NORMATIC AI

GUÍA TÉCNICA · LEY 21.719

El nuevo régimen de protección de datos personales en Chile

Guía de referencia para oficiales de cumplimiento, delegados de protección de datos, auditores y asesores legales.

● Descarga libre · Sin registro

Normatic AI · por Alchemical Data · Edición 2026

Índice

CAPÍTULO 01

Para qué sirve esta guía

El 1 de diciembre de 2026 entra en plena vigencia la Ley N° 21.719, la reforma más profunda al régimen chileno de protección de datos personales desde 1999. Alcanza a toda organización que trate datos personales en Chile, sin importar su tamaño ni su rubro.

Esta guía ordena lo esencial del nuevo régimen con una mirada operativa, pensada para quienes deben responder por el cumplimiento dentro de la organización. Directorios, gerencias, fiscalías, áreas de cumplimiento, auditoría interna y asesores externos encontrarán aquí un mapa de lo que cambia y de lo que conviene tener resuelto antes de la fecha de vigencia.

El documento recorre el marco general de la ley, los conceptos que hay que dominar, la nueva autoridad de control, los derechos de los titulares, las obligaciones del responsable, el régimen de sanciones y una hoja de ruta de implementación por fases. Incluye además un capítulo sobre la intersección entre la protección de datos y los sistemas de prevención de delitos, donde ambas regulaciones trabajan sobre la misma información.

EN SIMPLE

Si su organización guarda nombres, correos, RUT, fichas de clientes o datos de trabajadores, esta ley la toca. La pregunta ya no es si aplica, sino qué tan lista está para demostrar que cumple.

ADVERTENCIA

Esta guía tiene fines informativos y de orientación general. No constituye asesoría legal. Las decisiones de cumplimiento deben tomarse con asesoría profesional y a la luz del texto oficial de la Ley 21.719, sus reglamentos y los criterios que dicte la autoridad de control.

CAPÍTULO 02

Del régimen antiguo al nuevo

El punto de partida

La Ley N° 19.628, vigente desde 1999, reguló los datos personales en Chile durante más de dos décadas. Arrastraba tres debilidades de fondo que la práctica dejó en evidencia. No existía una autoridad de control especializada, el régimen de sanciones era de baja intensidad y los titulares debían reclamar sus derechos por la vía judicial, lenta y costosa. El resultado fue un mercado de datos con incentivos débiles al cumplimiento.

En 2018 una reforma constitucional elevó la protección de los datos personales a la categoría de derecho fundamental, en el artículo 19 N° 4 de la Constitución. Esa decisión sentó las bases de la reforma legal que llegó después.

La reforma

La Ley N° 21.719 fue publicada en el Diario Oficial el 13 de diciembre de 2024. No es un cuerpo legal separado, sino una reforma integral que reescribe la Ley 19.628 y le cambia el nombre a Ley sobre protección de los datos personales. Contempló un período de vacancia de veinticuatro meses, de modo que entra en plena vigencia el 1 de diciembre de 2026.

13 dic 2024	1 dic 2026	24 meses
Publicación en el Diario Oficial	Entrada en plena vigencia	Período de adecuación

La reforma se sostiene sobre cuatro ejes. La creación de una autoridad de control con potestades normativas, fiscalizadoras y sancionatorias. Un catálogo reforzado de derechos para los titulares. Un conjunto de obligaciones de cumplimiento demostrable, que mueve el estándar desde la declaración de políticas hacia la evidencia operativa. Y un régimen de multas significativas, graduadas según la gravedad.

Alineación internacional

El nuevo régimen se inspira en el Reglamento General de Protección de Datos de la Unión Europea, el GDPR, y en el Convenio 108+ del Consejo de Europa. Para una empresa chilena con clientes u operaciones en el extranjero esto tiene una consecuencia práctica. Cumplir la Ley 21.719 acerca a la organización al estándar que esos mercados exigen y facilita los contratos que involucran flujos internacionales de información.

