Marco Legal

Preguntas frecuentes sobre la Ley de Protección de datos personales en Chile

●●○ NIVEL INTERMEDIO

1. ¿Las inversiones de una empresa se consideran un dato personal?

De acuerdo al artículo 1 letra f) de la ley N° 21.719, que entrará en vigencia el 1º de diciembre del año 2026, un dato personal corresponde a cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Las inversiones de una empresa no son un dato personal. Este tipo de información constituye un dato comercial, financiero o de carácter corporativo. Que las inversiones de la empresa no requieran el cumplimiento de la Ley de Protección de Datos no significa que estén desprotegidas. Este tipo de información estratégica o sensible del negocio se resguarda bajo otros mecanismos legales tales como Ley de mercado Valores, acuerdos de confidencialidad (NDA), Ley de Propiedad intelectual y secreto comercial, entre otros.

Ante esto, es natural preguntarse ¿las inversiones de una organización y de una persona natural se regulan de la misma manera?

No. Las inversiones de una persona natural, sí corresponden a un dato personal (dato específico de carácter financiero) y se regulan directamente por la Ley N° 19.628 con las modificaciones introducidas por ley N° 21.719.

Excepción

Se puede dar la situación al traspasar el límite entre organización jurídica y persona, como establece el artículo 13 de la ley N° 21.719. Por ejemplo, al revisar una inversión de la empresa aparece el nombre o RUT de un socio, o accionista ("persona identificada"), o por si cruzando el monto invertido con el tipo de sociedad, se deduce inequívocamente quién es el dueño real ("persona identificable"), el dato corporativo pasa a ser protegido de inmediato por la ley de Protección de Datos Personales.

2. ¿Qué área de la organización debiera asumir el liderazgo y la responsabilidad de la gestión y la supervisión integral de la protección de datos?

Siempre hay que atender al tamaño, giro y recursos de la empresa. En este cuadro se visualiza, la manera óptima de establecer las distintas responsabilidades.

Es importante destacar que los procedimientos y políticas son promovidos por los altos mandos o directorio. Son implementados por el área de cumplimiento, pero los conocimientos técnicos los aporta el área de TI, quien entrega las herramientas y la viabilidad real de ejecución. Por eso, es esencial que los cargos operen de forma conjunta.

Tamaño empresa	Responsable legal	Ejecutor técnico	Encargado de cumplimiento (ejecutor operativo)
Micro y Pequeña	Gerente general /dueño	Soporte TI (interno o externo)	Asesor legal externo / consultor
Mediana	Gerente de administración/ finanzas	Jefe de informática / TI	Encargado de compliance o DPO externo
Gran Empresa	Directorio / fiscal de la organización	CISO / gerente de ciberseguridad	Delegado de Protección de Datos (DPO)

IMPORTANTE

¿Cuándo es obligatorio designar un DPO?

La Ley 21.719 no obliga a designar un Delegado de Protección de Datos (DPO) en todos los casos. La designación del DPO en Chile está vinculada al Modelo de Prevención de Infracciones (MPI), regulado en el artículo 49 de la ley.

¿Qué significa esto en la práctica?

Si una organización opta voluntariamente por certificar un Modelo de Prevención de Infracciones ante la Agencia de Protección de Datos, debe designar un DPO con autonomía e independencia funcional. El MPI funciona como atenuante en caso de sanciones.

Si tu organización no adopta el MPI, puede operar con un encargado interno de cumplimiento sin la figura formal de DPO, manteniendo siempre las obligaciones que la ley impone a todo responsable de datos.

La tabla anterior es una guía operacional sobre cómo asignar responsabilidades de cumplimiento dentro de la organización. No debe interpretarse como una obligación legal de designar DPO según el tamaño de la empresa.

En las micro, pequeñas y medianas empresas, el dueño o sus máximas autoridades podrán asumir las tareas del delegado de datos.

3. ¿Cómo debe una organización manejar la gestión de formularios y el mailing?

