

Ley 21.719

PROTECCIÓN DE LOS DATOS PERSONALES

Chile

Guía práctica para empresas y personas

Elaborado por Fransa J. Aravena

Textos simplificados por ChatGPT y Perplexity

Octubre 2025



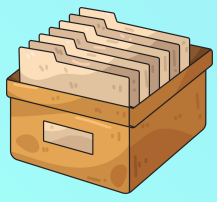
Ley N°21.719



Entra en **vigencia** el 1 de diciembre del 2026.

Afectará a todas las empresas, instituciones y profesionales que manejen información personal en Chile.

OBJETIVO: Garantizar que cada persona tenga control sobre sus datos personales y que las organizaciones los utilicen con transparencia, seguridad y responsabilidad.



Tipos de datos personales protegidos por la Ley 21.719

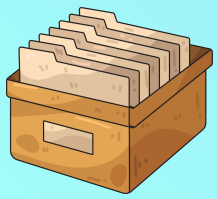
Datos personales: Información relativa a una persona natural identificable, cualquiera sea su formato o soporte. Incluyen, por ejemplo: nombre, RUT, dirección, correo electrónico, número telefónico, historial académico o laboral.

Estos datos solo pueden ser tratados con una base legal válida o consentimiento informado del titular.

Datos personales sensibles: Son aquellos que revelan aspectos íntimos de la persona, como origen étnico, opiniones políticas, creencias religiosas, afiliación sindical, datos biométricos, estado de salud, vida sexual o identidad de género.

Su tratamiento requiere consentimiento expreso y específico, o una autorización legal especial.

La ley exige mayor seguridad y confidencialidad, debido al riesgo que implica su divulgación o uso indebido.



Tipos de datos personales protegidos por la Ley 21.719

Datos biométricos: Datos obtenidos a partir de características físicas, fisiológicas o conductuales que permiten identificar de manera única a una persona (huellas digitales, reconocimiento facial, iris, voz, ADN, entre otros).

Su uso está restringido a fines específicos y legítimos, y requiere medidas de seguridad reforzadas y, en algunos casos, evaluaciones de impacto.

Datos de menores de edad: La ley otorga protección especial a la información de niños, niñas y adolescentes, reconociendo su vulnerabilidad y derecho a la privacidad.

El tratamiento de sus datos requiere el consentimiento de los padres o tutores legales, especialmente cuando se trate de datos sensibles.

Datos anonimizados: Son aquellos que no permiten identificar a una persona una vez que han sido sometidos a procesos técnicos de anonimización.

No se consideran datos personales si la reidentificación es irreversible, pero su manejo sigue sujeto a buenas prácticas de seguridad.



Principios fundamentales

Licitud y lealtad

Los datos solo pueden tratarse de forma legal, justa y transparente.

Las empresas deben poder acreditar la licitud del uso que hacen de los datos.

Finalidad

Los datos deben recopilarse con fines específicos, explícitos y lícitos.

No pueden usarse para otros propósitos, salvo consentimiento del titular o fundamento legal válido.

Proporcionalidad

Solo deben recopilarse los datos estrictamente necesarios.

Una vez cumplido el propósito, deben eliminarse o anonimizarse.

Calidad

Los datos deben ser exactos, actualizados y pertinentes según el uso previsto.



Principios fundamentales

Responsabilidad

Quienes traten datos personales son legalmente responsables de cumplir la ley y demostrar buenas prácticas.

Seguridad

Debe garantizarse la protección contra accesos no autorizados, pérdida o filtración mediante medidas adecuadas de seguridad.

Transparencia e información

El titular tiene derecho a conocer cómo, por qué y quién usa sus datos.

Las políticas deben ser claras, accesibles y gratuitas.

Confidencialidad

Todo quien acceda a datos personales debe guardar secreto profesional, incluso después de terminar la relación con el titular.



Derechos de las personas (titulares de datos)

Derecho de acceso

Permite al titular saber si sus datos están siendo tratados, acceder a ellos y conocer su origen, finalidad, destinatarios y tipo de tratamiento aplicado.

Derecho de rectificación

Faculta al titular a exigir que los datos sean corregidos, actualizados o completados cuando resulten inexactos, incompletos o desactualizados.

Derecho de supresión (eliminación)

Permite solicitar que los datos sean borrados cuando ya no sean necesarios, se hayan tratado ilícitamente o el titular haya revocado su consentimiento.

Derecho de oposición

El titular puede oponerse al tratamiento de sus datos cuando este se base en intereses legítimos, marketing directo u otros fines no autorizados.



