24 de julio de 2024

Comisión Mixta aprueba el texto final del proyecto de ley que modifica la Ley 19.628 sobre Protección de la Vida Privada

Hoy, 24 de julio de 2024, finalizó el proceso de discusión del proyecto de ley que modifica la ley 19.628 sobre Protección de Datos Personales (la Ley) en la Comisión Mixta, siendo aprobado por ésta.

Luego de esta etapa, resta que el texto aprobado por la Comisión Mixta sea aprobado tanto por el Senado como por la Cámara de Diputados. Una vez aprobado, será enviado al Presidente de la República para su aprobación y, eventualmente, sometido a un control de constitucionalidad por parte del Tribunal Constitucional.

La Ley tiene por objeto actualizar el marco normativo respecto de la protección y tratamiento de los datos personales, en línea con estándares internacionales sobre el manejo de dichos datos, inspirándose en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, para elevar los estándares de protección y enfrentar los desafíos de la economía digital, buscando un equilibrio entre la privacidad de las personas y la libre circulación de información.

De esta forma, la nueva Ley supone la implementación de aspectos y cambios relevantes en materia de protección de datos personales, dentro de los cuales se mencionan los siguientes:

I. *Agencia de Protección de Datos Personales*

La Ley contempla la creación de la Agencia de Protección de Datos Personales (la Agencia), que velará por la efectiva protección de los derechos que aseguran la privacidad y los datos personales de las personas, y fiscalizará la observancia de la Ley.

En particular, la Agencia tendrá facultades: **i) normativas**, tales como la de dictar instrucciones y normas generales, aplicar e interpretar normas legales y reglamentarias, proponer normas para asegurar la protección de los datos personales; **ii) fiscalizadoras**, en cuanto al cumplimiento de las disposiciones de la Ley por parte de los responsables, y al resolver las solicitudes y reclamos formulados por los titulares; y **iii) sancionadoras**, al ejercer la potestad sancionadora y determinar las infracciones e incumplimientos en que incurran los responsables del tratamiento.

II. *Ámbito de aplicación*

En primer término, la Ley se aplicará a toda persona natural o jurídica, inclusive órganos públicos, que realicen un tratamiento de datos personales, exceptuando aquellos tratamientos efectuados en ejercicio de las libertades de emitir opinión y de informar, como también al tratamiento realizado por personas naturales en relación con sus actividades personales.

La información contenida en esta alerta fue preparada por Carey y Cía. Ltda. sólo para fines educativos e informativos y no constituye asesoría legal.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43
Las Condes, Santiago, Chile.
www.carey.cl

En cuanto al **ámbito territorial**, la Ley se aplicará a todo tratamiento de datos personales realizado por aquellos "**responsables**" (definidos como "toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales") o "**mandatarios**" (es decir "la persona natural o jurídica que trata datos personales, por cuenta del responsable de datos"): i) establecidos en el territorio nacional; ii) que realicen operaciones de tratamiento de datos personales a nombre de un responsable establecido en el territorio nacional; y iii) cuyas operaciones de tratamiento de datos estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile.

En este sentido, resulta importante destacar que los responsables que correspondan a personas jurídicas **no constituidas en Chile**, deberán señalar por escrito y ante la Agencia (según se define más arriba), mediante un correo electrónico válido y operativo de una persona natural o jurídica, capaz de actuar en su nombre para los efectos de que el titular pueda ejercer sus derechos y comunicarse con el responsable, y donde se le practiquen válidamente las comunicaciones y notificaciones administrativas correspondientes.

III. *Principios que rigen el tratamiento de los datos personales*

La Ley introduce varios principios que los sujetos obligados deberán observar al momento de efectuar un tratamiento de datos personales. Entre estos principios se encuentran:

1. **Principio de licitud y lealtad**: el tratamiento de los datos personales debe ser lícito y leal, y el responsable tiene la carga de acreditarlo.
2. **Principio de finalidad**: los datos personales deberán ser recolectados con fines específicos, explícitos y lícitos, a los cuales se limitará el tratamiento.
3. **Principio de proporcionalidad**: los datos personales tratados deberán limitarse estrictamente a aquellos necesarios, adecuados y pertinentes en relación con los fines del tratamiento.
4. **Principio de calidad**: los datos personales deben ser exactos, completos, actuales y pertinentes según su proveniencia y fines del tratamiento.
5. **Principio de confidencialidad**: el responsable del tratamiento de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad de estos.
6. **Principio de responsabilidad**: los responsables del tratamiento de datos personales serán legalmente responsables del cumplimiento de los principios que señala la Ley.