CAPÍTULO 03

Conceptos que hay que dominar

La aplicación correcta de la ley exige precisión. Estos son los términos que estructuran el régimen.

Dato personal. Cualquier información vinculada a una persona natural identificada o identificable. La definición es amplia a propósito. Comprende identificadores directos, como el nombre o la cédula de identidad, e indirectos, como la dirección IP, la geolocalización o los patrones de comportamiento, siempre que permitan identificar a la persona por medios razonables.

Dato sensible. Categoría reforzada que comprende, entre otros, los datos de salud, el perfil biológico, la biometría, el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones religiosas y la vida sexual. Su tratamiento queda sujeto a condiciones de licitud más estrictas, por regla general el consentimiento expreso, y a deberes de seguridad agravados.

Titular. La persona natural a quien conciernen los datos. La ley protege a personas naturales. Las personas jurídicas no son titulares, sin perjuicio de que los datos de sus representantes o trabajadores sí lo sean.

Responsable de datos. Quien decide sobre los fines y los medios del tratamiento. Esta calidad no depende de quién ejecuta materialmente las operaciones, sino de quién las determina.

Encargado o mandatario. Quien trata datos por cuenta del responsable, en virtud de un contrato. Los proveedores de nube y los servicios externalizados que acceden a datos personales operan, por regla general, en esta calidad.

Tratamiento. Cualquier operación sobre datos personales, desde la recolección y el almacenamiento hasta la comunicación, la transferencia o la supresión. La amplitud del concepto implica que casi toda organización trata datos personales, aunque no lo conciba así.

Base de licitud. Todo tratamiento necesita un fundamento jurídico. El consentimiento del titular es la regla general, y la ley reconoce además, entre otras, el cumplimiento de una obligación legal, la ejecución de un contrato y el interés legítimo del responsable, con los resguardos que ella define. Identificar la base de licitud de cada tratamiento es la operación jurídica central del cumplimiento, y debe quedar documentada.

EN SIMPLE

Responsable y encargado se confunden seguido. El responsable es el arquitecto que decide qué se construye y para qué. El encargado es la constructora que ejecuta el plano que recibe, sin cambiar el diseño por su cuenta. La ley les pide cosas distintas a cada uno, así que conviene saber cuál es cuál en cada contrato.

CAPÍTULO 04

La Agencia de Protección de Datos Personales

La ley crea la Agencia de Protección de Datos Personales como corporación autónoma de derecho público, de carácter técnico y descentralizado, con personalidad jurídica y patrimonio propios. Se relaciona con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo. Es la primera autoridad de control especializada en la historia del país. La dirige un Consejo Directivo de tres consejeros designados por el Presidente con acuerdo del Senado.

Sus funciones

- **Función normativa e interpretativa.**
  Dicta instrucciones y normas generales, e interpreta administrativamente la ley.
- **Función fiscalizadora.**
  Requiere información, realiza inspecciones y verifica el cumplimiento de responsables y encargados.
- **Función sancionatoria.**
  Instruye procedimientos, ordena medidas correctivas y aplica las sanciones que la ley contempla.
- **Función de tutela y certificación.**
  Resuelve los reclamos de los titulares, administra el Registro Nacional de Sanciones y Cumplimiento, y certifica los modelos de prevención de infracciones que las organizaciones adopten.

> EL PUNTO QUE MÁS SE SUBESTIMA
>
> La fiscalización se dirige a la evidencia, no a las declaraciones. Un requerimiento de la Agencia se responde con registros, inventarios, contratos y logs de acceso fechados, no con buenas intenciones. Es la diferencia entre decir que sabe nadar y que lo tiren a la piscina. Y a diferencia del régimen anterior, cualquier titular disconforme puede activar un procedimiento, o la Agencia actuar de oficio.

