Neitcom
COMPLIANCE

GUÍA TÉCNICA

El nuevo régimen de protección de datos personales en Chile

Guía de referencia para directores, fiscales, oficiales de cumplimiento y asesores legales

Descarga libre · Sin registro

Neitcom Compliance · Edición junio 2026

Antes de comenzar

Nota de descarga libre. Este documento se distribuye sin registro previo. Neitcom no solicita datos personales para acceder a una guía sobre protección de datos personales. La coherencia también es una política de tratamiento.

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

CONTENIDO

Índice

CAPÍTULO 1

Presentación y alcance de esta guía

El 1 de diciembre de 2026 entra en plena vigencia la Ley N° 21.719, que reforma íntegramente el régimen chileno de protección de datos personales contenido en la Ley N° 19.628. Se trata de la modificación más relevante en la materia desde 1999 y afecta a la totalidad de las organizaciones, públicas y privadas, que traten datos personales en Chile, con independencia de su tamaño, rubro o naturaleza jurídica.

Esta guía sistematiza los aspectos centrales del nuevo régimen con un enfoque práctico, orientado a quienes deben responder por el cumplimiento dentro de sus organizaciones: directorios, gerencias generales, fiscalías, áreas de cumplimiento, auditoría interna y asesores externos.

El documento aborda el marco conceptual de la ley, la nueva institucionalidad, los derechos de los titulares, las obligaciones de los responsables, el régimen sancionatorio y una propuesta metodológica de implementación. Se incluye además un capítulo específico sobre la relación entre la protección de datos y los sistemas de prevención de lavado de activos y delitos corporativos, ámbito en el cual ambas regulaciones convergen sobre los mismos procesos y la misma información.

CAPÍTULO 2

Marco general: de la Ley 19.628 a la Ley 21.719

2.1 El régimen anterior y sus limitaciones

La Ley N° 19.628, sobre protección de la vida privada, rigió el tratamiento de datos personales en Chile desde 1999. Su diseño presentaba tres limitaciones estructurales que la práctica hizo evidentes: la ausencia de una autoridad de control especializada, un régimen sancionatorio de baja intensidad y la falta de mecanismos efectivos para el ejercicio de los derechos de los titulares, que debían reclamarse por vía judicial.

El resultado fue un mercado de datos con incentivos débiles al cumplimiento, en el que la cesión, comercialización y filtración de información personal operó durante décadas con consecuencias jurídicas marginales para los infractores.

2.2 La reforma

La Ley N° 21.719 fue publicada en el Diario Oficial el 13 de diciembre de 2024. Contempló un período de vacancia legal de veinticuatro meses, de modo que su entrada en plena vigencia se produce el 1 de diciembre de 2026. La norma reforma íntegramente la Ley 19.628, que pasa a denominarse Ley sobre Protección de los Datos Personales.

Los ejes de la reforma son cuatro:

a) La creación de una autoridad de control, la Agencia de Protección de Datos Personales, dotada de potestades normativas, fiscalizadoras y sancionatorias.

b) La consagración de un catálogo reforzado de derechos para los titulares de datos, con procedimientos de ejercicio ante el responsable y reclamación ante la autoridad.

c) Un conjunto de obligaciones de cumplimiento demostrable para los responsables y encargados de tratamiento, que desplaza el estándar desde la declaración de políticas hacia la evidencia operativa.

d) Un régimen sancionatorio con multas significativas, graduadas según la gravedad de la infracción.

2.3 Alineamiento internacional

El nuevo régimen se inspira en el Reglamento General de Protección de Datos de la Unión Europea (GDPR), estándar adoptado o replicado por una parte sustantiva de las economías desarrolladas. Este alineamiento tiene una consecuencia práctica relevante para las empresas chilenas con operaciones o clientes en el extranjero: el cumplimiento de la Ley 21.719 acerca a la organización al estándar exigido en esos mercados y facilita la negociación de contratos que involucran flujos internacionales de información.

Durante el período de transición, la autoridad administrativa avanzó en la dictación de instrumentos preparatorios, incluyendo cláusulas contractuales modelo para transferencias internacionales de datos, con el objeto de otorgar certeza jurídica desde la entrada en vigencia.

CAPÍTULO 3

Conceptos fundamentales

La correcta aplicación de la ley exige precisión conceptual. Los siguientes son los términos estructurales del régimen.

Dato personal. Cualquier información vinculada o referida a una persona natural identificada o identificable. La definición es deliberadamente amplia: comprende identificadores directos (nombre, cédula de identidad, domicilio) e indirectos (dirección IP, datos de geolocalización, identificadores de dispositivos, patrones de comportamiento), en la medida en que permitan identificar a la persona por medios razonables.

