

LEY PROTECCIÓN DATOS PERSONALES

El presente documento tiene por objetivo presentar un resumen ejecutivo con los principales cambios que la nueva Ley trae consigo y destacar la importancia de comenzar cuanto antes el proceso de adecuación a esta nueva normativa.

Objeto de la Ley y ámbito de aplicación

El **objeto de la Ley** es regular la forma y condiciones en las cuales se efectúa el tratamiento y la protección de los datos personales de las personas naturales.

Aplica a todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos.

No aplica:

- (i) Al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19, N° 12 de la CPR.
- (i) Al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales.

En cuanto al **ámbito de aplicación territorial**, aplica:

- A responsable o mandatario establecido o constituido en territorio nacional.
- A mandatario, independiente de dónde esté, que realice tratamiento de datos personales a nombre de un responsable establecido o constituido en territorio nacional.
- A responsable o mandatario no establecido o constituido en territorio nacional, pero que sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile, o a monitorear su comportamiento, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento.
- A responsable que, no estando establecido en territorio nacional, le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.

Conceptos clave

Dato personal: cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Para determinar si una persona es identificable deberán considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento.

Datos personales sensibles: tendrán esta condición aquellos datos personales que 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, la 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 de una persona natural.

Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.

Titular de datos o titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.

Principios del Tratamiento

Principios rectores que debe observar todo aquel que realice tratamiento de datos personales y durante todo su ciclo de vida:

- **Principio de licitud y lealtad:** datos personales solo pueden ser tratados de manera lícita y leal.
- **Principio de finalidad:** datos personales deben ser tratados para fines específicos, explícitos y lícitos.
- **Principio de proporcionalidad:** limitar datos personales a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.
- **Principio de calidad:** datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.
- **Principio de responsabilidad:** quienes realicen tratamiento de datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de la Ley.
- **Principio de seguridad:** responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción.
- **Principio de transparencia e información:** responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece esta ley, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales.

- **Principio de confidencialidad:** responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad de los mismos.

Bases de Licitud para el Tratamiento

Motivos por los cuales se realiza el tratamiento de datos personales y cuya licitud deberá acreditar el responsable:

- Cuando el titular otorgue su consentimiento.
- Cuando tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de la ley, incluidos los datos referidos a la situación socioeconómica del titular.
- Cuando tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o lo disponga la ley.
- Cuando tratamiento de datos sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas precontractuales.
- Cuando tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular (titular siempre podrá exigir ser informado sobre el tratamiento que lo afecta y el interés legítimo en base al cual se efectúa dicho tratamiento).
- Cuando el tratamiento de datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia u órganos públicos.

Derechos de los titulares de datos

Aquellos derechos que le asisten a los titulares de datos personales y que podrá ejercer ante los responsables del tratamiento:

- Acceso (Art. 5°)
- Rectificación (Art. 6°)
- Supresión (Art. 7°)
- Oposición (Art. 8°)
- A no ser objeto de decisiones individuales automatizadas (Art.8 bis)
- Bloqueo (Art. 8. Ter)
- Portabilidad de datos (Art. 9°)

Es relevante considerar que los **responsables de datos deberán implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz**. Los medios dispuestos por el responsable deben ser sencillos en su operación.

Nuevas responsabilidades y obligaciones

El responsable de datos tiene las siguientes **obligaciones**:

- Informar y poner a disposición del titular los antecedentes que acrediten la licitud del tratamiento de datos que realiza.
- Asegurar que los datos personales se recojan de fuentes de acceso lícitas con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.
- Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y actual.
- Suprimir o anonimizar los datos personales del titular cuando fueron obtenidos para la ejecución de medidas precontractuales.
- Cumplir con los demás deberes, principios y obligaciones.

Responsable que no tenga domicilio en Chile: y que realice tratamiento de datos de personas que residan en el territorio nacional, deberá señalar y mantener actualizado y operativo, un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y de la Agencia.

En cuanto a los **deberes**:

- Deber de secreto o confidencialidad.
- Deber de información y transparencia.
- Deber de protección desde el diseño y por defecto.
- Deber de adoptar medidas de seguridad.
- Deber de reportar las vulneraciones a las medidas de seguridad.

En caso de realizar tratamiento de datos a través de un tercero mandatario o encargado, se deberá cumplir y atender a las consideraciones contenidas en el artículo 15 bis. Dicho tratamiento se regirá por el contrato celebrado entre el responsable y el encargado y que deberá contener los elementos especiales que señala dicha norma.

