República de Panamá
Superintendencia de Bancos

ACUERDO No. 001-2022
(24 de febrero de 2022)

"Que establece lineamientos especiales para la protección de datos personales tratados por las entidades bancarias"

LA JUNTA DIRECTIVA
en uso de sus facultades legales, y

CONSIDERANDO

Que a raíz de la emisión del Decreto Ley No. 2 de 22 de febrero de 2008, el Órgano Ejecutivo elaboró una ordenación sistemática en forma de texto único del Decreto Ley No. 9 de 26 de febrero de 1998 y todas sus modificaciones, la cual fue aprobada mediante el Decreto Ejecutivo No. 52 de 30 de abril de 2008, en adelante la Ley Bancaria;

Que de conformidad con los numerales 2, 3 y 4 del artículo 5 de la Ley Bancaria, son objetivos de la Superintendencia de Bancos fortalecer y fomentar las condiciones propicias para el desarrollo de la República de Panamá como centro financiero internacional; así como promover la confianza pública en el sistema bancario y, velar por el equilibrio entre el sistema bancario y sus clientes;

Que de conformidad con el numeral 5 del artículo 11 de la Ley Bancaria, son atribuciones de carácter técnico de la Junta Directiva, fijar en el ámbito administrativo, la interpretación y alcance de las disposiciones legales o reglamentarias en materia bancaria;

Que de conformidad con el artículo 111 de la Ley Bancaria, los bancos solo podrán divulgar información acerca de sus clientes o de sus operaciones con el consentimiento de estos, salvo que la información fuese requerida por autoridad competente de conformidad con la ley, cuando deban proporcionarla en cumplimiento de las leyes relacionadas con la prevención de los delitos de blanqueo de capitales, financiamiento del terrorismo y delitos relacionados; así como también, cuando sea proporcionada a agencias calificadoras para fines de análisis de riesgo o a agencias u oficinas procesadoras de datos para fines contables y operativos;

Que de conformidad con el numeral 3 del artículo 194 de la Ley Bancaria, corresponde a derechos básicos e irrenunciables del cliente bancario la confidencialidad en lo que respecta a su relación con el banco frente a terceros, así como a su privacidad;

Que el artículo 3 del Acuerdo No. 8-2005 establece la obligación de las entidades bancarias de mantener la confidencialidad de la información de sus clientes, la cual sólo podrá ser divulgada con el consentimiento y autorización del cliente, salvo cuando medie solicitud de autoridad competente;

Que mediante Acuerdo No. 5-2011 sobre Gobierno Corporativo, la Superintendencia de Bancos establece los principios, responsabilidades y requisitos mínimos del Sistema de Control interno que deben implementar las entidades bancarias;

Que mediante los Acuerdos No. 6-2011 sobre Banca Electrónica, Acuerdo No. 3-2012 sobre riesgos de la tecnología de la información y Acuerdo No.11-2018 sobre Riesgo Operativo, la Superintendencia de Bancos estableció los parámetros y lineamientos para la gestión y administración de éstos riesgos, contemplándose la obligación para las entidades bancarias de contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información;

Que el artículo 42 de la Constitución Política de la República de Panamá, reconoce como garantías fundamentales el derecho a acceder a la información personal contenida en bases de datos o registros públicos o privados, y a requerir su rectificación y protección, así como su supresión de conformidad con lo previsto en la ley. Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular, o por disposición de autoridad competente con fundamento en lo previsto en la ley;

Que el Órgano Legislativo emitió la Ley No. 81 de 26 de marzo de 2019 que regula la protección de datos personales en la República de Panamá, estableciendo su entrada en vigor a partir del 29 de marzo de 2021;

Que en la citada Ley No. 81 de 26 de marzo de 2019 se establecen los principios, derechos, obligaciones y demás procedimientos que regulan la protección de datos personales por parte de las personas naturales y jurídicas que tratan datos personales;

Que los artículos 3 y 5 de la Ley No. 81 de 2019, establecen que se exceptúan de su ámbito de aplicación aquellos tratamientos que expresamente se encuentren regulados por leyes especiales o por las normativas que lo desarrollan; así como la base de datos de sujetos regulados por leyes especiales, siempre que las mismas establezcan estándares técnicos mínimos necesarios para la correcta protección y tratamiento de datos personales;

Que de conformidad con el artículo 7 de la Ley No. 81 de 2019 el responsable del tratamiento de datos personales contenidos en bases de datos deberá cumplir con los requerimientos mínimos de política de privacidad, protocolos, procesos y procedimientos de gestión, tratamiento y transferencia segura que establezca el regulador de cada sector, conforme a la referida Ley;

Que mediante Decreto Ejecutivo No. 285 de 28 de mayo de 2021 se reglamenta la Ley No. 81 de 2019 sobre Protección de Datos Personales;

Que el artículo 1 del Decreto Ejecutivo No. 285 de 2021, establece que, en el caso de sujetos regulados por leyes especiales, las mismas deberán regular aquellos requisitos especiales de tratamiento de datos que en ella se señalen; así como también los requerimientos de las políticas de privacidad, protocolos, procesos y procedimientos de tratamiento y transferencia segura, con el fin de complementar y ampliar las previsiones de la Ley No. 81 de 2019 y su reglamentación;

Que las entidades bancarias desde del inicio de la relación precontractual o contractual con clientes y a lo largo de la misma, recolectan, almacenan y utilizan un importante cúmulo de datos personales de clientes, de forma manual, automatizada o digital, que son necesarios para la debida operatividad y gestión diaria del negocio de banca;

Que tomando en consideración la naturaleza y el carácter especial de las operaciones bancarias y los diferentes tipos de riesgos al que se encuentran expuestos los bancos, resulta indispensable desarrollar una disposición especial que establezca los parámetros mínimos de tratamiento y custodia de datos personales que deberán cumplir las entidades bancarias, con el propósito de permitir la adecuada protección de los datos personales de los clientes y el ejercicio del negocio de banca;

Que las disposiciones consagradas en la Ley No. 81 de 2019 y su reglamentación vinculada con la protección de datos personales, así como los lineamientos del presente Acuerdo, sientan las bases iniciales para el desarrollo y futura implementación de un sistema financiero abierto, lo cual fomentaría las condiciones para el desarrollo de Panamá como un centro financiero internacional, estimulando con ello la competitividad de nuestro sistema;

Que en sesiones de trabajo de esta Junta Directiva se ha puesto de manifiesto la necesidad y conveniencia de establecer lineamientos especiales para la protección de los datos personales tratados por las entidades bancarias dentro del giro ordinario de sus operaciones, en concordancia con lo dispuesto en el régimen bancario y en seguimiento a los principios, derechos y aspectos generales de protección de datos personales que dispone la Ley No. 81 de 26 de marzo de 2019 y el Decreto Ejecutivo No. 285 de 28 de mayo de 2021, según corresponda.

