ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
COMISIÓN PERMANENTE ESPECIAL DE CIENCIA, TECNOLOGÍA Y EDUCACIÓN

Texto Actualizado

(26 de enero de 2023)

LEY DE PROTECCIÓN DE DATOS PERSONALES
EXPEDIENTE Nº 23097

PRIMERA LEGISLATURA

SEGUNDO PERÍODO DE SESIONES EXTRAORDINARIAS

ÁREA DE COMISIONES LEGISLATIVAS V
DEPARTAMENTO DE COMISIONES LEGISLATIVAS

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

LEY DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto

1. La presente Ley tiene por objeto:

a. Establecer un conjunto de principios y derechos de protección de datos personales con la finalidad de garantizar un debido tratamiento de los datos personales de los habitantes, independientemente de su nacionalidad.

b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

d. Facilitar el flujo internacional de los datos personales, con la finalidad de coadyuvar al crecimiento social y económico del país.

e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.

ARTÍCULO 2.- Definiciones

1. Para los efectos de la presente Ley se entenderá por:

a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos o plazos desproporcionados, teniendo en cuenta factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento.

b. Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado, independientemente de que los datos se encuentren respaldados en soportes físicos o electrónicos.

c. Cesión de datos: toda revelación de datos realizada a una persona, entidad u organización distinta del Titular.

d. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada del Titular de los datos personales o su representante, a través de la cual acepta, mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.

e. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas de una persona física que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros.

f. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

g. Datos personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

h. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular. Se consideran sensibles los datos personales que revelen el origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; condición socioeconómica, afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

i. Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria en el ámbito público o privado, que revelen información sobre su estado de salud;

j. Encargado: prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del Responsable, trata datos personales a nombre y por cuenta de éste.

k. Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en esta Ley.

l. Fuentes de acceso público: bases de datos que pueden ser accedidas por cualquier persona. Se entienden como fuentes de acceso público, las siguientes: 1) bases de datos de personas jurídicas, bienes inmuebles, bienes muebles, catastro y propiedad industrial del Registro Nacional, 2) los registros de nacimientos, matrimonios y defunciones del Registro Civil, 3) las bases de datos que acrediten la condición de colegiado a un colegio profesional o la habilitación o des habilitación de personas físicas para el ejercicio de determinados oficios, como el notariado, la condición de perito, curador o similares, 4) el diario oficial La Gaceta y el Boletín Judicial, independientemente del soporte físico o digital en el que se publiquen, 5) Las publicaciones realizadas en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación, 6) Las guías, publicaciones, anuarios, directorios y similares que tengan la finalidad comunicar públicamente la pertenencia de determinadas personas a organizaciones gremiales, asociaciones, colegios profesionales u otras organizaciones de la sociedad civil, en el tanto cuenten con el consentimiento del Titular y se cumpla la finalidad para la que dicho consentimiento fue otorgado por el Titular. El funcionamiento de las bases de datos de acceso público respetará los términos de la presente Ley, en especial en cuanto a los principios de legitimación y minimización.

m. Grupo económico: agrupación de sociedades o empresas, de hecho o de derecho, que se manifiesta mediante una unidad de decisión, es decir, la reunión de todos o una parte sustancial de los elementos de mando o dirección empresarial por medio de un centro de operaciones, y que se exterioriza mediante dos movimientos básicos: el criterio de unidad de dirección, ya sea por subordinación o por colaboración entre sus miembros,

o el criterio de dependencia económica de sus miembros, sin importar que su personalidad jurídica se vea afectada, o que su patrimonio sea objeto de transferencia.

n. Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

o. Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un Responsable o Encargado del tratamiento para transferencias, cesiones o un conjunto de transferencias y cesiones de datos personales a un Responsable o Encargado en uno o más países terceros, dentro de un grupo económico o una unión de empresas dedicadas a una actividad económica conjunta.

p. Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

q. Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

r. Sistema de identificación biométrica: sistema o software que se desarrolla empleando: a) estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado, el realizado por refuerzo, o el

aprendizaje automático; b) estrategias basadas en la lógica y el conocimiento; o c) estrategias estadísticas y análogas; destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada. Se entenderá que se utiliza un sistema de identificación biométrica “en tiempo real” cuando la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión.

s. Tercero: persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o Titular del dato, del Responsable del tratamiento, del Encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del Responsable del tratamiento o del Encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

t. Titular o interesado: persona física a quien le conciernen los datos personales.

u. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, cesión, transferencia, difusión, posesión, aprovechamiento, cotejo, interconexión, limitación, supresión, destrucción, y; en general, cualquier uso o disposición de datos personales.

v. Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos personales.

ARTÍCULO 3.- Ámbito de aplicación subjetivo

Esta Ley será aplicable a las personas físicas o jurídicas de carácter privado, y a la Administración Pública en sentido amplio, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones.

ARTÍCULO 4.- Ámbito de aplicación objetivo

1. Esta Ley será aplicable al tratamiento de datos personales de personas físicas que consten o estén destinados a constar en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. También se aplicará al tratamiento de datos personales, incluso cuando los datos personales no formen parte o no estén almacenados en una base de datos.

2. Esta Ley no será aplicable en los siguientes supuestos:

a. Cuando los datos personales estén destinados exclusivamente a actividades en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.

b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales

sometidos a un proceso de anonimización de tal forma que el Titular no pueda ser identificado o reidentificado.

ARTÍCULO 5.- Datos de personas fallecidas

1. En caso de fallecimiento del Titular de los datos, los derechos que reconoce la presente Ley pueden ser ejercidos por sus herederos, que, previa acreditación de su condición, podrán dirigirse al Responsable o Encargado del tratamiento con objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión

2. Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente por escrito o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

3. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

4. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales.

5. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de salvaguardia, si tales facultades se entendieran comprendidas en las medidas de salvaguardia prestadas por el designado.

ARTÍCULO 6.- Ámbito de aplicación territorial

1. Esta Ley resultará aplicable al tratamiento de datos personales efectuado:

a. Por un Responsable o Encargado con establecimiento en la República de Costa Rica.

b. Por un Responsable o Encargado sin establecimiento en la República de Costa Rica, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los habitantes de la República de Costa Rica, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en la República de Costa Rica.

c. Por un Responsable o Encargado que no cuente con establecimiento en la República de Costa Rica, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud de las normas del derecho internacional privado.

2. Para los efectos de la presente Ley, se entenderá por establecimiento el lugar de la administración central o principal del Responsable o Encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables.

3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del Responsable o Encargado.

4. Cuando el tratamiento de datos personales lo realice un grupo económico, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo económico, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

ARTÍCULO 7.- Excepciones generales al derecho a la protección de datos personales

1. No se podrá limitar el derecho a la protección de datos personales mediante ley, salvo de manera excepcional, cuando existan razones que justifiquen su necesidad, sean adecuadas y proporcionales en una sociedad democrática, y respeten los derechos y las libertades fundamentales de los Titulares.

2. Ninguna limitación del derecho fundamental a la protección de datos personales podrá vaciar de contenido este derecho, por lo que se respetará el cumplimiento de las garantías, principios y derechos del Titular que no sea necesario limitar o restringir para acometer el fin público perseguido. El deber de información deberá ser garantizado en todo momento. El incumplimiento de este inciso dará pie a responsabilidad disciplinaria de los funcionarios implicados y a responsabilidad administrativa del Estado, sin perjuicio de las demás sanciones previstas en el régimen sancionatorio de esta Ley o de las responsabilidades penales establecidas en el Código Penal.

3. Cualquier Ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:

a. La finalidad del tratamiento.

b. Las categorías de datos personales de que se trate.

c. El alcance de las limitaciones establecidas.

d. Las garantías adecuadas para evitar accesos, cesiones o transferencias ilícitas o desproporcionadas.

e. La determinación del Responsable o Responsables.

f. Los plazos de conservación de los datos personales.

g. Los posibles riesgos para los derechos y libertades de los Titulares.

h. El derecho de los Titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.

ARTÍCULO 8.- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al Responsable cuando así lo prevea una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras similares, que no deberán ser menores a las garantías y derechos establecidos en esta Ley.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al Responsable cuando derive de una competencia atribuida por una norma con rango de ley.

3. Las transferencias de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, así como todo tratamiento realizado con los datos transferidos, serán lícitas en la medida en que se cumplan las siguientes condiciones acumulativas:

a) Que una ley especial lo autorice expresamente, o que la transferencia sea estrictamente necesaria para cumplir con los fines de interés público asignados por ley a la entidad receptora de los datos. En el caso de esta segunda alternativa, la cesión solo se llevará a cabo previa autorización de la Agencia de Protección de Datos, quien deberá verificar, en un plazo no mayor a 10 días hábiles, el cumplimiento de las siguientes condiciones acumulativas:

> i) la cesión sea absolutamente necesaria para cumplir con el fin público invocado y asignado por ley a la entidad receptora;
> ii) que los datos a ceder son los estrictamente necesarios y adecuados para ese fin.
> iii) que la entidad receptora de los datos cuenta con las medidas de seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos.

b) Que el ente que cede los datos los haya obtenido con fundamento en una de las bases legales previstas en el artículo 15 y en el ejercicio de sus competencias asignadas por ley.

c) Que el ente receptor utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de sus competencias legales vigentes.

d) Que los datos involucrados en la cesión sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización de datos. Se prohíbe la cesión o transferencia masiva e indiscriminada de bases de datos.