Además, cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el **responsable del tratamiento deberá realizar**, previo al inicio de las operaciones del tratamiento, **una evaluación del impacto en protección de datos personales**.

Nuevo órgano de control especializado y Régimen sancionatorio

Desde la perspectiva del órgano de control y la exigibilidad de los derechos de las personas en materia de datos personales, con esta nueva Ley se avanza desde una lógica judicial a una de carácter administrativa, donde el organismo a cargo de fiscalizar este nuevo estándar

normativo será la **Agencia de Protección de Datos Personales, órgano administrativo de carácter técnico, con facultades regulatorias, interpretativas, fiscalizadoras y sancionatorias.**

En cuanto al **régimen sancionatorio**, ante incumplimientos de la Ley, la Agencia podrá:

- Imponer multas de hasta 100 UTM en caso de Infracciones leves; hasta 5.000 UTM en caso de Infracciones graves; y hasta 10.000 UTM en caso de Infracciones gravísimas;
- Triplicar las multas en caso de reincidencia;
- dichas multas pueden alcanzar hasta un 2% o 4% de los ingresos anuales de grandes empresas en caso de reincidencias de infracciones graves o gravísimas (con topes de 10.000 y 20.000 UTM), respectivamente;
- disponer la suspensión del tratamiento de datos hasta por 30 días como sanción accesoria;
- administrar el Registro Nacional de Sanciones y Cumplimiento (cuyas anotaciones serán de acceso público por 5 años) en que se consignará a los responsables sancionados y las respectivas sanciones.

Por su lado, una de las **principales novedades** que trae consigo la nueva Ley, a diferencia de otros modelos regulatorios a nivel regional como global, es la posibilidad de adoptar, voluntariamente, un **modelo de prevención de infracciones**, que incluye la implementación de un programa de cumplimiento que incluirá asimismo la designación de un Delegado de Protección de Datos Personales.

La adopción de este modelo de prevención de infracciones podrá ser certificado por la Agencia y, en tal caso, ser utilizado como atenuante de responsabilidad ante una eventual infracción a la ley, implicando una **reducción del monto de la multa** a ser impuesta.

Comentarios Finales

La Ley entrará en vigencia dentro de 24 meses luego de su publicación en el Diario Oficial. Con todo, la experiencia comparada (Ej. Unión Europea; Brasil) ha demostrado que incluso con "marchas blancas" de este tipo, las organizaciones tanto del sector público como privado **no alcanzan a adecuar sus procedimientos y políticas internas**, al tratarse de procesos extensos que involucran desembolsos económicos relevantes y, especialmente, un cambio cultural en la estructura organizativa de las empresas.

En Magliona Abogados participamos activamente de la discusión legislativa del proyecto de ley durante sus más de 7 años de tramitación en el Congreso Nacional, entendiendo su **importancia para el desarrollo del ecosistema digital de nuestro país**, y durante el cual se promovió equilibrar adecuadamente el libre flujo de la información, el fomento de la innovación y el desarrollo socioeconómico de una manera responsable y respetuosa de los derechos fundamentales de las personas.

Por ello, entendemos que adaptarse a estos nuevos requerimientos puede ser un desafío significativo. Ante este escenario, **contamos con un equipo especializado con amplia experiencia** en la asesoría y cumplimiento en materia de protección de datos personales, y otras áreas afines de igual relevancia e interrelacionadas entre sí, como lo es la ciberseguridad, prevención, mitigación y respuesta a delitos informáticos, así como los desafíos que en materia laboral y derechos de los consumidores, así como otros sectores regulados (ej. telecomunicaciones; banca y finanzas; fintech), puede implicar una normativa transversal como esta.

Nuestra perspectiva es que las organizaciones pueden utilizar eficientemente el período de vacancia, para diseñar una **adecuación y migración fluida** desde la normativa vigente de protección de datos personales a los estándares de la nueva Ley, integrando las exigencias de normas o sectores especiales y aprovechando los esfuerzos destinados a implementar otros marcos regulatorios afines en materia de ciberseguridad y delitos informáticos.

Andrés Bello 2687
Piso 24 Las Condes
Santiago
Chile

Tel: +56 2 3210 0030
Fax: +56 2 2 377 9451
Email: cmagliona@magliona.cl
Web: www.magliona.cl