Dato personal sensible. Categoría reforzada que comprende, entre otros, los datos relativos a la salud, el perfil biológico, la biometría, el origen étnico, la afiliación política o sindical, las convicciones religiosas, la vida sexual y la orientación sexual. Su tratamiento queda sujeto a condiciones de licitud más estrictas 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 de datos personales, sin perjuicio de que los datos de sus representantes, socios o trabajadores sí lo sean.

Responsable de datos. La persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento. La calidad de responsable no depende de quién ejecuta materialmente las operaciones sino de quién las determina.

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

Tratamiento. Cualquier operación o conjunto de operaciones sobre datos personales: recolección, registro, almacenamiento, consulta, comunicación, cesión, transferencia, anonimización, supresión. La amplitud del concepto implica que prácticamente toda organización trata datos personales, aunque no lo conciba así.

Bases de licitud. Todo tratamiento requiere un fundamento jurídico. El consentimiento del titular constituye la regla general, y la ley reconoce además otras bases, entre ellas la ejecución o cumplimiento de una obligación legal, la ejecución de un contrato en que el titular es parte, y el interés legítimo del responsable en los términos y con los resguardos que la propia ley define. La identificación de la base de licitud aplicable a cada tratamiento es la operación jurídica central del cumplimiento, y debe quedar documentada.

CAPÍTULO 4

La Agencia de Protección de Datos Personales

4.1 Naturaleza y funciones

La ley crea la Agencia de Protección de Datos Personales como corporación autónoma de derecho público, relacionada con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo. Es la primera autoridad de control especializada en la materia en la historia del país.

Sus funciones principales comprenden:

a) **Función normativa e interpretativa.** Dictar instrucciones y normas generales para la aplicación de la ley, e interpretar administrativamente sus disposiciones.

b) **Función fiscalizadora.** Requerir información, realizar inspecciones y verificar el cumplimiento de las obligaciones por parte de responsables y encargados.

c) **Función sancionatoria.** Instruir procedimientos administrativos, ordenar medidas correctivas y aplicar las sanciones que la ley contempla.

d) **Función de tutela.** Conocer y resolver los reclamos de los titulares cuyos derechos no hayan sido atendidos por el responsable.

4.2 Implicancia práctica

La existencia de una autoridad con estas potestades modifica el cálculo de riesgo de las organizaciones. Bajo el régimen anterior, la probabilidad de fiscalización era estadísticamente irrelevante. Bajo el nuevo régimen, cualquier titular disconforme puede activar un procedimiento ante la Agencia, y la Agencia puede actuar de oficio.

Debe subrayarse un punto metodológico: la fiscalización administrativa en esta materia se dirige a la evidencia, no a las declaraciones. Un requerimiento de información de la Agencia se responde con registros, inventarios, contratos, logs de acceso y documentación fechada. Las políticas no respaldadas por evidencia operativa tienen valor probatorio limitado.

CAPÍTULO 5

Derechos de los titulares

La ley consagra un catálogo de derechos de ejercicio gratuito ante el responsable, con plazos de respuesta definidos y reclamación posterior ante la Agencia en caso de denegación o silencio.

Derecho de acceso. Facultad del titular de solicitar y obtener confirmación de si sus datos están siendo tratados, así como acceder a ellos y a información sobre el origen, la finalidad y los destinatarios del tratamiento.

Derecho de rectificación. Facultad de exigir la modificación de los datos inexactos, desactualizados o incompletos.

Derecho de supresión (cancelación). Facultad de exigir la eliminación de los datos cuando, entre otras causales, carezcan de fundamento jurídico, hayan caducado, o su tratamiento no resulte necesario para la finalidad que motivó su recolección. Este derecho reconoce límites, en particular cuando existe una obligación legal de conservación que prevalece.

Derecho de oposición. Facultad de oponerse al tratamiento en los supuestos que la ley contempla.

Derecho de portabilidad. Facultad de obtener copia de los datos en un formato estructurado y de uso común, y de solicitar su transmisión a otro responsable cuando ello sea técnicamente posible.

Derechos relativos a decisiones automatizadas. El titular tiene derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos o le afecten significativamente, con las excepciones legales correspondientes, y a solicitar la intervención humana en la revisión de tales decisiones.

5.1 Carga operativa para el responsable

Cada derecho se traduce, para la organización, en un procedimiento que debe existir con anterioridad a la primera solicitud: canal de recepción identificable, verificación de identidad del solicitante, plazo de respuesta controlado, registro de la solicitud y de su resolución, y criterios documentados para resolver los casos en que el derecho colisiona con deberes legales de conservación.