4. En cualquiera de los anteriores supuestos, las cesiones deberán ponerse en conocimiento de todos los Titulares de los datos involucrados de manera segura y sin comprometer su confidencialidad, dentro de los siguientes quince días a la ejecución de la cesión. Además, la cesión debe documentarse en un convenio interinstitucional que deberá ser comunicado a la Agencia de Protección de Datos Personales, publicado y puesto a disposición de la ciudadanía para su escrutinio, mediante los medios que se disponga vía Reglamento, resguardando la confidencialidad de los datos personales involucrados en la cesión

5. Las transferencias o cesiones no serán de conocimiento público ni deberán ser puestas en conocimiento de los Titulares cuando tengan por objeto la investigación de un posible delito o para fines policiales, el ejercicio del poder público y potestades de fiscalización de la función pública, ni en aquellos casos donde la revelación de la transferencia o cesión a los Titulares pueda comprometer seriamente el objetivo de interés público perseguido con la transferencia o cesión. No obstante, lo anterior, el Titular tendrá derecho a conocer si sus datos fueron objeto de transferencia o cesión cuando cese el riesgo de que dicha revelación comprometa el interés público antes indicado.

6. No se considerará cesión ni transferencia de datos la remisión de datos personales realizada por un Responsable o Encargado del sector público ante una orden de una autoridad judicial competente en el marco de sus facultades legales, siempre que dicha orden se realice dentro de una investigación o procedimiento específico.

ARTÍCULO 9.- Tratamiento de datos personales de niñas, niños y adolescentes

1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes se privilegiará la protección del interés superior de éstos, conforme a

la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

2. Se promoverá en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

3. Los padres, madres, tutores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

ARTÍCULO 10.- Tratamiento de datos personales sensibles

1. Por regla general, queda prohibido el tratamiento de datos personales sensibles, que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, condición socioeconómica, la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean razonablemente necesarios para el ejercicio y cumplimiento de atribuciones y obligaciones previstas en una norma legal o en un contrato libremente consentido por el Titular de los datos.

b. Se dé cumplimiento a un mandato legal.

c. Sea necesario para proteger intereses vitales del Titular o de otra persona física, en el supuesto de que el Titular no esté capacitado, física o jurídicamente, para dar su consentimiento;

d. Se cuente con el consentimiento expreso del Titular para uno o más fines especificados, consentimiento que podrá derivar de un contrato donde el tratamiento de tales datos sensibles resulta indispensable, siempre que así conste que se haya informado al Titular.

e. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros, fundadas en ley especial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del Titular.

f. Sea necesarios para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, investigación en salud, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación aplicable a la materia o en virtud de un contrato con un profesional de la salud sujeto a la obligación de secreto profesional, o bajo su responsabilidad.

g. Sean necesarios por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, como pandemias debidamente declaradas por las autoridades de salud competentes, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, con fundamento en una legislación que establezca medidas

adecuadas y específicas para proteger los derechos y libertades del Titular, en particular el secreto profesional.

h. Sean con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, con fundamento en una ley especial que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del Titular.

i. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular.

j. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares;

k. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

2. Exclusivamente mediante ley aplicable en la materia podrá establecerse excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles.

ARTÍCULO 11.- Tratamiento de datos personales relativos a condenas e infracciones penales

1. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas. Solo podrá llevarse un registro completo de condenas penales bajo el control del Poder Judicial y/o el Ministerio de Justicia.

2. Además de los funcionarios judiciales involucrados, los abogados en ejercicio podrán realizar tratamiento de datos personales referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas cuando tengan por objeto tratar la información tratada por sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional.

ARTÍCULO 12.-Tratamiento de datos personales obtenidos de fuentes de acceso público

Los datos obtenidos de fuentes de acceso público solo podrán ser tratados para fines lícitos, y de conformidad con los principios de finalidad y minimización previstos en esta Ley, por lo que solo serán incluidos en estas bases los datos estrictamente necesarios, adecuados y pertinentes para cumplir la finalidad pública. Los Titulares gozarán de todos los derechos, principios y garantías establecidos en esta Ley respecto de sus datos personales que consten en fuentes de acceso público.

CAPÍTULO II

PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 13.- Principios aplicables al tratamiento de datos personales

El tratamiento de datos personales deberá realizarse conforme a los principios de exactitud, legitimación, lealtad, transparencia, limitación de la finalidad, minimización, responsabilidad proactiva, seguridad y confidencialidad.

ARTÍCULO 14.- Principio de exactitud

1. Los datos serán exactos, y si fuere necesario, actualizados. No será imputable al Responsable, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a. Hubiesen sido obtenidos por el Responsable directamente del afectado.

b. Hubiesen sido obtenidos por el Responsable de un Encargado que los recolectó en nombre propio para su transmisión al Responsable.

c. Fuesen sometidos a tratamiento por el Responsable por haberlos recibido de otro Responsable en virtud del ejercicio del afectado del derecho a la portabilidad previsto en esta Ley.

d. Fuesen obtenidos de un registro público por el Responsable.

2. En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales.

ARTÍCULO 15.- Principio de legitimación

1. El tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación:

a. El Titular otorgue su consentimiento para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas y se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del Titular ante una autoridad pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el Titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al Responsable.

g. El tratamiento sea necesario para proteger intereses vitales del Titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en una ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable o por un tercero, siempre que sobre dichos

intereses no prevalezcan los intereses o los derechos y libertades fundamentales del Titular que requiera la protección de datos personales, en particular cuando el Titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones.

2. Los supuestos establecidos en los incisos b, c, f y h estarán sujetos al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad.

ARTÍCULO 16.- Condiciones para el consentimiento

1. Cuando sea necesario obtener el consentimiento del Titular, el Responsable demostrará de manera indubitable que el Titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. Si el consentimiento del Titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente Ley.

4. No podrá supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

5. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el Titular podrá revocarlo en cualquier momento, para lo cual el Responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos. La revocación del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación.

6. Cuando los datos y/o el consentimiento se recaben a través de internet, aplicaciones móviles u otros medios electrónicos, el Responsable podrá cumplir su deber de información en capas, suministrando al interesado, en la misma sección donde se recolecta el consentimiento, un vínculo funcional que remita al interesado al sitio donde almacena el Responsable la información exigida en el artículo 6 de esta Ley.

ARTÍCULO 17.- Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de quince años. Se exceptúan los supuestos en que la ley exija la participación de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de quince años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, conforme lo previsto en la legislación respectiva.

ARTÍCULO 18.- Principio de lealtad

1. El Responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del Titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

2. Para los efectos de esta Ley, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los Titulares o excedan las expectativas razonables del Titular respecto a sus finalidades.

ARTÍCULO 19.- Principio de transparencia

1. Cuando se obtengan directamente de un Titular, datos personales relativos a él, el Responsable informará al Titular en el momento en que estos se obtengan sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

2. El Responsable proporcionará al Titular, al menos, la siguiente información:

a. Su identidad y datos de contacto.

b. Los datos de contacto del oficial de protección de datos, de haberlo.

c. Las finalidades del tratamiento a que serán sometidos sus datos personales y la base jurídica del tratamiento.

d. La existencia de cesiones y/o transferencias internacionales de datos personales, los destinatarios, las categorías de datos y finalidades que motivan la realización de las mismas.

e. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

f. El plazo durante el cual se conservarán los datos personales, o cuando no sea posible, los criterios utilizados para determinar ese plazo.

g. En su caso, el origen de los datos personales cuando el Responsable no los hubiere obtenido directamente del Titular.

h. El derecho del Titular a presentar una reclamación ante la Agencia de Protección de Datos.

3. La información proporcionada al Titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los Titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

4. Cuando los datos sean obtenidos del Titular, el Responsable del tratamiento podrá dar cumplimiento al deber de información facilitando al Titular la información básica contenida en los incisos a, b y d del inciso 2 de este artículo, e indicándole una dirección electrónica o proporcionándole un vínculo funcional u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

5. Todo Responsable contará con políticas de tratamiento de datos personales que recojan los principios y disposiciones establecidas en esta Ley.

ARTÍCULO 20.- Principio de finalidad

1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

2. El Responsable no podrá tratar los datos personales en su posesión para finalidades distintas, análogas o compatibles a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

ARTÍCULO 21.- Principio de minimización

1. El Responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

ARTÍCULO 22.- Principio de calidad

1. El Responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento y adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.