ACUERDA:

CAPÍTULO I

ASPECTOS GENERALES

ARTÍCULO 1. ÁMBITO DE APLICACIÓN. En seguimiento a los principios, derechos y obligaciones generales sobre protección de datos personales y a las facultades atribuidas en el Régimen de Protección de Datos Personales, las disposiciones sobre protección de datos personales establecidas en el presente Acuerdo serán aplicadas a las entidades bancarias establecidas en la República de Panamá.

ARTÍCULO 2. OBJETIVO. El presente Acuerdo tiene como objetivo establecer los protocolos, procesos, procedimientos, mecanismos y demás reglas especiales relativas al tratamiento, transferencia y custodia de bases de datos personales; así como los lineamientos para el ejercicio de los derechos de protección de datos personales que deberán seguir los bancos, como responsables del tratamiento de los datos personales de sus clientes.

ARTÍCULO 3. ALCANCE. Los lineamientos especiales sobre protección de datos personales dispuestos en el presente Acuerdo son mínimos y serán aplicados a los datos personales del cliente tratados por las entidades bancarias, por motivo de la prestación de un servicio, el suministro de un producto bancario y en general como resultado de sus operaciones bancarias.

La protección de datos personales del cliente será aplicada con independencia de la nacionalidad, residencia o domicilio del cliente y, el medio o las formas de su tratamiento por parte de la entidad bancaria.

Las disposiciones del presente Acuerdo se extienden al tratamiento de los datos personales tratados por un custodio de base de datos y proveedores de servicios bancarios que, en virtud de un contrato de tercerización u otra relación con el banco, tengan acceso o estén involucrados directa o indirectamente, total o parcialmente en el tratamiento de datos personales del cliente.

Será responsabilidad del banco asegurarse que el custodio de la base de datos y proveedores de servicios bancarios cumplan con los principios y estándares mínimos de protección de datos personales establecidos en el presente Acuerdo, cuando administren y lleven a cabo el tratamiento de datos personales.

PARÁGRAFO: Las disposiciones establecidas en el presente Acuerdo serán aplicables en conjunto con los parámetros y lineamientos que, sobre tratamiento, seguridad y manejo en general de la información del cliente, establece el régimen bancario.

Cualquiera disposición vinculada al tratamiento de datos personales que no se encuentre expresamente prevista en el régimen bancario y, en las demás leyes especiales relacionadas en materia de tratamiento de datos, se sujetaran a las disposiciones generales contenidas en el régimen de protección de datos personales en cuanto a sus principios generales y el ejercicio de los derechos fundamentales del cliente, siempre que estas no imposibiliten u obstruyan el debido ejercicio de la actividad bancaria y la forma como el banco, identifica, monitorea, mitiga y gestiona sus riesgos.

ARTÍCULO 4. TÉRMINOS Y DEFINICIONES. Para los efectos de aplicación de las disposiciones contenidas en el presente Acuerdo y sin limitar los definidos por la Ley No. 81 de 2019 y su reglamentación, se establece el siguiente glosario de términos:

1. **Almacenamiento de datos:** Conservación o custodia de los datos personales del cliente en una base de datos establecida en cualquier medio provisto, incluido el de la tecnología de la información y la comunicación por parte de una entidad bancaria o un custodio de bases de datos.

2. **Aviso de privacidad:** Comunicación generada por el banco, a través de medios físicos o digitales, dirigida al cliente para el tratamiento de sus datos personales, mediante la cual se informa, acerca de la existencia y características principales del tratamiento al que serán sometidos sus datos personales, la forma de acceder a los mismos, las finalidades del tratamiento que se pretende dar a los datos personales y demás elementos que le permita al cliente estar informado, al momento de la obtención de sus datos, sobre los propósitos del tratamiento de sus datos personales.

3. **Base de datos:** Conjunto ordenado de datos personales de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos del cliente entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio.

4. **Cliente:** Persona natural titular de los datos personales, que adquiere un servicio o producto bancario, activo o pasivo o aquel que se encuentra en la fase previa de adquisición de un servicio o producto bancario (potencial cliente). Se encuentra comprendido en este término, el concepto de consumidor bancario.

5. **Consentimiento:** Manifestación de la voluntad libre, especifica, informada e inequívoca del titular de los datos, mediante la cual se efectúa el tratamiento de estos.

6. **Custodio de la base de datos:** Persona natural o jurídica, de derecho público o privado, lucrativa o no, que actúa a nombre y por cuenta de la entidad bancaria responsable del tratamiento de los datos personales del cliente y le compete la custodia y conservación de la base de datos.

7. **Dato personal:** Cualquier información concerniente al cliente que lo identifica o lo hace identificable.

8. **Derechos ARCO:** Derechos irrenunciables básicos de los titulares de los datos, identificados como: derecho de acceso, rectificación, cancelación, oposición y portabilidad, de conformidad con los términos definidos en el Régimen de Protección de Datos Personales.

9. **Ficha Técnica:** Documento que contiene los registros, protocolos y reglas relacionados al almacenamiento y tratamiento de los datos personales, entendiéndose para efectos del presente Acuerdo como las políticas y procedimientos adoptadas por el Banco para el cumplimiento de las disposiciones sobre protección de datos personales, a las cuales hace referencia la sección II del capítulo IV de este Acuerdo.

10. **Proveedor de servicios bancarios:** Persona natural o jurídica, distinta del custodio de la base de datos, contratada por el banco para desarrollar y llevar a cabo actividades,

funciones o procesos vinculados con el negocio de banca y que está involucrada en el tratamiento de datos personales.

11. **Régimen Bancario:** Para los efectos de lo dispuesto en el presente Acuerdo comprende la Ley Bancaria, los Acuerdos y Resoluciones que la desarrollan, incluyendo el presente Acuerdo.

12. **Régimen de Protección de Datos Personales:** Para los efectos de lo dispuesto en el presente Acuerdo, comprende la Ley No. 81 de 2019 y el Decreto Ejecutivo No. 285 de 2021 y sus respectivas modificaciones.

13. **Responsable del tratamiento de los datos:** Entidad bancaria autorizada por la Superintendencia para ejercer el negocio de banca, que le corresponde las decisiones relacionadas con el tratamiento de los datos personales y que determina los fines, medios y alcance, así como cuestiones relacionadas con estos.

14. **Titular de los datos:** Persona natural a la que se refieren los datos personales.

15. **Tratamiento de datos**: Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier forma.