La capacidad de responder una solicitud de acceso dentro de plazo es, en la práctica, el primer test de madurez del sistema de cumplimiento: exige saber qué datos se tienen, dónde están y poder recuperarlos. Las organizaciones que no puedan ejecutar esa operación deben considerar ese hallazgo como el punto de partida de su plan de adecuación.

CAPÍTULO 6

Obligaciones de los responsables de datos

6.1 Principios rectores

El tratamiento debe sujetarse a los principios que la ley establece, entre ellos licitud y lealtad, finalidad, proporcionalidad (minimización), calidad, seguridad, transparencia e información, y responsabilidad (accountability). El principio de responsabilidad opera como cláusula de cierre: el responsable debe ser capaz de demostrar el cumplimiento de los demás principios.

6.2 Obligaciones operativas principales

a) Registro de actividades de tratamiento. El responsable debe mantener un inventario actualizado de los tratamientos que realiza, identificando categorías de datos, finalidades, bases de licitud, plazos de conservación, destinatarios y transferencias. Este registro es el documento estructural del sistema y el primer antecedente que la autoridad examinará.

b) Deber de información y transparencia. El titular debe ser informado, al momento de la recolección, acerca de la identidad del responsable, las finalidades del tratamiento, la base de licitud y los derechos que le asisten. Las políticas de privacidad deben reflejar el tratamiento real y no constituir formularios genéricos.

c) Medidas de seguridad. El responsable debe adoptar medidas técnicas y organizativas apropiadas al riesgo, considerando el estado de la técnica, la naturaleza de los datos y el impacto potencial sobre los titulares. En la práctica, ello comprende control de accesos basado en necesidad de conocimiento, cifrado de datos sensibles, registro de accesos y consultas, segregación de ambientes y gestión de respaldos.

d) Notificación de vulneraciones de seguridad. Producida una brecha que afecte datos personales, el responsable debe reportarla a la autoridad en los términos y condiciones que fija la ley, y comunicarla a los titulares cuando corresponda según el riesgo. La obligación presupone capacidad de detección, un procedimiento interno de evaluación y escalamiento, y registros que permitan reconstruir el incidente.

e) Delegado de protección de datos. La ley contempla la figura del encargado de prevención o delegado de protección de datos en los casos y condiciones que ella regula, como responsable interno de promover y supervisar el cumplimiento. Con independencia de la obligatoriedad en cada caso, la designación de un responsable interno con mandato formal constituye una buena práctica de gobernanza recomendable para toda organización de tamaño mediano o superior.

f) Contratos con encargados. El tratamiento por terceros debe regularse contractualmente, estableciendo el objeto y duración del encargo, las instrucciones del responsable, los deberes de confidencialidad y seguridad, el régimen de subcontratación y el destino de los datos al término del con-

trato. La revisión del parque contractual de proveedores es una de las tareas de mayor plazo dentro de los proyectos de adecuación, pues depende de contrapartes.

g) Transferencias internacionales. El flujo de datos hacia el extranjero queda sujeto a las reglas que la ley establece, contemplándose mecanismos como las decisiones de adecuación, las cláusulas contractuales y otras garantías. Las organizaciones deben identificar en su registro de actividades qué tratamientos implican transferencia internacional, incluyendo los derivados del uso de servicios de nube con infraestructura fuera de Chile.

6.3 Evaluaciones de impacto

Para los tratamientos que por su naturaleza, alcance o finalidad puedan generar alto riesgo para los derechos de los titulares, constituye buena práctica, y exigencia en los casos que la normativa determine, la realización de evaluaciones de impacto previas, documentando los riesgos identificados y las medidas de mitigación adoptadas.

CAPÍTULO 7

Régimen de infracciones y sanciones

7.1 Estructura

La ley clasifica las infracciones en leves, graves y gravísimas, asociando a cada categoría rangos de multa crecientes. El monto máximo puede alcanzar las 20.000 unidades tributarias mensuales para las infracciones gravísimas, y en hipótesis de reincidencia la ley contempla la posibilidad de sanciones calculadas como porcentaje de los ingresos anuales del infractor, con un techo de hasta el 4% para los casos más graves.

A título ilustrativo, integran las categorías superiores conductas tales como el tratamiento de datos sin base de licitud, el tratamiento indebido de datos sensibles, la omisión de reporte de vulneraciones de seguridad y el incumplimiento de las resoluciones de la autoridad.