2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el Responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

3. En la supresión de los datos personales, el Responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas

relacionadas con exigencias legales aplicables al Responsable. No obstante, el Responsable podrá conservar los datos más allá del plazo de conservación en cumplimiento de un interés legítimo, para el cumplimiento de la finalidad inicial de su tratamiento y con pleno respeto a los derechos y garantías del Titular. Asimismo, la ley podrá establecer excepciones respecto al plazo de conservación de los datos personales. De igual forma, se entenderán válidas las excepciones contenidas en leyes especiales en materia de archivo, investigación o estadística.

ARTÍCULO 23.- Principio de responsabilidad proactiva

1. El Responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en esta Ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al Titular y a la Agencia de Protección de Datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un Encargado a nombre y por cuenta del Responsable, así como al momento de realizar cesiones o transferencias de datos personales.

3. Entre los mecanismos que el Responsable podrá adoptar para cumplir con el principio de responsabilidad proactiva se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar medidas para el análisis de los riesgos asociados al tratamiento de datos personales, y en caso de que corresponda, evaluaciones de impacto de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del Responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los Titulares en los plazos establecidos en esta Ley.

h. Llevar el registro de tratamiento de datos personales, cuando corresponda conforme lo establecido en esta Ley.

i. Designar un oficial de protección de datos personales.

4. El Responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad proactiva, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

ARTÍCULO 24.- Principio de seguridad

1. El Responsable y el Encargado establecerán y mantendrán, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para mantener la confidencialidad, integridad y disponibilidad de los datos personales.

2. Para la determinación de las medidas referidas en el numeral anterior, el Responsable considerará los siguientes factores:

a. El riesgo para los derechos y libertades de los Titulares.

b. El estado de la técnica.

c. Los costos de aplicación.

d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

e. El alcance, contexto y las finalidades del tratamiento.

f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

g. El número de Titulares.

h. Las posibles consecuencias que se derivarían de una violación de la seguridad de los datos personales para los Titulares.

i. La violación de la seguridad de los datos personales previas ocurridas en el tratamiento de datos personales.

3. El Responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica, para garantizar un nivel de seguridad adecuado al riesgo, que podrá incluir entre otros:

a. La seudonimización y el cifrado de los datos personales.

b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resilencia permanentes de los sistemas y servicios de tratamiento.

c. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

4. El Responsable y el Encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del Responsable o del Encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del Responsable, salvo que esté obligada a ello en virtud de disposición legal aplicable.

5. Bajo ninguna circunstancia podrá una entidad u órgano de la Administración Pública o del Estado, invocando el ejercicio de potestades públicas o la satisfacción de intereses públicos, desaplicar o limitar el principio de seguridad aquí descrito.

ARTÍCULO 25.- Notificación de violación a la seguridad de los datos personales

1. Cuando el Responsable tenga conocimiento de una violación de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, aun cuando ocurra de manera accidental, notificará a la Agencia de Protección de Datos Personales y a los Titulares afectados en un plazo de 72 horas, desde que se tuviera conocimiento efectivo, sin dilación alguna.

2. La notificación a los Titulares no resultará aplicable cuando el Responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la violación de seguridad ocurrida, o bien, que se cumple alguna de las siguientes condiciones:

a. Cuando el Responsable ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b. Cuando el Responsable ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del Titulares involucrados;
c. Cuando suponga un esfuerzo desproporcionado para el Responsable. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los Titulares.

3. La notificación que realice el Responsable a los Titulares afectados estará redactada en un lenguaje claro y sencillo, posibilitando acreditar el envío de la notificación referida.

4. La notificación a que se refieren los numerales anteriores, tanto a la Agencia de Protección de Datos como a los Titulares afectados, contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.

b. Los datos personales que pueden considerarse comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al Titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

e. Los medios a disposición del Titular para obtener mayor información al respecto.

4. Cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas establecidas en el inciso primero, el Responsable deberá notificar la información de la que tenga conocimiento a ese momento, debiendo presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo.

5. El Responsable documentará toda violación de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la violación; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la Agencia de Protección de Datos.

6. El reglamento que se dicte a la presente Ley establecerá los efectos de las notificaciones de violaciones de seguridad que realice el Responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los Titulares afectados.

ARTÍCULO 26.- Principio de confidencialidad

1. Los Responsables y Encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad. Este deber será complementario de los deberes de secreto profesional de conformidad con la normativa aplicable.

2. El Responsable o Encargado establecerán controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el Titular.

CAPÍTULO III

DERECHOS DEL TITULAR

ARTÍCULO 27.- Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y de portabilidad

1. En todo momento el Titular o su representante podrán solicitar al Responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen.

2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro.

3. Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario.

ARTÍCULO 28.- Disposiciones generales sobre ejercicio de los derechos

1. Los derechos reconocidos en este Capítulo se ejercerán por medio escrito, y serán comunicados al Responsable en los medios que hubiese puesto a disposición del Titular, por medio del oficial de protección de datos (de haberlo), o, en su defecto, en su domicilio social o establecimiento comercial abierto al público. Podrán ejercerse directamente o por medio de representante legal o voluntario, debiendo estar estos debidamente acreditados. Cuando el Responsable tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

2. El Responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado.

3. El Encargado podrá tramitar, por cuenta del Responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el Responsable. Salvo que otro plazo se estableciera en esta Ley, la respuesta a una solicitud de ejercicio de derechos por parte de un afectado deberá comunicarse en un plazo de cinco días hábiles posteriores a su recepción, al medio señalado por el afectado.

5. En cualquier caso, los Titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley.

6. Serán gratuitas las actuaciones llevadas a cabo por el Responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos.

ARTÍCULO 29.- Derecho de acceso

1. El Titular, previa acreditación de su identidad, tendrá derecho de obtener del Responsable del tratamiento en el plazo de cinco días hábiles, confirmación de si se están tratando o no sus datos personales, y en tal caso, derecho de acceso en el mismo plazo indicado a los datos personales y a la siguiente información:

a. Las finalidades del tratamiento y las bases legales que las legitiman.

b. Las categorías de datos personales de que se trate.

c. Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales.

d. Información sobre las transferencias internacionales de datos que se hayan efectuado o se prevean efectuar, incluyendo los países de destino.

e. El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

f. La existencia del derecho a solicitar del Responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos

personales relativos al Titular, o a oponerse a dicho tratamiento o a presentar una reclamación ante la Agencia de Protección de Datos Personales.

g. Cuando los datos personales no se hayan obtenido del Titular, cualquier información disponible sobre su origen.

h. La existencia o no de decisiones automatizadas respecto del tratamiento de sus datos personales, incluida la elaboración de perfiles.

2. Cuando el Responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el Responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

3. El derecho de acceso se entenderá otorgado si el Responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el Responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

4. El Responsable facilitará una copia de los datos personales objeto de tratamiento. El Responsable podrá cobrar un canon razonable basado en los costos administrativos, por cualquier otra copia solicitada por el Titular. Cuando el Titular presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

5. Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para

ello. En dicho caso, el Responsable podrá denegar la solicitud por ese motivo hasta que transcurra dicho plazo.

ARTÍCULO 30.- Derecho de rectificación

1. El Titular tendrá el derecho a obtener del Responsable, en el plazo máximo de cinco días hábiles, la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

ARTÍCULO 31.- Derecho de cancelación o supresión

1. El Titular tendrá derecho a obtener del Responsable del tratamiento y en el plazo de cinco días hábiles, la cancelación de sus datos personales, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados.

b. El Titular revoque el consentimiento en que se basa el tratamiento, y este no se ampare en otra base legal.

c. El Titular haya ejercido su derecho de oposición con arreglo al artículo 32, y no prevalezcan otros motivos legítimos para el tratamiento.

d. Los datos personales hayan sido tratados ilícitamente.

e. Los datos personales deban suprimirse para el cumplimiento de una obligación legal o por orden de una autoridad competente.

2. El apartado 1 no se aplicarán cuando el tratamiento sea necesario:

a. Para ejercer el derecho a la libertad de expresión e información.

b. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por ley especial que se aplique al Responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al Responsable.

c. Por razones de interés público.

d. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

e. Para la formulación, el ejercicio o la defensa de reclamaciones.

f. Cuando los datos personales deban ser conservados durante los plazos previstos en disposiciones legales o contractuales, entre el Responsable o Encargado del tratamiento y el Titular de los datos.

ARTÍCULO 32.- Derecho de oposición

1. El Titular podrá oponerse en cualquier momento al tratamiento de sus datos personales, cuando dicho tratamiento se fundamente en las causales de los incisos h) e i) del artículo 15 (1) de esta Ley, cuando:

a. Tenga una razón legítima derivada de su situación particular, misma que deberá justificar en su solicitud de oposición.
b. El tratamiento de sus datos personales tenga por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

2. El Responsable del tratamiento deberá responder la solicitud en el plazo máximo de cinco días hábiles, y dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del Titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

3. Tratándose del inciso 1 (b) anterior, cuando el Titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

ARTÍCULO 33.- Derecho a no ser objeto de decisiones individuales automatizadas

1. El Titular tendrá derecho a no ser objeto de una decisión basada en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos o afecten sus intereses de manera significativa, destinadas a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica o crediticia, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el Titular y el Responsable o bien, se base en el consentimiento demostrable del Titular.