CAPÍTULO II

PRINCIPIOS Y DERECHOS PARA LA PROTECCIÓN DE DATOS PERSONALES

SECCIÓN I
LOS PRINCIPIOS

ARTÍCULO 5. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES. Los bancos como responsables del tratamiento de los datos personales deberán observar y aplicar los principios generales de protección de datos personales en el tratamiento diario de los datos personales del cliente que lleven a cabo en sus operaciones, los cuales comprende: principio de lealtad, de finalidad, de proporcionalidad, de veracidad, de exactitud, de seguridad de los datos, de transparencia, de confidencialidad, de licitud y de portabilidad establecidos en el Régimen de Protección de Datos Personales.

Dichos principios deberán estar comprendidos desde la etapa de diseño y comercialización de los productos y servicios bancarios, durante la vigencia de la relación contractual y, hasta tanto persista la obligación legal para su conservación, de conformidad con lo que para cada caso establezca el Régimen Bancario y, demás leyes especiales.

ARTÍCULO 6. PRINCIPIO DE TRANSPARENCIA. El banco, a solicitud del cliente informará sobre el flujo de información que sobre sus datos personales mantenga en su base de datos, a fin de facilitar y garantizar por cualquier medio (físico o digital) el debido ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad (ARCO) reconocidos en el Régimen de Protección de Datos Personales.

De igual manera, al momento de la obtención de los datos personales, el banco deberá tomar las medidas oportunas para facilitar al cliente o a su representante, de forma gratuita y por cualquier medio, físico o digital, toda la información indicada en los artículos 14 y 15 del Decreto Ejecutivo No. 285 de 2021.

Igualmente, el banco deberá facilitar los mecanismos de comunicación que le permitan al cliente acceder a la información requerida a través del ejercicio de sus derechos ARCO.

PARÁGRAFO. Sin perjuicio de lo dispuesto en el presente artículo respecto a los datos personales, las entidades bancarias también deberán asegurarse de dar cumplimiento a lo dispuesto en el numeral 1 del artículo 194 de la Ley Bancaria en lo que respecta al derecho del cliente de conocer de manera clara, veraz y sin costo alguno la información relacionada con un producto o servicio bancario.

ARTÍCULO 7. PRINCIPIO DE LICITUD A TRAVÉS DEL CONSENTIMIENTO. Constituye un elemento básico de protección de datos personales, la obtención por parte del banco del consentimiento libre, expreso, preciso, previo, informado e inequívoco del titular de los datos personales para el tratamiento y custodia de datos personales; así como para la transferencia de dichos datos durante todo el tiempo que persista su obligación legal de conservación, salvo las condiciones de licitud de tratamiento indicadas en el presente Acuerdo.

Para tales efectos, las entidades bancarias tomarán en consideración los siguientes aspectos al momento de obtener el consentimiento por parte del cliente:

1. Libre. No debe mediar error, mala fe, violencia, intimidación, dolo o cualquiera otra condición que pueda afectar o viciar la voluntad del titular de datos;

2. Específico. Se deberá referir a una o varias finalidades determinadas y definidas que justifiquen el tratamiento;

3. Informado. Se debe mantener informado por cualquier medio al cliente, previo al tratamiento de datos personales, con la información a que hace referencia el artículo 14 del Decreto Ejecutivo No. 285 de 2021;

Igualmente, cuando los datos no hayan sido obtenidos directamente del cliente, titular de los datos, se deberá informar al mismo en la primera comunicación, de conformidad con lo dispuesto en el artículo 15 del Decreto Ejecutivo No. 285 de 2021;

4. Inequívoco: Debe otorgarse por cualquier medio o mediante conductas inequívocas del cliente de forma tal que pueda demostrarse de manera indubitable su otorgamiento y que permita su consulta posterior.

Las condiciones y demás elementos para el tratamiento de los datos personales se regirán por las disposiciones establecidas en el artículo 10 del presente Acuerdo.

SECCIÓN II
LOS DERECHOS ARCO

ARTÍCULO 8. DERECHOS ARCO DEL TITULAR DE DATOS PERSONALES. Los derechos ARCO son derechos básicos e irrenunciables reconocidos a los titulares de los datos personales, los cuales comprenden los derechos de acceso, rectificación, cancelación, oposición y portabilidad (ARCO). Las entidades bancarias deberán asegurarse de que toda información del cliente que esté bajo su tratamiento y se mantenga almacenada en su base de datos permita en todo momento el pleno ejercicio de los derechos ARCO, de forma independiente, por medios físicos o digitales, sin que se requiera de uno para el ejercicio de otro derecho o sin que el ejercicio de uno excluya a otro derecho.

Todo cliente o su representante autorizado, independientemente del tipo servicio o producto bancario relacionado o vinculado, podrá solicitar en cualquier momento al banco el acceso,

rectificación, cancelación, oposición y portabilidad de sus datos personales que recabe, almacene o conserve el banco en su base de datos en su calidad de responsable del tratamiento de los datos personales, sin perjuicio de las limitaciones dispuestas en el artículo 31 del Decreto Ejecutivo No. 285 de 2021 y las establecidas en el artículo 9 del presente Acuerdo.

El banco deberá desarrollar y ofrecer mecanismos sencillos, accesibles y gratuitos, que permitan, el pleno y efectivo ejercicio de los derechos de protección de datos por parte de los clientes. Igualmente, el banco deberá asegurarse de atender la solicitud efectuada en el tiempo que establece el presente Acuerdo.

Una vez presentada la solicitud por el cliente o su representante autorizado, en la cual se indique la acción a realizar (derecho ARCO requerido), los datos específicos a que se refiere, y se complete cualquier información que el banco solicite para atender de forma efectiva la solicitud, el banco deberá dar respuesta a la misma dentro los términos correspondientes que establece el Régimen de Protección de Datos Personales.

ARTÍCULO 9. EJERCICIO DE LOS DERECHOS ARCO. En cumplimiento con las disposiciones de la Ley No. 81 de 2019, el banco deberá tomar en consideración los aspectos contemplados en el presente artículo, para el ejercicio de los derechos ARCO.

1. **DERECHO DE ACCESO.** El cliente tendrá derecho a obtener del banco la confirmación de si están o no tratando datos personales que le conciernen y, conocer y verificar su correcto tratamiento de conformidad con las disposiciones de del Régimen de Protección de Datos Personales y de acuerdo con los lineamientos establecidos en el presente numeral.

