Icaza
González-Ruiz
Alemán

PROTECCIÓN DE DATOS EN PANAMÁ

La protección de los datos personales es una garantía fundamental y está contenida en nuestra Constitución Nacional, la cual establece en su Artículo 42 lo siguiente:

> *"Artículo 42: Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley.*
> *Esta información solo 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."*

Como vemos, siempre se debe obtener el consentimiento del titular, es decir su manifestación de voluntad para tratar los datos y ser informados del fin específico para el cual se recopilan los datos. La Ley 81 establece que el consentimiento puede obtenerse de forma que permita su trazabilidad mediante documentación, ya sea electrónica o mediante otro mecanismo adecuado y podrá ser revocado, sin efecto retroactivo.

Así mismo, nuestra Constitución Nacional en su artículo 43 establece las garantías constitucionales en las cuales toda persona tiene derecho a solicitar información de acceso público o de interés colectivo y solicitar su rectificación. El artículo 44 establece que toda persona puede promover una acción de hábeas data para garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales.

El 29 de marzo de 2021 entró en vigencia la Ley de Protección de Datos Personales en la República de Panamá por medio de la Ley 81 de 26 de marzo de 2019. Esta Ley establece los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales en nuestro país para personas naturales y jurídicas. Luego por medio del Decreto Ejecutivo 285 de 2021 se reglamenta la Ley 81.

Es importante destacar que antes de la promulgación de la Ley 81 de 2019, existían disposiciones legales que actualmente regulan la protección de datos personales en Panamá, por medio de leyes especiales. Entre los cuales están la Ley bancaria, Ley de seguros, Ley de valores, Ley Fiduciaria, Ley que regula los Derechos y obligaciones de los pacientes, en materia de información u decisión libre e informada, entre otras.

A pesar que existen leyes especiales y normas que conforman el marco regulatorio que regula la protección de datos personales, la Ley 81 de 2019 se aplica de forma supletoria.

El regulador o autoridad reguladora de cada sector, debe establecer dentro de su normativa todos los protocolos, procesos y procedimientos de tratamiento y transferencia segura que deban cumplir los sujetos regulados.

Conceptos básicos de la Protección de Datos Personales

¿Qué es un Dato personal?

Un dato personal, es cualquier información concerniente a personas naturales que las identifica o

hace identificable.

¿Qué es un dato sensible?

La Ley define los datos sensibles, a aquellos que se refieren a la esfera íntima del titular, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para este.

Se consideran datos sensibles, los que pueden revelar aspectos como origen racial, o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual datos genéticos o datos biométricos, entre otros.

La Ley 81 establece que los datos sensibles no pueden transferirse sin el debido consentimiento explícito del titular, cuando sea necesario para salvaguardar la vida del titular y este se encuentre física o jurídicamente incapacitado, cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente, cuando tenga una finalidad histórica, estadística o científica, en cuyo caso deberán tomarse medidas de disociación de identidad.

Objeto, principios y aplicación

La Ley establece los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos.

Los principios generales son los que inspiran y rigen la protección de datos personales y que son la base para su interpretación y aplicación de la norma, también complementan algunos vacíos de la propia Ley 81:

1. Principio de lealtad: los datos personales se recaban sin engaño o falsedad y sin utilizar medios fraudulentos
2. Principio de finalidad: los datos personales deben recolectarse con fines determinados y no ser tratados posteriormente para fines distintos para los cuales se solicitaron, no conservarse por más tiempo del necesario para los fines del tratamiento.
3. Principio de proporcionalidad: solo se solicitan los datos adecuados, pertinentes y limitados al mínimo necesario en relación a la finalidad requerida.
4. Principio de veracidad y exactitud: deben ser exactos y responder con veracidad a la situación actual del propietario del dato.
5. Principio de seguridad de los datos: los responsables del tratamiento de los datos personales deben adoptar las medidas para garantizar la seguridad de los datos e informar al titular, lo más pronto posible, cuando los datos hayan sido sustraídos sin autorización o haya indicios que su seguridad ha sido vulnerada.
6. Principio de transparencia: la información y comunicación debe ser expresada en un lenguaje claro y sencillo.

7. Principio de confidencialidad: todas las personas que intervengan en el tratamiento de datos personales tienen la obligación de guardar secreto o confidencialidad respecto de estos.
8. Principio de licitud: los datos deben ser recolectados de forma licita, con el consentimiento previo, informado e inequívoco del titular o por fundamento legal.
9. Principio de portabilidad: el titular de los datos tiene el derecho a obtener de parte del responsable una copia de los datos personales en un formato genérico y de uso común.

El ámbito de aplicación de esta Ley se extiende a las bases de datos que se encuentren en el territorio de la República de Panamá, que almacenen o contengan datos personales de nacionales o extranjeros o que el responsable del tratamiento esté domiciliado en el país, quedan sujetos a la aplicación de esta Ley y su reglamentación.