3. No obstante, cuando el tratamiento automatizado sea necesario para la relación contractual o el Titular hubiere manifestado su consentimiento, éste tendrá derecho a obtener una intervención humana significativa; recibir una explicación sobre la decisión tomada, siempre que no se revelen con dicha explicación secretos comerciales; así como expresar su punto de vista e impugnar la decisión.

4. El Responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los Titulares, particularmente cuando se basen en datos sensibles, según son definidos en esta Ley.

ARTÍCULO 34.- Derecho a la portabilidad de los datos personales

1. Cuando se traten datos personales por vía electrónica o medios automatizados, el Titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro Responsable, en caso de que lo requiera.

2. El Titular podrá solicitar al Responsable que sus datos personales se transfieran directamente de Responsable a Responsable cuando sea técnicamente posible.

3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

4. Sin perjuicio de otros derechos del Titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el Responsable con base en los datos personales proporcionados por el Titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

ARTÍCULO 35.- Derecho a la limitación del tratamiento de los datos personales

1. El Titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el Responsable.

2. El Titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el Responsable, pero los necesite para formular una reclamación.

ARTÍCULO 36.- Ejercicio de los derechos ARCO y de portabilidad

1. El Responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al Titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

2. Será improcedente el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad en los siguientes casos:

a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público.

b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas expresamente establecidas en la ley.

c. Cuando el Responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del Titular.

d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal.

e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

3. Cuando las solicitudes de ejercicio de derechos sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el Responsable podrá:

a. Cobrar un cargo razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada.

b. Negarse a actuar respecto de la solicitud.

4. En todo caso, el Responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

CAPÍTULO IV

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

ARTÍCULO 37.- Obligaciones del Responsable del tratamiento

1. Los Responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad:

a. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;

b. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de los mismos;

c. Cumplir debidamente con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;

d. Tratar los datos personales bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f. Actualizar los datos personales, rectificar la información cuando sea incorrecta y adoptar medidas necesarias para que la misma se mantenga actualizada;

g. Tramitar debidamente las solicitudes presentadas por el Titular, respondiéndolas de manera completa y oportunamente;

h. Realizar la notificación de violaciones de seguridad en los términos y plazos previstos en esta Ley.

i. Cumplir las instrucciones, órdenes o requerimientos que imparta la Agencia de Protección de Datos Personales.

j. Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado, en entre corresponsables.

k. Verificar que los Encargados, o quienes éstos subcontraten, ofrecen garantías suficientes para realizar el tratamiento de datos personales conforme con los requisitos de la presente Ley y garantice la protección de los derechos del Titular. Dicha verificación debe realizarse con anterioridad a la contratación u realización de otro acto jurídico que lo vincule con el Encargado;

l. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;

2. Para la adopción de las medidas a que se refiere el apartado anterior los Responsables del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a. Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b. Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c. Cuando se produjese el tratamiento no meramente incidental o accesorio de datos sensibles, en los términos que son definidos en esta Ley, o de los datos relacionados con la comisión de infracciones administrativas.

d. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f. Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección por parte de la Agencia de Protección de Datos.

h. Cualesquiera otros que a juicio del Responsable o del Encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

ARTÍCULO 38.- Corresponsables del tratamiento

1. Cuando dos o más Responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente Ley, atendiendo a las actividades que efectivamente desarrolle cada

uno de los corresponsables del tratamiento, en particular en cuanto al ejercicio de los derechos del Titular y a sus respectivas obligaciones de transparencia a que se refiere el artículo 19 de esta Ley. Dicho acuerdo podrá designar un punto de contacto para los Titulares.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los Titulares. Se pondrán a disposición del Titular los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los Titulares podrán ejercer los derechos que les reconoce la presente Ley frente a, y en contra de, cada uno de los Responsables.

ARTÍCULO 39.- Cesión de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, en alguno de los supuestos previstos en el artículo 15.1 de esta Ley, y siempre que dicha cesión sea informada al Titular.

2. Aquel a quien se cedan los datos personales se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley, y a facilitar al Titular de los datos personales cedidos la siguiente información, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos:

a) la identidad y los datos de contacto del Responsable y, en su caso, de su representante;

b) los datos de contacto del oficial de protección de datos, de haberlo;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del Responsable de transferir datos personales a un destinatario en un tercer país.

3. Las disposiciones del apartado anterior no serán aplicables cuando y en la medida en que:

a) el Titular ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. En tales casos, el Responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del Titular;

c) la obtención o la comunicación esté expresamente establecida en una ley, o;

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional emanada en una norma de carácter legal.

ARTÍCULO 40.- Encargado de tratamiento

1. El Encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el Responsable.

2. El acceso por parte de un Encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al Responsable no se considerará cesión ni transferencia de datos siempre que se cumpla lo establecido en la presente Ley y en sus normas de desarrollo.

3. Tendrá la consideración de Responsable del tratamiento y no la de Encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los Titulares aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo siguiente. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de Responsable del tratamiento quien figurando como Encargado utilizase los datos para sus propias finalidades.

4. El Responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del Encargado, los datos personales deben ser destruidos, devueltos al Responsable o entregados, en su caso, a un nuevo Encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al Responsable, que garantizará su conservación mientras tal obligación persista.

5. El Encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el Responsable del tratamiento.

6. En el ámbito del sector público podrán atribuirse las competencias propias de un Encargado del tratamiento a un determinado órgano de la Administración Pública, siempre que sea mediante la adopción de un acto administrativo que deberá incorporar el contenido exigido por el artículo siguiente.

ARTÍCULO 41.- Formalización de la prestación de servicios del Encargado

1. La prestación de servicios entre el Responsable y Encargado se formalizará mediante la suscripción de un contrato de encargo, cuya formalización será responsabilidad del Responsable.

2. El contrato de encargo establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de Titulares, así como las obligaciones y responsabilidades del Responsable y Encargado.

3. El contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el Encargado:

a. Realizar el tratamiento de los datos personales conforme a las instrucciones del Responsable.

b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Responsable.

c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

d. Informar sin dilación alguna al Responsable cuando ocurra una violación de la seguridad de los datos personales que trata por sus instrucciones.

e. Informar sin dilación alguna al Responsable cuando un Titular ejercite sus derechos en materia de protección de datos a través del Encargado.

f. Guardar confidencialidad respecto de los datos personales tratados y garantizar que su personal y cualquier persona autorizada por el Encargado para tratar datos personales del Responsable cuenten con obligaciones contractuales o derivadas de una obligación legal que les obliguen a respetar la confidencialidad de los datos personales tratados.

g. Suprimir, devolver o comunicar a un nuevo Encargado designado por el Responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el Responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el Responsable autorice la comunicación de éstos a otro Encargado.

h. Abstenerse de ceder los datos personales, salvo en el caso de que el Responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

i. Permitir al Responsable o autoridad de control inspecciones y verificaciones en sitio. Estas verificaciones podrán hacerse a través de las certificaciones de seguridad de la información con las que cuente el Encargado.

j. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.

k. Colaborar con el Responsable en todo lo relativo al cumplimiento de la legislación aplicable en la materia, así como facilitar la información necesaria para demostrar el cumplimiento de las obligaciones en el

presente artículo, sea en el marco de una auditoría realizada al Responsable, de un procedimiento de fiscalización por una autoridad competente o cuando dicha obligación derive del contrato de encargo.

4. Cuando el Encargado incumpla las instrucciones del Responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de Responsable.

ARTÍCULO 42.- Subcontratación de servicios

1. El Encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del Responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el Encargado.

2. El subcontratado asumirá el carácter de Encargado.

3. El Encargado formalizará la prestación de servicios del subcontratado a través de un contrato, debiendo aportar las garantías recogidas en el artículo 41 de la presente Ley.

4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a cabo conforme a lo instruido por el Encargado, asumirá la calidad de Responsable.

ARTÍCULO 43.- Registro de actividades de tratamiento

1. Cada Responsable llevará un registro de las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a. El nombre y los datos de contacto del Responsable y, en su caso, del corresponsable, del representante del Responsable, y del oficial de protección de datos.

b. Los fines del tratamiento.

c. Una descripción de las categorías de Titulares y de las categorías de datos personales.

d. Las categorías de destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

e. En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional.

f. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24.

2. Cada Encargado llevará un registro de todas las categorías de actividades de tratamiento de datos personales efectuadas por cuenta de un Responsable que contenga:

a. El nombre y los datos de contacto del Encargado o Encargados y de cada Responsable por cuenta del cual actúe el Encargado, y del oficial de protección de datos, de haberlo.

b. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional.

c. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El Responsable o el Encargado del tratamiento y, en su caso, el representante del Responsable o del Encargado pondrán el registro a disposición de la Agencia de Protección de Datos cuando ésta lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 50 personas y se encuentre registrada y al día como PYME ante el Ministerio de Economía Industria y Comercio, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los Titulares, no sea ocasional, o incluya datos sensibles.