   1.1. Suministro de información. En el evento que el cliente solicite información sobre sus datos personales, el banco deberá brindarle a su requerimiento la información establecida en el artículo 24 del Decreto Ejecutivo No. 285 de 2021, que comprende los siguientes aspectos:

   a. Los fines del tratamiento;
   b. Las categorías de datos personales de que se trate;
   c. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales;
   d. El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
   e. El derecho al ejercicio de la rectificación o cancelación de datos personales, o a oponerse a dicho tratamiento, o a la portabilidad de los datos;
   f. Si los datos personales no se han obtenido del interesado, cualquier información sobre su origen;
   g. La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere la Ley No. 81 de 2019. En tal caso, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

   La obligación de suministrar información se dará por cumplida cuando se comunique o se pongan a disposición del cliente la información solicitada o bien cuando se facilite un sistema de acceso remoto, directo y seguro de los datos personales que garantice, de forma permanente, el acceso a la información. En caso de sistemas de acceso remoto de datos personales, los mismos deberán permitir el acceso a la información sin costo alguno.

   Los bancos deberán contar con mecanismos que permitan la transmisión de la información por medios físicos o digitales, de forma correcta, precisa y entendible.

   1.2. No aplicación del derecho de Acceso. El derecho de Acceso no aplicará en los siguientes casos:

a. Cuando el solicitante no sea el titular de los datos personales, o el representante no esté debidamente autorizado para ello;
b. Cuando en su base de datos o en la del custodio de la base de datos, no se encuentren los datos personales del cliente;
c. Cuando se configura alguna de las limitaciones establecidas en el artículo 31 del Decreto Ejecutivo No. 285 de 2021, así como en cualquier otra disposición legal o las normas que la desarrollen, cuando apliquen.

Las entidades bancarias deberán contar con mecanismos ágiles que permitan la comunicación al solicitante sobre la denegación o no viabilidad del acceso a la información solicitada y los hechos en que se fundamenta la misma.

2. DERECHO DE RECTIFICACIÓN. El cliente tendrá derecho a solicitar y obtener del banco responsable del tratamiento de los datos la corrección de sus datos personales que se encuentren incluidos en sus bases de datos, cuando los mismos sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

Una vez presentada la solicitud por el cliente o su representante autorizado, en la cual se indiquen los datos específicos a que se refiere y la acción de rectificación a realizar, y siempre que la acompañe con la documentación que sustente la inexactitud de los datos, el banco deberá proceder a su corrección.

El banco podrá aplicar medidas razonables para proceder a la rectificación de los datos personales sin el requerimiento del cliente, cuando exista prueba de la inexactitud de los datos de conformidad con el principio de exactitud.

El derecho de Rectificación no aplicará en los siguientes casos:

a. Cuando se configura alguna de las limitaciones establecidas en el artículo 31 del Decreto Ejecutivo No. 285 de 2021, así como en cualquier otra disposición legal o la norma que la desarrolle, cuando apliquen.
b. Cuando la rectificación haya sido previamente realizada.

3. DERECHO DE CANCELACIÓN. El cliente tendrá derecho a solicitar del banco responsable del tratamiento de los datos la supresión o eliminación de sus datos personales que se encuentren incluidos en sus bases de datos cuando los mismos sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

3.1 Viabilidad de la cancelación. Las entidades bancarias para el cumplimiento del derecho de cancelación deberán sujetarse a los supuestos establecidos en el artículo 27 del Decreto Ejecutivo No. 285 de 2021, así como a los establecidos en el presente numeral, que comprende lo siguiente:

a. Cuando los datos personales hayan sido tratados ilícitamente;
b. Cuando los datos personales ya no sean necesarios en relación con los fines para lo cual fueron recogidos o tratados;
c. Cuando el cliente retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
d. Cuando el cliente se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento;
e. Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.
f. Cuando la operación con el potencial cliente no llegara a perfeccionarse o concluirse;
g. Cuando se haya culminado o cumplido la relación contractual con el cliente y haya transcurrido el plazo legal para su conservación según lo que establecen las leyes y regulaciones vigentes;

Para los efectos de la solicitud a la cual hace referencia el presente numeral, el cliente deberá indicar en su solicitud de cancelación, la información de los datos personales a que se refiere, cuando corresponda.

3.2 No Viabilidad de la Cancelación. Sin perjuicio de las excepciones establecidas en el artículo 28 del Decreto Ejecutivo No. 285 de 2021, el derecho de cancelación no se aplicará en las circunstancias siguientes:

a. Cuando deban ser conservados o tratados para el cumplimiento de una disposición bancaria u otra disposición legal;
b. Cuando transcurrido el plazo legal para su conservación, exista una disposición especial que establezca otro plazo legal de conservación,
c. Cuando transcurrido el plazo legal para su conservación, medie un interés legítimo del banco para su conservación;
d. Cualquiera otra circunstancia que basada en un motivo legítimo requiera de su conservación, siempre que no prevalezca los derechos del titular de datos;
e. Cuando se configura alguna de las limitaciones establecidas en el artículo 31 del Decreto Ejecutivo No. 285 de 2021, así como en cualquier otra disposición legal o la norma que la desarrolle, cuando apliquen.
f. Cuando la cancelación haya sido previamente realizada.

4. DERECHO DE OPOSICIÓN. El cliente tendrá derecho a oponerse o negarse a proporcionar sus datos personales o a que ciertos datos sean objeto de tratamiento, conforme con las disposiciones establecidas en el Régimen de Protección de Datos Personales y de acuerdo con los lineamientos establecidos en el presente numeral.

4.1 Viabilidad de la Oposición. Las entidades bancarias para el cumplimiento del derecho de oposición deberán sujetarse a los supuestos establecidos en el artículo 29 del Decreto Ejecutivo No. 285 de 2021, así como a los establecidos el presente numeral, que comprende lo siguiente:

a. Cuando los datos sean tratados para fines distintos del determinado o sean incompatibles con los mismos;
b. Cuando el tratamiento tenga fines de comercialización o mercadeo;
c. Cuando los datos no sean necesarios en relación con la operación, servicio o producto a prestar o no corresponda a requerimientos regulatorios.

4.2 No viabilidad a la Oposición. En adición a lo dispuesto en el artículo 29 del Decreto Ejecutivo No. 285 de 2021, el derecho de oposición no aplicará, en los siguientes casos:

a. Cuando la información sea necesaria para la celebración o ejecución de un contrato y los servicios bancarios relacionados con la misma.
b. Los demás casos dispuesto por Ley o la regulación bancaria.
c. Cuando se configura alguna de las limitaciones establecidas en el artículo 31 del Decreto Ejecutivo No. 285 de 2021, así como en cualquier otra disposición legal o la norma que la desarrolle, cuando apliquen.

De resultar procedente la oposición, el banco no podrá tratar los datos relativos al titular de los datos.

