H · D
LEGAL

HDGROUP.CL

Alerta Legal

Compliance - Fintech

Agosto 2024

SE APRUEBA NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES QUE MODIFICA LA LEY N° 19.628 SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

H · D

Con fecha 26 de agosto de 2024, la Cámara de Diputados aprobó con 66 votos a favor el Proyecto de Ley, Boletín N°11144-07, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, quedando pendiente el control de constitucionalidad por parte del Tribunal Constitucional, y la posterior promulgación del Presidente de la República y publicación en el Diario Oficial.

I. Principales modificaciones.

1. Creación de una Agencia de Protección de Datos Personales.

Se crea la Agencia de Protección de Datos Personales, en adelante, la "Agencia", la cual tendrá por objeto velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales, de conformidad a la Ley, y fiscalizar el cumplimiento de sus disposiciones (Artículo 30 de la Ley).

2. Se explicitan los principios del tratamiento de los Datos Personales.

Se enumeran los principios que rigen el tratamiento de los datos personales, y que consisten en los siguientes (Artículo 3 de la Ley):

- **Principio de licitud y lealtad.** Los datos personales sólo pueden tratarse de manera lícita y leal.

- **Principio de finalidad.** Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento debe limitarse a dichos fines.

- **Principio de proporcionalidad.** Los datos personales que se traten deben limitarse estrictamente a aquellos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.

- **Principio de calidad.** Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.

- **Principio de seguridad.** El responsable debe garantizar estándares adecuados de seguridad para el tratamiento de los datos personales.

- **Principio de transparencia e información.** El responsable del tratamiento debe entregar al titular toda la información necesaria para el ejercicio de los derechos de los titulares.

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

- **Principio de responsabilidad.** Quienes realicen el tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes establecidos en la Ley.

3. Incorporación de los derechos ARSOP+.

Se establecen una serie de derechos para los titulares de los datos personales, y que consisten en los siguientes (Artículo 4 y siguientes de la Ley):

- **Derecho de Acceso.** Consiste en solicitar y obtener del responsable confirmación acerca de si los datos personales que le conciernen están siendo tratados por él, y en tal caso, acceder a dichos datos.

- **Derecho de Rectificación.** Consiste en solicitar y obtener del responsable la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos.

- **Derecho de Supresión.** Consiste en solicitar y obtener del responsable la eliminación de los datos personales que le conciernen, cumpliendo ciertas hipótesis.

- **Derecho de Oposición.** Consiste en oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernen, frente a ciertos supuestos.

- **Derecho de Bloqueo.** Consiste en solicitar la suspensión temporal de cualquier operación de tratamiento de sus datos personales cuando se ejerza una solicitud de rectificación, supresión u oposición, mientras dicha solicitud no sea resuelta.

- **Derecho de Portabilidad.** Consiste en solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato electrónico, estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otros responsables, concurriendo ciertas circunstancias.

- **Derecho a no ser sometido a decisiones individuales automatizadas, incluida la elaboración de perfiles.** Consiste en oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente.

4. Nuevas fuentes de licitud en el tratamiento.

Se establecen nuevas fuentes de licitud en el tratamiento de los datos personales (Artículo 12 y 13 de la Ley).

En este sentido, la regla general para el tratamiento lícito de los datos personales, y que consiste la fuente por antonomasia, es el **consentimiento del titular de los datos personales** (Artículo 12 de la Ley). Este consentimiento debe manifestarse en forma previa e inequívoca, además, debe ser libre, informado y específico en cuanto a su finalidad o finalidades.

Además del consentimiento, existen otras fuentes de licitud, en las cuales no es necesario el con sentimiento del titular, y que consisten en las siguientes (Artículo 13 de la Ley):

- Cuando el tratamiento esté referido a datos relativos a **obligación es de carácter económico, financiero, bancario o comercial, incluidos los datos referidos a la situación socio económica del titular.**

- Cuando el tratamiento sea necesario para la **ejecución o el cumplimiento de una obligación legal o lo disponga la ley.**

- Cuando el tratamiento sea necesario 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.

- Cuando el 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.

- Cuando el tratamiento sea necesario para la **formulación, ejercicio o defensa de un derecho** ante los tribunales de justicia u órganos públicos.

5. Creación de un régimen de infracciones y sanciones.

Se establece un régimen de infracciones de carácter leves, graves y gravísimas, cuyas sanciones van desde una amonestación escrita **hasta una multa de 20.000 U.T.M.**, que, a la fecha, 27 de agosto (UTM: $65.901), **asciende a $1.318.020.000 de pesos**, disponiendo también de agravantes y atenuantes, entre las agravantes, se encuentra la reincidencia, carácter continuado de la infracción, haber puesto en riesgo la seguridad de los derechos y libertades de los titulares (Artículo 33 y siguientes de la Ley); y entre las atenuantes, adquiere especial relevancia la adopción de un Modelo de Cumplimiento en materia de protección de datos personales.

A continuación, se desglosan a modo ejemplificativo, algunas infracciones calificadas de leves, graves y gravísimas.

