Personal Data Protection and Privacy Policy

With the aim to protect all persons' right to know, update, and correct the information stored about them in the databases or files, Banco de Bogotá establishes policies for the use, management, transmission, and other activities that involve personal data.

Not only as a result of Law 1581/2012 and Habeas Data Law 1266/2008, but also because it is established in the Colombian Constitution that people's private information is subject to confidentiality, no one who holds commercial information or personal data collected for a contractual relationship may use it for purposes different to those for which it was provided.

Through the issue of Law 1581, regulations were established on the personal information recorded in any database that is susceptible to treatment by public or private entities. This law is mandatory for financial institutions as responsible for this information as of October 18, 2012, the date it was published in the official newspaper.

Definitions

- Authorization: Prior express and informed consent by the data owner for the treatment of his/her personal data.
- Database: Organized set of personal data subject to treatment.
- Personal information: Any related information or data that can be associated with one or several specific or determinable individuals. Personal information may be public, semi-private or private.
- Party responsible for data treatment: The individual or legal entity of public or private that, acting on its own or collectively with others, decides on the database and/or data treatment. For the purposes of this document, the BANK is understood as responsible for data treatment.
- Data owner: Individual whose personal data is subject to treatment.
- Treatment: Any operation or set of operations on personal data, such as collection, storage, use, circulation, or deletion.

Guiding Principles for Personal Data Treatment by the Bank

Banco de Bogotá treats personal data in compliance with the general and special regulations on the matter and fully applies the following principles harmoniously:

- Principle of legality: Law 1581/2012 and the other provisions that develop, amend and/or add to it shall be applicable for the treatment of the information contained in the databases under the BANK's custody.

- Principle of purpose: The treatment of information contained in the databases under the BANK's custody complies with a legitimate purpose according to the Colombian Constitution and Law, which is duly and previously informed to the data owner.

- Principle of freedom: The treatment of information contained in the databases under the BANK'S custody shall only be exercised when the BANK has the free, prior, express, and informed consent of the data owner.

- Principle of veracity or quality: The information subject to treatment by the BANK must be true, complete, accurate, up-to-date, provable, and understandable. Partial, incomplete, or fragmented information, or data that leads to error shall not be subject to treatment.

- Principle of transparency: The BANK guarantees the data owner's right to obtain at any time and without restrictions information about the existence of data pertaining to the owner.

- Principle of access and restricted circulation: Treatment of information is subject to the limits resulting from the nature of the personal information, legal provisions, and the Colombian Constitution. Therefore, the data can only be treated by persons authorized by the data owner and/or the persons established by law. The BANK guarantees that the personal data, except public information, shall not be available on the internet or other mass media or means of disclosure except when access to the data can be controlled technically to provide access restricted to only the data owner or the third parties authorized by Law.

- Principle of security: The information subject to treatment covered by Law 1581/2012 shall be handled with the necessary technical, human and administrative measures to provide security to the records, preventing their falsification, loss, or unauthorized or fraudulent consultation, use or access.

- Principle of confidentiality: All persons involved in the treatment of non-public personal data shall be obliged to guarantee the confidentiality of the information, even after their relationship with any of the treatment tasks has ended, only being able to supply or communicate personal data when this is for the development of the activities authorized by Law 1581/2012 and the terms therein.

- Principle of time: The period for which the personal data is held shall be the time necessary to achieve the purpose for which the data has been collected and/or while the data owner has pending obligations with direct or indirect responsibility for the additional time required by special regulations or the time limits.

Scope

The Personal Data Protection Policy implemented by Banco de Bogotá applies for all our customers, users, suppliers, shareholders, employees, and visitors, establishing procedures for the use, management, transmission, and other activities involved in the processing of personal data. This is in full compliance with Law 1581/2012 and Habeas Data Law 1266/2008, which indicate that people's private information is subject to confidentiality, its use must be in accordance with the permissions granted by the owner, and under no circumstances must it be used for purposes other than the ones for which it was obtained.

Model

Banco de Bogotá constantly designs and implements controls to prevent, detect and promptly respond to undesired incidents and those to which the information could be exposed, adopting technologies and procedures focused on comprehensive data protection.