En caso de que el cliente revoque su consentimiento al tratamiento o a un determinado tratamiento, el banco deberá dejar de tratar los datos personales, salvo que existe una condición de licitud o motivo legítimo para el tratamiento que prevalezca sobre su derecho de oposición.

La revocación del consentimiento por parte del cliente o su representante no tendrá efectos retroactivos y, no afectará la licitud del tratamiento basado en el consentimiento previo.

5. **DERECHO DE PORTABILIDAD.** El cliente tendrá derecho a recibir u obtener una copia de sus datos personales que hubiera proporcionado al banco o que sean objeto de tratamiento, en un formato estructurado, genérico, de uso común y lectura mecánica, para ser utilizado para sí mismo o para que el banco los trasmita a otros responsables del tratamiento de los datos. Igualmente, el cliente tendrá derecho a que los datos personales se trasmitan directamente a él o que el responsable los transmita directamente a otro responsable cuando sea técnicamente posible por medios seguros e interoperables.

   5.1 Viabilidad de la Portabilidad: Las entidades bancarias para el cumplimiento del derecho de portabilidad deberán sujetarse a los supuestos establecidos en el artículo 30 del Decreto Ejecutivo No. 285 de 2021, que comprende lo siguiente:
   a. El cliente haya facilitado sus datos directamente al banco responsable;
   b. Que el tratamiento de datos se efectúe por medios automatizados, es decir por medios digitales o tecnológicos;
   c. Sea un volumen relevante de datos;
   d. El cliente haya dado su consentimiento para el tratamiento de datos o esté basado en un contrato.

   5.2 No viabilidad de la Portabilidad: En adición a lo dispuesto en el artículo 30 del Decreto Ejecutivo No. 285 de 2021, el derecho de portabilidad no aplicará, en los siguientes casos:

   a. Se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el banco con base en los datos personales proporcionados por el cliente;
   b. Cuando afecte los derechos de terceros y los derechos y libertades de otros titulares de los datos.

   El banco deberá adoptar mecanismos para que los datos personales puedan ser proporcionados en formatos interoperables que permitan la portabilidad de datos y, velando que la transmisión de los datos personales bajo dichos sistemas se sujete a la información requerida por el cliente. El Superintendente establecerá los estándares mínimos requeridos para asegurar la portabilidad de los datos personales.

CAPÍTULO III

DEL TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 10. CONDICIONES Y FORMALIDADES PARA EL TRATAMIENTO. Todo tratamiento de datos personales ejecutado por el banco estará sujeto al consentimiento previo, informado e inequívoco del titular de los datos o de su representante autorizado, salvo las excepciones previstas por el presente Acuerdo, el Régimen de Protección de Datos Personales y demás leyes especiales que lo dispongan.

Cuando el tratamiento se base en el consentimiento, el mismo deberá manifestarse por escrito, o por cualquier otro medio electrónico que garantice la identidad del titular de los datos personales a manera que exista certeza sobre su identidad que la identifique o la haga identificable. En caso de que el consentimiento se obtenga a través de medios electrónicos, el banco deberá asegurarse de cumplir con los requerimientos que establecen los Acuerdos Bancarios y las leyes especiales sobre la materia.

Los bancos dispondrán de los medios y procedimientos adecuados para el otorgamiento efectivo y eficaz del consentimiento, los cuales serán de fácil comprensión, acceso, gratuitos y debidamente identificados.

En el evento que el consentimiento del cliente se de en el contexto de una declaración escrita que también se refiere a otros asuntos o para una pluralidad de finalidades, será preciso que el consentimiento se distinga claramente de los demás asuntos o finalidades, de forma comprensible, de fácil acceso y utilizando lenguaje claro y sencillo, a fin de que conste el consentimiento otorgado para cada uno de ellos.

No podrá condicionarse la ejecución de un contrato o la prestación de un servicio al tratamiento de datos personales para finalidades que no guardan relación con las determinadas en la relación contractual o precontractual del cliente.

Todo tratamiento posterior con fines distintos que no resulte compatible o análogo a los fines inicialmente establecidos requerirá del conocimiento y consentimiento del cliente, salvo aquellos basados en un interés legítimo.

PARÁGRAFO 1. Los bancos deberán asegurarse de contar con los mecanismos que le permitan demostrar con certeza el consentimiento otorgado por el cliente y que el mismo ha sido otorgado adecuadamente para el tratamiento de sus datos personales.

PARÁGRAFO 2. El consentimiento obtenido por medios electrónicos o tecnológicos deberá cumplir los requerimientos para su validez y los demás controles de seguridad establecidos en los Acuerdos Bancarios.

En caso de que la recolección de la información del cliente se obtenga, a través de los canales electrónicos del banco, la información a la cual hace referencia el artículo 14 del Decreto Ejecutivo No. 285 de 2021 se podrá facilitar o completar mediante el aviso de privacidad o las condiciones de uso del servicio(s) o producto(s) ofrecido(s).

ARTÍCULO 11. AVISO DE PRIVACIDAD. El banco al momento de obtener los datos personales directamente del cliente a través de los canales electrónicos deberá facilitarle toda la información que se recaba del mismo y los propósitos del tratamiento de los datos personales, a través del aviso de privacidad o las condiciones de uso del servicio(s) o producto(s) ofrecido(s).

En adición a la información indicada en el artículo 14 del Decreto Ejecutivo No. 285 de 2021, el banco deberá asegurase que el aviso de privacidad contenga la información que se indica a continuación:

1. Descripción del tipo de información que se recopilará y tratará;
2. Los casos o supuestos en los cuales los datos personales del cliente serían compartidos a terceros y la finalidad de dicha transferencia;
3. Informar los mecanismos de seguridad que utiliza la entidad bancaria para proteger los datos personales recabados;
4. Indicación del periodo de vigencia de la información establecida en el aviso de privacidad. Igualmente indicar el procedimiento de su modificación;
5. Indicación de los mecanismos de reclamo para atender cualquier consulta relacionada con el tratamiento de los datos de los usuarios y direcciones de contactos en la entidad que puede atender cualquier consulta relacionada con el tratamiento de los datos de los usuarios;
6. El derecho de presentar reclamos ante la Superintendencia de Bancos.

El aviso de privacidad deberá considerar las características de los tratamientos de datos que se lleven a cabo para cada tipo de servicio o producto bancario ofrecido. En todos los casos, el banco deberá asegurarse que el aviso de privacidad contenga la información mínima antes

indicada y, que la misma sea proporcionada al cliente en las formas y plazos señalados en los artículos 15 y 16 del Decreto Ejecutivo No. 285 de 2021.

