ECIJA

Novedades en materia de protección de datos en Chile

NOTA INFORMATIVA

23.09.2024

Novedades en materia de protección de datos en Chile

SEPTIEMBRE 2024

El pasado 26 de agosto de 2024, tras más de siete años de ardua negociación, el Congreso Nacional de Chile aprobó finalmente el Proyecto de Ley de Datos Personales (en adelante, el "**Proyecto**"). Una vez sea sometido al control de constitucionalidad requerido por la legislación chilena ante el Tribunal Constitucional, será promulgado por el Presidente y publicado en el Diario Oficial para adquirir la categoría de Ley y dejar atrás la connotación de proyecto.

En palabras del legislador chileno, la futura norma tiene por objeto proteger los datos personales de las personas naturales, regulando la forma y condiciones bajo las cuales debe llevarse a cabo su procesamiento, apuntando directamente a resguardar un derecho fundamental.

Desde el momento de su entrada en vigor, **se introducirán cambios fundamentales en la regulación actual en materia de privacidad y protección de datos en todo el territorio chileno**, gobernada principalmente por la Ley 19.628, vigente desde 1999 y que ha quedado completamente desfasada al no poder dar una respuesta completa a los problemas que esta rama del Derecho plantea en la actualidad. El legislador chileno ha contemplado un plazo de 24 meses contados desde la publicación de la ley para adecuar las bases de datos a la nueva legislación desde la publicación.

De esta forma, Chile sigue el modelo de la mayoría de los países de Latinoamérica que han venido, en los últimos años, acercándose a los estándares europeos en materia de privacidad mediante la aprobación y promulgación de normas profundamente **inspiradas en el Reglamento General de Protección de Datos.**

Como consecuencia de ello, **las empresas que operen en el territorio chileno deberán adecuar sus modelos de negocio a las exigencias establecidas por la novedosa normativa. Teniendo en cuenta lo demandante que resulta este proceso, el período que ya transcurre hasta la entrada en vigor definitiva de la Ley se antoja fundamental para acometer esta adecuación.**

[1]Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE

Así, a continuación se incluye un breve resumen sobre las principales novedades que introduce el Proyecto:

1. Ámbito de aplicación territorial de la normativa

Las nuevas previsiones recogidas en el Proyecto y que incorporará la posterior Ley resultarán principalmente vinculantes para todo tratamiento de datos personales que se lleve a cabo:

a) Por un responsable o mandatario (o encargado, como se conoce bajo la normativa europea) establecido o constituido en Chile.

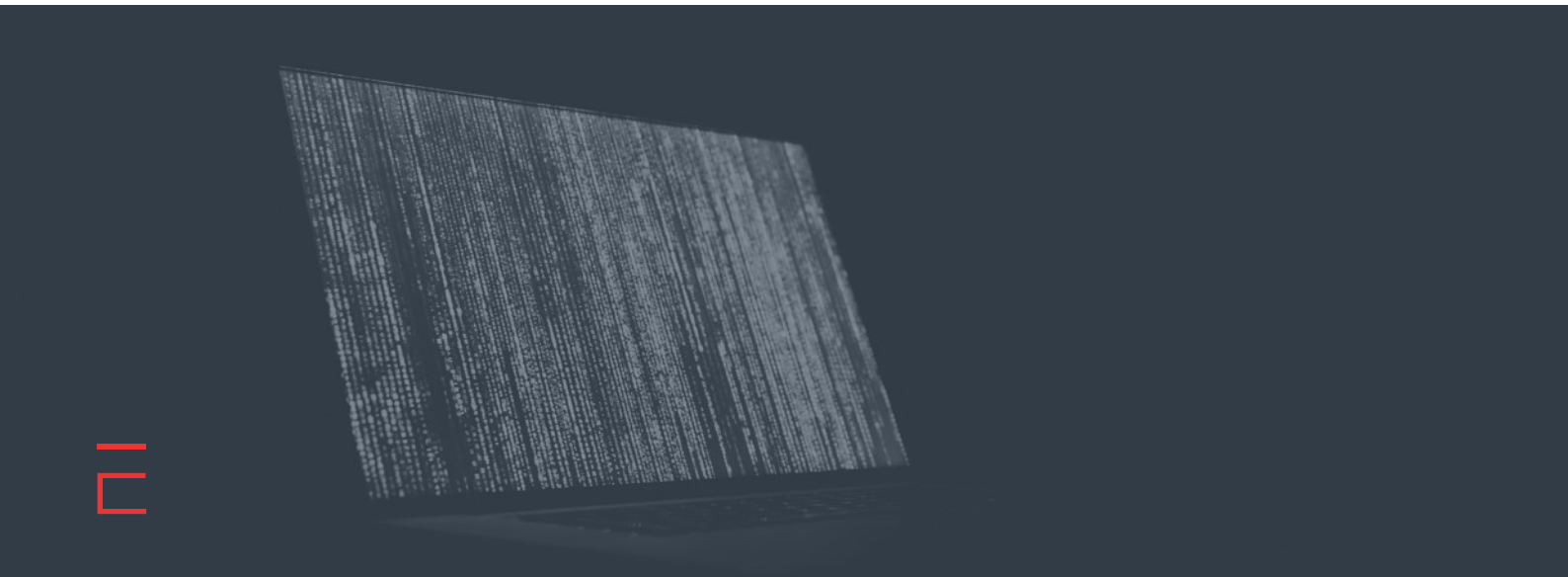
b) Por un mandatario, independientemente de dónde se encuentre, que lleve a cabo operaciones del tratamiento por cuenta de un responsable establecido o constituido en Chile.

