

ⓘ ALERTA LEGAL

Aprobación proyecto de ley de datos personales en el Congreso Nacional

27_08_2024

Aprobación proyecto de ley de datos personales en el Congreso Nacional

Este lunes 26 de agosto de 2024, el Congreso Nacional aprobó el proyecto de ley de datos personales (PDP). Así, sólo se encuentra **pendiente el examen de constitucionalidad** ante el Tribunal Constitucional y su posterior envío al Presidente de la República para su promulgación, lo cual se estima ocurrirá dentro de este semestre.

El PDP considera un **plazo de vacancia de 24 meses** desde su publicación en el Diario Oficial, y reemplaza el texto vigente de la Ley N° 19.628 sobre Protección de la Vida Privada por uno que sigue los principios y directrices del Reglamento Europeo de Protección de Datos (**GDPR**).

A. Ámbito de aplicación territorial

Las disposiciones del PDP se aplican al tratamiento de datos:

- Si el **responsable está establecido en Chile o contrata un mandatario** independiente de donde esté ubicado.
- Si el tratamiento de datos se realiza para **ofrecer bienes o servicios a personas en Chile o para monitorear su comportamiento**, independiente de que el responsable o mandatario estén ubicados en el país.

Para el PDP el responsable es quien decide sobre el tratamiento de datos, mientras que el mandatario o encargado actúa en nombre del responsable siguiendo sus instrucciones.

B. Conceptos básicos:

- **Datos Personales:** Cualquier información vinculada a una **persona natural** identificada o identificable, quienes son sus **titulares de datos**. Es decir, se incluye datos personales de clientes, proveedores de servicios y empleados.
- **Datos personales sensibles:** especie de datos personales que por su naturaleza **requieren una mayor protección**. El PDP incorpora una lista taxativa: se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género.

C. Derechos del Titular de los Datos Personales

Los titulares de datos tienen los derechos de acceso, rectificación, supresión, oposición, bloqueo, y portabilidad de sus datos personales.

- **Acceso:** Derecho a saber qué datos personales tiene una organización y cómo los usa.
- **Rectificación:** Derecho a corregir datos personales inexactos o incompletos.
- **Supresión (Derecho al olvido):** Derecho a solicitar la eliminación de los datos personales cuando ya no son necesarios o se han procesado ilegalmente.
- **Oposición:** Derecho a oponerse al procesamiento de datos personales, incluyendo tratamientos automatizados.
- **Bloqueo:** Derecho a solicitar suspensión temporal de cualquier operación de tratamiento cuando su exactitud no pueda ser establecida o su vigencia sea dudosa y respecto de los cuales no corresponda la supresión.
- **Portabilidad:** Derecho a recibir los datos personales en un formato estructurado y transferirlos a otro responsable.

D. Ejercicio de Derechos

El titular puede ejercer sus derechos mediante solicitud ante el responsable de los datos, quien debe **acusar recibo y responder la solicitud dentro de 30 días corridos**, extensibles por 30 días corridos adicionales.

E. Obligaciones del responsable de Datos

Garantizar la licitud del tratamiento y proteger los datos mediante medidas técnicas, organizativas y legales adecuadas que aseguren:

i. Información y Transparencia: Facilitar la información sobre finalidad del tratamiento, ejercicio de derechos, política de tratamiento de datos, base de legitimidad del tratamiento, entre otros.

ii. Confidencialidad: El responsable y cualquier persona con acceso a los datos personales deben guardar secreto sobre ellos, incluso después de finalizar su relación con el titular.

iii. Protección por Diseño y por Defecto: El responsable debe aplicar medidas técnicas y organizativas adecuadas desde el diseño y por defecto para garantizar la protección de los datos personales.

iv. Medidas de Seguridad: El responsable debe adoptar medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos y de los sistemas de tratamiento de datos.

v. Reporte de brechas de Seguridad: El responsable debe reportar cualquier vulneración a las medidas de seguridad a la Agencia de Protección de Datos por los medios más expeditos posibles y sin dilaciones indebidas las brechas y para algunas hipótesis deberá incluso notificar a los titulares afectados.

F. Bases legales para el Tratamiento de Datos

El PDP, siguiendo GDPR, amplía las bases de licitud que permiten el tratamiento de datos, considerando:

i. Consentimiento del titular: manifestación de voluntad libre, específica, informada e inequívoca por la que el titular acepta, ya sea mediante una declaración o una clara acción afirmativa (por medios digitales o analógicos), el tratamiento de datos personales que le conciernen para las finalidades informadas, las cuales deben ser específicas, explícitas y lícitas

ii. Ejecución de contractual: Se permite tratamiento de datos, sin autorización del titular, cuando es necesario para la ejecución de un contrato en el que el titular es parte, o para la aplicación de medidas precontractuales.

iii. Cumplimiento de obligación legal: Se autoriza el tratamiento de datos, sin autorización del titular, cuando es necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento.