Banco de Bogotá's commitment to personal data protection has enabled us to design an information security and cybersecurity model in line with internationally recognized standards and adopting the legal and regulatory guidelines and best industry practices. This is with the aim to ensure the confidentiality, integrity, availability, auditability, and privacy of the information of customers, suppliers, employees and third parties that authorize the BANK's treatment of their personal data.

The Information Security Model establishes the guidelines so that information is only accessed by those who, according to their roles and responsibilities, have a legitimate need for knowledge thereof. Additionally, it contains instructions to protect the data from unplanned alterations made either intentionally or unintentionally and for the data to be available when required, constantly recording the access and actions made to the information.

The aforementioned provisions and guidelines are extended to all levels of the organization, users, employees, shareholders, customers, suppliers, contractors, control bodies, and affiliates of Banco de Bogotá that either internally or externally access any personal data, regardless of its location (own or third-party infrastructure or in cyberspace). In addition, it applies to all the information created, stored, processed, or used in support of the business, regardless of the medium, format, presentation or place it is located.

Likewise, Banco de Bogotá has established risk management systems and organizational structures with roles and responsibilities for the effective deployment of the Privacy Policy, which are responsible for creating, implementing, and monitoring due compliance with Article 13 of the Colombian Constitution, Law 1581/2012, and Habeas Data Law 1266/2008 regarding personal data protection:

- Operational Risk Management System (ORMS): For the management of risks regarding information security, there is a method approved by the Board of Directors published for all the entity's employees in the ORMS Manual. It is also responsible for defining and reviewing the operational risks together with the process owners to establish and implement the necessary controls for their mitigation.

- Banking and Information Security Department: This aims to fully protect the information of the Bank and its customers regardless of the medium in which it is presented, through the deployment of security strategies, corporate policies and rules, procedures and resources assigned by the Bank to preserve the principles of integrity, availability, confidentiality, privacy and auditability of information, considering an optimum cost-benefit relation for the organization.

- Information Security and Cybersecurity Department: This aims to maintain the integrity, accuracy, availability, and protection of the data that support the business processes by establishing effective procedures and controls for the proper input, output, storage, backup, recovery and deletion of data, maintaining the quality, timeliness and availability of information for the business.

- Personal data protection officer: Person responsible inside the organization for ensuring compliance with current regulation, advising the organization on the deployment of projects, monitoring the response to requests related to personal data protection, and updating the policy and personal data protection manuals.

- Legal Management: Responsible for legal support in the creation of contracts that the entity signs with customers, suppliers and other third parties with the aim to verify whether they comply with the personal data treatment policies and advise on the amendment of policies

and articles for authorization of data treatment.

Disciplinary measures in case of breach

Zero-tolerance policy for breaches

The reports of incidents generated due to breaches of data privacy are made by sources such as the Security Department, Information Security and Cybersecurity Department, Ethics Hotline, Control and Compliance Unit Department and immediate supervisors. The case is analyzed according to the applicable regulations, which are established in the Code of Ethics, Work Rules of Procedure and the documented processes related to information security and cybersecurity. Once the situation is analyzed, the applicable disciplinary measures are established by Labor Relations Management according to the Work Rules of Procedure.

Any breach that compromises the confidentiality, integrity, availability, privacy and/or auditability of the information constitutes serious misconduct, which can lead to termination of the work contract and to the possible filing of legal proceeding under the applicable national and international laws.

Use of Banco de Bogotá's information must be for the purposes of the business and never for personal or third-party purposes, which also constitutes serious misconduct.

Additionally, Banco de Bogotá has established the Anti-fraud and Anti-corruption Policy, which with respect to the data protection principle has guidelines on asset protection that promote the appropriate use of all its tangible and intangible assets in accordance with the roles and responsibilities of each of its employees. The policy also aims to protect the Bank's assets against loss, theft, misuse, or unauthorized use.

Audit of compliance with the privacy policy

Different audit exercises are implemented in the Bank, which are based on criteria of independence and objectivity of assessment and inquiry, with the aim to add value and improve the processes, helping to comply with the policies and guidelines regarding information security, cybersecurity, and data privacy, assessing and improving their effectiveness in risk management and control.

The General Comptroller of Banco de Bogotá, who exercises the role of internal auditor, establishes an annual audit plan, which covers regulatory aspects, risks associated with the processes and assessment of the aspects that support the technology infrastructure of the business. Similarly, it constantly monitors compliance with the regulations issued by the Financial Superintendence of Colombia on information security and cybersecurity, and by the Superintendence of Industry and Commerce on personal data protection and privacy.

