



Ley de protección de datos personales

Módulo 1

Marco Legal

●●○ FICHA INTERMEDIA

Fecha	Abril 2025
Tpo. de lectura	25 min.

Lección 1

¿Qué son los datos personales y por qué es importante protegerlos?

Dato Personal: Concepto y Alcance

Se entiende por dato personal toda información vinculada o referida a una persona natural identificada o identificable. La definición es amplia e incluye cualquier tipo de información, ya sea objetiva o subjetiva, siempre que permita identificar directa o indirectamente a una persona.

FGE

az albagli
zaliasnik



Una persona es:

- **Identificada**, cuando puede ser individualizada directamente (por ejemplo, nombre o RUT).
- **Identificable**, cuando puede ser determinada mediante la combinación de distintos datos (por ejemplo, cargo, lugar de trabajo y ubicación).

Ejemplos de datos personales incluyen, entre otros: nombre, RUT, domicilio, correo electrónico, fotografías, videos, datos financieros, opiniones políticas y datos biométricos.

Categorías Especiales de Datos

La ley distingue ciertos tipos de datos que requieren una protección reforzada:

- **Datos sensibles:** Información relativa a la vida privada cuya divulgación indebida puede generar discriminación, como datos de salud, orientación sexual, identidad de género, creencias religiosas, afiliación sindical o situación socioeconómica.
 - Regla general: tratamiento sujeto a **consentimiento explícito** del titular, con excepciones limitadas.
- **Datos de niños, niñas y adolescentes (NNA):** Sujetos a un estándar de protección más estricto, considerando su especial situación de vulnerabilidad.
- **Otros datos especialmente protegidos:** Datos biométricos, de geolocalización y financieros, que exigen mayores deberes de información, seguridad y control.

¿Por qué proteger los datos personales?

Porque es un derecho fundamental que tiene como objetivo:

- Proteger la reputación de la empresa
- Prevenir abusos y delitos
- Evitar sanciones legales y riesgos financieros
- Promover la ética y responsabilidad corporativa

Lección 2

Contexto de la nueva ley

Análisis Integral de la Nueva Ley de Protección de Datos Personales en Chile (Ley 21.719)¹: Marco Normativo, Institucionalidad y Régimen de Responsabilidad

El panorama legal de la privacidad en Chile ha experimentado una transformación estructural con la aprobación y promulgación de la Ley 21.719, la cual introduce modificaciones profundas a la Ley 19.628 sobre Protección de la Vida Privada.

Este cambio legislativo responde a la necesidad imperante de actualizar un marco normativo que databa de 1999, el cual resultaba insuficiente frente a los desafíos de la economía digital, la inteligencia artificial y el procesamiento masivo de información. La nueva normativa no solo eleva los estándares de protección

¹ La ley fue aprobada y publicada en el año 2024, estableciendo un período de vacancia legal de 24 meses. Su entrada en vigencia está fijada para el 1 de diciembre de 2026, plazo destinado a permitir que las organizaciones públicas y privadas adecuen sus procesos, sistemas y estructuras internas a las nuevas exigencias regulatorias.



a niveles equivalentes al Reglamento General de Protección de Datos de la Unión Europea (GDPR), sino que también establece una arquitectura institucional robusta encabezada por la Agencia de Protección de Datos Personales.

Contextualización y Ámbito de Aplicación de la Ley 21.719

La transición de la Ley 19.628 hacia la nueva regulación marca el fin de una era de “autotutela” y sanciones nominales, para dar paso a un régimen de responsabilidad proactiva y fiscalización estatal efectiva. La ley tiene como objeto regular el tratamiento y protección de los datos personales de personas naturales, asegurando el respeto a los derechos y libertades fundamentales consagrados en el artículo 19, N° 4 de la Constitución Política de la República.

Aplicación Territorial y Extraterritorial

Uno de los avances más significativos de la Ley 21.719 es la clarificación del ámbito de aplicación territorial, adoptando un criterio de protección que trasciende las fronteras físicas del país. La normativa resulta aplicable bajo las siguientes circunstancias:

- 1. Establecimiento Nacional:** Cuando el responsable o el mandatario del tratamiento se encuentren constituidos o establecidos en el territorio nacional.
- 2. Operaciones a Nombre de un Residente:** Cuando el mandatario realiza operaciones de tratamiento a nombre de un responsable establecido en Chile, sin importar dónde se encuentre el mandatario.
- 3. Oferta de Bienes y Servicios:** Cuando el responsable o mandatario no están en Chile, pero sus actividades se dirigen a ofrecer bienes o servicios (gratuitos o pagados) a titulares que se encuentren en territorio chileno.
- 4. Monitoreo de Comportamiento:** Cuando las operaciones de tratamiento tengan por objeto monitorear el comportamiento de personas en Chile, incluyendo el seguimiento y la elaboración de perfiles.
- 5. Vínculo Contractual o Internacional:** Cuando al responsable le resulte aplicable la legislación nacional en virtud de un contrato o del derecho internacional.

Comparativa de ámbito de aplicación	Ley 19.628 (anterior)	Ley 21.719 (nueva)
Enfoque Territorial	Limitado al territorio nacional de forma genérica.	Criterio de establecimiento y criterio de mercado (oferta a residentes en Chile).
Responsables Extranjeros	No existía claridad sobre su sujeción a la norma chilena.	Sujetos a la ley si dirigen servicios o monitorean personas en Chile.
Sujetos Obligados	Personas naturales y jurídicas que traten datos.	Incluye órganos públicos, empresas privadas y prestadores extranjeros.



