

# ALERTA LEGAL

**Siete años de espera para un cambio estructural:  
¿Cómo transformará la nueva ley chilena de protección de datos a  
empresas e instituciones?**

---

*29 de agosto de 2024 | Juan Hurtado*

Tras una espera legislativa de siete años, la nueva ley de protección de datos personales en Chile está a punto de convertirse en realidad, y no es solo un cambio normativo: es un desafío directo para los dueños de empresas tanto consolidadas como startups, y para instituciones. **Además de introducir nuevas obligaciones, este nuevo marco legal impone también sanciones significativas por incumplimiento.** Antes de analizar la legalidad y, en palabras simples, se trata de cómo gestionar la información de los clientes y empleados, velando por la debida protección de su privacidad. Dado que la ley comenzará a regir en 24 meses a partir de su publicación -trámite todavía pendiente- **se sugiere a empresas e instituciones que se anticipen y que evalúen y ajusten sus prácticas cuanto antes**, asegurando que no solo se cumpla con la ley, sino que también se gane la confianza de tus clientes en un entorno cada vez más regulado.

En palabras del presidente ejecutivo del World Economic Forum, Klaus Schwab, estamos viviendo la "Cuarta Revolución Industrial", en la que tecnologías emergentes como la inteligencia artificial, la robótica y la biotecnología son las nuevas "máquinas", y los datos, el "combustible" que las impulsa. Estos datos se han convertido en un recurso invaluable, facilitando la toma de decisiones estratégicas y la personalización de servicios, lo que abre nuevas oportunidades para la innovación y el crecimiento. Sin embargo, estas oportunidades conllevan desafíos, especialmente en la protección de datos personales. **Con la nueva ley de protección de datos personales a punto de ser promulgada en Chile, las empresas deben ser más diligentes que nunca en la gestión y seguridad de la información que manejan.**

Es crucial que las empresas entiendan las implicancias legales de la nueva ley de protección de datos personales. Aprovechar las oportunidades que brindan los datos y la tecnología debe ir de la mano con el cumplimiento normativo para proteger la privacidad de los usuarios. A continuación, se hará un análisis normativo detallado, que permitirá identificar cómo esta legislación afectará las operaciones y qué acciones deben tomarse para asegurar el cumplimiento y evitar sanciones.

## **¿CUÁLES SON LAS PRINCIPALES IMPLICANCIAS DE LA NUEVA LEY DE PROTECCIÓN DE DATOS?**

En este análisis, nos enfocaremos en las principales áreas de impacto de la nueva ley, incluyendo los derechos de los titulares de datos, las responsabilidades de quienes gestionan dicha información y los procedimientos necesarios para garantizar el cumplimiento normativo. **Nuestro objetivo es ofrecer una guía clara y práctica que permita a las empresas adaptarse a este nuevo marco regulatorio, protegiendo adecuadamente los datos personales y reduciendo al mínimo los riesgos legales asociados.**

Para dar contexto al análisis, revisemos quiénes son los principales actores en el tratamiento de datos personales. Estos son: el **responsable de datos** y el **encargado de tratamiento**. A continuación, explicamos sus roles con ejemplos ilustrativos:

- **Responsable de datos:** Una tienda en línea que recopila información de sus clientes, como nombres, direcciones y detalles de pago, es la responsable de datos. Esta tienda decide para qué se usan esos datos, por ejemplo, para procesar pedidos y enviar promociones. Es su responsabilidad asegurar que el uso de esos datos cumpla con la ley.
- **Encargado de tratamiento:** Si la tienda en línea contrata a una empresa de servicios de correo electrónico para enviar sus newsletters a los clientes, esta empresa será la encargada de tratamiento. Aunque maneja los datos, lo hace bajo las instrucciones de la tienda y no decide cómo usarlos.

Estos ejemplos muestran cómo, aunque el encargado de tratamiento gestiona los datos, el responsable de datos es quien determina cómo y por qué se tratan. Ambos deben cumplir con la Ley de Protección de Datos Personales para garantizar la seguridad y privacidad de la información.

## I. Ámbito de aplicación de la Ley de Protección de Datos

Para iniciar el análisis de la norma habrá que definir primero quiénes van a ser las personas o instituciones afectadas por la Ley y dentro de qué ámbito territorial.