The external auditing firm KPMG assesses the general technology controls, which is part of the work to analyze the reasonableness of the information used by the Bank and the applications that support it, guaranteeing the reliability of the information through strong information security and cybersecurity systems that provide an ongoing guarantee to investors, customers, suppliers and interested third parties.

Banco de Bogotá is a subordinate company of Grupo Aval Acciones y Valores, which has a Corporate Comptroller that covers all the Group's companies. In compliance with its audit plan, it makes in-person visits to assess compliance with the general guidelines, criteria, standards, and good practices established by the Corporate Group and established as mandatory, including those related to the

Bank's technology infrastructure. The specialist auditors for computer systems, information security, cybersecurity, and data protection develop audit tests that enable them to generate risk indicators and issue improvement opportunities to strengthen the aspects related to IT.

In turn, as part of the supervision exercised by the Financial Superintendence of Colombia as the regulator of financial institutions, it conducts ongoing assessments on regulatory aspects, including those regarding information security, cybersecurity, and data privacy.

Purpose of the data

Banco de Bogotá uses personal data in accordance with Law 1581/2012 for the following purposes:

- Comply with the legal regulations of knowledge of the data owner.
- Establish, maintain, and strengthen the contractual relationship.
- Update the information.
- Assess credit risk.
- Improve products and services.
- Determine the level of debt in consolidation.
- Carry out marketing work or commercial research or produce statistics.
- Send messages that contain commercial, marketing, personal or institutional information on products or services, or those of any other kind that the BANK considers appropriate, via cellphone, email, post, or any other means.
- Be consulted, exchanged, or circulated by the BANK with any entity of the real sector, entities subject to inspection and oversight by the Financial Superintendence of Colombia and/or any domestic or foreign information operator and/or data bank.
- Carry out quality and performance assessments.

Rights of data owners

Personal data owners shall have the following rights:

- Know, update, and correct their personal data.
- Request proof of the authorization granted to the BANK except when this is expressly an exception to the requirement for treatment pursuant to Article 10 of Law 1581.
- Be informed by the BANK upon request of the treatment and use of their personal data.
- Submit grievances to the Superintendence of Industry and Commerce of breaches of Law 1581 and the other regulations that amend, add to, or complement it.
- Revoke the authorization and/or request the deletion of the data when the treatment of said data does not respect the constitutional and legal principles, rights and guarantees. The authorization shall be revoked and/or the information deleted when the Superintendence of Industry and Commerce has established that the BANK has acted in breach of this law and the Constitution in the treatment of the data.

Authorization by the data owner

For the purposes of personal data treatment, the prior and informed authorization of the data owner shall be requested, which shall be obtained by any means that can be subject to subsequent consultation in writing, verbally, or through unmistakable conducts of the data owner that lead to the reasonable conclusion that the data owner granted the authorization.

The data owner's authorization shall not be necessary in the following cases:

- Information required by a public or administrative entity in exercise of its legal functions or by

court order.
- Public data.
- Cases of medical or health emergency.
- Treatment of information authorized by law for historical, statistical, or scientific purposes, and data related to people's civil registration.

Duties of the party responsible for personal data treatment

As the party responsible for the data treatment, the BANK must fulfill the following duties, notwithstanding the other legal provisions and those that regulate its activity:

- At all times, ensure the data owner's full and effective exercise of the Habeas Data right. Request and keep a copy of the respective authorization granted by the data owner.
- Duly inform the data owner of the purpose of the information collection and the rights of the data owner by virtue of the authorization granted.
- Maintain the information with the necessary security to prevent its falsification, loss, or unauthorized or fraudulent inquiry, use or access.
- Guarantee that the information subject to treatment is true, complete, accurate, update, provable and understandable.
- Update the information.
- Correct incorrect information.
- Process the inquiries and claims made by the data owners under the terms indicated by law.
- Upon the data owner's request, report on the use given to the data.
- Inform the authority of data protection when there are violations of the security codes and there are risks in the management of the data owners' information.
- Comply with the instructions and requirements provided by the Superintendence of Industry and Commerce.