ARTÍCULO 12. DATOS PERSONALES OBTENIDOS DE OTRAS FUENTES. Los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos. En aquellos casos que la fuente de obtención de los datos personales provenga de otro responsable del tratamiento de datos domiciliado en la República de Panamá, el banco receptor de los datos deberá asegurarse que el cliente haya dado su consentimiento previo para tales fines. En el caso que la información provenga o se recolecte de fuentes públicas o accesibles en medios públicos, no se requerirá la autorización o el consentimiento por parte del cliente, para el tratamiento de sus datos.

Para los efectos de lo dispuesto en el presente artículo, se incluirá dentro de la consideración de fuentes de acceso público, la información de datos personales obtenida por el Banco a través de medios de comunicación, ya sean los medios tradicionales o medios digitales como redes sociales (Ejemplo: twitter, facebook, instagram, entre otras).

ARTÍCULO 13. TRATAMIENTOS QUE NO REQUIEREN DEL CONSENTIMIENTO. Los bancos no requerirán del consentimiento o autorización del cliente para el tratamiento de los datos personales, en los supuestos previstos en el artículo 111 de la Ley Bancaria y los Acuerdos que lo desarrollan.

Adicionalmente, en cumplimiento del artículo 8 de la Ley No. 81 de 2019 y del artículo 17 del Decreto Ejecutivo No. 285 de 28 de mayo de 2021, no se requerirá autorización o consentimiento para el tratamiento de los datos personales, en los siguientes casos:

1. Para aquellos tratamientos de carácter bancario que cuenten con el consentimiento previo;
2. Cuando sea necesario para la aplicación y ejecución de contratos bancarios en los que cliente sea parte o tenga interés;
3. Para aquellos tratamientos cuya finalidad sea la de preservar la seguridad de las personas y las instalaciones del banco;
4. Cuando el tratamiento sea necesario para la debida administración y gestión de los distintos riesgos bancarios;
5. Cuando sea necesario para el cumplimiento de requerimientos u obligaciones exigidas por la normativa bancaria;
6. Cuando los datos sean utilizados o compartidos por el banco con la propietaria de acciones bancarias, subsidiarias u otra sociedad del grupo bancario para el ejercicio de las funciones propias de la entidad bancaria, siempre que no sea para fines de mercadeo;
7. Cuando el tratamiento de datos sea necesario para el cumplimiento de los requerimientos establecidos por la Superintendencia de Bancos para el intercambio de información con otros organismos de supervisión financiera;
8. Cuando el tratamiento este basado en un interés legítimo del banco derivado de la relación o vínculo existente con el cliente, por razón de un servicio o producto bancario;
9. Cuando el tratamiento sea necesario para la transferencia, comunicación o interconexión de los datos personales a un custodio de bases de datos, a un proveedor de servicios bancarios o a terceros para la gestión de la relación contractual Banco-Cliente, siempre que sea relacionado con la prestación de un servicio o producto bancario y de mercadeo.
10. Los demás tratamientos establecidos por la Ley y la normativa que la desarrolla.

PARÁGRAFO 1. La remisión al cliente de comunicación de carácter publicitaria, comercial o de mercadeo sobre productos y servicios bancarios u otras análogas requerirá de su consentimiento, previo, informado e inequívoco.

PARÁGRAFO 2. Cuando el tratamiento de datos este basado en un interés legítimo del banco, este deberá evaluar la viabilidad de realizar el tratamiento bajo esta base jurídica.

ARTÍCULO 14. CUSTODIOS DE BASE DE DATOS. Las entidades bancarias deberán establecer políticas y procedimientos que aseguren que los custodios de bases de datos personales cumplen con las obligaciones y cuentan con los estándares mínimos vinculados con la protección de datos personales a los cuales hace referencia los artículos 47, 48 y 49 del Decreto Ejecutivo No. 285 de 2021.

Para tales efectos, las entidades bancarias deberán asegurarse que todo tratamiento de datos realizados por los custodios de la base de datos personales se efectúe de conformidad con las condiciones establecidas en el contrato suscrito.

El banco que contrate los servicios de custodio de base de datos mantendrá la responsabilidad en el tratamiento de los datos personales.

Los custodios de base de datos deberán contar con los suficientes conocimientos especializados, mecanismos y recursos que aseguren el cumplimiento de los requerimientos técnicos y de seguridad que garanticen la integridad y confidencialidad de los datos personales, conforme a los estándares y principios establecidos en el presente Acuerdo y demás Acuerdos Bancarios relacionados con la materia.

ARTÍCULO 15. REGISTRO DE TRANSFERENCIAS. De conformidad con los lineamientos establecidos en el artículo 31 de la Ley No. 81 de 2019, las entidades bancarias deberán llevar y conservar un registro de las trasferencias de datos personales realizadas a terceros que incluye a los proveedores de servicios bancarios, tal como son definidos en el presente Acuerdo. Igualmente, el banco deberá asegurarse que el custodio de bases de datos personales cuente con un registro de transferencia de los datos a terceros, cuando el contrato suscrito así lo permita.

Las entidades bancarias mantendrán actualizados dicho registro, de forma que la información responda al tratamiento histórico llevado a cabo.

Para los efectos del presente Acuerdo, no se considerará transferencia de datos a terceros, los datos que son transferidos por el banco al custodio de la base de datos.

ARTÍCULO 16. CONSERVACIÓN DE DATOS PERSONALES. Los datos personales tratados en el ejercicio del negocio de banca deberán ser conservados en base de datos que permita preservar la confidencialidad, integridad, disponibilidad y en general el manejo seguro de la información. Asimismo, deberán ser conservados durante el tiempo que para cada caso disponen los Acuerdos Bancarios o una ley especial.

Una vez extinguido el plazo legal de conservación de los datos personales, las entidades bancarias deberán asegurarse de no transferir ni comunicar dichos datos dentro del periodo de siete (7) años establecido por el artículo 28 de la Ley No. 81 de 2019, salvo que el cliente solicite lo contrario.

El banco deberá mantener la confidencialidad del tratamiento y de la información almacenada en la base de datos, aun después de finalizada su relación con el titular de datos, salvo los casos que por disposición legal sean relevados del mismo.

CAPÍTULO IV

GESTIÓN DE LOS DATOS PERSONALES

SECCIÓN I

RESPONSABILIDADES

ARTÍCULO 17. SISTEMA DE CONTROL INTERNO. Para el cumplimiento de las disposiciones establecidas en el presente Acuerdo, las entidades bancarias deberán asegurarse de aplicar los lineamientos contemplados en la regulación sobre Gobierno Corporativo emitida por esta Superintendencia, en lo que respecta al Sistema de Control Interno.