7.2 Circunstancias y graduación

La determinación de la sanción considera circunstancias atenuantes y agravantes, entre las que 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, la existencia de un modelo de prevención operativo y verificable incide en la posición de la empresa ante la autoridad.

7.3 Régimen especial para empresas de menor tamaño

Respecto de las empresas de menor tamaño conforme a la Ley N° 20.416, la normativa contempla un tratamiento diferenciado durante los primeros doce meses de vigencia, período en el cual las primeras infracciones dan lugar a amonestación escrita en lugar de multa, en los términos que la ley regula. Este régimen constituye una ventana de adecuación supervisada, no una exención de cumplimiento: la obligación legal rige desde el 1 de diciembre de 2026 para todas las organizaciones.

7.4 Riesgo no sancionatorio

El análisis de riesgo no debe limitarse a la multa. La experiencia comparada muestra que los costos reputacionales de una infracción publicitada, la pérdida de confianza de clientes y contrapartes, y la posición desmejorada en procesos de licitación o due diligence suelen exceder el impacto económico directo de la sanción.

CAPÍTULO 8

Protección de datos y compliance: la intersección con la prevención de delitos

Este capítulo aborda el ámbito en que la Ley 21.719 converge con las obligaciones de prevención de lavado de activos y de delitos corporativos, materia de especial relevancia para los sujetos obligados ante la UAF y para las empresas que han implementado modelos de prevención conforme a la Ley N° 20.393.

8.1 La debida diligencia como tratamiento de datos

Los procesos de conocimiento del cliente que exige la Ley N° 19.913 (identificación, verificación, determinación de beneficiario final, consulta de calidad de PEP, revisión contra listas de sanciones, monitoreo de operaciones) constituyen, en la taxonomía de la Ley 21.719, tratamientos de datos personales. El sujeto obligado actúa como responsable de esos datos, y sus proveedores tecnológicos de verificación y screening como encargados de tratamiento.

8.2 Base de licitud y sus límites

El tratamiento de datos efectuado para cumplir las obligaciones de la normativa de prevención de lavado de activos encuentra su base de licitud en el cumplimiento de una obligación legal. Esta base es sólida, pero su alcance es preciso: ampara los datos que la normativa exige recolectar y conservar, por los plazos que ella establece, y para las finalidades que ella define.

No quedan amparados por esa base los tratamientos que exceden la exigencia normativa: la recolección de datos adicionales por mera conveniencia comercial, la reutilización de los expedientes de debida diligencia para finalidades de marketing, o la conservación indefinida de información cuyo plazo legal de retención ha expirado. Para tales tratamientos, el responsable necesita una base de licitud distinta o debe abstenerse de realizarlos.

8.3 Tensiones operativas y su resolución

Solicitudes de supresión versus deberes de conservación. El titular que solicita la eliminación de su expediente de debida diligencia debe recibir una respuesta fundada que explique la obligación legal de conservación que prevalece, con indicación de su fuente normativa y plazo. La denegación fundada y documentada es cumplimiento; el silencio no lo es.

Confidencialidad del reporte de operaciones sospechosas. El deber de reserva que rige los reportes a la UAF prevalece respecto del derecho de acceso del titular en lo que a dichos reportes se refiere. Los procedimientos internos de respuesta a solicitudes de acceso deben contemplar expresamente esta hipótesis para evitar infracciones al régimen de prevención por la vía de cumplir el de datos.

Proveedores de verificación. Los contratos con proveedores de servicios de screening, verificación de identidad y consulta de listas deben ajustarse al estándar de contratos de encargo de tratamiento, incluyendo deberes de seguridad, confidencialidad, trazabilidad de consultas y localización de la información.

8.4 Sinergias

Las organizaciones con sistemas de prevención maduros disponen de capacidades directamente reutilizables para el cumplimiento de la Ley 21.719: cultura de documentación, trazabilidad de operaciones, gobierno de políticas, capacitación periódica y experiencia de interlocución con autoridades fiscalizadoras. La recomendación metodológica es coordinar ambos sistemas bajo una gobernanza común de cumplimiento, con roles diferenciados (oficial de cumplimiento y delegado de protección de datos) y procesos compartidos de gestión documental, capacitación y auditoría.

CAPÍTULO 9

Hoja de ruta de implementación

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

Fase 1. Diagnóstico (semanas 1 a 4)

- Levantamiento del inventario de tratamientos: qué datos, en qué sistemas y repositorios, con qué finalidades, quién accede.
- Identificación de la base de licitud de cada tratamiento y detección de tratamientos sin fundamento.
- Catastro de proveedores con acceso a datos personales y revisión preliminar de contratos.
- Identificación de transferencias internacionales, incluidas las derivadas de servicios de nube.
- Evaluación del estado de las medidas de seguridad respecto de los datos de mayor riesgo.