ESTADO DE IMPLEMENTACIÓN · 2026

La Agencia se encuentra en proceso de instalación, con su puesta en marcha anticipada al curso de 2026, y su reglamento y primeras normas técnicas en desarrollo. Existe además una iniciativa legislativa en trámite que podría ajustar algunos artículos antes de la vigencia. **Conviene seguir los criterios oficiales a medida que se publiquen y trabajar sobre el texto vigente, sin esperar el detalle reglamentario para empezar a adecuarse.**

CAPÍTULO 05

Los derechos de los titulares

La ley consagra un catálogo de derechos de ejercicio gratuito ante el responsable, con plazo de respuesta definido y reclamación posterior ante la Agencia en caso de denegación o silencio. Son derechos personales, intransferibles e irrenunciables.

Acceso. Obtener confirmación de si sus datos están siendo tratados y acceder a ellos, junto con su origen, finalidad y destinatarios.

Rectificación. Exigir la corrección de datos inexactos, desactualizados o incompletos.

Supresión o cancelación. Exigir la eliminación de los datos cuando carezcan de fundamento, hayan caducado o ya no resulten necesarios. Este derecho tiene límites, en particular cuando una obligación legal de conservación prevalece.

Oposición. Oponerse al tratamiento en los supuestos que la ley contempla.

Portabilidad. Obtener una copia de los datos en un formato estructurado y de uso común, y solicitar su transmisión a otro responsable cuando sea técnicamente posible.

Decisiones automatizadas. No ser objeto de decisiones basadas solo en tratamientos automatizados, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos o afecten de manera significativa, y solicitar intervención humana en su revisión.

30 + 30	Gratuito	Reclamo
Días para responder, prorrogables por otros 30 en casos justificados	El ejercicio de los derechos ante el responsable	Ante la Agencia si hay denegación o silencio

Cada derecho se traduce, para la organización, en un procedimiento que debe existir antes de la primera solicitud. Un canal de recepción identificable, verificación de identidad del solicitante, plazo controlado, registro de la solicitud y de su resolución, y criterios documentados para resolver los casos en que el derecho colisiona con un deber legal de conservación. Responder una solicitud de acceso dentro de plazo es, en la práctica, el primer test de madurez del sistema. Exige saber qué datos se tienen, dónde están y poder recuperarlos.

EN SIMPLE

Piense en la ficha que tiene de usted la clínica. Estos derechos son poder pedir verla, corregir lo que está malo, llevársela a otra parte y exigir que la borren cuando ya no corresponde guardarla. La empresa tiene un plazo para responder, y el silencio se paga.

CAPÍTULO 06

Las obligaciones del responsable

Principios rectores

El tratamiento debe sujetarse a ocho principios: licitud y lealtad, finalidad, proporcionalidad, calidad, seguridad, transparencia e información, confidencialidad y responsabilidad. Este último opera como cláusula de cierre. El responsable no solo debe cumplir los demás principios, debe ser capaz de demostrarlo.

Obligaciones operativas

- **Registro de actividades de tratamiento.** `Art. 14 ter`
  Un inventario actualizado de los tratamientos que realiza la organización, con categorías de datos, finalidades, bases de licitud, plazos de conservación, destinatarios y transferencias. Es el documento estructural del sistema y el primer antecedente que la autoridad revisará.

- **Protección desde el diseño y por defecto.** `Art. 14 quáter`
  Incorporar medidas técnicas y organizativas desde la concepción de cada tratamiento, y tratar por defecto solo los datos necesarios para la finalidad.

- **Información y transparencia.**
  El titular debe ser informado al momento de la recolección sobre la identidad del responsable, las finalidades, la base de licitud y sus derechos. La política de privacidad debe reflejar el tratamiento real, no un formulario genérico.

- **Medidas de seguridad.** `Art. 14 quinquies`
  Técnicas y organizativas apropiadas al riesgo. En la práctica comprende control de accesos por necesidad de conocimiento, cifrado de los datos sensibles, registro de accesos, segregación de ambientes y gestión de respaldos.

