

# Ley 21.719 de Datos Personales: guía práctica para pymes

Qué cambia el 1 de diciembre de 2026, qué te pueden exigir tus clientes y los primeros pasos para cumplir sin pagar de más. Orientación operativa, no asesoría legal.

VE Solutions · Dirección de tecnología e IA fraccional

Si guardas datos de clientes, trabajadores o proveedores —una lista de WhatsApp, una planilla de socios, fichas, correos, cámaras— la nueva ley de datos personales te aplica. No es solo para bancos ni para grandes empresas: es para cualquier negocio que trate datos de personas.

Esta guía te muestra lo esencial en lenguaje de dueño de negocio: qué cambia, qué pueden exigirte y por dónde partir. No reemplaza a un abogado; te deja preparado para conversar con uno sin partir de cero, y para no comprar 'cumplimiento mágico' que no necesitas.

## 1. Qué cambia y desde cuándo

La Ley 21.719 moderniza la protección de datos en Chile y entra en plena vigencia el 1 de diciembre de 2026. Crea una autoridad dedicada —la Agencia de Protección de Datos Personales— con facultades reales de fiscalización y sanción.

Las multas se aplican por tramos según la gravedad y, en los casos más graves, pueden llegar a montos que ponen en riesgo a una pyme completa. El punto no es memorizar cifras: es que por primera vez incumplir tiene un costo real y fiscalizable.

- Vigencia plena: 1 de diciembre de 2026.
- Nueva agencia fiscalizadora con sanciones por tramos (leves, graves y gravísimas).
- Aplica a empresas de cualquier tamaño que traten datos personales.
- Los datos de salud y otros datos sensibles tienen el estándar más alto.

## 2. Los derechos que tus clientes pueden exigirte

Cualquier persona cuyos datos guardes puede pedirte cuentas: qué tienes de ella, para qué lo usas, que lo corrijas, que lo borres, que dejes de usarlo para marketing o que se lo entregues en un formato portable. Y tienes plazos para responder.

Para una pyme, el riesgo práctico no es el cliente hostil: es no tener NINGÚN proceso para responder. Si una solicitud llega hoy a tu correo, ¿quién la ve, qué contesta y dónde queda registrada?

- Acceso: qué datos tienes y para qué.
- Rectificación: corregir lo que está mal.
- Supresión: borrar cuando corresponde.
- Oposición y bloqueo del marketing: dejar de usar sus datos para venderle.
- Portabilidad: entregar sus datos en un formato estándar.

## 3. Consentimiento: la casilla pre-marcada ya no sirve

El consentimiento válido debe ser libre, específico, informado e inequívoco. En la práctica: nada de casillas pre-marcadas, nada de 'al comprar aceptas recibir publicidad' escondido en los términos, y el consentimiento de marketing va SEPARADO del resto.

Igual de importante: debes poder DEMOSTRAR el consentimiento. Un registro simple —quién, cuándo, para qué, cómo— vale más que cualquier declaración bonita en tu sitio.

- Marketing siempre con casilla propia, sin marcar por defecto.
- Guarda evidencia: fecha, texto aceptado y canal.
- Darse de baja debe ser tan fácil como suscribirse.

## 4. Tus primeros 7 pasos (en orden)

No necesitas partir con un proyecto gigante. Necesitas partir en orden. Estos siete pasos cubren lo que una fiscalización básica miraría primero, y casi todos se pueden hacer con lo que ya tienes.

1. Inventario: qué datos tienes, de quién, dónde viven y quién accede.
2. Base de licitud: para cada uso, ¿contrato, consentimiento u otra base legal?
3. Política de privacidad visible y en cristiano, que describa lo que de verdad haces.
4. Consentimientos al día: formularios con casillas separadas y registro.
5. Contratos con quienes procesan datos por ti (software, agencias, contadores).
6. Seguridad mínima: contraseñas serias, accesos por persona, respaldo probado.
7. Un canal y un responsable para responder solicitudes de derechos, con plazo.

## 5. Dónde la tecnología ayuda (y dónde no)

La tecnología correcta baja el costo de cumplir: formularios que registran el consentimiento solos, respaldos automáticos, accesos por rol. Y cuando usas IA, el despliegue local marca la diferencia: un modelo que corre en tu propia infraestructura procesa tus datos sin que salgan de tu empresa.

Lo que NO existe es el 'software que te hace cumplir la ley' comprándolo y ya. El cumplimiento es proceso más evidencia; la herramienta solo lo hace más barato y más difícil de olvidar.

- Automatiza el registro (consentimientos, solicitudes, respaldos), no el criterio.
- Con datos sensibles, prefiere procesamiento local o proveedores con contrato claro.
- Desconfía de quien te venda 'cumplimiento total' sin mirar tu operación.

### Tres casos concretos

#### COMERCIO

##### La lista de WhatsApp de la carnicería

Una lista de difusión con 400 clientes es una base de datos personal. Necesita consentimiento de marketing separado y registrado, una forma simple de salir de la lista, y un responsable si alguien pide que borren su número. Nada de esto requiere software caro: requiere orden y evidencia.

#### SALUD

##### La veterinaria con fichas y recordatorios

Los datos de salud —también en clínicas, dentales y centros— son sensibles: estándar más alto, más cuidado con quién accede y con qué proveedor los procesa. Si un agente de IA confirma citas, debe identificarse como IA, registrar el consentimiento y derivar a una persona. Aquí el procesamiento local vale oro.

#### SERVICIOS

##### El gimnasio con socios, pagos y cámaras

Datos de socios, medios de pago y cámaras de seguridad conviven en el mismo negocio. Cada uno tiene su base legal distinta: el contrato del socio, la obligación de cobro, la seguridad del recinto. Mapearlos toma una tarde y ordena todas las decisiones que vienen después.

## Checklist de 10 puntos

Imprime esta página. Si marcas menos de 7, tienes trabajo pendiente antes de diciembre de 2026.

- ☐ Sé qué datos personales tengo y dónde están.
- ☐ Cada uso tiene una base legal identificada.
- ☐ Mi política de privacidad describe lo que realmente hago.
- ☐ El consentimiento de marketing es una casilla separada, sin marcar.
- ☐ Puedo demostrar cuándo y cómo consintió cada contacto.
- ☐ Tengo contrato con cada proveedor que toca mis datos.
- ☐ Los accesos son por persona y se revocan al salir alguien.
- ☐ Tengo respaldo automático y lo he probado restaurando.
- ☐ Hay un canal y un responsable para solicitudes de derechos.
- ☐ Si uso IA con datos de clientes, sé dónde se procesan y quién los ve.

## ¿Y si necesito ayuda?

Esta guía es orientación operativa, no asesoría legal: para interpretar la ley en tu caso, consulta a un abogado. Donde nosotros sí ayudamos es en la parte técnica y de proceso: diagnóstico express de cumplimiento desde \$390.000 + IVA, adecuación completa según tu caso, y tecnología que registra el cumplimiento sola —incluidos modelos de IA que corren en tu propia infraestructura, donde tus datos no salen.

**Conversemos tu caso en [vsol.cl](https://vsol.cl) · [contacto@vsol.cl](mailto:contacto@vsol.cl)**