**Estarán sujetas a esta ley todas las personas naturales y jurídicas, incluyendo organismos públicos, que traten datos personales en el país. Además, la normativa se extiende a organizaciones extranjeras que traten datos de personas en Chile, ya sea ofreciendo servicios o monitoreando su comportamiento.**

Así, **el ámbito territorial de la ley no se limita a las fronteras nacionales.** Cualquier tratamiento de datos que impacte a personas en Chile, sin importar el lugar de origen de la organización responsable, deberá cumplir con las nuevas disposiciones. Este enfoque busca garantizar la protección de los derechos de los individuos en un entorno digital globalizado.

## II. Principios del tratamiento de datos personales

Otro tema de gran importancia, y que fue desarrollado de mejor manera en este proyecto de ley que en la ley anterior, son los principios que rigen el tratamiento de los datos personales. Son de gran importancia, ya que constituyen la base de las obligaciones que recaerán sobre quienes manejan información personal, por lo que implementarlos de buena manera es clave para evitar sanciones.

1. **Principio de licitud y lealtad:** Todo tratamiento de datos debe ser legal y transparente. Esto significa que la recolección y uso de datos personales deben estar respaldados por una base legítima (lo que revisaremos a continuación) y comunicarse de manera clara al titular de los datos.
2. **Principio de finalidad:** Los datos personales solo pueden ser recolectados y utilizados para fines específicos, explícitos y legítimos. Está prohibido utilizar los datos para propósitos distintos de los informados originalmente, a menos que se obtenga un nuevo consentimiento o exista una justificación legal.
3. **Principio de proporcionalidad:** El tratamiento de datos debe limitarse a lo estrictamente necesario. Solo deben recolectarse los datos esenciales y conservarse por el tiempo mínimo requerido para cumplir con el propósito declarado.
4. **Principio de calidad:** La exactitud y actualidad de los datos es fundamental. Quienes manejen información personal deben asegurarse de que los datos sean precisos y pertinentes en todo momento, y actualizarlos cuando sea necesario.
5. **Principio de confidencialidad:** La protección de los datos personales es prioritaria. Se debe garantizar que la información esté resguardada contra accesos no autorizados, y este deber de secreto persiste incluso después de finalizada la relación con el titular.
6. **Principio de responsabilidad:** Los responsables del tratamiento de datos serán legalmente responsables de cumplir con todos estos principios. Esto implica implementar las medidas necesarias para garantizar un tratamiento de datos seguro y conforme a la ley.
7. **Principio de seguridad:** Se deben adoptar medidas técnicas y organizativas adecuadas para proteger los datos personales contra el tratamiento no autorizado o ilícito, así como contra la pérdida, filtración o destrucción accidental.
8. **Principio de transparencia e información:** Los titulares de los datos deben recibir toda la información necesaria para ejercer sus derechos. Esto incluye la comunicación clara y accesible sobre las políticas de privacidad y los tratamientos que se realizan.

Además de ser un requisito legal, el cumplimiento de estos principios representa una oportunidad estratégica para las empresas. Al adoptar estas prácticas, no solo cumplirán con la normativa, sino que también fortalecerán su reconocimiento y reputación ante sus clientes, construyendo una imagen de confianza y compromiso que puede ser clave para su éxito en el mercado.

### III. Bases de licitud para tratar datos personales

**La nueva Ley introduce cambios significativos en las bases de licitud para el tratamiento de datos personales.** Mientras que la legislación anterior se centraba casi exclusivamente en el consentimiento del titular y la autorización legal, la nueva normativa diversifica las bases que legitiman el tratamiento de datos, reduciendo la primacía del consentimiento y abriendo paso a nuevas justificaciones que, si no se manejan con cuidado, podrían comprometer los derechos y libertades del titular.

Las nuevas bases de licitud contempladas en la Ley son:

- 1. Consentimiento del titular:** El tratamiento de datos sigue siendo lícito cuando el titular otorga su consentimiento de manera libre, específica, informada e inequívoca. Aunque sigue siendo una base importante, el consentimiento pierde exclusividad en favor de otras justificaciones.
- 2. Tratamiento de datos económicos, financieros, bancarios o comerciales:** Los datos relacionados con obligaciones económicas, financieras, bancarias o comerciales pueden ser tratados sin consentimiento, siempre que se ajusten a las disposiciones específicas contempladas en el título correspondiente de la Ley.
- 3. Cumplimiento de una obligación legal:** Esta base legitima el tratamiento de los datos, cuando es necesario para cumplir con una obligación impuesta por la ley, como normativas fiscales o de seguridad social.
- 4. Ejecución de un contrato:** El tratamiento de datos es lícito cuando es imprescindible para la celebración o ejecución de un contrato en el que el titular es parte, por ejemplo, en la entrega de un servicio contratado.
- 5. Intereses legítimos del responsable o de un tercero:** Esta es una nueva base de licitud, que permite el tratamiento de datos cuando sea necesario para satisfacer intereses legítimos, siempre que no prevalezcan sobre los derechos y libertades del titular. Este criterio requiere un análisis cuidadoso para evitar abusos.
- 6. Formulación, ejercicio o defensa de un derecho:** Los datos pueden tratarse sin consentimiento cuando sea necesario para formular, ejercer o defender un derecho en procedimientos legales, administrativos o arbitrales.
- 7. Protección de intereses vitales:** Esta base de licitud aplica en situaciones excepcionales en las que el tratamiento de datos es necesario para proteger la vida o integridad física del titular o de otra persona.

Si bien ofrecen flexibilidad operativa, estas nuevas bases de licitud también conllevan riesgos que deben ser gestionados con rigor para garantizar la protección de los derechos de los titulares y evitar posibles conflictos legales. **La correcta implementación y vigilancia de estas bases será crucial para mantener la confianza y evitar sanciones bajo la nueva normativa.**

## **VI. Derecho de los titulares, formas para su ejercicio y deberes del responsable**

**Un aspecto fundamental de la nueva Ley de Protección de Datos Personales es el conjunto de derechos que se otorgan a los titulares de los datos, así como los mecanismos para que estos puedan ejercerlos de manera efectiva.**

La Ley garantiza que los titulares mantengan el control sobre su información personal, estableciendo derechos que son inalienables y que deben ser respetados por todos los responsables de tratamiento. Es importante recalcar que exigir al titular ejercer sus derechos de manera presencial será ilegal.

Los principales derechos que la Ley reconoce a los titulares son:

1. **Derecho de acceso:** Los titulares pueden solicitar información sobre si sus datos están siendo tratados, el propósito de dicho tratamiento, el origen de los datos y los destinatarios a quienes se han comunicado.
2. **Derecho de rectificación:** Permite a los titulares solicitar la corrección de sus datos cuando sean inexactos, incompletos o desactualizados.
3. **Derecho de supresión (derecho al olvido):** Los titulares pueden solicitar la eliminación de sus datos cuando estos ya no sean necesarios para los fines para los cuales fueron recogidos, o cuando el titular retire su consentimiento, entre otras razones.
4. **Derecho de oposición:** Los titulares tienen derecho a oponerse al tratamiento de sus datos en situaciones específicas, como cuando se basa en intereses legítimos del responsable o cuando los datos se usan para marketing directo.
5. **Derecho de portabilidad:** Los titulares pueden solicitar una copia de sus datos en un formato estructurado, de uso común y lectura mecánica, para transferirlos a otro responsable del tratamiento.
6. **Derecho de bloqueo:** Este derecho permite al titular solicitar la suspensión temporal del tratamiento de sus datos mientras se revisa una solicitud de rectificación, supresión u oposición.
7. **Derecho a no ser objeto de decisiones automatizadas:** Los titulares pueden exigir que no se tomen decisiones basadas únicamente en el tratamiento automatizado de sus datos, como la elaboración de perfiles, cuando estas decisiones los afecten significativamente.

**Para garantizar que los titulares puedan ejercer estos derechos, la Ley impone varias obligaciones a los responsables del tratamiento:**

- **Facilitar el ejercicio de los derechos:** Los responsables deben implementar mecanismos claros, accesibles y gratuitos para que los titulares puedan ejercer sus derechos de manera sencilla y eficiente. Esto incluye la obligación de proporcionar respuestas a las solicitudes dentro de los plazos establecidos por la Ley.
- **Transparencia y accesibilidad:** Es responsabilidad del responsable informar de manera clara y comprensible sobre los derechos de los titulares y los procedimientos para ejercerlos. Esta información debe estar siempre disponible y ser fácilmente accesible.
- **Protección de datos desde el diseño y por defecto:** El responsable debe adoptar medidas técnicas y organizativas desde el inicio del tratamiento que permitan a los titulares ejercer sus derechos de manera efectiva y sin obstáculos.
- **Respuesta oportuna:** Las solicitudes de los titulares deben ser atendidas dentro de un plazo máximo de 30 días corridos, con posibilidad de prorrogarse por el mismo periodo en casos excepcionales. Si se deniega una solicitud, el responsable debe justificar su decisión y notificar al titular sobre los recursos disponibles para impugnarla.