- **Notificación de brechas.** `Art. 14 sexies`
  Producida una vulneración que afecte datos personales, el responsable debe reportarla a la Agencia sin dilación indebida y, cuando sea posible, dentro de las 72 horas siguientes a tomar conocimiento, y comunicarla a los titulares cuando el riesgo lo justifique. Esto presupone capacidad de detección, un procedimiento de evaluación y escalamiento, y registros que permitan reconstruir el incidente.

- **Delegado de protección de datos.** `Arts. 49 a 51`
  La ley exige esta figura a los organismos públicos y a quienes tratan datos a gran escala o datos sensibles, y la convierte en pieza obligatoria del modelo de prevención de infracciones que la organización puede adoptar de forma voluntaria, y que la Agencia certifica. Con independencia de su obligatoriedad, designar un responsable interno con mandato formal es buena práctica para toda organización mediana o superior.

- **Contratos con encargados.**
  El tratamiento por terceros debe regularse por contrato, con instrucciones, deberes de confidencialidad y seguridad, régimen de subcontratación y destino de los datos al término. Revisar el parque contractual de proveedores es una de las tareas de mayor plazo, porque depende de las contrapartes.

- **Transferencias internacionales.**
  El flujo de datos al extranjero queda sujeto a reglas específicas, con mecanismos como las decisiones de adecuación, las cláusulas contractuales tipo y las normas corporativas vinculantes. Conviene identificar en el registro qué tratamientos implican transferencia, incluidos los derivados de servicios de nube con infraestructura fuera de Chile.

EN SIMPLE

El registro de actividades de tratamiento es el plano as-built de sus datos: el mapa fiel de qué dato vive en qué sistema, para qué se usa, quién lo toca y hasta cuándo se guarda. Si no tiene ese plano, no puede defender la casa cuando llegue la inspección.

CAPÍTULO 07

El régimen de sanciones

La ley clasifica las infracciones en tres niveles y asocia a cada uno un rango de multa creciente, expresado en unidades tributarias mensuales.

Categoría	Multa máxima	Ejemplos de conducta
Leves	5.000 UTM	Incumplimientos formales del régimen
Graves	10.000 UTM	Tratar datos sin base de licitud, no atender derechos
Gravísimas	20.000 UTM	Tratamiento indebido de datos sensibles, omitir el reporte de una brecha

Si el infractor no subsana la causa de la sanción dentro del plazo que la ley fija, la multa se incrementa. Y en caso de reincidencia, se contemplan sanciones calculadas como porcentaje de los ingresos anuales del infractor, con un techo de hasta el 4% para los casos más graves, o la multa triplicada, según lo que resulte mayor.

Graduación

La sanción considera atenuantes y agravantes. Entre las atenuantes destacan la colaboración con la autoridad, la autodenuncia, la adopción oportuna de medidas correctivas y la existencia de un programa de cumplimiento efectivamente implementado. Este último punto merece atención. Al igual que en el régimen de responsabilidad penal de las personas jurídicas, contar con un modelo operativo y verificable mejora la posición de la empresa ante la autoridad.

VENTANA PARA EMPRESAS DE MENOR TAMAÑO

Respecto de las empresas de menor tamaño según la Ley N° 20.416, durante los primeros doce meses de vigencia las primeras infracciones dan lugar a amonestación escrita en lugar de multa. Es una ventana de adecuación supervisada, no una exención. La obligación rige desde el 1 de diciembre de 2026 para todas las organizaciones.

El análisis de riesgo no debe limitarse a la multa. El costo reputacional de una infracción publicada en el Registro Nacional, la pérdida de confianza de clientes y contrapartes y una posición desmejorada en licitaciones suelen exceder el impacto económico directo de la sanción.

