Republic of Panama
Superintendency of Banks

RULE N.° 1-2022
(dated 24 February 2022)

"Whereby special guidelines for the protection of personal data processed by banks are established"

THE BOARD OF DIRECTORS
in use of its legal powers and,

WHEREAS:

Pursuant to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch re-edited Decree Law 9 dated 26 February 1998 and all its amendments as a consolidated text, and this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Pursuant to Article 5 (2), (3), and (4) of the Banking Law, strengthening and fostering favorable conditions for the development of the Republic of Panama as an international financial center; promoting public trust in the banking system; and safeguarding the judicial balance between the banking system and its clients are objectives of the Superintendency of Banks;

Pursuant to Article 11 (I)(5) of the Banking Law, establishing the administrative interpretation and scope of the legal provisions and regulations on banking matters is among the technical duties of the Board of Directors;

Pursuant to Article 111 of the Banking Law, banks may only release information about their clients or their operations with their clients' consent, unless the information is required by a competent authority in accordance with the law; when banks must supply the information in compliance with laws related to the prevention of money laundering, terrorism financing and related crimes; when the information is supplied to rating agencies for risk analysis or to data processing centers for accounting and operating purposes;

Pursuant to Article 194 (3) of the Banking Law, bank clients shall have the right to strict confidentiality of the information on his/her relationship with the bank and of his/her privacy;

Pursuant to Article 3 of Rule 8-2005, banks are strictly required to keep the privacy of their clients' information, which can only be disclosed with the client's consent and authorization, unless there is a formal request from a competent authority;

Pursuant to Rule 5-2011 on Corporate Governance, the Superintendency of Banks establishes the principles, responsibilities and minimum requirements of the Internal Control System that must be implemented by banks;

Pursuant to Rules 6-2011 on E-banking; 3-2012 on Information Technology Risks; and 11-2018 on Operational Risk, the Superintendency of Banks established the parameters and guidelines for the management and administration of these risks, including the obligation for banks to have an information security management system, aimed at guaranteeing information integrity, confidentiality, and availability;

Pursuant to Article 42 of the Political Constitution of the Republic of Panama, it is recognized as fundamental guarantee the right to access personal information contained public or private databases or records and to require [information] accuracy, protection, and deletion, according to the law. This information may be collected for specific purposes only, with the subject's consent or stipulated by a competent authority based on the provisions of the law;

Pursuant to the issuance of Law 81, dated 26 March 2019, the Legislative Branch regulated the personal data protection in the Republic of Panama, establishing its entry into force as of 29 March 2021;

Pursuant to Law 81, dated 26 March 2019, the principles, rights, obligations, and other procedures that regulate personal data protection by natural and legal persons who process personal data, are established;

Pursuant to Articles 3 and 5 of Law 81 of 2019, the processing that is expressly regulated by special laws or by their regulations as well as the databases of entities regulated by special laws are exempted from the field of application, provided that they establish the minimum technical standards necessary for the correct personal data protection and processing;

Pursuant to Article 7 of Law 81 of 2019, the entity responsible for processing personal data stored in databases must comply with the minimum requirements of privacy policy, protocols, processes, and procedures for management, processing and secure transmission established by the regulatory body of each sector, in accordance with the cited Law;

Pursuant to Executive Decree 285, dated 28 May 2021, Law 81 of 2019 on Personal Data Protection is regulated;

Pursuant to Article 1 of Executive Decree 285 of 2021, it is established that, in the case of entities regulated by special laws, these special laws must regulate the special data processing requirements indicated therein, as well as the requirements of privacy policies, protocols, processes, and procedures for processing and secure transmission to complement and expand the provisions of Law 81 of 2019 and its regulations;

At on-boarding or from the beginning of the contractual relationship with clients and throughout it, banks collect, store, and use an important amount of clients' personal data, manually, automatically, or electronically which are necessary for the duly operation and daily management of the banking business;

Considering the special nature and character of banking operations and the different types of risks to which banks are exposed, it is fundamental to develop a special regulation that establishes the minimum parameters for processing and safekeeping personal data that banks must comply with, aimed at allowing the proper protection of clients' personal data and the exercise of the banking business;

The provisions enshrined in Law 81 of 2019 and its personal data protection regulations, as well as the guidelines of this Rule, lay the foundations for the development and future implementation of an open financial system, which would foster the conditions for the development of Panama as an international financial center, thereby stimulating the competitiveness of our system;

During its work sessions, the Board of Directors determined it was necessary and advisable to establish special guidelines for the protection of personal data processed by banks, within the regular course of business, in accordance with the provisions of the Banking Law and in compliance with the personal data protection principles, rights and general aspects provided by Law 81 dated 26 March 2019 and Executive Decree 285 dated 28 March 2021, as appropriate.