**Cumplir con estas obligaciones no solo es crucial para evitar sanciones, sino que también tiene un impacto directo en la reputación y competitividad de las empresas.** Una gestión eficiente y transparente de los derechos de los titulares refuerza la confianza de los clientes, mejora la imagen corporativa y puede convertirse en un diferenciador clave en el mercado. Además, implementar un sistema robusto para el manejo de estos derechos minimiza riesgos legales y protege a la empresa de posibles conflictos que podrían afectar su operación y relaciones comerciales. **En un entorno en el que la protección de datos es cada vez más valorada, responder adecuadamente a estas exigencias legales se traduce en una ventaja competitiva significativa.**

Ahondando en la protección de datos desde el diseño y por defecto y agregando la significancia que tendrá la **Evaluación de Impacto en la Protección de Datos**, la nueva Ley de Protección de Datos Personales impone **dos obligaciones clave** relacionadas con la gestión proactiva de la privacidad.

### 1. Privacidad desde el diseño y por defecto

- Los responsables del tratamiento de datos deben incorporar medidas técnicas y organizativas adecuadas desde la fase de diseño de cualquier proceso, producto o servicio que involucre el manejo de datos personales.
- Estas medidas deben garantizar que, **por defecto**, solo se recolecten y procesen los datos necesarios para cumplir con fines específicos, minimizando la exposición y el riesgo de los datos personales.

### 2. Evaluaciones de Impacto en la Protección de Datos (EIPD)

- La ley obliga a realizar una EIPD cuando el tratamiento de datos pueda implicar un alto riesgo para los derechos y libertades de los titulares, especialmente en casos de uso de nuevas tecnologías o tratamientos masivos.
- La EIPD consiste en un análisis exhaustivo que identifica riesgos y determina las medidas necesarias para mitigarlos, asegurando así la conformidad con la ley y la protección adecuada de los datos.

**Además de los deberes ya mencionados, la ley establece otros en relación con la actividad del responsable de datos, a saber:**

1. **Deber de confidencialidad:** El responsable de datos debe asegurar la confidencialidad de la información personal que trata, evitando su divulgación no autorizada. Este deber persiste incluso después de finalizada la relación con el titular de los datos.
2. **Deber de información y transparencia:** El responsable está obligado a proporcionar información clara y accesible sobre el tratamiento de datos personales, incluyendo la finalidad del tratamiento, los derechos del titular y los mecanismos para ejercerlos. Esta información debe estar permanentemente disponible y ser fácilmente comprensible para los titulares.

3. **Deber de adopción de medidas de seguridad:** El responsable debe implementar medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, pérdida, destrucción o alteración. Estas medidas deben ser proporcionales a los riesgos asociados al tratamiento y al tipo de datos manejados.
4. **Deber de reportar vulneraciones:** En caso de una vulneración de seguridad que comprometa los datos personales, el responsable está obligado a notificar a la Agencia de Protección de Datos Personales y, en ciertos casos, a los titulares afectados. La notificación debe realizarse sin demora injustificada.
5. **Deber de regular la relación con encargados de tratamiento:** Si el responsable delega el tratamiento de datos a un tercero (encargado de tratamiento), debe formalizar esta relación mediante un contrato que establezca las obligaciones del encargado en cuanto a la protección de los datos personales.

## V. Modelos de Prevención de Infracciones y DPO

La nueva Ley de Protección de Datos Personales ofrece herramientas que, correctamente implementadas, pueden actuar como **atenuantes ante posibles sanciones**. Entre ellas destacan los **Modelos de Prevención de Infracciones** y la figura del **Delegado de Protección de Datos (DPO)**, ambos con elementos de obligatoriedad en ciertas circunstancias.

- **Modelos de prevención de infracciones**

Estos modelos son programas de cumplimiento que, aunque su adopción es voluntaria, son altamente recomendados, especialmente para organizaciones que manejan grandes volúmenes de datos o datos sensibles. **Un Modelo de Prevención efectivo incluye políticas claras, procedimientos específicos, capacitación continua y mecanismos de auditoría. La implementación de un Modelo de Prevención certificado por la nueva Agencia de Protección de Datos Personales puede ser clave para reducir sanciones en caso de una infracción**, al demostrar un esfuerzo proactivo de la empresa de cumplir con la ley.