CAPÍTULO 08

Datos y prevención de delitos

La Ley 21.719 converge con las obligaciones de prevención de lavado de activos y de delitos corporativos. Para los sujetos obligados ante la UAF y para las empresas con un modelo de prevención conforme a la Ley 20.393, ambos mundos trabajan sobre la misma información.

La debida diligencia es tratamiento de datos

Los procesos de conocimiento del cliente que exige la Ley 19.913 son, en el lenguaje de la Ley 21.719, tratamientos de datos personales. El sujeto obligado actúa como responsable de esos datos. La base de licitud está en el cumplimiento de una obligación legal, base sólida pero de alcance preciso. Ampara los datos que la normativa exige recolectar y conservar, por los plazos que ella define, y para las finalidades que ella establece. No ampara la reutilización de esos expedientes para marketing ni la conservación indefinida una vez expirado el plazo legal.

Tensiones que conviene anticipar

- **Supresión frente a conservación.**
  El titular que pide eliminar su expediente de debida diligencia debe recibir una respuesta fundada que explique la obligación legal de conservación que prevalece, con su fuente y plazo. La denegación fundada y documentada es cumplimiento. El silencio no lo es.
- **Confidencialidad del reporte.**
  El deber de reserva que rige los reportes a la UAF prevalece sobre el derecho de acceso del titular en lo que a esos reportes se refiere. Los procedimientos de respuesta deben contemplar esta hipótesis de manera expresa.

Una sola gobernanza

Las organizaciones con sistemas de prevención maduros disponen de capacidades reutilizables para la Ley 21.719. Cultura de documentación, trazabilidad de operaciones, gobierno de políticas y capacitación periódica. La recomendación es coordinar ambos sistemas bajo una gobernanza común de cumplimiento, con roles diferenciados y procesos compartidos de gestión documental, capacitación y auditoría.

EN SIMPLE

Si ya tiene aceitada la maquinaria de prevención de delitos o de lavado de activos, no parte de cero. Las mismas correas de trazabilidad, documentación y capacitación mueven también el cumplimiento de datos. La idea es un solo motor con varias salidas, no tres motores compitiendo por el mismo espacio.

CAPÍTULO 09

Hoja de ruta de implementación

Una secuencia de adecuación en cuatro fases, ajustable a la escala y la complejidad de cada organización.

FASE 1 · DIAGNÓSTICO · SEMANAS 1 A 4

- Levantar el inventario de tratamientos: qué datos, en qué sistemas, con qué finalidades y quién accede.
- Identificar la base de licitud de cada tratamiento y detectar los que carecen de fundamento.
- Catastrar proveedores con acceso a datos e identificar las transferencias internacionales, incluidas las derivadas de la nube.

FASE 2 · GOBERNANZA Y DOCUMENTACIÓN · SEMANAS 5 A 10

- Designar al responsable interno de protección de datos y definir su mandato y recursos.
- Formalizar el registro de actividades de tratamiento y la política de retención y eliminación, con plazos fundados por categoría.
- Actualizar políticas de privacidad y avisos al titular para reflejar el tratamiento real.

FASE 3 · CONTROLES TÉCNICOS Y CONTRACTUALES · SEMANAS 8 A 18

- Diseñar los procedimientos de ejercicio de derechos, con canal, verificación de identidad, plazos y registro.
- Adecuar los contratos con encargados, priorizando los que tratan datos sensibles o volúmenes altos.
- Reforzar controles de acceso, cifrado de datos sensibles e implementar el procedimiento de gestión de brechas.

FASE 4 · CULTURA Y VERIFICACIÓN · SEMANAS 16 A 24

- Capacitar de forma diferenciada por audiencia y dejar registro de ello.
- Ejecutar una simulación completa: responder una solicitud de acceso y gestionar una brecha de principio a fin, midiendo plazos.
- Auditar el cierre y definir el plan de mantenimiento. El cumplimiento es un proceso continuo, no un proyecto con fecha de término.