iv. Protección intereses vitales: El tratamiento de datos sin autorización es legítimo si es necesario para proteger intereses vitales del titular o de otra persona física.

v. Interés público o ejercicio de poderes públicos: Es legítimo el tratamiento de datos sin autorización del titular si se realiza dentro de los ámbitos de competencia del organismo público.

vi. Tratamiento referido a datos socioeconómicos: Será legítimo el tratamiento de datos sin autorización del titular, si estos datos son relativos a obligaciones de carácter económico, financiero, bancario o comercial y siempre que el tratamiento se realice de conformidad con las normas del Título III de la ley.

vii. Intereses legítimos: Se permite el tratamiento sin autorización del titular si ello es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, salvo que prevalezcan los derechos y libertades fundamentales del titular. Por lo anterior, el responsable deberá implementar una evaluación de interés legítimo de forma previa al tratamiento de datos.

G. Nueva Agencia de Protección de Datos Personales ("Agencia")

Esta Agencia será el organismo público **encargado de asegurar el cumplimiento del PDP**, contando, entre otras, con las siguientes funciones y atribuciones:

- a) Dictar instrucciones y normas generales y obligatorias con el objeto de regular las operaciones de tratamiento de datos personales.
- b) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de protección de los datos personales.
- c) Fiscalizar el cumplimiento de las disposiciones de la ley.
- d) Determinar las infracciones e incumplimientos en que incurran quienes realicen tratamiento de datos personales.
- e) Ejercer la potestad sancionadora.
- f) Resolver las solicitudes y reclamos.
- g) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Sanciones y Cumplimiento.

H. Multas y Sanciones

Las infracciones a la ley pueden resultar en **multas y otras sanciones administrativas**.

INFRACCIÓN	DESCRIPCIÓN	SANCIONES
Leves	<ul style="list-style-type: none"> a) Incumplir deber de información y transparencia. b) Falta de datos de contacto actualizados. c) No responder o responder tarde a solicitudes de titulares. d) Omitir comunicaciones obligatorias a la Agencia. e) Incumplir instrucciones generales de la Agencia. f) Otras infracciones no graves o gravísimas. 	Amonestación escrita o multa hasta 5.000 UTM.
Graves	<ul style="list-style-type: none"> a) Tratar datos sin consentimiento o base legal. b) Comunicar o ceder datos sin autorización. c) Tratar datos innecesarios. d) Tratar datos inexactos o desactualizados. e) Obstaculizar derechos de titulares. f) No responder o denegar solicitudes de bloqueo de datos. g) Tratar datos de menores en contravención a la ley. h) Incumplir requisitos para personas jurídicas sin fines de lucro. i) Vulnerar secreto o confidencialidad. j) Incumplir seguridad en tratamiento de datos. k) No reportar vulneraciones de seguridad. l) Medidas de seguridad insuficientes. m) Transferencias internacionales de datos fuera de la ley. n) Incumplir resoluciones de la Agencia. 	<p>Multa hasta 10.000 UTM.</p> <p>En caso de reincidencia, sólo para medianas y grandes empresas, se aplicará dicha multa o el 2% de los ingresos anuales por ventas y servicios en el último año calendario, prefiriéndose la más alta.</p>
Gravísimas	<ul style="list-style-type: none"> a) Tratar datos de forma fraudulenta. b) Usar datos con malicia para fines no consentidos. c) Comunicar datos falsos, incompletos o inexactos. d) Vulnerar secreto sobre datos sensibles. e) Tratar datos sensibles o de menores fuera de la ley. f) No reportar vulneraciones de seguridad deliberadamente. g) Tratar masivamente datos sin autorización legal. h) Transferir datos internacionales fuera de la ley deliberadamente. i) Incumplir resoluciones sobre derechos de titulares. j) Proveer información falsa en registro o certificación. k) Incumplir artículo 15 ter (Evaluación de impacto en protección de datos personales). 	<p>Multa hasta 20.000 UTM.</p> <p>En caso de reincidencia, sólo para medianas y grandes empresas, se aplicará dicha multa o el 4% de los ingresos anuales por ventas y servicios en el último año calendario, prefiriéndose la más alta.</p>

En caso de que se impongan multas por infracciones gravísimas reiteradas, en un período de veinticuatro meses, la Agencia podrá disponer la **suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable**, hasta por un término de treinta días.

Las sanciones que se impongan se publicarán en **Registro Nacional de Sanciones y Cumplimiento**, administrado por la Agencia. El registro será público y su acceso gratuito y se publicará de forma electrónica en la web de la Agencia.

Contacto:



Carolina Flisfich
Socia y líder del área tecnología, privacidad y medios.



Rodrigo Lavados
Consultor del área de tecnología, privacidad y medios.



Gabriel Pensa
Asociado senior, líder de proyectos de datos personales y ética publicitaria.



Eduardo Vilches
Asociado senior, líder de proyectos ciberseguridad y contratación tecnológica.