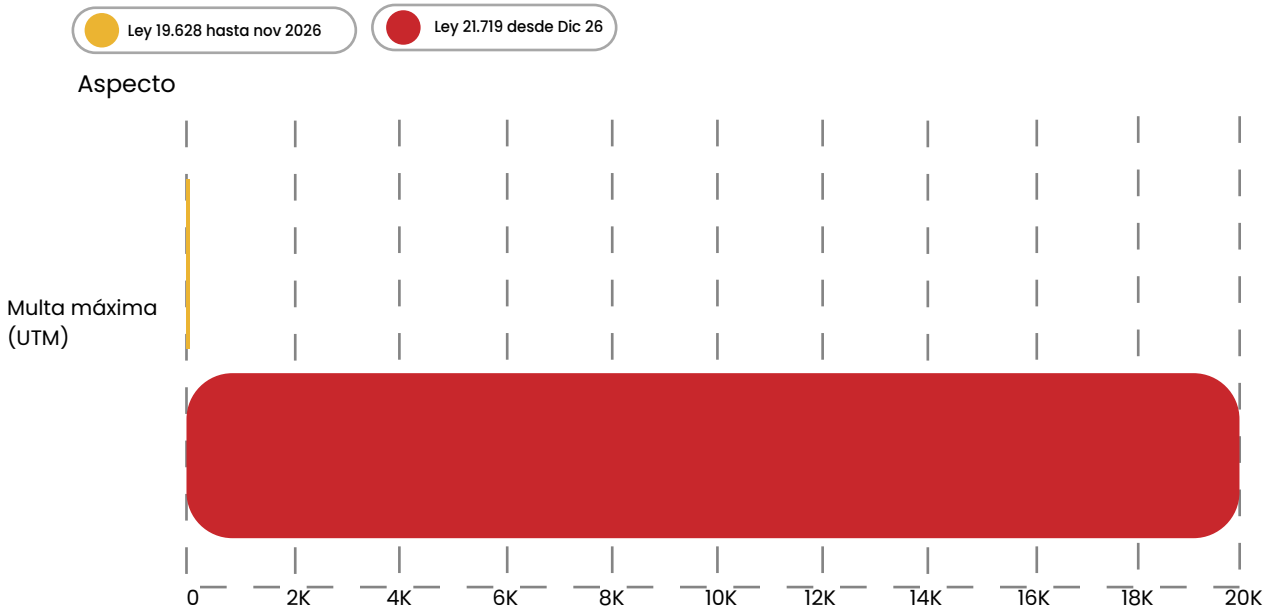
3HTP CLOUD SERVICES

Protección de Datos Personales en Chile: *Alcance de la Ley N° 21.719*

Un análisis técnico para organizaciones que tratan datos personales de personas naturales en Chile. Publicado por 3HTP Cloud Services

¿POR QUÉ CAMBIA EL MARCO LEGAL?

La ***Ley Nº 19.628 de 1999*** quedó obsoleta frente a la economía digital. Chile actualiza su normativa para ***alinearse con estándares*** internacionales como el RGPD europeo y la LGPD brasileña, reconociendo la protección de datos como un derecho fundamental. La ***Ley Nº 21.719*** no deroga la anterior — la reescribe sustancialmente, introduciendo una agencia fiscalizadora autónoma, nuevos derechos para los titulares y un régimen sancionatorio de primer nivel.



Aspecto	Ley 19.628 (Hasta nov26)	Ley 121.719 (Desde dic26)
Autoridad fiscalizadora	No existe	APDP (autónoma)
Multa Máxima	~50 UTM (vía judicial)	20.000 UTM~$1.430M CLP
Politica de privacidad	Opcional	Obligatoria
Plazo respuesta solicitudes	2 días hábiles	30 días corridos

Fecha de vigencia y período de transición

1

13 DIC 2024

Publicación en el Diario Oficial. Inicio del período de transición de dos años

HASTA 30 NOV26

Sigue vigente la Ley 19.628 original. Las organizaciones deben prepararse para el cambio

2

3

1 DIC 2026

Vigencia plena. Rige el articulado completo, incluyendo el régimen sancionatorio

Primeros 6 meses post-vigencia

Plazo para dictar los reglamentos de implementación conforme a la ley

4

⚠ El Consejo Directivo de la APDP debe quedar designado antes del 1 de junio de 2026, conforme a la Ley 21.806. Las organizaciones que no estén listas al 1º de diciembre de 2026 quedan expuestas al régimen sancionatorio completo.