c) Por un responsable o mandatario que, aunque no se encuentren establecidos en Chile, sus operaciones de tratamiento estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile.

2. Creación de la Agencia de Protección de Datos y el Registro Nacional de Sanciones

El Proyecto contempla la creación de dos importantes organismos: por un lado, **la Agencia de Protección de Datos Personales**, 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 lo establecido en la nueva norma, y fiscalizar el cumplimiento de sus disposiciones; y, por otro lado, el **Registro Nacional de Sanciones y Cumplimiento**, el cual será administrado por la Agencia, y en el que se publicarán las sanciones impuestas a las empresas que infrinjan la normativa.

El acceso a dicho Registro será libre y gratuito, lo que incrementa la importancia para toda entidad de adecuarse correctamente a la nueva normativa y contar con procesos claros y preventivos ya que el daño reputacional que puede suponer figurar en este Registro resulta incalculable.



3. Régimen sancionador y responsabilidad de las empresas

El Proyecto introduce un novedoso y férreo sistema de sanciones que clasifica las infracciones como leves, graves y gravísimas, en detrimento del laxo régimen que regulaba la Ley 19.628. Así, a partir de ahora las sanciones pueden ser categorizadas como:

INFRACCIONES **leves**	Multa de hasta **5.000 UTM (USD 387.000**) en casos de, por ejemplo, no informar adecuadamente a los titulares sobre el tratamiento.
INFRACCIONES **graves**	Multa de hasta **10.000 UTM (USD 775.000)** en casos de, por ejemplo, tratar datos sin base legal.
INFRACCIONES **gravísimas**	Multa de hasta **20.000 UTM (USD 1.550.000)**, en casos de, por ejemplo, la utilización fraudulenta de los datos.

Es importante resaltar que la reincidencia en infracciones graves o gravísimas acarrea también el riesgo de que las multas no solo se basen en el monto asignado, sino que puedan alcanzar un **2% o 4% de los ingresos anuales** de la empresa, según la gravedad.

A su vez, el Proyecto establece un régimen de responsabilidad civil que, en resumen, establece que el responsable deberá indemnizar el daño patrimonial y extrapatrimonial que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios establecidos en la norma, así como los derechos y obligaciones establecidos y les cause un perjuicio.

Al margen de las elevadas cuantías económicas que pueden acarrear las sanciones impuestas por la Agencia, no se puede olvidar el daño reputacional que provoca en cualquier empresa ser señalada como infractora de la normativa sobre protección de datos, lo que merma enormemente la confianza que las personas depositan en las entidades.

4. Relación entre responsables y mandatarios o encargados

Los requisitos que debe reunir toda relación entre un **responsable** y un **mandatario o encargado** se asemejan en gran medida a los establecidos al respecto por el RGPD, ampliándose de manera relevante la regulación otorgada en la Ley 19.628 en este sentido, introduciendo la obligación de formalizar **acuerdos contractuales detallados** que establezcan claramente las responsabilidades de cada parte y las características principales del tratamiento, así como el régimen de la subcontratación, el destino de los datos al finalizar el encargo o la consideración del encargado o mandatario como responsable en caso de destinar dichos datos a la consecución de sus propias finalidades, entre otros.

5. Nuevo catálogo de derechos para los interesados

Los derechos en materia de protección de datos de los ciudadanos chilenos también traen novedades. El Proyecto incorpora nuevos derechos al catálogo de derechos existente en la ley 19.628, sumando a los ya existentes, estos son, acceso, rectificación, cancelación, oposición y bloqueo, los derechos de portabilidad y oposición a decisiones individuales automatizadas.

Para la correcta atención en tiempo y forma de estas solicitudes, las empresas deberán configurar sistemas y elaborar procedimientos y protocolos que permitan gestionar debidamente los ejercicios de derechos en un plazo de 30 días naturales desde que se reciba la solicitud, plazo que podrá ser prorrogable por 30 días adicionales. En caso de que el titular no quede conforme con la respuesta, tendrá 30 días naturales, prorrogables por otros 30 días para formular una reclamación ante la Agencia.