RESOLVES:

CHAPTER I
GENERAL PROVISIONS

ARTICLE 1. FIELD OF APPLICATION. Pursuant to the personal data protection principles, rights, and general obligations and the powers granted by the Personal Data Protection Law, the personal data protection provisions set herein shall be applied to the banks established in the Republic of Panama.

ARTICLE 2. PURPOSE. The purpose of this Rule is to establish the protocols, processes, procedures, mechanisms, and other special rules related to processing, transmitting and

safekeeping of personal databases, as well as the guidelines for the exercise of personal data protection rights that banks must follow as controllers of their clients' personal data.

ARTICLE 3. SCOPE. The special personal data protection guidelines provided herein are minimal and will be applied to the client's personal data processed by banks, resulting from the provision of a service, the supply of a banking product and, overall, as a result of their banking operations.

Client's Personal data will be protected regardless of the client's nationality, residence or domicile and the method or ways of processing by the bank.

The provisions herein extend to the processing of personal data processed by a data custodian and a banking service provider who, by virtue of an outsourcing contract or other relationship with the bank, have access to or are directly or indirectly, totally or partially, involved in processing the client's personal data.

It will be the bank's responsibility to ensure that the data custodian and the banking service provider comply with the minimum personal data protection principles and standards established herein, when handling and processing personal data.

PROVISO: The provisions established herein will be applicable in conjunction with the parameters and guidelines that the banking regime established on processing, securing, and general management of the client's information.

Any provision related to the processing of personal data that is not expressly provided for in the banking regime, and in other special laws related to data processing, will be subject to the general provisions contained in the personal data protection regime insofar as to its general principles and the exercise of the client's fundamental rights, provided that these do not prevent or obstruct the proper exercise of banking activity and the fashion in which the bank identifies, monitors, mitigates, and manages its risks.

ARTICLE 4. TERMS AND DEFINITIONS. For the purposes of applying the provisions contained herein and without limiting those defined by Law 81 of 2019 and its regulations, the following glossary is established:

1. **Data storage:** The record or custody of the client's personal data in a database established in any provided means, including information technology and communication by a bank or a data custodian.

2. **Privacy notice:** Any communication produced by the bank, through physical or electronic means, addressed to the client for processing his/her personal data, through which he/she is informed about the existence and main features of processing to which his/her personal data will be subjected, how to access them, the purposes of processing that is intended to be given to his/her personal data and other elements that allow the client to be informed, at the time of obtaining his/her data, about the purposes of the processing of his/her personal data.

3. **Database:** An ordered set of personal data of any nature, whatever the form or modality of its creation, organization or storage, which allows the client's data to be related to each other, as well as to carry out any type of processing or transmission by the custodian.

4. **Client:** Any natural person who owns the personal data, who acquires a banking service or a lending or deposit product, or who is at the on-boarding phase of acquiring a banking service or product (potential client). The concept of banking consumer is included in this term.

5. **Consent:** The expression of the free, specific, informed, and unequivocal will of the data subject, through which the processing of these is conducted.

6. **Data custodian:** Any natural or legal person, public or private, for profit or not, who acts in the name and on behalf of the bank responsible for processing the client's personal data and who is responsible for the custody and safeguarding of the database.

7. **Personal data:** Any information concerning the client that identifies him/her or makes him/her identifiable.

8. **ARCO Rights:** Basic inalienable rights of data subjects identified as: right of access, to rectification, to erasure, to object, and to data portability, in accordance with the terms defined in the Personal Data Protection regime.

9. **Technical specifications:** Document containing the records, protocols, and rules related to personal data storage and processing; for the purposes of this Rule it is understood as the policies and procedures adopted by the bank to comply with the personal data protection provisions referred to in Section II of chapter IV herein.

10. **Banking service provider:** Any natural or legal person, other than the data custodian, contracted by the bank to develop and carry out activities, functions, or processes related to the banking business and who is involved in personal data processing.

11. **Banking Regime:** For the purposes of this Rule, it includes the Banking Law, the Rules and the Resolutions that develop it, including this Rule.

12. **Personal Data Protection Regime:** For the purposes of this rule, it comprises Law 81 of 2019 and Executive Decree 285 of 2021 and their respective amendments.

13. **Controller:** Any bank authorized by the Superintendency to engage in the banking business, who is responsible for any decisions related to processing personal data and who determines the purpose, means, scope, and issues related to them.

14. **Data subject:** Any natural person to whom the personal data refers.

15. **Data processing:** Any operation or set of operations or technical procedures which is performed on personal data, whether or not by automated means, which allow data collection, storage, recording, organization, selection, retrieval, use, confrontation, interconnection, association, dissociation, communication, assignment, exchange, transfer, transmission, erasure.