Ámbito de aplicación: ¿a quién aplica?

La ley aplica a **toda persona natural o jurídica**,pública o privada, que realice tratamiento de datos personales de personas naturales. **No existe umbral de tamaño ni de volumen de datos** para quedar sujeto a sus obligaciones — desde una startup hasta una multinacional están bajo su alcance. El alcance es también **extraterritorial:** aplica aunque el responsable no tenga presencia física en Chile, si sus operaciones están destinadas a ofrecer bienes o servicios a titulares ubicados en territorio chileno. Este principio sigue el modelo del RGPD europeo.

Quedan excluidos:

- **Tratamiento de datos en ejercicio de libertad de opinión e información (medios de comunicación)**
- **Datos tratados por personas naturales en actividades estrictamente personales o domésticas**

¿Tu organización está incluida?

Si tu empresa, startup, organismo público o proveedor de servicios recopila, almacena, procesa o comunica datos de personas naturales en Chile — ***sí aplica, independientemente de dónde estén tus servidores.***

Empresas locales

Empresas extranjeras con clientes en Chile

Organismos públicos

Roles clave: Responsable y Encargado del Tratamiento

Responsable del Tratamiento

Persona natural o jurídica que decide sobre los fines y medios del tratamiento. Determina qué datos se recopilan y para qué. Es el principal obligado ante la APDP y ante los titulares.

Encargado del Tratamiento (Mandatario)

Quien trata datos por cuenta y bajo instrucciones del responsable. Proveedores cloud, call centers, consultoras y procesadores de pago que trabajan con datos de clientes son encargados.

Los contratos con proveedores de servicios cloud o SaaS deben incluir cláusulas de tratamiento de datos que cumplan con la Ley 21.719. Sin estas cláusulas, el responsable puede enfrentar sanciones aunque la vulneración la cometa el proveedor.

3HTP CLOUD SERVICES

Principios que rigen el tratamiento de datos

LICITUD Y LEALTAD

El tratamiento debe tener una base legal válida y no engañar al titular sobre el uso de sus datos.

FINALIDAD

Los datos solo pueden usarse para el propósito declarado al momento de su recolección. Usos distintos requieren nueva base legal.

Proporcionalidad (minimización)

Solo se deben recopilar los datos estrictamente necesarios para la finalidad declarada. Menos datos = menos riesgo.

RESPONSABILIDAD PROACTIVA

El responsable debe poder demostrar cumplimiento en todo momento. Privacy by Design desde el inicio de cada proyecto, no como una capa posterior.

CONFIDENCIALIDAD Y SEGURIDAD

Obligación de mantener secreto y adoptar medidas técnicas y organizativas apropiadas al riesgo del tratamiento.

Bases de licitud: cuándo es legal tratar datos

Todo tratamiento requiere una ***base jurídica válida***. El consentimiento (Art. 12)
es la regla general, pero no el único camino. El Art. 13 reconoce cinco fuentes alternativas de licitud que no requieren
consentimiento expreso del titular.

⚠

El consentimiento no debe usarse como comodín. Si existe otra base de licitud aplicable, es preferible usarla — el consentimiento puede revocarse en cualquier momento.

1. Obligaciones económicas, financieras, bancarias o comerciales
Reguladas en el Título III de la ley.

2. Cumplimiento de obligación legal
Cuando la ley exige el tratamiento de datos para cumplir un mandato normativo.

3. Ejecución de un contrato
Cuando el tratamiento es necesario para cumplir un contrato entre el titular y el responsable.

4. Interés legítimo del responsable Con límites y ponderación frente a los derechos del titular.

5. Misión de interés público O ejercicio de potestades públicas conferidas al responsable.

3HTP CLOUD SERVICES

Datos Sensibles: régimen de protección

El Art. 16 define categorías de datos cuya exposición puede causar discriminación o daño irreparable. ***Tratarlos sin base legal es la infracción más grave: hasta 20.000 UTM***. Su tratamiento requiere consentimiento explícito o una base de licitud reforzada.

Salud física o mental

Origen racial o étnico

Opiniones políticas

Creencias religiosas o filosóficas

Datos biométricos y genéticos

Situación migratoria

Las bases de datos que contengan estas categorías requieren controles de acceso más estrictos, cifrado de datos en reposo y tránsito, y la realización de Evaluaciones de Impacto en la Protección de Datos (EIPD) antes de iniciar el tratamiento.