El almacenamiento o transferencia de datos personales originados o almacenados dentro de la República de Panamá que sean confidenciales, sensibles o restringidos, que reciban un tratamiento transfronterizo es permitido siempre que el responsable del almacenamiento o custodio de los datos cumpla con los estándares de protección de datos personales y obtenga el consentimiento.

El Decreto Ejecutivo 285 del 2021 que reglamenta la Ley 81 establece que el registro de las bases de datos transferidas a terceros constará por escrito, por cualquier medio, inclusive por medios electrónicos.

¿Qué excepciones aplican y cuándo se puede tratar los Datos Personales?

Existen excepciones al ámbito de aplicación de la Ley, para aquellos datos que expresamente se encuentren regulados por leyes especiales o por normativas que las desarrollen y que hemos detallado al inicio.

Dentro de las excepciones se encuentran:

1. Los que realice una persona natural para actividades exclusivamente personales o domésticas.
2. Los que realicen autoridades competentes con fines de prevención, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
3. Los que se efectúen para el análisis de inteligencia financiera relativos a la seguridad nacional
4. Cuando se trata de tratamiento de datos relacionados con organismos internacionales en cumplimiento de tratados o convenios internacionales
5. Los resultantes de información obtenida mediante un procedimiento previo de anonimización.

El tratamiento de datos personales solo se puede realizar cuando: i) Se obtenga el consentimiento del titular, ii) Que el tratamiento sea necesario para la ejecución de una obligación contractual, iii) Que el tratamiento sea necesario para el cumplimiento de una obligación legal, iv). Que el tratamiento esté autorizado por una ley especial.

Icaza González-Ruiz Alemán

Responsable del tratamiento de datos personales, custodio de la base de datos y Oficial de Protección de datos

El responsable del tratamiento de datos es una persona natural o jurídica, pública o privada lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y determina los fines, medios y alcance.

El responsable del tratamiento de datos es quien establecerá los protocolos, procesos y procedimientos de gestión y transferencia segura, protegiendo los derechos de los titulares. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) con el apoyo de la Autoridad Nacional para la Innovación Gubernamental (AIG) son las autoridades que fiscalizarán y supervisarán lo anterior.

El custodio de la base de datos, así como todo aquel que tenga acceso deberá cuidar de estos con la debida diligencia, y será igualmente responsable por los daños y perjuicios ocasionados.

Como medida de responsabilidad para el cumplimiento de la utilización de los datos personales el Decreto Ejecutivo 285 establece la figura del Oficial de Protección (ODP) para las entidades públicas y recomendado, pero no obligatorio para el sector privado. El ODP desempeñará sus funciones de forma independiente. Sus funciones serán de participar en tiempo y forma en las cuestiones referidas a la protección de datos, informar y asesorar al responsable y al custodio, supervisar el cumplimiento de la normativa, promover la capacitación de las personas que traten datos, entre otras.

Tanto el responsable del tratamiento de datos personales como el custodio de la base de datos que transfieran datos, deben llevar un registro de las bases de datos y deben estar a disposición de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) cuando lo requiera, incluso la base de datos debe identificar e indicar el periodo de todas las personas que ingresen datos personales dentro de los quince días hábiles desde que se inicia dicha actividad.

Los responsables del tratamiento de datos y/o custodios de las bases de datos, así como todas las personas que intervengan en cualquier fase del tratamiento de los datos, estarán sujetas al deber de secreto o confidencialidad. Esta obligación será complementaria al secreto profesional, se aplicará durante todo el tiempo que dure el tratamiento y se mantendrá aun cuando hubiese finalizado la relación del empleado o funcionario.

Los responsables del tratamiento y/o custodios de las bases de datos deben garantizar el cumplimiento y quedan sujetos a la fiscalización y supervisión de la ANTAI a través de la Dirección de Protección de Datos Personales.

¿Cuándo no se requiere autorización para el tratamiento de los datos personales?

No se requiere autorización para el tratamiento de los datos personales en los siguientes casos:

1. Fuentes de dominio público
2. Los que recolecta la administración pública.

3. Los de carácter económico, financiero o bancario con consentimiento previo.
4. Listas de personas en organizaciones, profesiones.
5. Aquellos dentro de una relación comercial establecida.
6. Tratamiento de organizaciones privadas para uso de los asociados.
7. Urgencia médica o sanitaria.
8. Fines históricos, estadísticos o científicos.

Derechos irrenunciables de los titulares de datos personales

Como muchos países nuestro país reconoce los derechos ARCO, es decir el Derecho de Acceso, Derecho de Rectificación, Derecho de Cancelación, Derecho de Oposición y Derecho a la Portabilidad.

Nuestra Ley permite al titular de los datos personales a solicitar su información a los responsables del tratamiento de datos, y deberá ser proporcionada en un plazo no mayor de diez días hábiles. El suministro de información, su modificación, bloqueo o eliminación será gratuito.

