Datos personales tratados por las entidades bancarias

El pasado mes de febrero la Superintendencia de Bancos de Panamá (SBP) aprobó el Acuerdo No. 001-2022 que establece lineamientos especiales para la protección de datos personales tratados por las entidades bancarias.

Este acuerdo nace de los parámetros dados por la Ley 81 de 2019 comentada en Progreso 19 y su normativa de desarrollo[1], ambas vinculadas con la protección de datos personales, que sientan las bases para la implementación de un sistema adecuado y robusto aplicable a todo el sistema financiero nacional, alineando sus políticas y procedimientos internos a los derechos ARCO.

Objetivo y alcance

Este Acuerdo es de obligatorio cumplimiento para las entidades bancarias establecidas en la República de Panamá, las cuales deberán establecer protocolos, procesos, procedimientos, mecanismos y demás reglas especiales relacionadas al tratamiento de datos personales. Los lineamientos dados en esta norma deben ser aplicados a los datos de todo cliente que sea tratado por una entidad bancaria, independientemente de su nacionalidad, residencia o domicilio.

Principios Generales de Protección de Datos

Las entidades bancarias deberán 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: 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.

Estos 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.

Derechos ARCO

En virtud del principio de transparencia, las entidades financieras, a solicitud del cliente, informarán

sobre el flujo de información que sobre sus datos personales mantenga en su base de datos para 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:

Derecho de Acceso: el cliente tendrá derecho de obtener la confirmación del banco de sí se están o no tratando sus datos personales.
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 la base de datos.
Derecho de Cancelación: el cliente tendrá derecho a solicitar del banco responsable la supresión o eliminación de sus datos cuando los mismos sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.
Derecho de Oposición: el cliente tendrá derecho a oponerse o negarse a proporcionar sus datos.

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.

Consentimiento

Constituye un elemento básico de protección de datos personales y en virtud del principio de licitud del tratamiento, deberá ser obtenido por parte del titular de los datos de manera libre, ser expreso, preciso, previo, informado e inequívoco

En aquellos casos en los que el consentimiento del cliente se realice a través de medios electrónicos o tecnológicos, los bancos deberán contar con mecanismos que le permitan demostrar la identidad del cliente, el cumplimiento con los requerimientos para su validez y controles de seguridad dados en los acuerdos bancarios vigentes.

La norma establece además, algunas situaciones en las que no se requerirá autorización o consentimiento para el tratamiento de datos personales:

Tratamientos de carácter bancario que cuenten con consentimiento previo.
Cuando sea necesaria la aplicación de contratos bancarios en los que el cliente sea aparte o tenga interés.
Aquellos tratamientos con finalidad de preservar la seguridad de las personas y las instalaciones del banco.
Cuando el tratamiento sea necesario para la debida administración y gestión de distintos riesgos bancarios.
Cuando sea necesario para el cumplimiento de requerimientos exigidos por la normativa bancaria, o establecidos por la Superintendencia de Bancos para el intercambio de información con otra entidad reguladora.
Cuando los datos utilizados sean compartidos o utilizados 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.
Cuando el tratamiento esté basado en interés legítimo del banco, derivado de la relación o vínculo del cliente por razón de un servicio o producto.
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 terceros relacionados para la gestión de la relación Banco-Cliente, orientado siempre a la prestación de un servicio bancario o producto.

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). El aviso de privacidad deberá contener la siguiente información:

La descripción del tipo de información que se recopilará y tratará
Los supuestos en los cuales los datos personales del cliente serían compartidos a terceros y la finalidad de dicha transferencia
Los mecanismos de seguridad que utiliza la entidad bancaria para proteger los datos personales recabados
El periodo de vigencia de la información establecida en el aviso de privacidad
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
El derecho de presentar reclamos ante la SBP

Responsabilidades de la Junta Directiva

Las Juntas Directivas de las entidades bancarias deberán establecer y velar por una estructura organizativa adecuada a la nueva norma: aprobar recursos necesarios para el desarrollo de las medidas; aprobar políticas, procedimientos, programas de capacitación, actualización y certificación para el cumplimiento de las obligaciones regulatorias en materia de protección de datos personales, así como propiciar una cultura institucional orientada a cumplir con la regulación de protección de datos, en todos los niveles de la entidad.

Adicionalmente, se requerirá que dentro de los sesenta días siguientes al cierre fiscal de cada año, el banco remita al regulador una certificación de cumplimiento del régimen de protección de datos, suscrita por el presidente y secretario de la Junta Directiva.

Obligaciones de las entidades

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 datos personales incluyendo las medidas adoptadas por la entidad para cumplir con los principios y derechos y obligaciones de protección de datos personales.

Asimismo deberán asegurarse que el tratamiento y transferencia se aplican las disposiciones establecidas en el Acuerdo para la Gestión del Riesgo de la Tecnología de la Información y el Acuerdo sobre Banca Electrónica de la SBP.

Por otro lado, deberán comunicar al titular de los datos personales cualquier incidente de violación a la seguridad de los datos personales detectado así como a la SBP

Nueva figura: Oficial de Protección de Datos

El artículo 22 y 23 del acuerdo establecen la obligatoriedad de designar un Oficial de Protección de Datos y sus funciones, cuyo nombramiento o reemplazo deberá ser previamente notificado a la SBP. El oficial deberá contar con independencia, teniendo interlocución directa con la Alta Gerencia, y rindiendo informes a la Junta Directiva o al Comité designado.

Se establece que el oficial podrá desempeñar otras funciones en la entidad, siempre y cuando no sean incompatibles al cargo; como son las funciones desarrolladas por las áreas de Auditoría Interna, Riesgos y Cumplimiento.

Proceso de Reclamos

En caso de que se considere vulnerado el ejercicio de sus derechos, el titular de los datos personales podrá presentar su reclamo en la entidad bancaria. Si el banco no atendiese su queja o se encontrase inconforme con la resolución del reclamo, podrá elevar su queja ante la SBP, dentro de los 30 días calendario siguientes, desde recibida la respuesta de la entidad bancaria. Como última instancia, establece el Acuerdo que el titular de los datos podrá interponer su queja ante la Autoridad Nacional de Transparencia (ANTAI).

Sanciones y vigencia del acuerdo

El acuerdo establece sanciones desde $1,000.00 a $10,000.00, cuyas infracciones se calificarán en leves, graves y muy graves, con sujeción al procedimiento administrativo establecido por el Acuerdo No. 12-2015. La norma entró en vigor el 24 de febrero de 2022, salvo los aspectos recogidos en los artículos 22 y 23, en relación al Oficial de Protección de Datos y sus funciones, dando así un plazo de

12 meses a las entidades bancarias para las adecuaciones correspondientes.

[1] Decreto Ejecutivo 285 comentado en Progreso 25