

LEY 21.719 · DATOS PERSONALES

12 puntos para preparar tu organización

Para municipios, servicios públicos e instituciones de educación. Marca lo que ya tienes resuelto y mira en qué punto estás. Basado en la Ley 19.628, modificada por la Ley 21.719.

Vigencia fijada por la ley

1 de diciembre de 2026

Proyecto en el Senado (boletín 18.623-07) propone

1 de diciembre de 2027

1 Gobernanza

**Hay una persona o equipo a cargo del cumplimiento, con respaldo formal de la autoridad.**

El delegado de protección de datos es voluntario: el responsable «podrá designar» uno ([art. 50](#)). Igual conviene que alguien tenga el tema asignado por escrito.

**La autoridad conoce el régimen de sanciones que le aplica.**

En los órganos públicos la multa es personal: del 20 % al 50 % de la remuneración mensual del jefe superior del servicio; con datos sensibles, 50 % y suspensión de hasta 30 días ([art. 44](#)).

2 Conocer tus datos

**Tienes un inventario de qué datos personales tratas, para qué, dónde se guardan y quién accede.**

La ley no nombra un «registro de tratamientos», pero llevarlo es la forma práctica de demostrar cumplimiento.

**Identificaste los datos sensibles, como los de salud, y tienen resguardos reforzados.**

Es el caso que la ley sanciona con más fuerza. Revisa fichas, certificados médicos, justificaciones y beneficios.

**Cada uso de datos tiene su fundamento definido.**

Consentimiento, obligación legal o, en órganos públicos, el ejercicio de sus funciones legales ([arts. 20 a 23](#)).

Con o sin prórroga, implementar toma meses. Levantar el inventario, redactar políticas, ajustar sistemas y capacitar no se resuelve en una semana. El régimen de sanciones no cambia con el proyecto de prórroga.

3 Transparencia y derechos

- ☐ **Informas a las personas cómo tratas sus datos.**
Política de privacidad y avisos en formularios, sitios y sistemas ([art. 14 ter](#)).
- ☐ **Tienes un procedimiento para responder solicitudes de acceso, rectificación, supresión, oposición, portabilidad y bloqueo.**
Con responsable, canal de entrada y control del plazo legal de respuesta ([arts. 4 a 9](#)).

4 Seguridad

- ☐ **Tus sistemas tienen medidas de seguridad proporcionales al riesgo.**
Control de accesos por rol, respaldos probados, cifrado donde corresponde y registro de quién consulta qué.
- ☐ **Tienes un procedimiento para vulneraciones de seguridad.**
Detectar, contener y reportar «sin dilaciones indebidas» ([art. 14 sexies](#)). La ley de datos no fija 72 horas; esos plazos vienen de la Ley 21.663 de ciberseguridad, para quienes deben reportar al CSIRT.
- ☐ **Evalúas el impacto antes de iniciar tratamientos de alto riesgo.**
Evaluación de impacto en protección de datos ([art. 15 ter](#)), por ejemplo al usar IA con datos de personas o datos de salud.

5 Proveedores

- ☐ **Los proveedores que tratan datos por ti tienen contrato con cláusulas de protección de datos.**
Plataformas en la nube, sistemas contratados, herramientas de IA y correo ([art. 15 bis](#)). Revisa también si los datos salen del país.

6 Personas y evidencia

- ☐ **Los funcionarios que manejan datos están capacitados y queda evidencia de todo lo anterior.**
Actas, resoluciones, registros de capacitación y versiones de las políticas. Cumplir incluye poder demostrarlo.

0 a 4

Prioridad alta. Conviene partir por gobernanza e inventario.

5 a 8

Vas en camino. Faltan piezas formales o de seguridad.

9 a 12

Bien encaminado. Revisa evidencia y proveedores.

Diagnóstico sin costo

Revisamos contigo este checklist en 30 minutos y te decimos por dónde partir. Implementación completa en 8 semanas.

mindigital.cl/#contacto

jonathan@mindigital.cl · +56 9 7397 5099