Fase 2. Gobernanza y documentación (semanas 5 a 10)

- Designación del responsable interno de protección de datos y definición de su mandato, reporte y recursos.
- Formalización del registro de actividades de tratamiento.
- Actualización de políticas de privacidad y avisos de información al titular, reflejando el tratamiento real.
- Definición de la política de retención y eliminación de datos, con plazos fundados por categoría.
- Diseño de los procedimientos de ejercicio de derechos: canal, verificación de identidad, plazos, registro, criterios de denegación fundada.

Fase 3. Controles técnicos y contractuales (semanas 8 a 18)

- Adecuación de contratos con encargados de tratamiento, priorizando los proveedores que tratan datos sensibles o volúmenes significativos.
- Implementación o reforzamiento de controles: gestión de accesos, cifrado de datos sensibles, registro de consultas, depuración de repositorios no controlados.
- Procedimiento de gestión de vulneraciones de seguridad: detección, evaluación, escalamiento, notificación y registro.
- Incorporación de los mecanismos de transferencia internacional que corresponda.

Fase 4. Cultura y verificación (semanas 16 a 24)

- Programa de capacitación diferenciado por audiencia (directorio, jefaturas, áreas de tratamiento intensivo, personal general).
- Ejercicio de simulación: respuesta a una solicitud de acceso y gestión de una brecha simulada, de extremo a extremo, con medición de plazos.
- Auditoría interna de cierre y plan de mantenimiento: el cumplimiento de la Ley 21.719 es un proceso continuo, no un proyecto con fecha de término.

9.1 Indicadores mínimos de preparación

Una organización puede considerarse razonablemente preparada cuando es capaz de responder afirmativamente, con evidencia, a las siguientes preguntas:

1. ¿Existe un registro de actividades de tratamiento actualizado y aprobado formalmente?
2. ¿Cada tratamiento tiene una base de licitud identificada y documentada?
3. ¿Puede la organización responder una solicitud de acceso dentro de plazo?
4. ¿Existen contratos de encargo vigentes con todos los proveedores que tratan datos personales?
5. ¿Existe un procedimiento probado de gestión y notificación de vulneraciones?
6. ¿El personal que trata datos ha sido capacitado y existe registro de ello?
7. ¿Los plazos de conservación están definidos y se aplican efectivamente?

CAPÍTULO 10

Glosario

Agencia de Protección de Datos Personales (APDP). Autoridad de control creada por la Ley 21.719, con potestades normativas, fiscalizadoras y sancionatorias en materia de datos personales.

Anonimización. Procedimiento irreversible en cuya virtud un dato deja de ser asociable a una persona identificada o identificable, quedando fuera del ámbito de la ley.

Base de licitud. Fundamento jurídico que autoriza un tratamiento de datos (consentimiento, obligación legal, ejecución de contrato, interés legítimo, entre otros).

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

Dato personal. Información vinculada o referida a una persona natural identificada o identificable.

Dato sensible. Categoría de datos personales sujeta a protección reforzada (salud, biometría, origen étnico, convicciones, vida sexual, entre otros).

Delegado de protección de datos. Responsable interno de promover y supervisar el cumplimiento de la normativa de datos en la organización.

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

Evaluación de impacto. Análisis previo de los riesgos que un tratamiento puede generar para los derechos de los titulares y de las medidas de mitigación.

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

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

Titular. Persona natural a quien se refieren los datos personales.

Tratamiento. Cualquier operación sobre datos personales, desde la recolección hasta la supresión.

UTM. Unidad tributaria mensual, unidad de cuenta utilizada para la determinación de multas.

CAPÍTULO 11

Acerca de Neitcom

Neitcom es una empresa tecnológica chilena especializada en software de compliance desde 2004. Sus soluciones apoyan los procesos de debida diligencia, consulta de personas expuestas políticamente, verificación contra listas de sanciones nacionales e internacionales y cumplimiento de las obligaciones derivadas de las leyes 19.913, 20.393 y 21.595, con trazabilidad completa de cada consulta.

La información tratada en esos procesos es, precisamente, información personal. Por ello, las plataformas de Neitcom se diseñan bajo principios de registro de operaciones, control de acceso y trazabilidad que facilitan a sus clientes la demostración de cumplimiento ante las autoridades fiscalizadoras.

Contacto. www.neitcom-compliance.cl · contacto@neitcom-compliance.cl

---