Toda organización que recopila datos a través de formularios web o realiza envíos de email marketing está tratando datos personales. Esto incluye fundaciones, corporaciones, Pymes y cualquier entidad que gestione una base de contactos, independiente de su tamaño o giro.

¿Qué se necesita para hacerlo correctamente?

El consentimiento. La Ley N° 21.719, en su artículo 12, establece que el tratamiento de datos personales es lícito cuando el titular otorga su consentimiento de manera **libre, informada y específica**. Esto no es una formalidad: define concretamente cómo deben diseñarse los formularios y cómo debe gestionarse el email marketing.

¿Qué debe incluir un formulario y un envío de email marketing?

Para cumplir con este estándar, todo formulario y envío de email marketing debe:

a. Contener una casilla de verificación desmarcada: ya que el marcar la casilla implica una acción positiva del titular.

b. Informar la finalidad, ya que esos datos no podrán tratarse a futuro para otra finalidad. Si se pretende extender el tratamiento de otros fines, se debe expresar ese consentimiento para ello también.

   Ejemplo:

   [ ] Acepto los Términos y la Política de Privacidad para gestionar mi solicitud (casilla obligatoria).

   [ ] Acepto recibir ofertas, promociones y comunicaciones comerciales (Opcional).

c. Enunciar quién es el Responsable del tratamiento de datos [Razón Social de la empresa].

d. Comunicar los derechos que le pertenecen al titular de los datos personales de manera breve junto al canal de contacto (correo electrónico).

e. Remisión a la Política de Privacidad de la organización para más detalle.

f. Para el caso del email marketing, cada correo debe incluir en el pie de página un botón o enlace visible para "Darse de baja" o "Cancelar suscripción", con un solo click.

   Se debe tener en cuenta que los formularios como el email marketing está íntimamente relacionados, en virtud que los formularios son la captación o entrada del cliente a una base de datos otorgando su consentimiento. El email marketing aplica a una base de datos donde los titulares ya otorgaron sus consentimiento por haber marcado la casilla opcional: *[ ] Acepto recibir ofertas, promociones y comunicaciones comerciales*.

4. ¿Cómo fundamentamos la utilización de cámaras de vigilancia en las organizaciones?

La Ley N° 21.719 habla del interés **legítimo**. El artículo 13 letra d), consagra explícitamente el **interés legítimo**, señalando que el tratamiento es lícito cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable (la organización) o por un tercero, siempre que sobre dichos intereses no prevalezcan los derechos y libertades fundamentales del titular.

Esto debe complementarse necesariamente, con las normas del Código del Trabajo, **artículo 154 inciso final** que es el pilar más importante para la protección de datos en el ámbito laboral. El inciso final estipula textualmente "toda medida de control, sólo podrán efectuarse por medios idóneos y concordantes con la naturaleza de la relación laboral y, en todo caso, su aplicación deberá ser general, garantizándose la impersonalidad de la medida, para respetar la dignidad del trabajador."

Es decir, los requisitos generales de toda medida de control, son los siguientes:

a. Deben necesariamente incorporarse en el Reglamento Interno de Higiene y Seguridad de la organización.

b. Sólo pueden efectuarse por medios idóneos y concordantes con la naturaleza de la relación laboral.

c. Su aplicación debe ser general.

d. Debe respetarse la dignidad del trabajador.

e. En especial, con medidas de control audiovisual, no deben dirigirse directamente al trabajador, sino que, en lo posible, orientarse en un plano panorámico.

f. Deben ser conocidos por los trabajadores, estableciéndose carteles que den noticia de dicha medida.

g. Su emplazamiento no debe abarcar lugares, aun cuando ellos se ubiquen dentro de las dependencias de la organización dedicados al esparcimiento de los trabajadores, tales como, comedores y salas de descanso, aquellos en los que no se realiza actividad de tipo laboral, como los baños, casilleros, salas de vestuarios, etc.

Lectura complementaria ORD. N°2328/130

5. ¿Qué es el Privacy by Design y cómo protege a tu organización ante la Agencia de Protección de Datos?