ARTÍCULO 44.- Bloqueo de los datos

1. El Responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Público o las instituciones competentes, en particular de la Agencia de Protección de Datos, para la exigencia de posibles

responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia de Protección de Datos podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el Responsable del tratamiento.

CAPÍTULO V

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

ARTÍCULO 45.- Reglas generales para las transferencias internacionales de datos personales

1. Regla general sobre transferencias internacionales de datos: Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional, si el Responsable y el encargad del tratamiento cumplen las condiciones establecidas en el presente

capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán e interpretarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por la presente Ley no se vea menoscabado.

2. Casos en los que la transferencia internacional de datos es procedente: El Responsable y Encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

a. Consentimiento del Titular: Cuando el Responsable cuente con el consentimiento informado del Titular de los datos.

b. Transferencia fundamentada en un tratado internacional: Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte.

c. Transferencia fundamentada en una decisión de adecuación: Cuando el país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte de la Agencia de Protección de Datos, o bien, el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado, que no podrán ser menores que las reconocidas en la presente Ley.

d. Transferencias fundamentadas en garantías adecuadas del exportador: Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de condiciones mínimas suficientes, derechos exigibles y el acceso a acciones

legales efectivas. Se considerarán como garantías suficientes el cumplimiento de alguna de las siguientes:

i) Que el exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes del cumplimiento de la presente Ley y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los principios y derechos de los Titulares.

ii) Que el exportador y destinatario adopten un esquema de autorregulación vinculante, normas corporativas vinculantes, código de conducta o un mecanismo de certificación local o internacionalmente reconocidos, siempre y cuando estos sean acordes con las disposiciones previstas en esta Ley.

3. En todos los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, deberá asegurar que el importador de los datos personales se encuentre sujeto a la jurisdicción de una o varias autoridades de supervisión independientes -tales como una autoridad de protección de datos y los tribunales que pudieran resultar competentes en el país de destino- de manera que los Titulares cuenten con acciones legales efectivas -administrativas y judiciales- para proteger sus derechos. Asimismo, el acuerdo o mecanismo que instrumente la transferencia deberá reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Agencia de Protección de Datos y de los tribunales de Costa Rica que resulten competentes.

4. Cuando el Titular de forma libre, voluntaria y por su propia iniciativa, transfiera sus datos a un Responsable situado en una jurisdicción diferente a la del Titular.

CAPÍTULO VI

MEDIDAS PROACTIVAS EN EL TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 46.- Reconocimiento de medidas proactivas

Se establecen como medidas que promueven el mejor cumplimiento de la legislación y que coadyuvan a fortalecer y elevar los controles de protección de datos personales implementados por el Responsable, las que a continuación se indican en el presente Capítulo.

ARTÍCULO 47.- Privacidad por diseño y privacidad por defecto

1. Teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares, el Responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en esta Ley.

2. El Responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en esta Ley. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del Titular, a un número indeterminado de personas.

ARTÍCULO 48.- Oficial de protección de datos personales

1.El Responsable, en aplicación del principio de responsabilidad proactiva y cuando lo estime conveniente, podrá designar a un oficial de protección de datos personales.

2. Los Responsables que designen un oficial de protección de datos, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga.

3. Los oficiales de protección de datos podrán ejercer su función a tiempo completo o parcial, dependiendo del volumen de tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los Titulares, y siempre que las otras funciones que desempeñen no den lugar a un conflicto de interés. El oficial de protección de datos podrá ser una persona física o jurídica, interna o externa a la organización, y deberá acreditar conocimientos especializados en el derecho y la práctica de protección de datos.

4. El Responsable o el Encargado estarán obligados a respaldar al oficial de protección de datos personales, de haberlo, en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.

5. El oficial de protección de datos personales, de haberlo, desempeñará al menos, las siguientes funciones:

a. Informar y asesorar al Responsable o el Encargado respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.

b. Coordinar, al interior de la organización del Responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación aplicable en la materia.
c. Supervisar al interior de la organización del Responsable y del Encargado el cumplimiento de la legislación aplicable en la materia y de sus políticas.

6. Cuando se trate de una persona física integrada en la organización del Responsable o Encargado del tratamiento, el oficial de protección de datos no deberá ser removido ni sancionado por el Responsable por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del oficial de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

7. En el ejercicio de sus funciones el oficial de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el Responsable o el Encargado la existencia de cualquier deber de confidencialidad o secreto.

8. Cuando el oficial de protección de datos tenga conocimiento de la existencia de una violación de seguridad en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del Responsable o Encargado.

9. El oficial de protección de datos personales estará obligado por el secreto profesional y el deber de confidencialidad en lo que respecta al desempeño de sus funciones establecidas en esta Ley."

ARTÍCULO 49.- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos

1. Cuando el Responsable o Encargado hubiera designado un oficial de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquel ante la Agencia de Protección de Datos, dirigirse al oficial de protección de datos de la entidad contra la que se reclame.

En este caso, el oficial de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de cinco días hábiles a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia de Protección de Datos esta podrá remitir la reclamación al oficial de protección de datos a fin de que este responda en el plazo de cinco días hábiles.

Si transcurrido dicho plazo el oficial de protección de datos no hubiera comunicado a la Agencia de Protección de Datos la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en esta Ley y en sus normas de desarrollo.

ARTÍCULO 50.- Mecanismos de autorregulación

1. El Responsable y el Encargado podrán adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de esta Ley y establecer procedimientos de resolución de conflictos entre el Responsable y Titular, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del Titular.

2. Para los efectos del numeral anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral.

3. La Agencia de Protección de Datos establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales.

ARTÍCULO 51.- Evaluación de impacto a la protección de datos personales

1. Cuando el Responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, realizará, de manera previa a la implementación del mismo, una evaluación del impacto a la protección de los datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El Responsable del tratamiento recabará el asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b. Tratamiento a gran escala de datos sensibles o relativos a condenas e infracciones penales previstos en esta Ley.

c. Observación sistemática a gran escala de una zona de acceso público.

4. La Agencia de Protección de Datos deberá promulgar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, asimismo podrá establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

5. La evaluación de impacto deberá incluir como mínimo:

a. Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el Responsable del tratamiento.

b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c. Una evaluación de los riesgos para los derechos y libertades de los Titulares a que se refiere el apartado 1.

d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los Titulares y de otras personas afectadas.

6. El Responsable consultará a la Agencia de Protección de Datos antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección

de los datos pusiera de manifiesto que existe un alto riesgo si el Responsable no toma medidas para mitigarlo. Cuando la Agencia de Protección de Datos considere que el tratamiento previsto podría infringir la normativa vigente en materia de protección de datos, o cuando el Responsable no haya identificado o mitigado suficientemente el riesgo, podrá, en un plazo de dos meses desde la solicitud de la consulta, asesorar por escrito al Responsable, y en su caso al Encargado. Dicho plazo podrá prorrogarse dos meses, en función de la complejidad del tratamiento previsto. La Agencia de Protección de Datos informará al Responsable y, en su caso, al Encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderle hasta que la Agencia de Protección de Datos haya obtenido la información solicitada a los fines de la consulta.

CAPÍTULO VII

DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS

ARTÍCULO 52.- Tratamientos con fines de videovigilancia

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio o bien privado.

3. Los datos serán suprimidos en el plazo máximo de dos meses desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

4. El deber de información previsto en el artículo 19 de esta Ley se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del Responsable y la posibilidad de ejercitar los derechos previstos en el artículo 27 de esta Ley. El Responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el artículo 19 antes citado. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

5. Al amparo del artículo 4.2.a) de la presente Ley, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. Se excluye de esta disposición el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por parte de cuerpos de policía y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones

penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

7. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo siguiente.

8. Se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de video vigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas.

ARTÍCULO 53.- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores del sector público o privado, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores del sector público o privado, se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 52.4 de esta Ley.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores del sector público o privado, tales como vestuarios, servicios sanitarios, salas de lactancia, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

ARTÍCULO 54.- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores del sector público o privado previstas, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores del sector público o privado y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

ARTÍCULO 55.- Datos relativos al comportamiento crediticio del sector financiero y no financiero

1. Los datos personales relativos al comportamiento crediticio tratados por el Centro de Información Crediticia (CIC) se regirán por las normas dictadas por la Superintendencia General de Entidades Financieras respetando las garantías, principios y derechos concedidos en esta Ley, de modo que el acceso a dichos datos permita a las entidades financieras y de crédito valorar el nivel de riesgo de crédito de sus clientes. Esto sin perjuicio del tratamiento que sobre datos crediticios puedan hacer otros Responsables del sector no financiero, en los términos

indicados en el presente artículo y respetando el principio de minimización establecido en esta Ley.