Tratamiento de Datos Personales

El tratamiento de datos personales comprende cualquier operación o conjunto de operaciones, automatizadas o no, que permitan recolectar, almacenar, procesar, comunicar, transmitir, utilizar o eliminar datos personales. La ley regula todo el ciclo de vida del dato, desde su obtención hasta su supresión. La normativa aplica a todo tipo de datos tratados por una organización, incluyendo aquellos de trabajadores, clientes, proveedores, postulantes a empleo y otros terceros, sin importar el volumen o la categoría del dato.

Bases de Licitud del Tratamiento

Todo tratamiento debe estar justificado en una base de licitud expresamente reconocida por la ley. El nuevo marco amplía significativamente este catálogo:

1. Consentimiento libre, previo, específico e inequívoco del titular.
2. Autorización legal expresa.
3. Interés legítimo del responsable del tratamiento, previa ponderación con los derechos del titular.
4. Celebración o ejecución de un contrato.
5. Ejercicio o defensa de derechos ante tribunales u órganos públicos.
6. Tratamiento de datos relativos a obligaciones económicas.

El consentimiento deja de ser la única base predominante, permitiendo un enfoque más flexible, pero exige mayor rigor en su obtención y gestión, considerando además su posible revocación.

Principios del Tratamiento de Datos Personales

Los principios establecidos por la ley constituyen obligaciones permanentes para los responsables del tratamiento:

- Licitud y lealtad: Existencia de una base legal válida.
- Finalidad: Uso de los datos solo para fines específicos, explícitos y lícitos.
- Proporcionalidad: Tratamiento adecuado y no excesivo en relación con la finalidad.
- Transparencia e información: Deber de informar clara y oportunamente al titular.
- Responsabilidad: El responsable responde legalmente por el cumplimiento normativo.
- Seguridad: Implementación de medidas técnicas y organizativas apropiadas.
- Confidencialidad: Deber de secreto respecto de los datos tratados.
- Calidad: Exactitud, actualización y pertinencia de los datos.

Lección 3

Derechos de los titulares de los datos

La ley fortalece el principio de **autodeterminación informativa**, reconociendo derechos personales, irrenunciables e intransferibles. El catálogo se amplía de cuatro a seis derechos:

1. **Acceso:** Conocer qué datos se tratan, cómo y con qué base de licitud.
2. **Rectificación:** Solicitar la corrección de datos inexactos o desactualizados.
3. **Supresión:** Obtener la eliminación de datos cuando concurra una causal legal.
4. **Oposición:** Impedir determinados tratamientos en casos justificados.
5. **Bloqueo:** Suspensión temporal del tratamiento mientras se resuelve otro derecho.
6. **Portabilidad:** Obtener los datos en formato electrónico para transferirlos a otro responsable.



Nueva Agencia de Protección de Datos Personales

Se crea una **Agencia de Protección de Datos Personales**, como órgano administrativo técnico e independiente, con facultades para:

- Dictar directrices, reglamentos y estándares.
- Fiscalizar el cumplimiento de la ley.
- Ejercer potestad sancionatoria.

Este organismo actuará como autoridad central en la supervisión del sistema de protección de datos en Chile.

Seguridad, Reporte de Incidentes y Modelos de Prevención

La ley impone la obligación de adoptar **medidas de seguridad técnicas y organizativas**, tales como cifrado y seudonimización², orientadas a garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.

Asimismo, se establece el **deber de reportar vulneraciones de seguridad** a la Agencia y, en ciertos casos, a los propios titulares de los datos.

Se contempla además la posibilidad de implementar un **Modelo de Prevención de Infracciones**, de carácter voluntario y certificable, cuya adopción actúa como atenuante de responsabilidad. Este modelo incluye la designación de un **Delegado de Protección de Datos (DPO)** con independencia funcional.

Transferencias Internacionales y Régimen Sancionatorio

Las transferencias internacionales de datos personales quedan expresamente reguladas, permitiéndose solo hacia países con niveles de protección adecuados o mediante garantías contractuales equivalentes. El nuevo régimen sancionatorio clasifica las infracciones en **leves, graves y gravísimas**, incorporando la figura de la reincidencia, que puede implicar la suspensión temporal de las operaciones de tratamiento hasta por 30 días.

IMPORTANTE

Entrada en vigencia: 1 de diciembre de 2026

Impacto esperado: fortalecimiento de derechos fundamentales, aumento de la responsabilidad organizacional y consolidación de Chile como un entorno confiable para el tratamiento de datos personales.

² La seudonimización es una técnica de seguridad que sustituye identificadores personales (nombres, DNI, teléfonos) por alias o códigos, permitiendo el tratamiento de datos sin identificar directamente al interesado.

FUENTE: el contenido de esta ficha fue elaborado a partir de la transcripción de video que acompaña que corresponde al módulo 1 del curso Nueva Ley de protección de datos personales/serie FGE Mejores prácticas en integridad y cumplimiento y extractos de información sobre el tema encontrados en bcn.cl
Ley Chile - Ley 21719 - Biblioteca del Congreso Nacional - BCN