Esto es un tema técnico y tiene una importancia trascendental para efectos del monitoreo y fiscalización de la Agencia de Protección de Datos Personales (APDP). Es lo que se llama Protección desde el diseño y por defecto (Privacy By Design), que el **Artículo 14 quáter** vincula el diseño técnico con el cumplimiento legal. Exige que las medidas técnicas y organizativas de protección estén incorporadas desde el inicio y durante todo el ciclo de vida del tratamiento de datos

La empresa debe demostrar con evidencias técnicas (como registros de auditoría o logs) que el sistema fue diseñado para evitar el consentimiento automático o por error.

En términos prácticos, esto significa que la organización debe poder responder ante la Agencia de Protección de Datos las siguientes preguntas:

- ¿Cuándo otorgó el titular su consentimiento?
- ¿Es posible verificar la fecha y hora en que otorgó el consentimiento?
- ¿Qué versión de la política de privacidad estaba vigente en ese momento?
- ¿La casilla estaba desmarcada por defecto?

No se trata de acreditar que el usuario leyó el documento, sino de demostrar que el sistema nunca le permitió avanzar sin ejecutar una acción positiva y consciente. Para lograrlo, la organización debe adoptar decisiones de diseño concretas desde el inicio:

- El formulario nunca debe tener casillas pre-marcadas.
- El botón de envío o de avance debe estar inhabilitado hasta que el usuario marque activamente la casilla de consentimiento (acción positiva del titular de datos).
- La política de privacidad debe estar disponible mediante un enlace visible antes de que el usuario otorgue su consentimiento, no después. Y cada vez que la política se actualice, el sistema debe volver a solicitar el consentimiento de manera expresa.

Estas decisiones de cumplimiento deben estar documentadas, y aprobadas por la Dirección de la organización, y revisadas periódicamente.

6. ¿Cuál es el tiempo máximo para mantener un dato dentro de la organización?

La organización no puede mantener datos de manera indefinida. Ello conlleva a tener datos inexactos, incoherentes, o incluso desactualizados. Por otro lado, la ley no establece un plazo límite. El límite lo constituye la propia finalidad, por la cual se recolectaron los datos. Por lo mimos, es importante determinar, ante todo, el tipo de dato recolectado.

Alcance de la Categorización de Datos

Esta tabla que se muestra a continuación opera como una guía matriz de referencia general. En la práctica, la estructura de información de la organización es dinámica y cada categoría se desglosa de manera granular en función de su finalidad, contexto de uso y nivel de riesgo regulatorio.

Por ejemplo, los datos comerciales se segregan internamente (separando el registro transaccional y de facturación de un simple lead de prospección), al igual que los datos de salud (distinguiendo una ficha clínica de una licencia médica). En consecuencia, ante la coexistencia de normativas o la presencia de leyes especiales que exijan un mayor resguardo, prevalecerá y se aplicará automáticamente el plazo de conservación más estricto aplicable a la subcategoría.

Categoría de dato	Plazo orientativo	Fuente de referencia
Datos de contacto comercial (ej. leads, perfiles de preferencias e historial de interacciones de marketing)	Hasta 3 años sin actividad	Criterio general Ley 19.628 con Ley 21.719
Datos laborales (contratos, liquidaciones u otra documentación laboral)	5 años desde término de relación laboral	Jurisprudencia administrativa[1]
Datos tributarios y contables (ej. facturas, boletas e historial de compras y ventas asociado al cliente[2])	6 años desde la expiración del plazo legal en que debió efectuarse el pago del impuesto correspondiente.	Código Tributario art. 200
Datos de salud (ej. ficha clínicas)	Es la categoría de datos sensibles. Tratándose de fichas clínicas, 15 años desde el último registro de información en la ficha clínica.	Art 6° y 11° del Decreto 41 del Minsal / art 13° Ley 20.584
Datos de consentimiento (registro técnico de aceptación)	Mientras se mantenga el tratamiento. Tras el cese, se eliminan los datos comerciales y se conserva únicamente el registro de aceptación como evidencia por 4 años (por prescripción de responsabilidad civil[3]).	Ley 21.719 art. 12 °, 13° letra e) art 40° / art 2332 Código Civil

NOTAS ACLARATORIAS DE LA MATRIZ

[1] **Notas sobre datos Laborales:** Conforme a la doctrina de la Dirección del Trabajo (DT) en sus Dictámenes ORD. N°834 y ORD. N°1291.