ARTÍCULO 18. RESPONSABILIDADES DE LA JUNTA DIRECTIVA. Sin perjuicios de las responsabilidades establecidas en el Régimen de Protección de Datos Personales, en materia de protección de datos personales, el banco a través de la junta directiva tendrá las siguientes responsabilidades:

1. Establecer y velar porque se mantenga una estructura organizativa y operativa adecuada de delegación de facultades y de segregación de funciones que garantice la aplicación de los principios y derechos de protección de datos personales a través de toda la organización;
2. Aprobar los recursos necesarios para el adecuado desarrollo de las medidas de protección de datos personales establecidas en la Ley No. 81 de 2019 y la normativa que la desarrolla;
3. Aprobar las políticas y los procedimientos que implementará la entidad para el cumplimiento de las obligaciones regulatorias relativas a la protección de datos personales;
4. Aprobar los programas de capacitación, actualización y certificación en materia de protección de datos;
5. Propiciar una cultura de protección de datos personales a todos los niveles de la organización, extensivas a los custodios de datos y proveedores de servicios bancarios;
6. Aprobar los procedimientos para recibir y responder solicitudes y reclamaciones de los titulares de los datos.

ARTÍCULO 19. CERTIFICACIÓN DE CUMPLIMIENTO DE LA JUNTA DIRECTIVA. Anualmente, el banco remitirá a la Superintendencia una certificación, suscrita en representación de la junta directiva por su presidente y su secretario, que haga constar lo siguiente:

a. Que la junta directiva conoce los estándares contemplados en el Régimen de Protección de Datos Personales y las disposiciones establecidas en el presente Acuerdo;
b. Que el banco cuenta con las políticas y procedimiento para la gestión de la protección de los datos personales;
c. Que la junta directiva ha sido puesta en conocimiento sobre la efectividad de las medidas de protección de datos personales implementadas por la entidad bancaria.

Dicha certificación podrá ser presentada en documento colectivo o individual y las firmas deberán ser notariadas o a través de firma electrónica calificada. Esta certificación será suscrita y remitida dentro de los sesenta (60) días siguientes al cierre fiscal.

En el caso de bancos que sean sucursales de bancos extranjeros, la declaración de cumplimiento establecida en el presente artículo podrá evidenciarse, mediante una certificación anual de la unidad responsable de la administración de datos personales de su casa matriz o su posición equivalente en la cual se acredite que el banco cuenta con las políticas para la protección de datos personales equivalentes o superiores a lo previsto en la normativa local sobre protección de datos personales. Esta declaración deberá ser remitida a esta Superintendencia de Bancos dentro del plazo señalado en el párrafo anterior.

ARTÍCULO 20. DE LA UNIDAD DE ADMINISTRACIÓN DE RIESGO. La Unidad de Administración de Riesgo deberá identificar, evaluar y controlar los riesgos inherentes a la protección de datos personales, para el cumplimiento de las responsabilidades establecidas en las regulaciones sobre gestión de riesgos.

ARTÍCULO 21. AUDITORÍA INTERNA Y SEGUIMIENTO DEL SISTEMA DE CONTROL INTERNO. En atención a las disposiciones establecidas en el Acuerdo de Gobierno Corporativo, la Unidad de Auditoría Interna es responsable del seguimiento del Sistema de Control Interno.

Para tales efectos, dicha Unidad evaluará el cumplimiento de las políticas y procedimientos utilizados para la protección de los datos personales, de conformidad con las disposiciones establecidas en el Régimen de Protección de Datos Personales y el presente Acuerdo. Igualmente, deberá asegurarse de evaluar la efectividad de los controles implementados para mitigar los riesgos que atenten contra los datos personales.

ARTÍCULO 22. OFICIAL DE PROTECCIÓN DE DATOS. Las entidades bancarias a lo interno de su organización deberán designar a un Oficial de Protección de Datos, que de acuerdo al tamaño y grado de complejidad de sus actividades, operaciones, servicios y, el tipo, volumen y medio de los datos tratados, le permita gestionar adecuadamente las funciones asignadas por el Régimen de Protección de Datos Personales y el presente Acuerdo.

Para tales efectos, el Oficial de Protección de datos designado desempeñará sus funciones con independencia, teniendo una interlocución directa con la Gerencia Superior o Alta Dirección, como órgano de toma de decisiones. De igual manera, deberá mantener confidencialidad de la información obtenida en el ejercicio de sus funciones.

El oficial de protección de datos deberá contar con una experiencia profesional en áreas afines a la banca o sector financiero, en materia de protección de datos, cuyo nombramiento o reemplazo deberá ser previamente notificado a la Superintendencia de Bancos.

El banco deberá atribuirle al oficial de protección de datos la suficiente autoridad, jerarquía, independencia dentro de la organización y, facilitarle los recursos necesarios que garanticen el desempeño de sus funciones y, su participación en todos los asuntos relacionados con la protección de datos personales.

El Oficial de Protección de Datos deberá informar a la Junta Directiva o al Comité designado para tratar estos temas, sobre la eficacia de los programas, medidas, controles implementados y el cumplimiento de las obligaciones regulatorias en materia de protección de datos personales.

PARÁGRAFO. Con la finalidad de procurar la independencia del Oficial de Protección de datos a lo interno de la organización, el banco deberá asegurarse que, dentro de su estructura organizativa, se evidencie la jerarquía e independencia de su cargo.

ARTÍCULO 23. FUNCIONES DEL OFICIAL DE PROTECCIÓN DE DATOS. En adición a las funciones establecida en el artículo 44 del Decreto Ejecutivo No. 285 de 2021, el Oficial de Protección de Datos tendrá las siguientes funciones:

1. Llevar un registro de cualquier suceso que afecte la protección de los datos personales tratados por el Banco;
2. Reportar toda deficiencia detectada en las medidas de protección de datos personales a la Gerencia Superior o Alta Dirección, así como a la Unidad de Administración de Riesgo y la Unidad de Auditoría Interna;
3. Coordinar con el área de seguridad de la información los sucesos de seguridad que impacten la protección de los datos personales;
4. Proporcionar sugerencias respecto a las medidas correctivas que pueden implementarse para subsanar las deficiencias detectadas en el tratamiento de los datos personales;
5. Mantener una comunicación con las áreas de riesgo, auditoría interna y cumplimiento con la finalidad de identificar las mejoras necesarias en los controles de protección de datos personales;
6. Coadyuvar en conjunto con el responsable del área de seguridad de la información en la atención de los incidentes de seguridad que impacten el tratamiento de los datos personales;
7. Ser la unidad de enlace con la Superintendencia de Bancos en los temas relativos al tratamiento de los datos personales,
8. Coordinar el plan anual de capacitación en materia de protección de datos personales;

9. Ser la unidad de enlace con el titular de los datos, sin perjuicio que administrativamente, cuando aplique, se pueda apoyar en el responsable del Sistema de Atención de Reclamos.