2. Queda expresamente autorizado el tratamiento de datos personales relativos al comportamiento crediticio cuando tengan la finalidad de informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos datos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial y/o crediticio que permitan evaluar los riesgos de contratación, la conducta comercial y/o la capacidad de pago del Titular. Lo anterior, en los casos en que dichos datos personales sean obtenidos de fuentes de acceso público, y/o procedentes de informaciones facilitadas por el acreedor con base en su interés legítimo prevalente, o en las circunstancias previstas en la presente Ley.

3.Cuando se realice una cesión de datos personales para el fin indicado en el párrafo anterior, el acreedor, en calidad de Responsable de los datos, deberá mantener un registro del Titular de los datos cedidos, que podrá ser requerido por la Agencia de Protección de Datos en el marco de una investigación o procedimiento sancionatorio.

4. Los datos personales relativos al comportamiento crediticio que sean significativos para evaluar la solvencia económica o financiera podrán conservarse durante el plazo que resulte necesario, y como máximo, podrán conservarse hasta por cuatro años, desde el vencimiento del plazo original de la operación de crédito. El plazo se reduce a dos años cuando el deudor cancele o extinga la obligación, plazo a contar a partir de la fecha en que lo hace, debiendo constar esta información en el informe crediticio.

5. Cuando se cancele una obligación incumplida registrada en una base de datos de solvencia, o exista una orden judicial o administrativa que así lo ordene, el acreedor de la obligación deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo a todos los Responsables de bases de datos de

solvencia a quienes hubiera informado sobre el incumplimiento de la obligación por parte del deudor. Una vez recibida la comunicación por el Responsable de la base de datos de solvencia, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación en el informe crediticio.

6. Los Responsables de las bases de datos relativos al comportamiento crediticio deberán en todo momento velar por realizar valoraciones objetivas de la información, sin que esta pueda prestarse para ningún tipo de discriminación. Dichas condiciones serán supervisadas por la Agencia de Protección de Datos.

ARTÍCULO 56.- Tratamiento de datos en la investigación en salud

1. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a. El Titular o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica, en los términos previstos en la Ley 9234 Ley Reguladora de Investigación Biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b. Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En tales casos, los Responsables deberán publicar la información establecida en el artículo 19 de la presente Ley, en un lugar fácilmente accesible de la página web corporativa de la institución donde se realice la investigación o estudio clínico,

y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

c. Se considera lícito el uso de datos personales anonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales anonimizados con fines de investigación en salud pública y biomédica requerirá: a) Una separación técnica y funcional entre el equipo investigador y quienes realicen la anonimización y conserven la información que posibilite la reidentificación. b) Que los datos anonimizados únicamente sean accesibles al equipo de investigación cuando:

   i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

   ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Sólo podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

d. Cuando se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

   i) Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 51 de esta Ley. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización de los datos.

ii) Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

iii) Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

iv) Para que responda por el cumplimiento de las obligaciones derivadas de esta Ley, designar un representante legal establecido en la República de Costa Rica, si el promotor de un ensayo clínico no está establecido en el territorio nacional.

e. El uso de datos personales anonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité ético de la investigación previsto en la Ley 9234 Ley Reguladora de Investigación Biomédica. En defecto de la existencia del mencionado Comité, la entidad Responsable de la investigación requerirá informe previo del oficial de protección de datos o, en su defecto, de un experto con los conocimientos en protección de datos personales.

ARTÍCULO 57.- Utilización de medios tecnológicos y datos personales en las actividades electorales

1. El tratamiento de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales deberá respetar lo indicado en el artículo 10 de la presente Ley.

2. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

3. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

4. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

ARTÍCULO 58.- Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su número de cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

2. Cuando se trate de la notificación por medio de edictos, se identificará al afectado exclusivamente mediante el número completo de su cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

3. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

ARTÍCULO 59.- Derecho de rectificación en Internet

1. Toda persona tiene derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.

ARTÍCULO 60.- Tratamiento de datos de contacto de empresarios individuales y profesionales liberales

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 15.1.i) el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a. Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b. Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los Responsables o Encargados del tratamiento a los que se refiere el artículo 79 de esta Ley podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

CAPÍTULO VIII

AGENCIA DE PROTECCIÓN DE DATOS

ARTÍCULO 61.- Disposiciones generales

1. La Agencia de Protección de Datos Personales es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República.

2. Será un órgano desconcentrado del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt). Contará con grado de desconcentración administrativa con idoneidad especial y técnica, dotada de independencia operativa, técnica, administrativa y la potestad legalmente otorgada de dictar reglamentaciones específicas a la presente Ley, en la materia de su especialidad. Para garantizar la calidad e idoneidad de su personal, contará con los profesionales y técnicos que requiera en las materias de su competencia, incluidas personas científicas de datos y expertas en informática, ciberseguridad, entre otros, los cuales estarán sujetos a lo dispuesto por la Ley Marco de Empleo Público, No. 10.159.

Su organización se definirá reglamentariamente y ajustará sus actuaciones a las disposiciones contenidas en esta Ley.

3. Podrá celebrar todo tipo de contratos y convenios permitidos por la ley, con entidades públicas o privadas, tanto a nivel nacional como internacional. Su competencia también abarca facultades plenas para conocer y resolver, ya sea por medio de denuncias o de oficio, así como sancionar, en caso de decidirlo discrecionalmente, toda conducta material o formal que configure una violación de los derechos de las personas a la protección de sus datos personales, en los términos establecidos en esta Ley y sus normas de desarrollo.

4. Sus decisiones darán por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones ante el MICITT ni ser avocadas sus competencias por este.

ARTÍCULO 62.- Régimen económico presupuestario

1. El presupuesto de la Agencia de Protección de Datos estará constituido por:

a. Una transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve coma cero cinco (5 309,05) salarios base, en concordancia con la normativa dispuesta en la Ley N.° 9635, Fortalecimiento de las Finanzas Públicas, de 3 de diciembre de 2018. La Dirección elaborará el presupuesto de la Agencia de Protección de Datos y lo remitirá al jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, para su incorporación dentro del presupuesto de esta cartera ministerial, de conformidad con lo dispuesto en la Ley N.° 9524, Fortalecimiento del Control Presupuestario de los Órganos Desconcentrados del Gobierno Central, de 7 de marzo de 2018. La denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993.

b. Las donaciones y las subvenciones provenientes de otros Estados, entidades públicas u organismos internacionales, que no comprometen la independencia y la transparencia de la Agencia de Protección de Datos, en los términos que establezca el reglamento a esta Ley. No se aceptarán donaciones de empresas que se dediquen a la comercialización de datos personales, sean nacionales o internacionales.

c. Los ingresos por el cobro de sanciones producto del régimen sancionador previsto en esta Ley.

d. Los ingresos producto del canon que establece la presente ley

2. El funcionamiento ordinario de la Agencia de Protección de Datos, así como su presupuesto, estarán sujetos a la fiscalización de la Contraloría General de la República y de la auditoría interna del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, según las competencias establecidas en la normativa vigente.

3. El o la jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones tendrá injerencia en la asignación y ejecución del presupuesto de la Agencia de Protección de Datos Personales.

4. Se autoriza a las instituciones del Estado y entidades públicas estatales, así como a organismos nacionales e internacionales para que efectúen donaciones o aportes a la Agencia de Protección de Datos Personales y le asignen temporalmente el personal calificado para cumplir sus fines y ejecutar proyectos específicos.

ARTÍCULO 63.- Funciones

La Agencia de Protección de Datos tendrá las siguientes funciones:

a. Supervisar la aplicación de esta Ley y sus normas de desarrollo.

b. Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos de acuerdo con el tratamiento de los datos. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención.

c. Emitir criterio a la Asamblea Legislativa, al Poder Ejecutivo y otras instituciones y organismos sobre las medidas legislativas y administrativas

relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento.

d. Promover la sensibilización de los Responsables y Encargados del tratamiento acerca de las obligaciones que les incumben.

e. Previa solicitud, facilitar información a cualquier Titular, en relación con el ejercicio de sus derechos y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados.

f. Investigar, resolver y sancionar, de oficio o a ante denuncia, cualquier infracción atribuida a una persona física o jurídica, del sector público o privado, e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g. Promover acciones de cooperación y armonización normativa con autoridades de protección de datos personales de otros países y entidades u organismos internacionales; celebrar convenios de cooperación y contratos con organizaciones públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia, para el cumplimiento de sus funciones; cooperar con autoridades de protección de datos personales de otros países en la sustanciación de procedimientos sancionatorios, en particular, coordinando sus investigaciones o intervenciones o llevando a cabo acciones conjuntas, y proveyendo asistencia para el ejercicio de los derechos establecidos en esta Ley

h. Llevar a cabo investigaciones sobre la aplicación de la normativa nacional en materia de protección de datos, en particular cuando se basa en la información recibida de otra autoridad de control u otra autoridad.

i. Efectuar un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.

j. Fomentar el uso de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos.

k. Ser el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier convenio internacional en el que sea parte la República de Costa Rica que atribuya a una autoridad nacional de control esa competencia.

l. Emitir dictámenes no vinculantes a solicitud de interesados, con el objeto de brindar criterios generales sobre el cumplimiento de las obligaciones y ejercicio de derechos contemplados en esta Ley y los reglamentos que la desarrollen.

m. Gestionar y administrar sus recursos y presupuesto, para lo que podrá aprobar los contratos de obras y servicios, de acuerdo con el ordenamiento jurídico vigente.

n. Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.

o. Todas aquellas otras que le conceda la presente Ley.