Derechos del titular: ARCOP+B

La ley reconoce seis derechos ejercibles por el titular. El responsable tiene **30 días corridos** para responder desde la recepción de la solicitud. El incumplimiento puede derivar en multas de hasta **10.000 UTM** por parte de la APDP.

Acceso

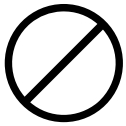
Saber qué datos tiene la empresa, con qué finalidad, por cuánto tiempo y a quién se han comunicado.

Rectificación

Corregir datos inexactos en todos los sistemas y repositorios donde estén replicados.

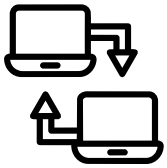
Cancelación

Eliminar o anonimizar datos cuando ya no sean necesarios para la finalidad que justificó su recolección.



Oposición

Oponerse al tratamiento, especialmente en decisiones automatizadas con efectos significativos.



Portabilidad

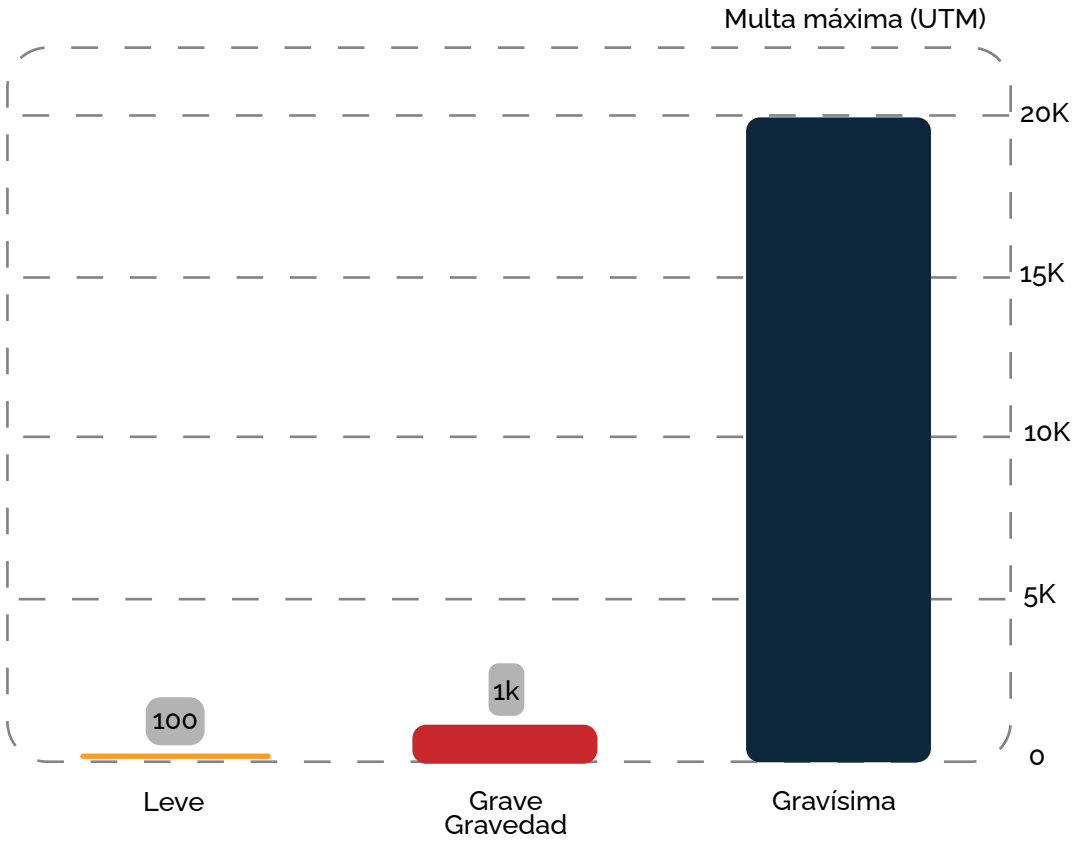
Recibir sus datos en formato estructurado (CSV, JSON) y transferirlos a otro responsable cuando aplique.

Bloqueo

Suspender el tratamiento temporalmente mientras se resuelve una disputa o se verifica la exactitud de los datos.

La Agencia de Protección de Datos Personales

La APDP es el **organismo autónomo** creado por la Ley 21.719, encargado de fiscalizar, investigar y sancionar el incumplimiento de la normativa. Representa el cambio más estructural respecto a la ley anterior: por primera vez Chile contará con una autoridad de control independiente con facultades reales de enforcement.