Los datos deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos dentro de un término de cinco días hábiles siguientes a la solicitud de modificación. Quien sea responsable debe proceder cuando existan pruebas de inexactitud de los datos.

Si el responsable no se pronuncia sobre la solicitud del titular dentro del término, el titular puede recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI). En casos sujetos a leyes especiales, al regulador o autoridad reguladora. En el caso que en dichas leyes no se encuentren las sanciones a las faltas cometidas, el regulador deberá aplicar las sanciones establecidas en esta Ley, sin perjuicio que el titular pueda también presentar su queja ante la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) para que aplique las sanciones correspondientes y a los tribunales de justicia para solicitar la indemnización por daño patrimonial y/o moral.

El responsable del tratamiento de los datos personales o el custodio de la base de datos no puede transferir o comunicar en ningún caso los datos que relacionen a una persona después de transcurridos siete años, desde que se extinguió la obligación legal de conservarla, al menos que se pacte otro periodo. Estos datos tienen que eliminarse o volver a mantener una relación con el titular de los datos y explicarle por qué aún se mantienen los datos y cuál es el nuevo fin.

La transferencia de datos es lícita si cumple al menos una de las condiciones siguientes:

1. Consentimiento del titular.
2. Que el país u organismo receptor proporcione mejor nivel de protección.
3. Que se encuentre previsto en una Ley o Tratado.
4. Para prevención de diagnóstico médico.

5. Que sea efectuada a cualquier sociedad de un mismo grupo económico siempre que no sean usadas para fines distintos.
6. En virtud de un contrato.
7. Necesario para la salvaguarda de un interés público.
8. Para el reconocimiento o defensa de un derecho en un proceso judicial.
9. Para el mantenimiento o cumplimiento de una relación jurídica.
10. Requerida para transferencias bancarias o bursátiles.
11. Para cooperación internacional entre organismos de inteligencia para luchar contra el crimen organizado, terrorismo, narcotráfico, etc.
12. Que el responsable que transfiere los datos adopte mecanismos de autorregulación vinculante.
13. En caso de cláusulas contractuales.

Consejo Consultor y Autoridad supervisora

Se crea un Consejo de Protección de datos personales como ente consultivo en la materia que asesora a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), recomienda políticas públicas relacionadas a la materia, evalúa los casos que sean presentados, brinda recomendaciones y desarrolla su reglamento interno.

La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) a través de una Dirección, creada para conocer esta materia, está facultada para sancionar al responsable del tratamiento de los datos personales, así como al custodio de la base de datos que se compruebe que han infringido los derechos del titular de los datos personales. El Decreto ejecutivo establece los criterios para la graduación de las sanciones, que dependerán de la intencionalidad, la reincidencia, la naturaleza y cuantía de los perjuicios causado, afectación de derechos, adopción de medidas correctivas entre otras.

Las decisiones de la Dirección serán impugnables mediante recurso de reconsideración y son apelables ante el Director de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

Infracciones y sanciones

La Autoridad podrá fijar sanciones desde $1,000.00 a $10,000.00 balboas.
Las infracciones se califican en leves, graves y muy graves:

- **Leves:** no remitir o informar a la autoridad la información dentro del plazo y puede conllevar una citación de la autoridad.
- **Graves:** efectuar el tratamiento sin el consentimiento del titular, infringir los principios y garantías establecidos, infringir el compromiso de confidencialidad, restringir los derechos

ARCO, incumplir el deber de informar al titular del tratamiento de los datos, almacenar o archivar datos sin las condiciones de seguridad, no atender la reiteración de los requerimientos y obligaciones de la autoridad, lo anterior puede conllevar según su proporcionalidad una multa de US$1,000 a $10,000 balboas.

- **Muy graves:** recopilar datos persones en forma dolosa, no observar las regulaciones, no suspender el tratamiento cuando exista previo requerimiento de la autoridad, almacenar o transferir internacionalmente datos personales y reincidir en las faltas graves, lo anterior puede conllevar la clausura de los registros de la base de datos y multa correspondiente e incluso la suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento.

Finalmente, el Decreto Ejecutivo establece plazos para la prescripción de la acción y de la sanción:

- Prescripción de la acción:
  1. Las infracciones leves en el plazo de 1 año.
  2. Las infracciones graves en el plazo de 3 años.
  3. Las infracciones muy graves en el plazo de 5 años.

- Prescripción de la sanción:
  1. Las sanciones leves en el plazo de 3 años.
  2. Las infracciones graves en el plazo de 5 años.
  3. Las infracciones muy graves son imprescriptibles.

La Ley 81 de 26 de marzo de 2019 fue publicada en la Gaceta Oficial No.28743-A, entró en vigencia el 29 de marzo de 2021 y el Decreto Ejecutivo 285 de 28 de mayo de 2021 entró en vigencia a partir de su promulgación el día 28 de mayo de 2021 y fue publicada en la Gaceta Oficial No.29296-A.

Redactado por: Mariela de la Guardia Oteiza
8 de junio, 2021