Procedures

Account information

The data owners or their assignees may consult their personal information stored in the BANK's database with prior validation and accreditation of their identity according to the BANK's procedures. The inquiry shall be resolved within a maximum of ten (10) business days from the date the inquiry is received. When it is not possible to resolve the inquiry within said term, the interested party shall be informed, stating the reasons for the delay, and indicating the date by when shall be answered, which under no circumstances may be longer than five (5) business days following the expiry of the first term.

Claims

The data owner or their assignees that consider that the information contained in the database needs to be corrected, updated, or deleted, or when they warn of an alleged breach of any of the duties contained in Law 1581, must submit a claim, which shall be processed under the following terms:

The claim shall be prepared by a request addressed to the BANK with the ID of the data owner, a description of the events that led to the claim, and the home and email address and telephone number of the data owner, accompanied by the documents that validate it through the established channels.

If the claim is incomplete, the reception of the completed claim shall be required from the interested party within five (5) business days from the receipt of the incomplete claim. Once two (2) months have passed from the date of the request without the applicant submitting the required information, it shall be understood that the data owner has withdrawn the claim.

In the event that the person who receives the claim is not competent to resolve it, the claim shall be transferred to the relevant person within a maximum of two (2) business days and the interested party shall be informed of the situation.

The maximum term to resolve the claim shall be fifteen (15) business days counted from the date of its receipt. When it is not possible to resolve the claim within said term, the interested party shall be informed of the reasons for the delay and the date by when the claim shall be answered, which under no circumstances may be longer than five (8) business days following the expiry of the first term.

Revocation of the authorization and/or deletion of the data

At any moment, data owners may request that the BANK delete their personal data and/or revoke the authorization granted for the treatment of them, by submitting a claim in accordance with Article 15 of Law 1581/2012. The request for deletion of the information and revocation of the authorization shall not be fulfilled when the data owner has a legal or contractual duty to remain in the database.

Grievance filed with the Financial Superintendence of Colombia

The data owner or assignee may only escalate a grievance to the Superintendence of Industry and Commerce once it has exhausted the procedure of inquiry or claim with the BANK.

Communication

For the exercise of the rights granted by Law (Law 1581/2012 and other applicable regulations) and if applicable, the email servicioalcliente@bancodebogota.com.co and customer service line are made available to the data owner.

Through this policy, customers and other stakeholders are informed of the use of information and due personal data protection with respect to the nature of the captured information, use of the collected information, use and processing of personal data, in accordance with Law 1581/2012, as well as the possibility to exclude voluntary information, request to access data held by the bank, the capacity to request whether or not the data is transferred to other service providers and update, correct or eliminate data. Moreover, we supervise 100% of our customers' information.

Annex. 1 Customer privacy information

The nature of the information (e.g.: data of customers) captured by the bank:

The information the bank captures is the data customers deliver when acquiring our products, and they are informed of it the moment they accept the processing of their data. See: Purpose of the data in this policy.

The use of the captured information:

This information is in the privacy policy https://www.bancodebogota.com/wps/themes/html/banco-de-bogota/pdf/atencion-al-cliente/ley-1581-2012.pdf, in the section of the purpose of the data, and is complemented in the data use authorization each customer signs or accepts when acquiring any of our products: See: Purpose of the data in this policy.

The possibility of customers deciding upon their collected, used, stored, and processed information, as follows:

The possibility of removing the information and description of the process: this information is in the privacy policy in the section on revoking and/or deleting the data, complemented with the section on communication.

Possibility of requesting access to the Bank's information.

This information is in the privacy policy in the section on consultations.

Possibility of transferring data to service providers.

Customers are informed in the data use authorization they sign or accept when acquiring any of our products. See: Communication in this policy.

Possibility of requesting data to be corrected.

This information can be found in the privacy policy in the section on claims in this policy.

Possibility of requesting data to be eliminated.

This information is in the privacy policy in the section on revoking and/or deleting the data, complemented with the section on communication, in this policy.

How long is information stored in corporate files

The Organic Statute of the Financial System, in article 96, and the Basic Legal Public Notice force Banco de Bogotá to apply the principle of customer knowledge, keep the records corresponding to their information while the contractual relationship is in effect and keep them afterwards for the established time.

Information disclosed to third parties, such as public and private entities.

Customers' information is not shared with third parties outside of the bank's operations.

Percentage of customers whose information is used for other purposes

Customer information is used solely and exclusively for the bank's primary business and is not used for other purposes, so the percentage is 0%.