ARTÍCULO 64.- Potestades

1. Para llevar a cabo las funciones de investigación, la Agencia de Protección de Datos podrá:

a. Ordenar al Responsable y al Encargado del tratamiento, sea organismo público o privado, que faciliten cualquier información requerida para el desempeño de sus funciones.

b. Llevar a cabo investigaciones en forma de auditorías de protección de datos.

c. Notificar al Responsable o al Encargado del tratamiento las presuntas infracciones en materia de protección de datos, y, transcurridos los procedimientos respectivos, aplicar las sanciones previstas en esta Ley.

d. Obtener del Responsable y el Encargado del tratamiento, el acceso a todos los datos personales y toda la información necesaria para el ejercicio de sus funciones.

e. Efectuar inspecciones, físicas o virtuales, a todos los locales del Responsable y el Encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de lo cual levantará un acta que cumpla las formalidades previstas en el artículo 270 de la Ley General de la Administración Pública.

f. Dictar las disposiciones que fijen los criterios a que responderá la actuación de la Agencia en la aplicación de la presente Ley, que se denominarán circulares. Para su elaboración se deberán contar con los informes técnicos y jurídicos necesarios, y conceder audiencia a los interesados. Las circulares serán obligatorias una vez publicadas en el Diario Oficial La Gaceta.

g. Elaborar y publicar guías y manuales dirigidos a los Responsables, Encargados y ciudadanía en general, sobre asuntos relacionados con la protección de datos personales, para orientar a los actores hacia el cumplimiento de la legislación.

h. Acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones de la presente Ley, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los Responsables objeto de la auditoría.

i. Dictar y ejecutar medidas cautelares en sede administrativa para garantizar la protección de los datos personales de los habitantes.

Las potestades de inspección y recolección de información otorgadas a la Agencia de Protección de Datos en esta Ley, deberán ser ejercidas con sujeción a los principios de razonabilidad, proporcionalidad e interdicción de la arbitrariedad administrativa, en resguardo de los derechos involucrados, y previa comprobación de indicios suficientes que justifiquen la intervención, o la hagan necesaria para averiguar la verdad real de los hechos investigados, salvo en el caso de auditorías preventivas, en cuyo caso podrá actuar sin comprobación previa de indicios.

ARTÍCULO 65.- Dirección de la Agencia de Protección de Datos

1. La Dirección de la Agencia de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Dirección de la Agencia de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar determinadas funciones técnicas sustantivas como administrativas, y que, en ausencia temporal de la Dirección, le sustituirá en todas sus funciones. La Dirección ejercerá sus funciones con plena independencia y objetividad

3. La Dirección de la Agencia de Protección de Datos y su Adjunto serán nombrados por el Consejo de Gobierno, a propuesta del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, mediante concurso público de antecedentes entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Tienen impedimento para ser nombrados como Director y/o Adjunto los parientes, hasta tercer grado de consanguinidad o afinidad del presidente de la República, los vicepresidentes, los ministros y viceministros o con vínculo civil por afinidad hasta el mismo grado.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones ordenará la publicación en el Diario Oficial La Gaceta así como en medios de comunicación colectiva, la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de las personas candidatas, el MICITT propondrá y el Consejo de Gobierno designará a la Dirección y el Adjunto de la Agencia de Protección de Datos. Una vez que el Consejo de Gobierno haya nombrado al director o directora tanto propietario como adjunto, enviará el nombramiento junto con el expediente del concurso a la Asamblea Legislativa, que dispondrá de un plazo de treinta días naturales para objetar el nombramiento por mayoría calificada. Si en ese lapso no se produjera objeción, se tendrán por ratificados. En caso contrario, el Consejo de Gobierno sustituirá a la persona cuyo nombramiento fue objetado y el nuevo nombramiento deberá seguir el mismo procedimiento previsto anteriormente.

5. El mandato de la Dirección y del Adjunto de la Agencia de Protección de Datos tiene una duración de cinco años y puede ser renovado para un único período adicional de igual duración.

La Dirección y el Adjunto solo cesarán de su cargo antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Gobierno, por:

a. Incumplimiento grave de sus obligaciones.

b. Incapacidad física o cognitiva sobrevenida para el ejercicio de su función por un plazo superior a seis meses.

c. Incompatibilidad grave por hechos sobrevenidos que impidan o dificulten que pueda ejercer las funciones atribuidas en esta Ley de forma imparcial e independiente, y en cumplimiento del interés público.

d. Condena firme por delito doloso, incluso en grado de tentativa.

La remoción de la Dirección de la Agencia de Protección de Datos por las causales de los incisos a) y c) anteriores deberá tramitarse ante el Consejo de Gobierno, mediante el procedimiento ordinario establecido en la Ley N.º 6227, Ley General de la Administración Pública, de 2 de mayo de 1978 y sus reglamentos. Una vez tramitado el procedimiento, pero de previo a la adopción de la resolución final que decida sobre la separación, el Consejo de Gobierno enviará a la Procuraduría General de la República el expediente, para que ésta se manifieste, en un plazo razonable, sobre el carácter “grave” de la falta o la incompatibilidad y la procedencia de la separación. El criterio de la Procuraduría no será vinculante pero el Consejo deberá motivar su decisión de separarse de dicho criterio, si fuera el caso.

6. Los actos y disposiciones dictados por la Dirección de la Agencia de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la jurisdicción contencioso administrativa.

CAPÍTULO IX

PROCEDIMIENTO EN CASO DE POSIBLE VULNERACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS

ARTÍCULO 66.- Régimen de reclamaciones

1. Todo Titular tendrá derecho a presentar su reclamación ante la Agencia de Protección de Datos, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación aplicable en la materia.

ARTÍCULO 67.- Admisión a trámite de las reclamaciones

1. Cuando se presente ante la Agencia de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia de Protección de Datos podrá inadmitir la reclamación cuando el Responsable o Encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a. Que no se haya causado perjuicio al afectado en el caso de las infracciones leves previstas en el artículo 76 de esta Ley.

b. Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia podrá remitir la misma al oficial de protección de datos que hubiera, en su caso, designado el Responsable del tratamiento.

La Agencia podrá igualmente remitir la reclamación al Responsable o Encargado del tratamiento cuando no se hubiera designado un oficial de protección de datos, en cuyo caso el Responsable o Encargado deberá dar respuesta a la reclamación en el plazo de un mes.

5. La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia de Protección de Datos.

ARTÍCULO 68.- Actuaciones previas de investigación

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia de Protección de Datos podrá llevar a cabo una investigación preliminar a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

2. La investigación preliminar no podrá tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha de la

resolución por la que se decida su iniciación cuando la Agencia de Protección de Datos actúe de oficio.

ARTÍCULO 69.- Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora

1. Concluidas, en su caso, las actuaciones preliminares a las que se refiere el artículo anterior, corresponderá a la Dirección de la Agencia de Protección de Datos, cuando así proceda, ordenar el inicio del procedimiento para el ejercicio de la potestad sancionadora, mediante un traslado de cargos en el que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

ARTÍCULO 70.- Medidas provisionales y de garantía de los derechos

1. Durante la realización de investigación preliminar o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos.

2. En los casos en que la Agencia considere que la continuación del tratamiento de los datos personales, su cesión o transferencia internacional comportará un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los Responsables o Encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos el artículo 27 de esta Ley, la Agencia podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad

sancionadora, mediante resolución motivada y previa audiencia del Responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

ARTÍCULO 71.- Sustanciación de actuaciones

En lo no expresamente previsto en esta Ley, el procedimiento administrativo se sustanciará de conformidad con las reglas para el procedimiento ordinario regulado el Libro Segundo de la Ley General de la Administración Pública.

CAPÍTULO X

RÉGIMEN SANCIONADOR

ARTÍCULO 72.- Sujetos responsables

1. Están sujetos al régimen sancionador establecido en la presente Ley:

   a. Los Responsables o corresponsables de los tratamientos.

   b. Los Encargados de los tratamientos, en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento.

2. No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este Capítulo.

ARTÍCULO 73.- Infracciones

1. Constituyen infracciones los actos y conductas que resulten contrarias a la presente Ley. Si se ha incurrido en alguna de las infracciones tipificadas en esta Ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:

a. Para las faltas leves, una multa hasta de entre cinco y diez salarios base.

b. Para las faltas graves, una multa de diez a cincuenta salarios base.

c. Para las faltas gravísimas, una multa de cincuenta hasta cien salarios base, y, en caso de personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa, el monto superior entre cien salarios base y hasta un dos por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.