CHAPTER II
PERSONAL DATA PROTECTION PRINCIPLES AND RIGHTS

SECTION I
PRINCIPLES

ARTICLE 5. PERSONAL DATA PROTECTION GENERAL PRINCIPLES. Banks, as personal data controllers, must observe and apply the personal data protection general principles during the daily processing of the client's personal data, which consists of: fairness, purpose, proportionality, truthfulness, accuracy, data security, transparency, confidentiality, lawfulness, and portability established in the Personal Data Protection Regime.

These principles must be understood from the design and marketing phase of banking products and services, during the term of the contractual relationship and until the legal obligation to preserve them persists, in accordance with the provisions of the Banking Regime for each case and other special laws.

ARTICLE 6. PRINCIPLE OF TRANSPARENCY. The bank, at the client's request, will report on the flow of information that it maintains in its database regarding his/her personal data, to facilitate and guarantee by any means (physical or electronic) the due exercise of the rights of access, to rectification, to erasure, to object, and to data portability (ARCO, for its acronym in Spanish) recognized in the Personal Data Protection Regime.

Similarly, at the time of obtaining personal data, the bank must take the appropriate measures to provide the client or his/her representative, free of charge and by any physical or electronic means, all the information indicated in Articles 14 and 15 of Executive Decree 285 of 2021.

Likewise, the bank must facilitate the communication mechanisms that allow the client to access the information required through the exercise of his/her ARCO rights.

PROVISO: Notwithstanding the personal data provisions of this article, banks must also ensure that they comply with the provisions of Article 194 (1) of the Banking Law with regard to the client's right to know in a clear and truthful manner and free of charge the information related to a banking product or service.

ARTICLE 7. PRINCIPLE OF LAWFULNESS THROUGH CONSENT. It is a basic element of personal data protection by means of which the bank obtains the free, express, precise, prior, informed, and unequivocal consent of the data subject for personal data processing and custody, as well as the transmission of these data while its legal preservation obligation persists, except for the conditions of lawfulness of processing indicated herein.

For such purposes, the banks will take into consideration the following aspects when obtaining the client's consent:

1. **Free.** There must be no error, mala fides, violence, intimidation, fraud, or any other condition that may affect or corrupt the data subject's will;

2. **Specific.** It must refer to one or several specific and defined purposes that justify processing;

3. **Informed.** The client must be kept informed by any means, prior to processing personal data, with the information referred to in Article 14 of Executive Decree 285 of 2021.

   Likewise, when the data has not been obtained directly from the client, data subject, the client must be informed in the first communication, in accordance with the provisions of Article 15 of Executive Decree 285 of 2021;

4. **Unequivocal.** It must be granted by any means or through the client's unequivocal behavior in such a way that its granting can be unequivocally demonstrated and that it allows subsequent consultation.

The conditions and other elements for processing personal data will be governed by the provisions of Article 10 herein.

SECTION II
ARCO RIGHTS

ARTICLE 8. ARCO RIGHTS OF THE DATA SUBJECT. ARCO rights are basic inalienable rights of data subjects, which includes the right of access, to rectification, to erasure, to object, and to data portability. Banks must ensure that all client information that is processed and stored in their databases allows the full exercise of ARCO rights at all times, independently, by physical or electronic means, without requiring one [right] for the exercise of the other or that the exercise of one [right] excludes the other.

Any client or his/her authorized representative, regardless of the type of related or linked banking product or service, may request the bank, at any time, the access, rectification, erasure, objection, or portability of his/her personal data collected, stored or kept in the bank's database as personal data controller, without prejudice to the limitations set forth in Article 31 of Executive Decree 285 of 2021 and those established in Article 9 herein.

The bank must develop and offer simple, accessible, and free mechanisms that allow the full and effective exercise of data protection rights by clients. Likewise, the bank must ensure that it meets the request made within the time established herein.

Once the request bas been made by the client or his/her authorized representative, in which the action to be conducted (ARCO right required) is indicated, the specific data to which it refers, and any information that the bank solicits to respond the request effectively, the bank must respond to it within the corresponding terms established by the Personal Data Protection Regime.

ARTICLE 9. EXERCISE OF ARCO RIGHTS. In compliance with the provisions of Law 81 of 2019, the bank must take into consideration the aspects contained herein, for the exercise of ARCO rights.

1. **RIGHT OF ACCESS.** The client shall have the right to obtain from the bank a confirmation as to whether or not the personal data concerning him/her is being processed and to know and verify its correct processing in accordance with the provisions of the Personal Data Protection Regime and in accordance with the guidelines established in this paragraph.

