etiqampus
e·Learning en Integridad

Guía Comparada Protección de Datos Personales: caso caso Chile

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	23 min.

La gestión responsable de la información se ha convertido en uno de los principales desafíos para las organizaciones en un escenario marcado por la digitalización de los procesos, el uso intensivo de nuevas tecnologías y el creciente intercambio de datos. Esta realidad ha impulsado a distintos países de Latinoamérica y del mundo a revisar y modernizar sus marcos regulatorios, estableciendo mayores exigencias para resguardar los derechos de las personas y asegurar un tratamiento adecuado de sus datos personales.

Este nuevo escenario normativo no solo supone el cumplimiento de obligaciones legales. También exige que las empresas revisen la manera en que recopilan, utilizan, almacenan, comparten y protegen la información, incorporando la privacidad y la seguridad de los datos como componentes permanentes de su gestión. La evolución de las regulaciones y el fortalecimiento de las facultades de supervisión plantean, por tanto, desafíos que pueden impactar procesos internos, relaciones comerciales e incluso determinados modelos de negocio.

A partir de esta realidad, especialistas de reconocidas firmas jurídicas pertenecientes a 18 países miembros de Compliance Latam reunieron su experiencia y conocimiento en esta guía. La publicación ofrece una mirada comparada sobre el escenario regulatorio de la región, sus principales avances y las tendencias que están definiendo el futuro de la protección de datos personales. Asimismo, busca entregar criterios y herramientas que permitan a las organizaciones anticipar riesgos, fortalecer sus sistemas de cumplimiento e incorporar buenas prácticas en el tratamiento de la información.

A continuación te presentamos la sección dedicada a Chile escrita por los siguientes profesionales del estudio AZ:

- Rodrigo Albagli, Socio.
- Yoab Bitran, Director Grupo Compliance.
- Antonia Nudman, Asociada Senior, Grupo IP, Tech and Data.

FUENTE: el texto de esta portadilla se elaboró a partir de la introducción de la "Guía Comparada Protección de Datos Personales" publicada por la plataforma "Compliance Latam".

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



albagli zaliasnik

Autor:

Rodrigo Albagli, Socio.

Yoab Bitran, Director Grupo Compliance.

Antonia Nudman, Asociada Senior, Grupo IP, Tech and Data.

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?

La protección de datos personales está garantizada como derecho fundamental por la Constitución Política de la República, en el artículo 19 N°4. La protección y el tratamiento de la información personal están regulado en la Ley N°19.628, de 1999. Sin embargo, recientemente se aprobó la Ley N°21.719, que modifica la normativa actual, elevando los estándares existentes junto con crear una Agencia de Protección de Datos Personales. Esta nueva regulación entrará en vigor el 1 de diciembre de 2026.

2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?

Sí, la nueva Ley N°21.719 incorporó un nuevo tipo de modelo de prevención de infracciones de protección de datos personales (compliance), el cual comenzará a regir a partir del 1° de diciembre de 2026.

Los nuevos programas de compliance no son obligatorios, sin embargo, de implementarse y ser certificados por la futura Agencia de Protección de Datos Personales, servirán como atenuante de responsabilidad en caso de que la organización sea sancionada por dicho organismo.

3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?

El programa de cumplimiento deberá contener, al menos, los siguientes elementos:

a) La designación de un delegado de protección de datos personales.

b) La definición de medios y facultades del delegado de protección de datos.

c) La identificación del tipo de información que la entidad trata, el ámbito territorial en que opera, la categoría, clase o tipos de datos o bases de datos que administra, y la caracterización de los titulares de datos.

d) La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en la ley.

e) El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en la ley, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de infracciones.

f) Los mecanismos de reporte interno sobre el cumplimiento de lo dispuesto en la presente ley y los mecanismos de reporte a la autoridad de protección de datos para el caso de vulneraciones de medidas de seguridad.

g) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o castigo de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?

Contar con un programa de cumplimiento en protección de datos personales trae múltiples beneficios, entre ellos:

• Evita sanciones y multas al asegurar el cumplimiento normativo.

• Reduce riesgos reputacionales y genera confianza con clientes,colaboradores y socios.

• Protege la información sensible y minimiza el impacto de brechas de seguridad.

• Facilita la gestión de derechos de los titulares y mejora la transparencia.

• Optimiza procesos internos, promoviendo una cultura organizacional de privacidad y seguridad.

• Asegura la continuidad operativa, evitando interrupciones por incumplimientos legales.

Asimismo, en términos procesales, el modelo podría servir como medio de prueba para demostrar ante entidades públicas que se están tomando las medidas necesarias para cumplir la ley. Además, si el programa está certificado por la Agencia, podría servir como atenuante de responsabilidad según la nueva Ley N°21.719.

5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?

Sí, la nueva ley establece que los programas de prevención de infracciones serán certificados por la Agencia de Protección de Datos Personales, y serán incorporados en el Registro Nacional de Sanciones y Cumplimiento.

Además, se dictará un reglamento que establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos.

6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?

En general no es obligatorio, pero si la compañía cuenta con un modelo de prevención de infracciones que someterá al proceso de certificación de la Agencia de Protección de Datos Personales, su incorporación es obligatoria.

7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

Sí, bajo la legislación actual las multas son de hasta USD$3.500 U, Sin embargo, la Ley N°21.719, que entra en vigencia el 1° de diciembre de 2026, las incrementa ostensiblemente de la siguiente manera:

Infracciones leves: Amonestación por escrito y multa de hasta USD$350.000.

Infracciones graves: Multas de hasta USD $700.000.

Infracciones gravísimas: Multa de hasta USD $1.400.000.