6. Bases de legitimación para el tratamiento de los datos

Uno de los mayores vacíos legales que presentaba la Ley 19.628 era la ausencia de un abanico de diferentes bases de legitimación que permitiesen a las empresas llevar a cabo con garantías operaciones del tratamiento de los datos que no dependiesen del consentimiento de la persona afectada o de que dicho tratamiento estuviese contemplado expresamente en una norma.

Así, y aunque el consentimiento sigue siendo un pilar fundamental en ese sentido -de hecho, ha sido reforzado, dado que el Proyecto establece claramente que este deberá ser **explícito, informado y revocable**- se han introducido nuevas bases de legitimación para el tratamiento de los datos en reflejo del RGPD, como el **cumplimiento de obligaciones legales**, la **ejecución de contratos** con el interesado, o el **interés legítimo**, del responsable. Esto obliga irremediablemente a llevar a cabo un proceso interno de revisión de las bases de legitimación en las que actualmente las empresas confían para desarrollar sus tratamientos y así asegurar el cumplimiento de la nueva normativa en este sentido.

7. Establecimiento de principios sobre protección de datos

Tal y como estableció en su momento el RGPD, el Proyecto recoge determinados principios que todo tratamiento de datos personales debe cumplir y respetar, incluidos algunos, que la Ley 19.628 no contemplaba. Estos principios se encuentran, nuevamente, inspirados directamente en la norma europea, y son los siguientes:

- Principios de licitud y lealtad.
- Principio de finalidad.
- Principio de proporcionalidad.
- Principio de calidad.
- Principio de responsabilidad.
- Principio de seguridad.
- Principio de transparencia e información.
- Principio de confidencialidad.

8. Obligaciones nuevas para los responsables

El Proyecto también establece un elevado número de obligaciones y tareas que deben acometer todas las empresas para cumplir correctamente con la nueva normativa y garantizar tratamientos de datos seguros y fiables para las personas afectadas.

i. Evaluaciones de impacto

Los tratamientos que impliquen alto riesgo para los derechos de las personas deberán ser sometidos a la realización de **evaluaciones de impacto previas.** Este requisito se vuelve crucial -y obligatorio- en escenarios de tratamiento masivo de datos personales o en situaciones que podrían comprometer sensiblemente la privacidad de los interesados como, por ejemplo, en actividades que impliquen la evaluación sistemática y exhaustiva de aspectos personales, basadas en tratamiento o decisiones automatizadas la observación o monitoreo sistemático de una zona de acceso público, o el tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento. La realización de estas evaluaciones será esencial para prevenir sanciones por parte de la Agencia.

. ii. Vulneraciones de seguridad

Las vulneraciones que comprometan la seguridad de los datos personales y que impliquen un riesgo razonable para los derechos y libertades de los titulares, deberán ser reportadas sin dilaciones a la Agencia de Protección de Datos.

En caso de que las vulneraciones involucren datos sensibles o datos de menores de edad, también se deberá notificar a los titulares afectados. Establecer protocolos de respuesta ante incidentes de seguridad es una necesidad inmediata para cumplir con la ley y evitar sanciones.

iii. Regularización de las transferencias internacionales de datos

De acuerdo con lo establecido en el Proyecto, a partir de su entrada en vigor las transferencias de datos personales realizadas desde Chile a un destinatario que se encuentre en un tercer territorio o estado únicamente estarán permitidas si se siguen los nuevos requisitos establecidos en la normativa como, por ejemplo, que el ordenamiento jurídico del país o territorio donde se encuentre el receptor de los datos pueda proporcionar un **nivel adecuado de protección para los datos** o que la transferencia de datos quede amparada por **cláusulas contractuales, normas corporativas vinculantes, u otros instrumentos jurídicos** suscritos entre las partes involucradas. La nueva regularización de las transferencias limita la operativa de todas las empresas que mantengan relaciones comerciales con el exterior, lo que exige la suscripción de los instrumentos jurídicos correspondientes en aquellos casos en los que no existan con anterioridad.

iv. Protección de datos desde el diseño y por defecto

El Proyecto también establece la obligación de integrar la protección de datos desde la fase de diseño de los sistemas, asegurando que **por defecto** solo se procesen los datos estrictamente necesarios para cada actividad, lo que requiere la adopción de **medidas técnicas y organizativas** desde el inicio de los proyectos y durante todo su ciclo de vida.

Ello exige la implicación de la totalidad de los departamentos de toda empresa bajo la coordinación del Delegado de Protección de Datos o responsable de privacidad interno, resultando ser un proceso complejo y prolongado en el tiempo.

