be exercised through written communication, provided there are no legal or contractual obligations that require data retention. Additionally, data subjects may limit the scope of their authorization to restrict data usage solely to the Bank and exclude affiliated entities, in accordance with Law 1581 of 2012 and internal data protection policies.

Inclusion Consent Requirement

The onboarding process requires full completion of the “Onboarding Form” for both individuals and legal entities. This form contains essential information for full client identification, including ID data, economic activity, financial details, source of funds, and ownership structure (in the case of legal entities).

It must be signed and validated by the assigned manager or commercial director. The Bank also requires a personal interview, document verification, and formal approval before initiating any contractual relationship. Collected information must be entered into the IBS system for internal control and regulatory review. Except for pension-related accounts, consent and the completed form are mandatory. Clients must also declare whether they are Politically Exposed Persons (PEPs) or manage government funds.

Therefore, inclusion consent is not only required but forms the legal basis for the client–Bank relationship.

Exercising Specific Data Rights

- **Access to Stored Data**
  Data subjects may request free access to their stored personal data, find out how it has been used, and obtain proof of the authorization granted.
- **Transfer to Other Providers**
  Personal data may be transferred to other service providers upon express authorization and under principles of privacy, security, and legality.
- **Data Correction**
  Data subjects have the right to update, correct, or rectify any partial, inaccurate, incomplete, or misleading data, or any data processed without authorization.
- **Data Deletion**
  Deletion of personal data may be requested when it is not being processed according to legal principles. However, deletion is not possible if legal or

contractual obligations require data retention. Banco de Occidente stipulates that personal data must be deleted using secure technological methods, such as overwriting, ensuring the data cannot be reconstructed or accessed by unauthorized personnel. The process follows internal document management policies, and once legal or contractual obligations cease, data must be eliminated under supervision. Data subjects may request deletion in accordance with Law 1581 of 2012, provided no other applicable regulation requires its retention.

Data Retention Period

Personal data will be retained for the time necessary to fulfill its intended purpose and while contractual, legal, or commercial obligations exist:

- According to anti-money laundering laws, data may be retained for 5 to 10 years after the relationship ends.
- In compliance with commercial law, financial regulations, tax law, and accounting standards, data may be retained for up to 10 years following the termination of the business relationship.

Data Protection Measures

Banco de Occidente must implement the necessary mechanisms to safeguard information through its IT systems, developing internal capabilities to anticipate and respond to cyber threats. This includes defending and protecting data, systems, services, and critical applications across internal networks and cyberspace. Information is secured through technological, administrative, and physical controls, including secure systems, verification mechanisms, and controlled access. Additionally, personal data may circulate among different departments within the Bank and authorized third parties to fulfill purposes such as commercial management, legal compliance, security, transaction analysis, customer service, and fraud prevention.

Channels for Exercising Data Subject Rights

Clients and data subjects may submit requests through the following channels:

• Nationwide network of branch offices and Credicentros available on the Bank's official website

• Customer Service Lines: National 01 8000 514 652 / Bogotá 307 70 27

• Email: **datospersonales@bancodeoccidente.com.co**

Requirements: The requester must verify their identity or submit documentation confirming that they are acting as a legal representative. In case of complaints, a clear description of the issue and supporting documents must be provided.

Response Times

• Inquiries: within 10 business days (extendable by 5 more)

• Complaints: within 15 business days (extendable by 8 more)

Third-Party Disclosure Policy

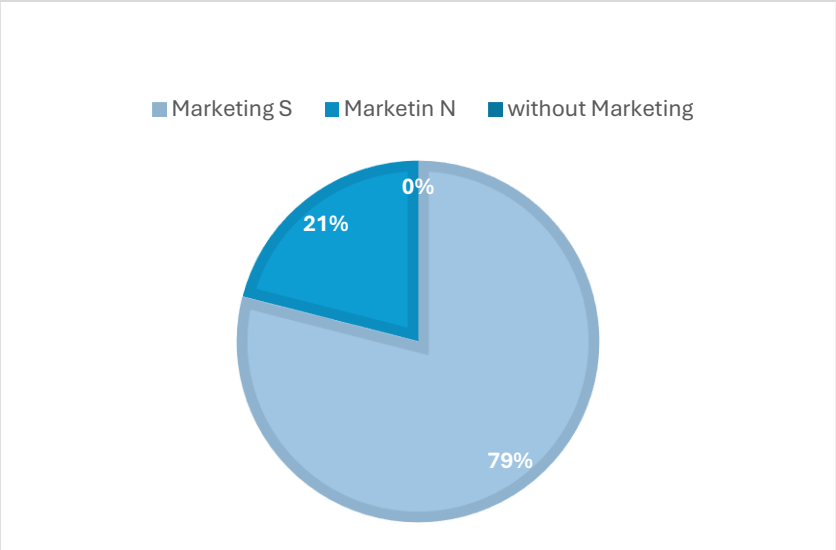
Banco de Occidente's personal data processing policy includes the possibility of disclosing or transferring data to third parties, including private and public entities, domestic and international, subject to prior authorization by the data subject and in accordance with Law 1581 of 2012. These transfers may be made to service providers, commercial partners, regulatory authorities, information operators, telemarketing teams, and other processors acting on behalf of the Bank, under conditions that ensure lawful, secure, and confidential handling. Additionally, the data subject retains the right to restrict the scope of such authorization through a written request.

Monitoring of Secondary Use of Personal Information

According to the current database of active individual clients, the Bank maintains 100% of client records marked as "S" for those who authorize

commercial contact by the Bank, and “N” for those who authorize data processing only for activities related to the existing contractual relationship and do not consent to commercial contact.

INDICATOR	CURRENT	% POPULATION
Marketing S	762,051	79%
Marketin N	201,627	21%
without Marketing	0	0%
Total	963,678	100%



Data Protection Population Percentage Indicator – Law 1581 as of May 21, 2025

Zero-Tolerance Policy Regarding Improper Data Processing

Banco de Occidente enforces disciplinary and corrective measures in cases of non-compliance with personal data processing policies, aligned with a zero-tolerance approach toward actions that compromise data protection. The Superintendence of Industry and Commerce may impose sanctions including fines of up to 2,000 legal monthly minimum wages, suspension of related activities, and temporary or permanent closure of operations involving the processing of sensitive data. Furthermore, as part of the Bank’s risk

management system, internal audits and compliance supervision are conducted to reinforce enforcement of consequences at both institutional and individual levels.