SIETE PREGUNTAS DE CONTROL

Una organización está razonablemente preparada cuando puede responder que sí, con evidencia, a estas preguntas. ¿Existe un registro de actividades de tratamiento aprobado? ¿Cada tratamiento tiene una base de licitud documentada? ¿Puede responder una solicitud de acceso dentro de plazo? ¿Hay contratos de encargo vigentes con todos los proveedores? ¿Existe un procedimiento probado de gestión de brechas? ¿El personal fue capacitado y queda registro? ¿Los plazos de conservación están definidos y se aplican?

CAPÍTULO 10

Cómo acompaña Normatic AI

Normatic AI es la suite de cumplimiento normativo de Alchemical Data, pensada para el trabajo diario del oficial de cumplimiento y su equipo. Reúne en un mismo espacio las herramientas que sostienen un programa vivo y auditable.

NORMATIC AI

DISPONIBLE **Gestor de Cumplimientos (GRC).** Levanta tu matriz de riesgos, define controles y planes de acción y monitorea el avance desde un tablero único. La trazabilidad y la documentación que la Ley 21.719 exige se generan como subproducto natural de operar el programa.

DISPONIBLE **Canal de Denuncias.** Recibe, gestiona e investiga denuncias con confidencialidad y trazabilidad, una pieza común a la Ley Karin, al modelo de prevención de delitos y a la cultura de cumplimiento que la protección de datos también supone.

PRÓXIMAMENTE **Módulo de Protección de Datos.** En desarrollo, orientado a la Ley 21.719. Cubrirá el inventario de tratamientos, la gestión de los derechos de los titulares, el registro de consentimientos y el apoyo a la gestión de brechas. Si quieres saber cuándo esté disponible, conversemos.

Esta guía tiene fines informativos y no constituye asesoría legal. Normatic AI es una herramienta de apoyo al cumplimiento y no reemplaza el criterio de un asesor profesional. contacto@normatic.ai · WhatsApp +56 9 6352 7553 · normatic.ai

CAPÍTULO 11

Glosario

Agencia de Protección de Datos Personales. Autoridad de control creada por la Ley 21.719, con potestades normativas, fiscalizadoras y sancionatorias.

Anonimización. Procedimiento irreversible por el cual un dato deja de ser asociable a una persona identificable, quedando fuera del ámbito de la ley.

Base de licitud. Fundamento jurídico que autoriza un tratamiento, como el consentimiento, una obligación legal, un contrato o el interés legítimo.

Brecha de seguridad. Incidente que ocasiona la pérdida, alteración, comunicación o acceso no autorizado a datos personales.

Consejo Directivo. Órgano colegiado que dirige la Agencia, integrado por tres consejeros designados por el Presidente con acuerdo del Senado.

Dato sensible. Categoría de datos con protección reforzada, como salud, biometría, origen étnico, convicciones o vida sexual.

Delegado de protección de datos. Responsable interno de promover y supervisar el cumplimiento de la normativa de datos, y punto de contacto con la Agencia.

Encargado de tratamiento. Quien trata datos por cuenta del responsable en virtud de un contrato.

Evaluación de impacto. Análisis previo de los riesgos de un tratamiento de alto riesgo y de las medidas para mitigarlos.

Modelo de prevención de infracciones. Programa de cumplimiento voluntario que la Agencia puede certificar, y que opera como atenuante ante una eventual sanción.

Portabilidad. Derecho del titular a obtener sus datos en formato estructurado y a transmitirlos a otro responsable.

Registro de actividades de tratamiento. Inventario formal de los tratamientos que realiza una organización.

Responsable de datos. Quien decide sobre los fines y los medios del tratamiento.

Transferencia internacional. Comunicación de datos personales a un destinatario ubicado fuera de Chile, sujeta a reglas y garantías específicas.

UTM. Unidad tributaria mensual, unidad de cuenta que se usa para determinar las multas.