9. Implementación de modelos de prevención

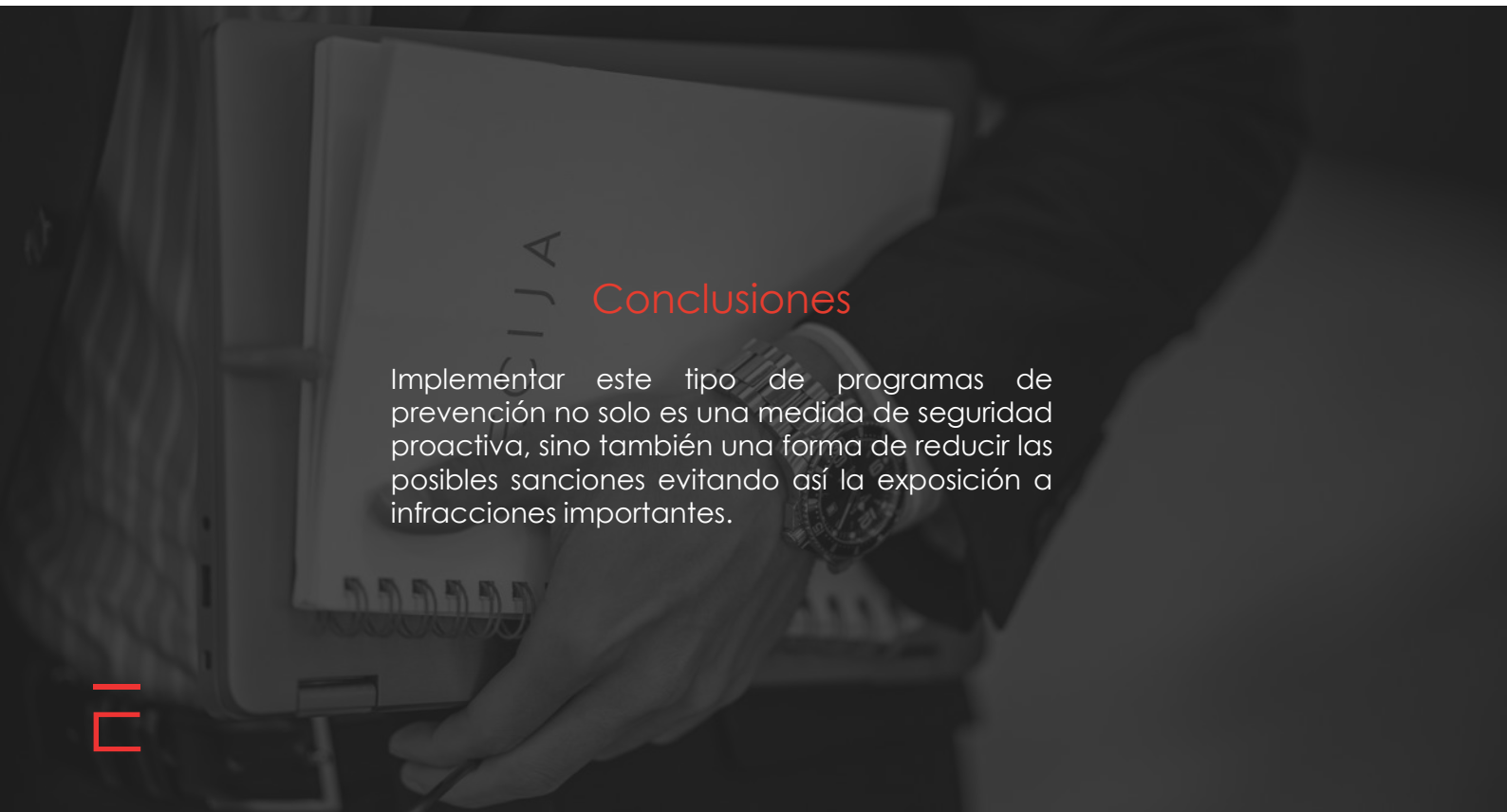
Una de las novedades que el Proyecto introduce es la posibilidad de que los responsables **adopten un modelo de prevención de infracciones consistente en un programa de cumplimiento**. Estos programas de cumplimiento deben incluir, al menos:

La designación de **un delegado de protección de datos,** junto a sus medios y facultades.

La identificación de los tipos de datos tratados y de los procesos que podrían incrementar el riesgo de infracciones.

Protocolos y mecanismos de reporte tanto internos como hacia la Agencia, en caso de vulneraciones de seguridad.

La existencia de **sanciones administrativas internas,** así como de procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.



Conclusiones

Implementar este tipo de programas de prevención no solo es una medida de seguridad proactiva, sino también una forma de reducir las posibles sanciones evitando así la exposición a infracciones importantes.

Área de Protección de Datos de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60

Calle Serrano, 69.
28006 Madrid
www.ecija.com