IV. *Regla general del tratamiento y base de licitud*

La Ley amplía también el catálogo de base de licitud para el tratamiento de datos personales, que estará permitido en los siguientes casos:

1. Cuando su titular otorgue el consentimiento para ello, consentimiento que deberá ser libre, informado y específico en cuanto a la finalidad del tratamiento. En este sentido, se presume que el consentimiento para tratar datos no ha sido libremente otorgado cuando el responsable lo recaba en el marco de la ejecución de un contrato o la prestación de un servicio en que no es necesario efectuar esa recolección.
2. Cuando se trate de datos relativos a obligaciones económicas, financieras, bancarias o comerciales, y se sujeten a las disposiciones específicas del Título correspondiente de la Ley.
3. Cuando el tratamiento sea necesario para la ejecución de una obligación legal.
4. Cuando el tratamiento sea imprescindible para la celebración de un contrato entre el titular y el responsable.

5. Cuando el tratamiento sea indispensable para la satisfacción de intereses legítimos del responsable o de un tercero.
6. Cuando el tratamiento sea necesario para la formulación, ejercicio o defensa de un derecho ante tribunales u organismos públicos
7. Cuando así lo disponga la Ley.

V. *Derechos de los titulares de datos personales (Derechos ARCOP)*

La Ley señala que toda persona, actuando por sí o representada, tendrá los derechos de: i) acceso; ii) rectificación; iii) supresión; iv) oposición; v) oposición a decisiones individuales automatizadas; vi) portabilidad; y vii) bloqueo de sus datos personales, los que serán personales, intransferibles e irrenunciables.

1. **Derecho de acceso**: el titular podrá exigir del responsable: i) confirmación de si sus datos están siendo tratados por él; ii) cuáles son los datos tratados y su origen; iii) finalidad del tratamiento; iv) destinatarios de los datos en caso de cesión; v) tiempo de tratamiento, entre otros.
2. **Derecho de rectificación**: el titular podrá requerir del responsable la rectificación de sus datos personales cuando estos sean inexactos, desactualizados o incompletos.
3. **Derecho de supresión**: el responsable, a solicitud del titular, deberá eliminar los datos personales que le conciernen bajo diversas hipótesis.
4. **Derecho de oposición**: el titular podrá oponerse a un tratamiento específico o determinado que realice el responsable, cuando: i) la base de licitud sea la satisfacción de intereses legítimos; ii) los fines del tratamiento sean exclusivamente la mercadotecnia o marketing directo de bienes; y iii) se realice únicamente sobre la base de haber obtenido los datos de una fuente de acceso público.
5. **Derecho de oposición a decisiones individuales automatizadas:** el titular podrá oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales, salvo bajo determinados supuestos.
6. **Derecho de portabilidad**: el titular podrá solicitar y recibir del responsable una copia de los datos que le conciernen, bajo determinados supuestos.
7. **Derecho de bloqueo**: el titular podrá solicitar la suspensión temporal de cualquier operación de tratamiento de sus datos, bajo determinados supuestos.

VI. *Deberes de los responsables del tratamiento de datos*

El responsable, además de las obligaciones correlativas que se derivan del ejercicio de los distintos derechos del titular, estará sujeto a las siguientes obligaciones, entre otras:

1. **Deber de secreto o confidencialidad**: el responsable deberá mantener el secreto o confidencialidad acerca de los datos personales del titular, salvo cuando éste los hubiere hecho públicos, lo que subsistirá aún después de concluida la relación entre ambos.
2. **Deber de información y transparencia**: el responsable deberá facilitar y mantener permanentemente a disposición del público la información relativa a sus políticas de privacidad y a los tratamientos llevados a cabo.
3. **Deber de protección desde el diseño y por defecto**: el responsable deberá aplicar medidas técnicas y organizativas adecuadas desde el diseño, con anterioridad y durante el tratamiento de los datos personales. Asimismo, que garanticen, por defecto, que sólo sean objeto de tratamiento los datos personales específicos y estrictamente necesarios para dicha actividad.
4. **Deber de adoptar medidas de seguridad**: el responsable deberá adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad,

y así garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

5. **Deber de reportar vulneraciones a las medidas de seguridad**: el responsable está obligado a reportar a la Agencia las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos, o la comunicación o acceso no autorizados a los mismos.
6. **Deber de realizar una Evaluación de Impacto en Protección de Datos Personales (EIPDP)**: La Ley establece la obligación de realizar una EIPDP bajo determinados supuestos.La EIPDP consiste en un análisis de riesgo que evalúa posibles lesiones a los derechos de los titulares de datos, y se cierra con la emisión de un informe que permite identificar los riesgos y determinar qué medidas es necesario adoptar, ya sea para eliminar dichos riesgos o minimizarlos.
7. **Regular el procesamiento de datos con el mandatario o encargado:** cuando el responsable realice el tratamiento de datos a través de un tercero mandatario o encargado, dicho tratamiento se regirá por el contrato celebrado entre el responsable y el encargado, contrato que deberá regular algunos términos indicados en la Ley.