Derechos de las personas (titulares de datos)

Derecho de portabilidad

Da derecho a recibir una copia de los datos personales en formato electrónico estructurado y transferirlos a otro responsable cuando el tratamiento sea automatizado y basado en consentimiento.

Derecho de bloqueo

Posibilita suspender temporalmente el tratamiento de los datos mientras se revisa una solicitud de rectificación, supresión u oposición.

Derecho a no ser objeto de decisiones automatizadas

Protege al titular frente a decisiones basadas únicamente en tratamientos automatizados (como perfilamientos) que produzcan efectos jurídicos o significativos, garantizando la posibilidad de intervención humana.



Deberes y obligaciones de las empresas

Deber de licitud, transparencia e información

Las empresas deben tratar los datos de forma lícita, leal y transparente, actuando con base legal (consentimiento, contrato, obligación legal o interés legítimo).

Además, deben informar claramente al titular quién recolecta sus datos, con qué finalidad, durante cuánto tiempo y cómo puede ejercer sus derechos.

Deber de finalidad y limitación del uso

Los datos deben recolectarse solo con fines específicos, explícitos y lícitos, y su uso debe limitarse al cumplimiento de esos fines.

No pueden utilizarse para otros propósitos sin consentimiento o base legal válida.

Deber de exactitud y actualización

Las empresas deben mantener los datos exactos, completos y actualizados, suprimiendo o corrigiendo información errónea o desactualizada.

Deber de supresión o anonimización

Cuando los datos ya no sean necesarios para el fin que motivó su recolección, deben eliminarse o anonimizarse de forma segura.



Deberes y obligaciones de las empresas

Deber de confidencialidad: Toda persona que acceda a datos personales está obligada a guardar secreto o confidencialidad, incluso después de terminada la relación con el titular. El responsable debe asegurar que sus colaboradores y terceros cumplan este deber.

Deber de seguridad: Deben implementarse medidas técnicas y organizativas adecuadas para proteger los datos frente a pérdida, acceso no autorizado, filtración o destrucción.

Deber de reportar vulneraciones: Si ocurre una violación de seguridad o filtración, el responsable debe notificar inmediatamente a la Agencia de Protección de Datos y, si existe riesgo, también a los titulares afectados.

Deber de designar contacto o delegado: Las empresas sin domicilio en Chile deben contar con un medio de contacto operativo (correo u otro) para la Agencia y los titulares.

Deber de responsabilidad proactiva: No basta con cumplir, las empresas deben demostrar que cumplen. Esto implica mantener registros, políticas internas, evaluaciones de impacto y evidencia de cumplimiento normativo.



Alcance internacional y empresas extranjeras

La Ley 21.719 también aplica a empresas extranjeras que procesen datos de personas residentes en Chile, aun cuando no tengan domicilio en el país. Estas deben contar con un medio de contacto operativo y cumplir los mismos principios y obligaciones que las empresas locales.

“El responsable de datos 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.”

Artículo 14



Multas y sanciones

Tipos de infracciones

Leves

Falta de información, retrasos o errores menores.

- Multa hasta 5.000 UTM o amonestación.

Graves

Uso de datos sin consentimiento, sin seguridad adecuada o sin notificar filtraciones.

- Multa hasta 10.000 UTM.

Gravísimas

Uso indebido de datos sensibles o de menores, o incumplimiento reiterado.

- Multa hasta 20.000 UTM y posible suspensión de operaciones por 30 días.

Registro público

Toda sanción se inscribirá en un Registro Nacional de Sanciones, accesible al público.

Reincidencia

Las multas pueden triplicarse. En empresas grandes, pueden alcanzar hasta el 4% de los ingresos anuales.



Cómo prepararte desde ahora

REVISA qué datos personales recolectas y con qué propósito.

ACTUALIZA tu política de privacidad y asegúrate de que sea clara.

CAPACITA a tu equipo sobre manejo responsable de datos.

DEFINE un encargado o responsable de protección de datos.

IMPLEMENTA medidas de seguridad, respaldo y notificación incidentes

EVALÚA los riesgos si utilizas herramientas digitales o IA que procesen información personal.

Cumplir con la Ley 21.719 no es solo una obligación legal, sino un compromiso ético con la privacidad y la confianza de las personas.

Este documento es un resumen informativo basado en la Ley N°21.719 sobre Protección de Datos Personales, publicada por la Biblioteca del Congreso Nacional de Chile.

No reemplaza la lectura del texto oficial ni constituye asesoría legal.

Más detalles en: [Biblioteca del Congreso Nacional de Chile](#)

Creado por una humana, mejorado por Inteligencia Artificial



[Fransa J. Aravena](#)