   1.1. **Supply of information.** In case the client requests information on his/her personal data, the bank must respond to his/her request with the information established in Article 24 of Executive Decree 285 of 2021, including the following aspects:

   a. The purpose of the processing;

   b. The categories of personal data in question;

   c. The recipients or categories of recipients to whom the personal data was or will be disclosed;

   d. The expected term for which the personal data will be stored, or, if not possible, the criteria used to determine this term;

   e. The right to request rectification or erasure of personal data or to object to such processing or to data portability;

   f. If the personal data has not been obtained from the data subject, any information about his/her origin;

   g. The existence of automated decision-making, including profiling, referred to in Law 81 of 2019. In such case, meaningful information about the logic involved, as well as the significance and the expected consequences of such processing for the data subject.

   The obligation to provide information will be considered fulfilled when the requested information is communicated or made available to the client or when a personal data remote, direct, and secure access system that permanently guarantees access to information is provided. In the case of personal data remote access systems, they must allow access to the information at no cost.

   Banks must have mechanisms in place that allow the transmission of information by physical or electronic means, in an accurate, precise, and understandable manner.

   1.2. **Non-application to the right of access.** The right of access will not be applicable in the following cases:

   a. When the requesting party is not the data subject, or if the representative is not duly authorized to do so;

   b. When the client’s personal data is not stored in the bank’s or the custodian’s database;

   c. When any of the limitations established in Article 31 of Executive Decree 285 of 2021 is set, as well as in any other legal provision or regulation that develops it, when applicable.

   Banks must have efficient mechanisms in place that allow communication with the requesting party about the denial or non-feasibility to access to the information requested and the grounds on which the denial or non-feasibility is based.

2. **RIGHT TO RECTIFICATION.** The client shall have the right to request and obtain from the bank the rectification of the personal data that is included in its databases, when the information is incorrect, irrelevant, incomplete, outdated, inaccurate, false, or impertinent.

   Once the client or his/her authorized representative has submitted the request indicating the specific data to which he/she refers and the rectification to be conducted, and

provided that the documentation that supports the inaccuracy of the data is attached, the bank shall proceed to its rectification.

The bank may apply reasonable measures to rectify the personal data without the client's request when there is proof of the data inaccuracy in accordance with the principle of accuracy.

The right to rectification will not be applicable in the following cases:

a. When any of the limitations established in Article 31 of Executive Decree 285 of 2021 is set, as well as in any other legal provision or regulation that develops it, when applicable.

b. When the rectification has been previously made.

3. RIGHT TO ERASURE. The client shall have the right to obtain from the bank the erasure of the personal data that is included in its databases, when the information is incorrect, irrelevant, incomplete, outdated, inaccurate, false, or impertinent.

3.1. Feasibility of erasure. For the fulfillment of the right to erasure, banks must abide by the grounds established in Article 27 of Executive Decree 285 of 2021, as well as those established in this paragraph, which includes the following:

a. When the personal data has been unlawfully processed;

b. When the personal data is no longer necessary regarding the purposes for which it was collected or processed;

c. When the client withdraws the consent on which the processing is based, and the processing is not based on another legal ground;

d. When the client objects to the processing and other lawful grounds for processing do not prevail;

e. When the personal data must be erased to comply with a legal obligation that applies to the controller;

f. When the operation with the potential client is not consummated or concluded;

g. When the contractual relationship with the client has been terminated or fulfilled and the legal term for its preservation has elapsed as established by current laws and regulations.

For the purposes of the request to which this paragraph refers, the client must indicate in his/her erasure request, the piece of personal data to which he/she refers, when appropriate.

3.2. Non-feasibility of erasure. Without prejudice to the exceptions established in Article 28 of Executive Decree 285 of 2021, the right to erasure will be applicable in the following circumstances:

a. When the personal data must be kept or processed for the fulfillment of a banking provision or other legal provision;

b. When the legal term for its preservation has elapsed, there is a special provision that establishes another legal term of preservation;

c. When the legal term for its preservation has elapsed, there is the bank's lawful interest to preserve the personal data;

d. Any other circumstance that based on a lawful ground requires its preservation, provided that the data subject's rights do not prevail;

e. When any of the limitations established in Article 31 of Executive Decree 285 of 2021 is set, as well as in any other legal provision or regulation that develops it, when applicable;

f. When the erasure has been previously made.

4. RIGHT TO OBJECT. The client shall have the right to object or refuse to provide his/her personal data or for certain data to be processed, in accordance with the provisions established in the Personal Data Protection Regime and in accordance with the guidelines established in this paragraph.

4.1. Feasibility to object. For the fulfillment of the right to object, banks must abide by the grounds established in Article 29 of Executive Decree 285 of 2021, as well as those established in this paragraph, which includes the following:

a. When the data is processed for purposes other than the one determined or is incompatible with them;

b. When the processing has marketing purposes;

c. When the data is not necessarily related to the operation, service, or product to be provided or does not correspond to regulatory requirements.