PARÁGRAFO. El Oficial de Protección de Datos podrá desempeñar otras funciones a lo interno de la organización, siempre que las mismas no representen incompatibilidades con las funciones establecidas en el presente artículo y no vulneren la independencia de sus funciones. Se considerarán funciones incompatibles aquellas que, dentro de la estructura del Banco, lleven a cabo las áreas de Auditoria Interna, Riesgos y Cumplimiento, dentro de las cuales no podrá formar parte el Oficial de Protección de Datos.

SECCIÓN II

DEL TRATAMIENTO Y TRANSFERENCIA DE LOS DATOS PERSONALES

ARTÍCULOS 24. POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES. Los bancos deberán establecer y documentar los procedimientos y procesos para la inclusión, conservación, almacenamiento, modificación, supresión, transferencia y cualquiera otra acción de tratamiento de los datos personales, en base a las normas sobre protección de datos personales y las políticas de tratamiento de protección de datos personales adoptadas por la entidad y aprobadas por la junta directiva. Lo anterior, se entenderá como la ficha técnica a la cual hace referencia la Ley No. 81 de 2019.

Las políticas internas o fichas técnicas que adopte el banco deberán incluir las medidas adoptadas por la entidad para cumplir con los principios, derechos y obligaciones de protección de datos personales desde el diseño de los servicios y productos. Dichas medidas podrán incluir la aplicación de medidas de disociación a los datos o cualquiera otra medida que permita reducir los riesgos inherentes al tratamiento.

ARTÍCULO 25. SEGURIDAD DEL TRATAMIENTO DE DATOS PERSONALES. Las entidades bancarias deberán asegurarse que para el tratamiento y transferencia segura de los datos personales, aplicar las disposiciones establecidas en el Acuerdo para la Gestión del Riesgo de la Tecnología de la Información y el Acuerdo sobre Banca Electrónica emitidos por esta Superintendencia de Bancos.

ARTÍCULO 26. INCIDENTE DE SEGURIDAD DE LOS DATOS PERSONALES. Los bancos deberán comunicar al titular de los datos personales de cualquier incidente de violación a la seguridad de los datos personales detectado, que involucre daño, pérdida, alteración, destrucción, acceso y, en general cualquier uso ilícito o no autorizado de los datos personales que afecten de forma significativa.

De igual manera, deberá comunicar dicho hecho a la Superintendencia de Bancos, a través de su oficial de Seguridad de la Información, siguiendo los lineamientos que al respecto establecen los Acuerdo de Banca Electrónica y Gestión del Riesgo de Tecnología de la Información.

La obligación establecida en el presente artículo se extiende al custodio de base de datos, para lo cual el Banco deberá asegurarse de establecer los protocolos de comunicación para tales efectos.

CAPÍTULO V

DISPOSICIONES FINALES

ARTÍCULO 27. RECLAMOS ANTE LA SUPERINTENDENCIA. El titular de datos personales que considere vulnerado el ejercicio de los derechos ARCO podrá presentar ante el banco responsable del tratamiento de los datos toda solicitud, reclamación, queja y controversia vinculada con la protección de datos personales, las cuales serán atendidas a través del Oficial de Protección de Datos o el ejecutivo designado por el banco para tales fines.

En caso de que el banco no cumpla con atender la solicitud concerniente al ejercicio de los derechos ARCO o el cliente se encuentre disconforme con la decisión adoptada por el banco, el mismo podrá interponer un reclamo ante la Superintendencia de Bancos. Para tales fines, el cliente tendrá un plazo de 30 días calendario, los cuales empezarán a contarse a partir de la fecha en que obtuvo respuesta formal por parte del banco o cuando el banco no haya cumplido con resolver la solicitud o reclamo en el plazo correspondiente.

Los bancos deberán poner a disposición del cliente, los medios y formas simplificadas de comunicación que considere pertinente para facilitar el ejercicio de sus derechos y atender o suministrar la información solicitada.

Los reclamos presentados a la Superintendencia de Bancos estarán sujetos a los procedimientos y recursos establecidos en la Ley Bancaria y en los Acuerdos bancarios relacionados con la materia. Una vez comunicada y ejecutoriada la Resolución que resuelve el proceso interpuesto ante la Superintendencia, se entenderá agotada la vía gubernativa, sin perjuicio de los recursos que correspondan en la vía contencioso-administrativa.

PARÁGRAFO. En atención a lo dispuesto en el artículo 18 de la Ley No. 81 de 2019, el titular de los datos personales solo podrá interponer reclamos ante la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) en el evento que luego de interponer su reclamo ante la Superintendencia de Bancos, ésta no emita un pronunciamiento en base al proceso administrativo correspondiente.

ARTÍCULO 28. PROCEDIMIENTO DE SEGUIMIENTO, CONTROL Y SUPERVISIÓN. La Superintendencia de Bancos podrá solicitar y verificar el cumplimiento de los principios y las medidas de carácter técnicas, organizativas y de seguridad interna adecuadas para la protección de datos personales que se establecen en el presente Acuerdo y demás normas relacionadas, a fin de garantizar que los bancos cumplen con los principios y estándares de protección de datos personales objeto de tratamiento.

Los bancos deberán tener a disposición de la Superintendencia de Bancos toda la información que considere necesaria, para una adecuada supervisión del cumplimiento de las disposiciones contenidas en el presente Acuerdo.

ARTÍCULO 29. SANCIONES. En caso de incumplimiento de las disposiciones contenidas en el presente Acuerdo y el Régimen de Protección de Datos Personales, la Superintendencia aplicará las sanciones correspondientes de conformidad a los montos y gravedad de las faltas establecidas en la Ley No. 81 de 2019 con sujeción al procedimiento administrativo sancionatorio establecido por el Acuerdo No. 12-2015. Lo anterior, sin perjuicio de la aplicación de las sanciones establecidas en el título IV de la Ley Bancaria, por infracción a la confidencialidad bancaria, relacionada a la divulgación de información del cliente sin su consentimiento.

ARTÍCULO 30. VIGENCIA. Las disposiciones del presente Acuerdo empezaran a regir a partir de su firma. No obstante lo anterior, las disposiciones establecidas en los artículos 22 y 23

tendrán un plazo de adecuación de doce (12) meses contados a partir de la firma del presente Acuerdo.

Dado en la ciudad de Panamá, a los veinticuatro (24) días del mes de febrero de dos mil veintidós (2022).

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

EL PRESIDENTE **EL SECRETARIO**

Rafael Guardia Pérez Felipe Echandi