En casos de reincidencia, las multas podrían triplicar el monto asignado como multa. Asimismo, cuando el infractor corresponda a una empresa de mediano o gran tamaño, que reincida en una infracción de carácter grave o gravísima, la multa podrá alcanzar a la más gravosa entre las señaladas anteriormente o hasta el monto correspondiente al 2% o 4% de los ingresos anuales por ventas,servicios y otras actividades del giro en el último año calendario, según se trate de infracciones graves o gravísimas, respectivamente.

Además, en caso de que se impongan multas por infracciones gravísimas reiteradas, en un período de veinticuatro meses, la Agencia podrá disponer la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de treinta días.

8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

La normativa clasifica las conductas prohibidas en infracciones leves, graves y gravísimas.

Se consideran infracciones leves las siguientes conductas:

1. Falta de transparencia en el deber de información al titular de datos.

2. No contar con un medio de contacto actualizado (domicilio, correo electrónico o equivalente) para atender solicitudes de los titulares.

3. No responder, responder fuera de plazo o de forma incompleta las solicitudes de los titulares de datos.

4. No enviar a la Agencia las comunicaciones obligatorias establecidas en la ley.

5. Incumplir instrucciones generales de la Agencia, salvo que constituyan infracción grave o gravísima.

6. Otras infracciones menores a los derechos y obligaciones de la ley que no sean catalogadas como graves o gravísimas.

Se consideran infracciones graves las siguientes conductas:

1. Tratamiento ilícito de datos sin consentimiento o sin base legal válida.

2. Cesión o comunicación no autorizada de datos personales.

3. Uso de datos innecesarios para la finalidad del tratamiento.

4. Manejo de datos inexactos, incompletos o desactualizados.

5. Obstrucción o impedimento del ejercicio de derechos del titular (acceso, rectificación, supresión, oposición o portabilidad).

6. Negativa o demora injustificada en la respuesta a solicitudes de bloqueo temporal de datos.

7. Tratamiento indebido de datos de menores de edad.

8. Incumplimiento de requisitos específicos en organizaciones sin fines de lucro con fines políticos, filosóficos, religiosos, culturales, sindicales o gremiales.

9. Vulneración del deber de secreto o confidencialidad.

10. Incumplimiento de medidas de seguridad en el tratamiento de datos.

11. Falta de comunicación o registro de brechas de seguridad.

12. Deficiencias en la seguridad de datos con fines históricos, estadísticos o científicos.

13. Transferencia internacional de datos sin cumplir las normas legales.

14. Desacato a resoluciones o requerimientos de la Agencia.

Las siguientes conductas se consideran infracciones gravísimas según la ley:

1. Tratamiento fraudulento de datos personales.

2. Uso malicioso de datos para una finalidad distinta a la consentida o permitida por la ley.

3. Comunicación o cesión intencionada de datos inexactos o desactualizados.

4. Vulneración del secreto o confidencialidad de datos sensibles o sobre infracciones legales.

5. Tratamiento indebido de datos sensibles o de menores de edad.

6. Omisión deliberada de notificación de brechas de seguridad que afecten la integridad de los datos.

7. Uso masivo no autorizado de datos sobre infracciones penales, civiles o administrativas.

8. Transferencia internacional de datos en contravención a la ley.

9. Desacato a resoluciones de la Agencia en materia de derechos de los titulares.

10. Provisión intencional de información falsa en procesos de certificación del modelo de prevención de infracciones.

11. Incumplimiento de obligaciones específicas establecidas respecto de las evaluaciones de impacto.

9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?

Sí, actualmente existen varios organismos que ejercen estas laborares en forma parcelada. Por ejemplo, para el sector público existe el Consejo para la Transparencia y para el privado el Servicio Nacional de Protección del Consumidor, el que tiene estas atribuciones pero sólo respecto de las relaciones de consumo.

A partir del 1° de diciembre de 2026, será la Agencia la que tendrá dichas atribuciones en general.

10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?

En Chile las organizaciones normalmente comienzan aplicando la nueva normativa de protección de datos personales identificando las brechas de cumplimiento y designando, de ser necesario, un Delegado de Protección de Datos (DPD), especialmente si manejan grandes volúmenes de datos, tratan datos sensibles y/o son multinacionales.

Además, debeben establecer un registro de actividades de tratamiento, evaluar los riesgos asociados a la gestión de datos y definir protocolos claros para la atención de los derechos de los titulares. Asimismo, debieran diseñar un programa de cumplimiento que contemple políticas internas, capacitaciones periódicas, medidas de seguridad adecuadas y procedimientos de auditoría.

También deben implementar controles robustos de seguridad de la información y definir estrategias para la gestión de incidentes y la notificación de brechas, garantizando así una adecuada gobernanza de los datos personales.

Finalmente, deben capacitar a sus colaboradores y, cuando corresponda, a sus proveedores, con el objetivo de sensibilizarlos sobre la importancia de proteger y gestionar responsablemente el tratamiento de datos personales de terceros, fomentando una cultura organizacional basada en la privacidad y el cumplimiento normativo.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?

En general, la ley se aplica a responsables y mandatarios establecidos o constituidos en Chile o a operaciones de tratamiento de datos personales que se realicen en el país. Sin embargo, podría tener aplicación extraterritorial en los siguientes casos:

• Cuando el mandatario, con independencia de su lugar de establecimiento o constitución, realice las operaciones de tratamiento de datos personales a nombre de un responsable establecido o constituido en el territorio nacional.

• Cuando el responsable o mandatario no se encuentren establecidos en el territorio nacional pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile, independientemente de si a éstos se les requiere un pago, o a monitorear el comportamiento de titulares que se encuentran en el territorio nacional, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento.

• La ley también se aplicará al tratamiento de datos personales que sea realizado por un responsable al que, sin estar establecido en el territorio nacional, le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.