4.2. Non-feasibility to object. In addition to the provisions of Article 29 of Executive Decree 285 of 2021, the right to object will not be applicable in the following cases:

a. When the information is necessary for the execution of a contract and the banking services related to it;

b. Other cases provided by law or banking regulation;

c. When any of the limitations established in Article 31 of Executive Decree 285 of 2021 is set, as well as in any other legal provision or regulation that develops it, when applicable.

If the right to object is appropriate, the bank will not be able to process the data related to the data subject.

In the event that the client withdraws his/her consent to processing or to a certain processing, the bank must stop processing the personal data, unless there is a lawful condition or ground for the processing that prevails over his/her right to object.

The withdrawal of consent by the client or his/her representative will not have retroactive effects and will not affect the lawful processing based on prior consent.

5. RIGHT TO PORTABILITY. The client shall have the right to receive or obtain a copy of his/her personal data that he/she has provided to the bank or that is subject to processing, in a structured, generic, commonly used, and machine-readable format, to be used by him/herself or for the bank to transmit this data to other controllers. Likewise, the client shall have the right to have the personal data transmitted directly to him/her or that the controller transmits them directly to other controller when it is technically possible through secure, interoperable means.

5.1. Feasibility to portability. For the fulfillment of the right to portability, banks must abide by the grounds established in Article 30 of Executive Decree 285 of 2021, as well as those established in this paragraph, which includes the following:

a. The client has provided his/her data directly to the controller;

b. The data processing is conducted through automated means, i.e. electronical or technological means;

c. It is a significant amount of data;

d. The client has given his/her consent for the data processing or it is based on a contract.

5.2. Non-feasibility to portability. In addition to the provisions of Article 30 of Executive Decree 285 of 2021, the right to portability will not be applicable in the following cases:

a. It is information inferred, derived, created, produced, or obtained from the analysis or processing conducted by the bank based on the personal data provided by the client;

b. When it affects the rights of third parties and the rights and freedoms of other data subjects.

Banks must have mechanisms in place so that personal data can be provided in interoperable formats that allow data portability and, ensuring that personal data transmitted through said systems are subject to the information required by the client. The Superintendent will establish the minimum standards required to ensure personal data portability.

CHAPTER III
PERSONAL DATA PROCESSING

ARTICLE 10. CONDITIONS AND FORMALITIES FOR PROCESSING. All personal data processing conducted by the bank will be subject to the prior, informed, and unequivocal consent of the data subject or his/her authorized representative, unless for the exceptions provided for herein, the Personal Data Protection Regime and other special laws.

When the processing is based on consent, it must be expressed in writing, or by any other electronic means that guarantees the data subject's identity in such a way that there is certainty about the identity that identifies him/her or makes him/her identifiable. If the consent is obtained through electronic mans, the bank must ensure that it complies with the requirements established in the Banking Rules and the special laws on the matter.

Banks will have the appropriate means and procedures in place for the effective and efficient granting of consent, which will be easily understood, accessible, free of charge, and duly identified.

If the client's consent is given in the context of a written statement that also refers to other matters or for several purposes, it will be necessary for the consent to be clearly distinguished from the other matters or purposes, in an understandable manner, easily accessible, and using clear and simple language, in order to record the consent granted for each.

The execution of the contract or the provision of a service may not be conditioned to the processing of personal data for purposes other than those determined in the client's contractual or at-onboarding relationship.

Any subsequent processing for different purposes that are not compatible or similar the originally established purposes will require the client's awareness and consent, except those based on lawful interest.

PROVISO 1. Banks must ensure that they have mechanisms in place that allow them to demonstrate with certainty the consent granted by the client and that it has been properly granted for the processing of his/her personal data.

PROVISO 2. The consent obtained by electronic or technological means must meet the requirements for its validity and other security controls established in Banking Rules.

If the gathering of the client information is obtained through the bank's electronic channels, the information referred to in Article 14 of Executive Decree 285 of 2021 may be provided or completed through the privacy notice or the terms of use of the service(s) or product(s) offered.

ARTICLE 11. PRIVACY NOTICE. The bank, at the time of obtaining personal data directly from the client through electronic channels, must provide all the information that is collected from it and

the purposes of personal data processing, through the privacy notice or the terms of use of the service(s) or product(s) offered.

In addition to the information indicated in Article 14 of Executive Decree 285 of 2021, the bank must ensure that the privacy notice contains the following information:

1. A description of the type of information that will be collected and processed;

2. The cases or grounds on which the client's personal data would be shared with third parties and the purpose of such transmission;

3. Report the security mechanisms used by the bank to protect the personal data collected;

4. An indication of the validity period of the information established in the privacy notice. Also indicate the procedure for its modification;

5. An indication of the claim mechanisms to file any query related to the users' data processing and the contact addresses in the entity that can respond any query related to the users' data processing;

6. The right to lodge claims with the Superintendency of Banks.

The privacy notice must consider the characteristics of the data processing conducted for each type of banking service or product offered. In all cases, the bank must ensure that the privacy notice contains the minimum information indicated above and that it is provided to the client in the forms and terms indicated in Articles 15 and 16 of Executive Decree 285 of 2021.

