



¿Qué debe saber el dueño de una PYME de la ley de protección de datos personales?

Pymes y organizaciones solidarias

● ○ ○ FICHA BÁSICA

Fecha	Julio 2025
Tpo. de lectura	16 min.

Ley 21.719, que entra en vigencia el 1º de diciembre del 2026, busca

- Proteger los **datos personales de las personas**, es decir, toda información que permita identificarlas directa o indirectamente (como nombre, RUT, teléfono, correo, dirección, historial de compras, etc.).
- Asegurar que las personas tengan **control sobre sus datos**: saber quién los usa, para qué, y exigir que se respeten ciertos derechos (como eliminar, corregir o limitar el uso de su información).



Aplica tanto para una empresa grande, como para una PYME, un emprendimiento o un profesional independiente y significa que NO puede usar datos personales de clientes, trabajadores ni proveedores como se quiera. Al contrario, se debe hacer de manera responsable, transparente y con el consentimiento del dueño del dato (el titular).

Ejemplos de soportes donde se manejan **datos personales dentro de empresas**:

- Base de clientes con nombres, correos y teléfonos.
- CV de personas que postularon a tu empresa.
- Cámaras de vigilancia.
- Formulario web para cotizaciones.
- Promociones enviadas por WhatsApp o correo electrónico.

IMPORTANTE: una PYME está legalmente obligada, al igual que una empresa grande, a manejar esos datos con cuidado, evitar filtraciones y respetar los derechos de las personas.

Obligaciones básicas que toda PYME debe tener presente al recolectar datos personales:

1. Obtener consentimiento claro y específico.

No se puede recolectar ni usar datos sin autorización. El consentimiento debe ser informado y voluntario.

Por ejemplo, si vas a usar el correo de un cliente para enviarle promociones, debe haber aceptado eso específicamente. Informar para qué se usarán los datos

Debes decirle al cliente (o trabajador, proveedor, etc.) para qué estás pidiendo sus datos y por cuánto tiempo los conservarás.

2. Usar los datos sólo para el fin autorizado.

Si un cliente entrega su número para coordinar una entrega, no se puede después usar para enviarle publicidad, a menos que haya aceptado eso también.

4. Respetar los derechos del titular.

Cualquier persona puede pedir que se le informe sobre qué datos tienen de ella, corregirlos o eliminarlos. Y se debe cumplir con eso en un plazo razonable.

3. Proteger los datos.

Es obligatorio tomar medidas de seguridad razonables (como contraseñas, antivirus, sistemas de respaldo). No se puede tener datos personales en planillas sueltas, sin clave o en equipos compartidos sin control.



La ley también aplica para los datos de los trabajadores de una pyme (como RUT, teléfono, salud previsual, dirección o antecedentes laborales) ya que **son datos personales** y están protegidos por la ley.

Las obligaciones básicas respecto del manejo de esta información son:

- No se puede compartir esos datos con terceros sin su consentimiento.
- Se debe proteger la información personal en contratos, planillas de sueldo, licencias médicas, etc.
- No se puede usar su información personal para fines distintos a la relación laboral. Por ejemplo: no se puede usar el correo de un trabajador para enviarlo a una lista de difusión de la empresa sin su permiso.

Para los sitios web se debe considerar

- Aplicar la política de privacidad si estos recolectan cualquier tipo de dato personal a través de formularios de contacto, inscripciones a newsletter, reservas, compras, chatbots o cualquier otra función que recolecte datos como nombre, correo o teléfono.

- La **política de privacidad debe ser visible y accesible**.

¿Dónde ponerla?

- En el menú principal del sitio (footer).
- Al lado o bajo cada formulario de contacto.
- Junto a los términos y condiciones de venta.

Consejo: que sea simple y en lenguaje amigable. No necesitas llenarla de lenguaje legal.

- **Avisar el uso de cookies si estas recolectan datos personales** o hacen seguimiento del comportamiento del usuario (como cookies de Google, Facebook Ads, *remarketing*, etc.).

¿Qué se debe hacer?

- Informar que usas cookies.
- Explicar para qué sirven (ej. analizar navegación, mostrar publicidad, etc.).
- Permitir que el usuario acepte o rechace (idealmente con un banner de consentimiento).

Ejemplo texto de aviso básico: “Este sitio utiliza cookies para mejorar tu experiencia. Puedes aceptar o configurar tu uso. Más información en nuestra política de cookies.”

¿Qué hacer ante un incidente o filtración de información?



Ante una filtración de datos debes:

1. Detener el acceso indebido o la pérdida.
2. Informar al afectado.
3. Registrar lo ocurrido.
4. Notificar a la Agencia de Protección de Datos del incidente.

¿Mi pyme cumple con la ley de protección de datos?

Haga este *checklist* simple para saberlo. Responda sí o no. Si tiene muchos “no”, es momento de hacer ajustes.

Pregunta	¿Sí / No?
¿Informo a las personas por qué y para qué recolecto sus datos?	
¿Pido consentimiento antes de enviar correos o promociones?	
¿Tengo una política de privacidad, aunque sea básica?	
¿Protejo los datos con contraseña o acceso limitado?	
¿Evito compartir datos con terceros sin avisar al cliente?	
¿Permito que el cliente me pida eliminar o corregir sus datos?	
¿Tengo un registro claro de los datos que recolecto y para qué los uso?	
¿Evito recolectar más datos de los estrictamente necesarios?	
¿Tengo cartel visible si uso cámaras de vigilancia?	
¿Tengo respaldo o ayuda profesional si tengo dudas legales?	

Política de privacidad para pymes

Aunque no sea obligatorio por ley tener un documento formal en todos los casos, es altamente recomendable tener una **política de privacidad simple** que demuestre que la empresa **cumple con la ley y respeta a sus clientes**.

Una **política de privacidad sencilla debe decir**:

- Qué datos recolecta (nombre, correo, RUT, etc.)
- Para qué se usan (ej.: envío de productos, promociones, contacto postventa)
- Cómo se protegen
- Si se comparten datos con terceros (por ej. empresas de envío)
- Cómo el cliente puede pedir acceso, corrección o eliminación de sus datos

Se puede poner en el sitio web, en el pie de los correos, o incluso impresa en el local o contrato. No tiene que ser un documento largo o legalista.



¿Qué pasa si no cumpla con esta ley? ¿Hay sanciones?

Las sanciones pueden ser altas, y se aplicarán una vez que entre en vigor la nueva institucionalidad (la Agencia de Protección de Datos). Las multas podrán llegar hasta 10.000 UTM (más de \$650 millones) en casos graves.

Además de las multas, una empresa que no protege bien los datos puede sufrir:

- Demandas civiles de clientes o usuarios.
- Daño a la reputación, especialmente si se filtran datos personales.
- Pérdida de confianza de sus clientes.
- En el futuro, habrá restricciones para contratar con el Estado si no cumple con la normativa.

IMPORTANTE: Aunque aún hay aspectos de implementación (como la agencia fiscalizadora), las obligaciones de esta ley ya están vigentes, y mientras más te adelantes, menos riesgo tendrás cuando la fiscalización comience de forma activa.

Contenido desarrollado por FGE con base en la Ley N° 21.719.