- **Delegado de Protección de Datos (DPO)**

Aunque no obligatorio para todas las empresas, contar con un DPO es altamente recomendable, especialmente para aquellas que manejan grandes volúmenes de datos o datos sensibles. El DPO supervisa el cumplimiento normativo y asesora sobre buenas prácticas. **Su nombramiento, como parte de un Modelo de Prevención, también puede atenuar sanciones**, al evidenciar un compromiso serio con la protección de datos.

**El efecto práctico para las empresas de contar con un Modelo de Prevención de Infracciones y un Delegado de Protección de Datos es la reducción del riesgo de sanciones y la mitigación de su gravedad en caso de infracción**, ya que demuestran un esfuerzo proactivo por cumplir con la normativa.

#### IV. Datos sensibles y categorías especiales

La nueva Ley de Protección de Datos Personales establece una **protección especial para los datos sensibles, que incluyen información sobre origen étnico, creencias religiosas, opiniones políticas, salud, vida sexual y datos biométricos**. El tratamiento de estos datos está estrictamente restringido, generalmente requiriendo el consentimiento expreso del titular, salvo en circunstancias excepcionales como razones de interés público en salud o defensa legal.

Además, la Ley clasifica como categorías especiales **ciertos tipos de datos que requieren un tratamiento aún más cuidadoso**, entre los que se incluyen **los datos de menores de edad, datos utilizados con fines científicos o estadísticos, y datos de geolocalización**. Estas categorías están sujetas a regulaciones adicionales para asegurar que su uso no comprometa los derechos y libertades de los titulares.

El correcto manejo de datos sensibles y categorías especiales es esencial para las empresas, ya que cualquier incumplimiento puede conllevar sanciones severas y afectar gravemente la reputación corporativa.

#### VII. Nueva autoridad de protección de datos, régimen de responsabilidad, infracciones y sanciones

La nueva Ley de Protección de Datos Personales establece la **Agencia de Protección de Datos Personales**, un organismo autónomo responsable de supervisar el cumplimiento de la normativa, emitir directrices y ejercer facultades sancionadoras. Esta Agencia tendrá amplias competencias para fiscalizar a las organizaciones, investigar posibles infracciones y aplicar sanciones cuando corresponda.

Las **infracciones** se clasifican en tres categorías, cada una con sanciones específicas:

- **Infracciones leves**

Ejemplos: Incumplimiento parcial del deber de información y transparencia o no atender de manera oportuna una solicitud de acceso a datos.

Sanción: Multa de hasta 5.000 UTM.

- **Infracciones graves**

Ejemplos: Tratamiento de datos personales sin una base de licitud o uso de datos para una finalidad distinta a la informada al titular.

Sanción: Multa entre 5.001 y 10.000 UTM.

- **Infracciones gravísimas**

Ejemplos: Tratamiento de datos personales de forma fraudulenta o el manejo de datos sensibles sin las medidas de protección adecuadas.

Sanción: Multa entre 10.001 y 20.000 UTM.

**En el caso de grandes empresas, la reincidencia en infracciones graves puede sancionarse con una multa de hasta el 2% de los ingresos anuales por ventas y servicios. Para las infracciones gravísimas, la reincidencia puede llevar a multas que alcancen hasta el 4% de dichos ingresos.** Estas sanciones reflejan la gravedad del incumplimiento repetido y subrayan la importancia de adoptar medidas de cumplimiento efectivas. **Las empresas de mayor tamaño no solo enfrentan multas más elevadas, sino que también deben considerar el impacto financiero y reputacional que podría derivarse de tales sanciones, lo que hace imperativo el establecimiento de un robusto sistema de protección de datos.**

Además de las sanciones económicas, la Agencia de Protección de Datos Personales puede imponer **medidas adicionales**, como la **suspensión temporal de las operaciones de tratamiento de datos**. Esta medida es particularmente relevante para grandes empresas, ya que la interrupción de sus actividades puede tener consecuencias significativas, tanto operativas como reputacionales.

---

Para más información sobre estas materias, contactar a nuestro abogado

Juan Hurtado  
Palma Tech  
[jhurtado@palma.cl](mailto:jhurtado@palma.cl)