ARTICLE 12. PERSONAL DATA OBTAINED FROM OTHER SOURCES. Personal data must be collected without deception or falsehood and without using fraudulent, unfair, or unlawful means. In those cases where the source for obtaining the personal data comes from another controller domiciled in the Republic of Panama, the bank receiving the data must ensure that the client has given his/her prior consent for such purposes. If the information comes from or is collected from public sources or is accessible in public media, the client's authorization or consent will not be required for the processing of his/her data.

For the purposes of the provisions herein, personal data information the bank has obtained from public access sources, whether traditional or digital media such as social networks (e.g. Twitter, Facebook, Instagram, among others), will be included within the consideration of public access sources.

ARTICLE 13. PROCESSING THAT DO NOT REQUIRE CONSENT. Banks will not require the client's consent or authorization for processing personal data on the grounds provided in Article 111 of the Banking Law and the Rules that develop it.

Additionally, in compliance with Article 8 of Law 81 of 2019 and Article 17 of Executive Decree 285 dated 28 May 2021, authorization or consent will not be required for processing personal data in the following cases:

1. For those processing of a banking nature that have prior consent;

2. When necessary for the application and execution of banking contracts in which the client is a party or has an interest;

3. For those processing whose purpose is to preserve the people's safety and the bank's facilities;

4. When the processing is necessary for the proper administration and management of the different banking risks;

5. When necessary to comply with requirements or obligations required by banking regulations;

6. When the data is used or shared by the bank with the bank holding company, subsidiaries, or another company of the banking group for discharging the functions of the banking entity, if it is not for marketing purposes;

7. When data processing is necessary to comply with the requirements established by the Superintendency of Banks for the exchange of information with other financial supervisory bodies;

8. When the processing is based on the bank's lawful interest derived from the existing relationship or bond with the client, because of a banking product or service;

9. When the processing is necessary for the transmission, communication or interconnection of personal data to a data custodian, a banking service provider or third parties for the management of the Bank-Client contractual relationship, provided that it is related to the provision of a banking product or service and marketing;

10. The other processing established by the Law and the regulations that develop it.

PROVISO 1. Sending advertising, commercial or marketing communications of banking products and services or similar information to the client will require the client's prior, informed, and unequivocal consent.

PROVISO 2. When data processing is based on the bank's lawful interest, the bank must evaluate the feasibility of carrying out the processing under this legal basis.

ARTICLE 14. DATA CUSTODIANS. Banks must have policies and procedures in place that ensure that data custodians comply with the obligations and have the minimum personal data protection-related standards referred to in Articles 47, 48, and 49 of Executive Decree 285 of 2021.

For such purposes, banks must ensure that all data processing performed by data custodians is carried out in accordance with the conditions established in the signed contract.

The banks that hire data custodian services will maintain responsibility for personal data processing.

Data custodians must have sufficient specialized knowledge, mechanisms, and resources to ensure compliance with the technical and security requirements that guarantee personal data integrity and confidentiality, in accordance with the standards and principles established herein and in other banking rules related to the matter.

ARTICLE 15. TRANSMISSION RECORDS. In accordance with the guidelines established in Article 31 of Law 81 of 2019, banks must keep and preserve a logbook of personal data transmitted to third parties, including banking service providers, as defined herein. Likewise, the bank must ensure that the data custodian has a logbook of data transmitted to third parties, when the signed contract so allows.

Banks will keep said logbook up to date, so that the information responds to the historical processing carried out.

For the purposes of this Rule, the data that is transmitted by the bank to data custodians will not be considered a data transmission to third parties.

ARTICLE 16. PERSONAL DATA RECORDKEEPING. The personal data processed during the exercise of the banking business must be kept in a database that allows preserving the confidentiality, integrity, availability, and, in general, the secure handling of information. Likewise, they must be kept for the time that the Banking Rules or a special law provide for each case.

Once the legal term of personal data preservation has expired, banks must ensure that they do not transmit or communicate said data within the seven (7) -year period established by Article 28 of Law 81 of 2019, unless the client requests otherwise.

The bank must maintain the confidentiality of the processing and the information stored in the database, even after the end of its relationship with the data subject, except in cases that are relieved from it by legal provision.

CHAPTER IV
PERSONAL DATA MANAGEMENT

SECTION I
RESPONSIBILITIES

ARTICLE 17. INTERNAL CONTROL SYSTEM. To comply with the provisions established herein, banks must ensure that they apply the guidelines included in the rule on Corporate Governance, issued by the Superintendency, regarding the Internal Control System.