[2] **Nota sobre el Historial de Compras:** Se explicita su categorización en la fila "Tributaria y contable" (6 años) y su exclusión de la fila "Comercial" (3 años), debido a que el historial de transacciones constituye el soporte e histórico contable obligatorio ante el Servicio de Impuestos Internos (SII), el cual no puede ser destruido de forma anticipada bajo argumento de inactividad comercial del titular.

[3] **Nota sobre evidencia de Consentimiento:** Tras el fin de la relación comercial, la organización cesa el tratamiento de los datos operativos del titular, pero la ley en el art.13° letra e) el resguardo de la evidencia necesaria para la defensa jurídica de la empresa ante eventuales acciones de responsabilidad civil extracontractual (Art. 2332 del Código Civil.

7. ¿Es lo mismo no tratar un dato que eliminarlo?

No es lo mismo. La ley es clara en manifestar que el tratamiento es cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.

Terminado el plazo de conservación de datos personales, la organización entra en una etapa de obligación legal inmediata y proactiva; se pierde la base de la licitud y se debe proceder a la eliminación completa de las bases de la organización.

Entonces **la eliminación es el proceso final de ciclo del tratamiento de dato**. Depende de una acción activa del responsable de dato, no una inactividad. En cambio, el no tratar el dato, significa que el dato no se ha recolectado, recibido ni guardado por la organización.

Cumplir con la eliminación del dato, permite a la organización mitigar el riesgo legal por la Agencia de Protección de Datos.

Situación de Pymes en la implementación de la Ley 21.719

La Ley 21.719 contempla un régimen transitorio especial para las empresas de menor tamaño, en reconocimiento de las dificultades operacionales y económicas que enfrentan estas organizaciones para adecuar sus procesos al nuevo estándar regulatorio.

El **artículo sexto transitorio** de la Ley 21.719 establece que, durante los primeros doce meses de vigencia de la ley, es decir, entre el 1 de diciembre de 2026 y el 1 de diciembre de 2027, la Agencia de Protección de Datos Personales podrá aplicar una **amonestación escrita** en reemplazo de la multa económica, cuando el infractor sea una empresa calificada como de menor tamaño bajo la Ley N° 20.416 (clasificación según sus ventas anuales en micro, pequeñas y medianas empresas [1]).

Consideraciones importantes:

- **No exime del cumplimiento:** las Pymes están obligadas a cumplir con el estándar regulatorio de la ley.
- **Facultad de la agencia:** la decisión final dependerá del criterio del organismo fiscalizador y del análisis de proporcionalidad del caso.
- **La amonestación queda registrada:** sujeta al deber de registrarse en el Registro Nacional de Sanciones y Cumplimiento.
- **Conclusión:** la situación transitoria es una oportunidad de adecuación, no una excusa para postergar. Las Pymes que utilicen este período para diagnosticar brechas, documentar procesos y construir su modelo de cumplimiento llegarán a diciembre de 2027 en condiciones de operar con seguridad jurídica.

[1] La Ley 20.416 clasifica a las empresas de menor tamaño, en micro, pequeñas y medianas empresas. según su nivel de ventas anuales por ventas y servicios y otras actividades. Microempresa (Ingresos anuales hasta 2.400 UF), Pequeña empresa (ingresos anuales entre 2.401 y 25.000 UF), Mediana empresa (ingresos anuales entre 25.001 y 100.000 UF).

Contenido desarrollado a partir del webinar sobre la Ley N° 21.719, organizado por FGE y expuesto por Sebastián Achondo, asociado de AZ, con adaptación y responsabilidad editorial de Etiqampus.