- **Infracciones leves.**

- Incumplimiento total o parcial del deber de información y transparencia establecido en la Ley.
- Carecer de la individualización del domicilio postal, correo electrónico o medio electrónico equivalente que permita comunicarse con el responsable de datos o su representante legal, actualizado y operativo.
- Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por los titulares de datos.
- Omitir el envío a la Agencia de las comunicaciones previstas obligatoriamente en la Ley o sus reglamentos.

- **Infracciones graves.**

- Tratar los datos personales sin contar con el consentimiento del titular de datos o sin un antecedente o fundamento legal que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.
- Comunicar o ceder datos personales, sin el consentimiento del titular, en los casos en que dicho consentimiento sea necesario, o comunicar o ceder los datos para un fin distinto del autorizado.

- Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento vulnerando el principio de proporcionalidad establecido en la Ley.
- Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, supresión, oposición o portabilidad del titular.
- Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

- **Infracciones gravísimas.**
  - Efectuar tratamiento de datos personales en forma fraudulenta.
  - Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la Ley que autoriza su tratamiento.
  - Comunicar o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos.
  - Realizar a sabiendas operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.
  - Incumplimiento de una resolución de la Agencia que resuelve la reclamación de un titular sobre el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, portabilidad o bloqueo temporal.

6. **Regulación de las transferencias internacionales de datos personales.**

Se regulan los casos en virtud de los cuales se autoriza la transferencia internacional de datos personales, considerando especialmente los niveles de adecuación que tenga el país receptor de los datos personales y cuya fiscalización de dichas operaciones de transferencia le corresponderá a la Agencia (Artículo 27 y siguientes de la Ley).

La vigencia de esta Ley comenzará a regir 24 meses con posterioridad a su publicación en el Diario Oficial.

II. Nuestras recomendaciones.

Frente al establecimiento de cuantiosas multas y sanciones por el incumplimiento de la Ley, resulta relevante determinar por parte de los Responsables[1] las formas de cumplir con estas nuevas obligaciones y estándares, para así, evitar o mitigar sanciones frente a las fiscalizaciones de la Agencia.

A partir de lo anterior, resulta importante que las propias organizaciones establezcan un Modelo de Prevención de Infracciones en materia de Protección de Datos Personales. A mayor abundamiento, la propia Ley dispone que los responsables de datos podrán **voluntariamente adoptar un modelo de prevención de infracciones consistente en un programa de cumplimiento**, en adelante, el "Programa de Cumplimiento" o "Modelo de Cumplimiento", indistintamente, (Artículo 49 de la Ley), estableciendo elementos mínimos que deberá contener, entre ellos:

- Designación de un Delegado de Protección de Datos Personales, en adelante, el "Delegado";
- Definición de medios y facultades del Delegado;

[1] *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 (Artículo 2 letra n) de la Ley).*

- Identificación de la información que se trata, el ámbito territorial de aplicación, la categoría o clase de datos o bases de datos que administra, la caracterización de los titulares de datos;
- Entre otros.

Además de cumplir con los elementos mínimos requeridos por la Ley, las organizaciones podrán adoptar medidas adicionales a modo de complemento, como, por ejemplo:

- Políticas de Privacidad, con el objeto de cumplir con el principio de información y transparencia;
- Adopción de canales y medios para el correcto ejercicio de los derechos ARSOP+, y de denuncias frente a infracciones;
- Capacitaciones de sensibilización y creación de una cultura de cumplimiento para los colaboradores;
- Cláusulas de cumplimiento;
- Matrices de riesgos;
- Protocolos y procedimientos internos en materia de protección de datos personales;
- Canales de denuncias y aplicación de sanciones;
- Entre otras.

A partir de las referidas medidas y buenas prácticas, se podrá garantizar un correcto y lícito tratamiento de los datos personales de conformidad a la Ley. Asimismo, todas las medidas adoptadas por el Responsable permitirán obtener por parte de la Agencia una certificación del Programa de Cumplimiento, que se registrará y que tendrá una vigencia de 3 años.

Por último, cabe destacar que el hecho de que los Responsables dispongan de un Programa de Cumplimiento en materia de Protección de Datos Personales certificado por la Agencia generará una serie de impactos favorables para ellos, entre los que podemos mencionar, los siguientes: la prevención de comisión de conductas infractoras y, en caso de ocurrir, la aplicación de atenuantes de responsabilidad; la generación de un impacto reputacional favorable, en virtud del cual, los titulares de datos personales tendrán conocimiento y certeza de que dichas personas están cumpliendo con la Ley; y, eventualmente, la creación de un impacto comercial positivo, favoreciendo las relaciones de negocios, especialmente en materia de transferencia internacional de datos con otras empresas que se encuentren en países catalogados como “adecuados” en materia de protección de datos personales.

Para más información, contactar a:

Rebeca Zamora
Socia Compliance
rzamora@hdgroup.cl

Matías Langevin
Socio Fintech
mlangevin@hdgroup.cl

Camilo Sanhueza
Asociado Compliance
csanhueza@hdgroup.cl

Fernanda Aillach
Asociada Fintech
faillach@hdgroup.cl