ARTICLE 18. BOARD OF DIRECTORS RESPONSIBILITIES. Without prejudice to the responsibilities established in the Personal Data Protection Regime, in terms of personal data protection, the banks, through the board of directors, will have the following responsibilities:

1. Establish and ensure that an appropriate organizational and operational structure is maintained for powers delegation and functions segregation that guarantees the application of personal data protection principles and rights throughout the entire organization;

2. Approve the necessary resources for the adequate development of personal data protection measures established in Law 81 of 2019 and the regulations that develop it;

3. Approve the policies and procedures the entity will implement to comply with the regulatory obligations related to personal data protection;

4. Approve data protection training, updating and accreditation programs;

5. Promote a personal data protection culture at all organizational levels, extensive to data custodians and banking service providers;

6. Approve the procedures to receive and respond to data subject requests and claims.

ARTICLE 19. COMPLIANCE CERTIFICATE ISSUED BY THE BOARD OF DIRECTORS. Annually, the bank will submit to the Superintendency a certificate, signed by the chairman and secretary on behalf of the board of directors, stating that:

a. The board of directors knows the standards included in the Personal Data Protection Regime and the provisions established herein;

b. The bank has the policies and procedures in place for personal data protection management;

c. The board of directors has been made aware of the effectiveness of the personal data protection measures implemented by the bank.

Said certificate may be submitted in a joint or individual document and the signatures must be notarized or through a qualified electronic signature. This certificate will be signed and submitted within sixty (60) days following the fiscal closing.

In the case of banks that are branch offices of foreign banks, the compliance certificate established herein may be proven through an annual certificate issued by the unit responsible for personal data management at the parent company or its equivalent position, in which it is certified that the bank has policies in place for personal data protection that are similar or greater than that provided for in local personal data protection regulations. This certificate must be sent to the Superintendency of Banks within the term indicated above.

ARTICLE 20. RISK MANAGEMENT UNIT. The Risk Management Unit must identify, assess, and control the risks inherent to personal data protection, for the fulfillment of the responsibilities established in the risk management regulations.

ARTICLE 21. INTERNAL AUDIT AND MONITORING OF THE INTERNAL CONTROL SYSTEM. In accordance with the provisions established in the Rule on Corporate Governance, the Internal Audit Unit is responsible for monitoring the Internal Control System.

For such purposes, said Unit will evaluate compliance with the policies and procedures used for personal data protection, in accordance with the provisions established in the Personal Data Protection Regime and this Rule. Likewise, the Unit must ensure that it evaluates the effectiveness of the controls implemented to mitigate the risks threatening personal data.

ARTICLE 22. DATA PROTECTION OFFICER. Banks must designate a Data Protection Officer, within their organizational structure, who, according to the size and sophistication of their activities, operations, services, and the type, volume and means of the data processed, allows him/her to adequately manage the functions assigned by the Personal Data Protection Regime and this Rule.

For such purposes, the designated Data Protection Officer will perform his/her duties independently, having a direct communication with the Top Management or Senior Management, as a decision-making body. Similarly, the designated Data Protection Officer must maintain the confidentiality of the information obtained during the performance of his/her duties.

The Data Protection Officer must have professional experience in areas related to the banking or financial sector, in terms of data protection, whose appointment or replacement must be previously notified to the Superintendency of Banks.

The bank must grant the Data Protection Officer sufficient authority, hierarchy, independence within the organization, and provide him/her with the necessary resources to guarantee the performance of his/her duties and his/her participation in all personal data protection-related matters.

The Data Protection Officer must inform the Board of Directors or the Committee designated to deal with these matters, on the effectiveness of programs, measures, implemented controls, and compliance with the regulatory personal data protection requirements.

PROVISO. To ensure the Data Protection Officer's independence within the organization, the bank must ensure that the hierarchy and independence of the position is evidenced within its organizational structure.

ARTICLE 23. DATA PROTECTION OFFICER FUNCTIONS. In addition to the functions established in Article 44 of Executive Decree 285 of 2021, the Data Protection Officer will have the following functions:

1. Keep a logbook of any event that affects the protection of personal data processed by the bank;

2. Report any deficiency detected in personal data protection measures to the Top Management or Senior Management, to the Risk Management Unit and the Internal Audit Unit;

3. Coordinate with the Information Security area the security breaches that affect personal data protection;

4. Provide suggestions regarding the corrective measures that can be implemented to remedy the deficiencies found in personal data processing;

5. Maintain communication with the Risk, Internal Audit, and Compliance areas to identify the necessary improvements in personal data protection controls;

6. Assist together with the person responsible for the Information Security area in dealing with security breaches that affect personal data processing;

7. To be the liaison party with the Superintendency of Banks in matters related to personal data processing;

8. Coordinate the personal data protection annual training program;

9. To be the liaison party with the data subject, notwithstanding that administratively, when applicable, he/she can be supported by the Claims Management System Officer.