VII. *Transferencias internacionales de datos personales*

La Ley establece determinadas situaciones en que las operaciones de transferencia internacional de datos están permitidas, dentro de las cuales están las siguientes:

1. Cuando la transferencia se realice a una persona, entidad u organización pública o privada, sujeta al ordenamiento jurídico de un **país que proporcione niveles adecuados de protección** de datos personales (la Agencia será quien determine cuáles países proporcionan niveles adecuados de protección).
2. Cuando la transferencia de datos quede amparada por **cláusulas contractuales** u otros instrumentos jurídicos suscritos entre el responsable que efectúa la transferencia y el responsable o tercero mandatario que la reciba, estableciendo garantías adecuadas para la protección de los datos personales transferidos.
3. Cuando las dos partes involucradas en la transferencia adopten un **modelo de cumplimiento o mecanismo de certificación,** donde se establezcan garantías adecuadas para la protección de los datos personales transferidos.
4. Cuando existe **consentimiento expreso del titular** de los datos para realizar una transferencia internacional de datos específica y determinada.
5. Cuando se refiera a **transferencias bancarias, financieras o bursátiles específicas**.
6. Cuando la transferencia sea necesaria para la **celebración o ejecución de un contrato entre el titular y el responsable**, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.

VIII. *Categorías especiales de datos personales*

La Ley establece una regla general para el tratamiento de datos sensibles (es decir, aquellos 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, 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) sujetando el tratamiento de estos datos al consentimiento del titular, salvo algunas excepciones, y regulando distintas subcategorías de datos sensibles, tales como aquellos relativos a la salud y al perfil biológico humano y aquellos biométricos.

Por otro lado, la Ley introduce nuevas categorías especiales de: (i) datos personales de niños y niñas y datos de adolescentes; (ii) datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones, y (iii) datos de geolocalización, regulando específicamente su tratamiento.

IX. *Infracciones y sanciones asociadas*

La Ley prevé diversas sanciones aplicables a causa de la infracción de las obligaciones establecidas, las que se clasifican en tres categorías: leves, graves y gravísimas.

A modo meramente ejemplar, la Ley considerará como infracción leve el incumplimiento total o parcial del deber de información y transparencia; como infracción grave el tratamiento de datos personales sin base de licitud o con una finalidad distinta para la cual se recolectaron; y como infracción gravísima el tratamiento de datos personales de forma fraudulenta.

En cuanto a las sanciones aplicables, la Ley contempla la imposición de multas a beneficio fiscal, dependiendo del tipo de infracción en que incurra el responsable:

1. **Infracciones leves**: Multa de hasta 5.000 UTM;
2. **Infracciones graves**: Multa hasta 10.000 UTM;
3. **Infracciones gravísimas**: Multa hasta 20.000 UTM.

X. *DPO y Modelo de Prevención de Infracciones*

La Ley introduce el concepto de Modelo de Prevención de Infracciones consistente en programas de cumplimiento que los responsables pueden voluntariamente adoptar como un mecanismo de prevención de infracciones a la Ley.

La Ley establece los requisitos mínimos de un Modelo de Prevención de Infracciones y regula su proceso de certificación e inscripción en un Registro Nacional de Sanciones y Cumplimientos, administrado por la Agencia. Cabe señalar que el cumplimiento por parte del responsable de los deberes de dirección y supervisión del Modelo de Prevención de Infracciones certificado por la Agencia pueden constituir una circunstancia atenuante.

A diferencia de regulaciones de otras jurisdicciones, bajo la Ley no existirá obligación para el responsable de contar con un Delegado de Protección de Datos Personales (también conocido como *Data Protection Officer*, o DPO), la figura al interior de la estructura operacional de una entidad que cumple con la función de informar y asesorar a ésta respecto del cumplimiento de la normativa de protección de datos personales. Sin embargo, será imperativo contar con un DPO si se decide adoptar un Modelo de Prevención de Infracciones.

XI. *Entrada en vigencia*

La Ley entrará en vigencia después de **veinticuatro meses** contados desde su publicación en el Diario Oficial.

En los próximos días estaremos actualizando la información disponible en el sitio web que hemos preparado especialmente en relación con el presente proyecto de ley en el siguiente enlace: protecciondedatos.carey.cl

AUTORES: *José Ignacio Mercado, Iván Meleda.*