Las sanciones escalan desde 100 UTM (~$7,1M CLP) para infracciones leves hasta 20.000 UTM (~$1.430M CLP) para las gravísimas — como el tratamiento ilícito de datos sensibles.

Obligaciones técnicas clave para equipos de TI

PRIVACY BY DESIGN
Incorporar controles de privacidad desde el diseño de sistemas y arquitecturas. La privacidad no es una capa posterior — es un requisito funcional desde el día cero de cada proyecto.

EVALUACIÓN DE IMPACTO (EIPD)
Obligatoria para tratamientos de alto riesgo, especialmente datos sensibles o decisiones automatizadas. Debe documentarse y actualizarse ante cambios relevantes en el sistema.

NOTIFICACIÓN DE VULNERACIONES
Reportar brechas de seguridad a la APDP y a los titulares afectados dentro de los plazos establecidos. Se requiere un protocolo de respuesta a incidentes documentado y probado.

CONTRATOS CON ENCARGADOS
Los acuerdos con proveedores cloud, SaaS o terceros que traten datos deben incluir cláusulas de cumplimiento, instrucciones de tratamiento y medidas de seguridad exigibles.

Hoja de ruta hacia el cumplimiento

La cuenta regresiva hacia el 1º de diciembre de 2026 ya comenzó.
Organizaciones que inicien hoy tienen tiempo suficiente para cumplir en forma ordenada. Quienes esperen al último trimestre enfrentarán presión operacional y riesgo de sanciones desde el primer día de vigencia.

01
Inventario de datos Mapear todos los flujos de datos personales: qué se recopila, para qué, dónde se almacena y quién accede.

02
Identificar bases de licitud Asignar una base legal válida a cada tratamiento. No usar el consentimiento como comodín.

03
Actualizar contratos Revisar acuerdos con proveedores cloud y SaaS para incluir cláusulas de encargado de tratamiento.

04
Implementar derechos ARCOP+B Habilitar canales y procesos internos para responder solicitudes dentro de los 30 días corridos exigidos.

05
Política de privacidad
Publicar aviso de privacidad obligatorio con toda la información exigida por la ley.

06
Plan de respuesta a brechas Definir protocolo de detección, contención y notificación de incidentes de seguridad.

3HTP CLOUD SERVICES

¿Cómo puede ayudarte 3HTP Cloud Services?

En 3HTP Cloud Services acompañamos a organizaciones en la implementación de arquitecturas cloud seguras y conformes con la Ley 21.719, desde el diseño hasta la operación continua.

1

Diagnóstico de brechas

Evaluación de cumplimiento en infraestructura y sistemas existentes frente a los requisitos de la Ley 21.719.

2

Arquitecturas cloud seguras

Diseño e implementación de soluciones cloud con Privacy by Design integrado desde la arquitectura base.

3

Controles de seguridad

Implementación de cifrado, gestión de accesos, auditoría de eventos y medidas técnicas requeridas por la ley.

4

Asesoría contractual

Soporte en contratos con proveedores y redacción de cláusulas de encargado de tratamiento conformes a la normativa

Fuentes

- **Ley 21.719 Chile — Guía Completa 2026 + Plantillas Gratis PrivacidadWeb**
- **Chile establece una nueva Ley de Protección de Datos — DLA Piper**
- **Ley 21.719 — Guía de cumplimiento para empresas en Chile · Silocydata**
- **Ley N° 21.719 — Conoce más sobre la Nueva Ley de datos personales | DOE Actualidad Jurídica**
- **Cómo elegir la base de licitud correcta en la Ley 21.719 Confidata Chile Blog**
- **Datos Sensibles: Qué Son y Cómo Protegerlos según la Ley 21.719 PrivacidadWeb**
- **Derechos ARCO en la Ley 21.719: cómo responder dentro de plazo XMS**
- **Informe Ley N°21.719 sobre Protección de Datos — RSM Chile**

3HTP CLOUD SERVICES

www.3htp.com

¿LISTO PARA INICIAR TU HOJA DE RUTA AGÉNTICA?

En 3HTP Cloud Services acompañamos a organizaciones del sector telco en el diseño e implementación del ciclo de soporte inteligente:

Detección preventiva, diagnóstico automatizado, corrección automática y corrección de errores en código con IA desde la hoja de ruta hasta la integración con sus ecosistemas ITSM, BSS/OSS, repositorios de código y pipelines CI/CD.

contacto@3htp.com

www.3htp.com