PROVISO. The Data Protection Officer may perform other functions within the organization, if these functions do not represent incompatibilities with the functions established herein and do not breach the independence of his/her functions. Incompatible functions will be considered those that, within the Bank's structure, are conducted by the Internal Audit, Risk, and Compliance areas, within which the Data Protection Officer may not be an employee.

SECTION II
PERSONAL DATA PROCESSING AND TRANSMISSION

ARTICLE 24. PERSONAL DATA PROCESSING POLICIES. Banks must establish and document the procedures and processes for the inclusion, preservation, storage, modification, erasure, transmission, and any other personal data processing action, based on the personal data protection standards and the personal data processing policies adopted by the entity and approved by its board of directors. The foregoing shall be understood as the technical file referred to in Law 81 of 2019.

The internal policies or technical files adopted by the bank must include the measures adopted by the entity to comply with the personal data protection principles, rights, and obligations from the design of the services and products. Said measures may include the application of dissociation measures to the data or any other measure that allows reducing the risks inherent to processing.

ARTICLE 25. SECURITY OF PERSONAL DATA PROCESSING. Banks must ensure that they apply the provisions established in the Rule on Information Technology Risk Management and the Rule on E-Banking, issued by the Superintendency of Banks, for processing and transmitting personal data.

ARTICLE 26. PERSONAL DATA BREACH. Banks shall inform the data subject of any detected personal data breach, involving damage, loss, alteration, destruction, access, and, in general, any unlawful or unauthorized use of the personal data that affects it significantly.

Likewise, the bank's Information Security Officer must communicate said breach to the Superintendency of Banks, following the guidelines established in that regard in the Rules on E-Banking and Information Technology Risk Management.

The obligation established herein extends to the Data Custodian, for which the Bank must ensure that communication protocols for such purposes are in place.

CHAPTER V
FINAL PROVISIONS

ARTICLE 27. CLAIMS LODGE WITH THE SUPERINTENDENCY. The data subject who deems the exercise of ARCO rights breached may submit to the bank responsible for data processing any request, claim, complaint, and dispute related to personal data protection, which will be processed through the Data Protection Officer or the employee designated by the bank for such purposes.

If the bank does not comply with the request concerning the exercise of ARCO rights or the client is dissatisfied with the decision made by the bank, the client may file a claim with the Superintendency of Banks. For such purposes, the client will have a 30-calendar day period, from the date on which he/she received a formal response from the bank or when the bank has not complied with resolving the request or claim within the corresponding period.

Banks must make available to the client the means and simplified forms of communication that they deem appropriate to facilitate the exercise of the client's rights and respond to or provide the requested information.

The claims lodge with the Superintendency of Banks will be subject to the procedures and resources established in the Banking Law and in the Banking Rules related to the matter. Once the Resolution that resolves the process filed with the Superintendency has been communicated and executed, the governmental channels will be understood to be exhausted, without prejudice to the corresponding resources in the adversarial channels.

PROVISO. In accordance with the provisions of Article 18 of Law 81 of 2019, the data subject may only lodge complaints with the National Authority for Transparency and Access to Information (ANTAI, for its acronym in Spanish) in the event that after lodging the claim with the Superintendency of Banks, it does not issue a statement based on the corresponding administrative process.

ARTICLE 28. MONITORING, CONTROL, AND SUPERVISION PROCEDURE. The Superintendency of Banks may request and verify compliance with the principles and the appropriate technical, organizational, and internal security measures for personal data protection established herein and in other related regulations, to guarantee that banks comply with the principles and standards for the protection of personal data subject to processing.

Banks must make available to the Superintendency of Banks all the information it deems necessary for proper supervision of compliance with the provisions contained herein.

ARTICLE 29. SANCTIONS. In case of non-compliance with the provisions contained herein and the Personal Data Protection Regime, the Superintendency will apply the corresponding sanctions in accordance with the amounts and severity of the offenses established in Law 81 of 2019 subject to the sanctioning administrative procedure established by means of Rule 12-2015. The foregoing is without prejudice to the application of the sanctions established in Title IV of the Banking Law, for banking confidentiality breaches, related to disclosing client information without his/her consent.

ARTICLE 30. EFFECTIVE DATE. The provisions of this Rule shall take effect upon its signature. Notwithstanding the foregoing, the provisions established in Articles 22 and 23 will have an adaptation term of twelve (12) months from the signing of this Rule.

Given at Panama City this twenty-fourth (24th) day of February, two thousand twenty-two (2022).

FOR COMMUNICATION, PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN, **THE SECRETARY,**

Rafael Guardia Pérez Felipe Echandi