ARTÍCULO 74.- Infracciones consideradas gravísimas

1. Se consideran gravísimas y prescribirán a los tres años las siguientes infracciones:

a. El tratamiento de datos personales vulnerando algunos o todos los principios establecidos en el artículo 13 de esta Ley.

b. El tratamiento de datos personales sin que concurra alguna de las condiciones de legitimación del tratamiento establecidas en el artículo 15 de esta Ley.

c. El incumplimiento de los requisitos exigidos para la validez del consentimiento.

d. La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e. El tratamiento de datos personales sensibles sin que concurra alguna de las circunstancias previstas en el artículo 10 de esta Ley

f. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 11 de esta Ley."

g. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 12 de esta Ley.

h. La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en el artículo 19 de esta Ley.

i. La vulneración del deber de confidencialidad establecido en el artículo 26 de esta Ley.

j. La exigencia del pago de un canon para facilitar al afectado la información a la que se refiere el artículo 19 de esta Ley, o por atender las solicitudes de ejercicio de derechos de los afectados previstos en el artículo 27 de esta Ley, fuera del supuestos establecido en el artículo 29 párrafo 4.

k. El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en el artículo 27 de la presente Ley.

l. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en la presente Ley.

m. El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere la presente Ley.

n. El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 44 de esta Ley cuando la misma sea exigible.

o. La resistencia u obstrucción del ejercicio de la función inspectora de la Agencia de Protección de Datos.

p. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

q. La cesión interinstitucional de datos personales en incumplimiento de lo establecido en el artículo 8 de la presente Ley.

r. La utilización de sistemas de identificación biométrica en tiempo real en espacios públicos.

ARTÍCULO 75.- Infracciones consideradas graves

1. Se consideran graves y prescribirán a los dos años las siguientes infracciones:

a. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela.

b. El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, cancelación o supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

c. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

d. La contratación por el Responsable del tratamiento de un Encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.

e. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 41 de esta Ley.

f. La contratación por un Encargado del tratamiento de otros Encargados sin contar con la autorización previa del Responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

g. La infracción por un Encargado del tratamiento de lo dispuesto en la presente Ley, al establecer relaciones en su propio nombre con los afectados aun cuando exista un contrato de encargo, conforme a lo dispuesto en el artículo 41 de esta Ley.

h. No disponer del registro de actividades de tratamiento establecido en el artículo 43 de la presente Ley.

i. No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 43 de la presente Ley.

j. El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 37 de esta Ley.

k. El incumplimiento del deber del Encargado del tratamiento de notificar al Responsable del tratamiento las violaciones de seguridad de los datos personales de las que tuviera conocimiento.

l. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos personales de conformidad con lo previsto en el artículo 25 de la presente Ley.

m. El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

n. No posibilitar la efectiva participación del oficial de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

ARTÍCULO 76.- Infracciones consideradas leves

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal, en particular, las siguientes:

a. El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por el artículo 19 de la presente Ley.

b. No atender las solicitudes de ejercicio de los derechos establecidos en el artículo 27 de esta Ley, salvo que resultase de aplicación lo dispuesto en el artículo 74.1.j) de esta Ley.

c. El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan cedido o transferido los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

d. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 5 de esta Ley.

e. La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 38 de esta Ley o la inexactitud en la determinación de las mismas.

f. No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 38 párrafo 2 de esta Ley.

g. El incumplimiento por el Encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del Responsable del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al Responsable o al Encargado del tratamiento.

h. Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 43 de esta Ley.

i. La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales.

j. El incumplimiento de la obligación de documentar cualquier violación de seguridad.

k. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, salvo que resulte de aplicación lo previsto en el artículo 75.1 l) de esta Ley.

l. No publicar los datos de contacto del oficial de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando hubiere sido designado.

ARTÍCULO 77.- Interrupción de la prescripción de la infracción

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

ARTÍCULO 78.- Sanciones y medidas correctivas

1. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, se tendrá debidamente en cuenta:

a. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de Titulares afectados y el nivel de los daños y perjuicios que hayan sufrido.

b. La intencionalidad o negligencia en la infracción.

c. El carácter continuado de la infracción.

d. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

e. Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f. La afectación a los derechos de los menores.

g. Haber designado de manera proactiva a un oficial de protección de datos, en los términos previstos en esta Ley.

h. Cualquier medida tomada por el Responsable o Encargado del tratamiento para paliar los daños y perjuicios sufridos por los Titulares.

i. El grado de responsabilidad del Responsable o del Encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.

j. Toda infracción anterior cometida por el Responsable o el Encargado del tratamiento.

k. El grado de cooperación con la Agencia de Protección de Datos con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.

l. Las categorías de los datos de carácter personal afectados por la infracción.

m. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el Responsable o el Encargado notificó la infracción y, en tal caso, en qué medida.

n. Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un Responsable o un Encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones de la presente Ley, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones más graves.

4. Será objeto de publicación en el Diario Oficial La Gaceta la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la sanción resulte de una la constatación de una falta grave o gravísima y el infractor sea una persona jurídica o entidad pública.

ARTÍCULO 79.- Régimen aplicable a determinadas categorías de Responsables o Encargados del tratamiento

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean Responsables o Encargados:

a. El Presidente de la República o sus vicepresidentes.

b. La Asamblea Legislativa

c. El Poder Judicial y los órganos jurisdiccionales.

d. El Tribunal Supremo de Elecciones.

e. La Administración Pública centralizada y descentralizada, excluyendo empresas públicas.

f. La Defensoría de los Habitantes.

g. Las Municipalidades.

h. Las Universidades Públicas.

2. Cuando los Responsables o Encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refiere la presente Ley, la Agencia de Protección de Datos Personales dictará resolución sancionando a las mismas con apercibimiento. La resolución ordenará asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al jerarca de la entidad Responsable o encargada del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de Titulares, en su caso.

3. Los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

4. Se deberán comunicar a la Agencia Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán a la Defensoría de los Habitantes las resoluciones dictadas al amparo de este artículo.

ARTÍCULO 80.- Prescripción de las sanciones

1. Las sanciones impuestas en aplicación de esta Ley prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la notificación al investigado, del procedimiento de investigación, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

CAPÍTULO XI

DERECHO DE INDEMNIZACIÓN

ARTÍCULO 81.- Reparación del daño

1. El Titular que sufra daños y perjuicios derivados de una violación de su derecho a la protección de datos personales gozará del derecho de reclamar el resarcimiento de los daños y perjuicios ocasionados en infracción de las disposiciones de la presente Ley. Si dicho daño fue ocasionado por un Responsable y un Encargado, ambos responderán solidariamente de los daños efectivamente ocasionados.

2. El ejercicio de acciones tendientes a la reparación de los daños sufridos será ejercido en la vía judicial y operará un plazo de prescripción de tres años a partir de la existencia del mismo.

ARTÍCULO 82.- Deróguese la Ley 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, del 07 de julio de 2011.

ARTÍCULO 83.- Las plazas de personal, el presupuesto, bienes, equipos y todos los demás activos asignados a la Agencia de Protección de Datos de los Habitantes (PRODHAB) se trasladarán a la Agencia de Protección de Datos Personales creada en esta Ley, a fin de que continúen destinados al cumplimiento de los fines de esta última.

TRANSITORIO I.- El Poder Ejecutivo, mediante las entidades competentes, en un plazo máximo de doce meses contados a partir de la publicación de esta Ley, deberá concretar el traslado de los recursos, bienes y personal de la PRODHAB a la Agencia de Protección de Datos Personales, e iniciar los procedimientos para el nombramiento de los puestos de dirección de esta, en los términos previstos por esta Ley.

TRANSITORIO II.- La PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de doce meses a partir de la publicación de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización.

TRANSITORIO III. El siguiente Presupuesto Ordinario de la República que formule el Poder Ejecutivo después de la publicación de esta Ley, deberá reflejar el traslado

de las partidas presupuestarias del programa presupuestario de la PRODHAB hacia el título presupuestario que se creará, correspondiente a la Agencia de Protección de Datos. La Dirección de la Agencia de Protección de Datos Personales continuará con la misma base salarial que mantiene la Dirección de la PRODHAB, y se tomará como base para el establecimiento de la nuestra estructura de puestos.

TRANSITORIO IV. Las personas físicas y jurídicas, públicas y privadas que ostenten condición de Responsables o Encargadas de datos personales gozarán de un periodo de doce meses a partir de la publicación de esta Ley para adecuar su funcionamiento y tratamiento de datos personales a las disposiciones de esta Ley.

TRANSITORIO V. La Agencia de Protección de Datos emitirá la reglamentación requerida de esta Ley en el plazo de doce meses después de su entrada en funcionamiento.

TRANSITORIO VI. La Superintendencia General de Entidades Financieras dictará las regulaciones requeridas de acuerdo al artículo 55 de esta Ley, en el plazo de doce meses a partir de la publicación de esta Ley.

Rige doce meses posteriores a su publicación.