plutto

Ebook

Ley de Protección de Datos Personales

Qué cambia, qué te exige la ley y cómo prepararse.

Lo que necesitas saber para preparar a tu empresa ante la nueva ley.

La Ley 21.719 **cambia el estándar con que las empresas en Chile tratan datos personales**, y el 1 de diciembre de 2026 se vuelve plenamente exigible. Esta guía te explica, sin tecnicismos, qué cambia, qué te exige la ley y cómo llegar preparado.

La organizamos en tres miradas que se complementan: la legal (qué exige realmente la ley), la de los datos de tus colaboradores y la de los datos de tus proveedores.

En cada una vas a encontrar el contexto, qué significa en la práctica para tu empresa y recomendaciones concretas para empezar a ordenarte.

Sobre el contenido

Parte de este contenido nació de nuestro webinar "Nueva Ley de Protección de Datos Personales", que hicimos junto a Buk y Carey. Agradecemos a José Ignacio Mercado, Jaime Henríquez, Lorena Cantergiani y Felipe Domínguez por sus aportes.

Por qué importa ahora

La Ley 21.719 es la nueva ley de protección de datos personales en Chile. Modifica substancialmente la antigua Ley 19.628, y **sube bastante el estándar con que las empresas deben tratar los datos**: de forma segura, trazable y, sobre la base de una base de licitud válida, según corresponda.

Se publicó en diciembre de 2024, pero recién se vuelve plenamente exigible y fiscalizable el 1 de diciembre de 2026. Ese plazo no es casual: la ley es técnica y de alto impacto, y se dio tiempo para que las empresas adapten sus operaciones. **El momento de prepararse es ahora.**

Hay un punto que no todos tienen presente, buena parte de los datos personales de una empresa no los trata la empresa directamente, sino sus proveedores. Ese riesgo se traslada a la cadena. Por eso **hoy los proveedores pasan a ser una pieza clave** en cómo se gestiona el cumplimiento, y es el hilo que conecta las tres miradas de este ebook.

La **gestión de riesgos es el elemento base** para poder conocer, gestionar e implementar adecuadamente este tipo de normativa.

José Ignacio Mercado, Director Grupo de Protección de Datos y Tecnología, Carey

Para Webinar Ley de Datos Personales

Perspectiva legal: Qué exige la ley

La Ley 21.719 regula cómo las empresas tratan los datos personales en Chile. Su lógica de fondo es de protección: limita el tratamiento para que siempre se haga de forma segura, trazable, siempre con una base de licitud y, como regla general, con consentimiento del titular. Protege un derecho de las personas.

¿A quién aplica?

A toda organización que trate datos personales, sin importar su tamaño; comprendida dentro del ámbito de aplicación considerando ciertas reglas especiales. Así podría ser desde una empresa con un simple formulario de contacto hasta una gran compañía proveedora de servicios tecnológicos.

¿Qué se considera dato personal?

Cualquier información que identifique o pueda identificar a una persona natural: RUT, correo, teléfono, incluso una foto y datos que puedan ser inferidos. Los datos personales solo se refieren a personas naturales, de carne y hueso.

¿Qué es un dato sensible?

La ley trata con especial cuidado los llamados datos sensibles: **los que tocan la intimidad de la persona**. Para tratarlos, por regla general necesitas su consentimiento y un estándar de protección más alto.

Se consideran sensibles, entre otros: salud, datos biométricos (tales como huella, rostro), perfil biológico humano, origen racial o étnico, afiliación política, sindical o gremial, creencias religiosas o filosóficas, vida y orientación sexual, e identidad de género. En Chile se agrega además la situación socioeconómica, algo propio de nuestra ley.

Recomendación

Empieza por identificar qué datos personales tratas hoy, con qué base los tratas y quién los toca dentro y fuera de tu empresa. Sin ese mapa, el resto de la ley no se puede cumplir.

La gran novedad: Nuevo órgano fiscalizador

La ley crea la **Agencia de Protección de Datos Personales**, un órgano técnico encargado de fiscalizar y ejercer las demás facultades que la ley encomienda. Hasta ahora no existía un ente así, todo dependía de denuncias particulares y procesos largos en tribunales.

Que sea técnico cambia las reglas, porque fiscaliza con criterio experto y sobre evidencia operativa, no sobre buenas intenciones.

Las sanciones

Las sanciones dependen de la gravedad de la infracción. Para las infracciones más graves pueden llegar hasta 20.000 UTM. Y en casos de reincidencia, para empresas que no son de menor tamaño, la multa puede alcanzar hasta el 4% de los ingresos anuales de la empresa. Esa severidad es justamente la razón del plazo de adaptación.

Los derechos de las personas

La ley le da a cada persona derechos sobre sus datos. Cuando alguien ejerce uno de ellos —por ejemplo, pide acceder a sus datos o eliminarlos—, tu empresa tiene que responder dentro de un plazo definido.

Principales:

- **Acceso**
  Saber qué datos tienes de la persona, para qué los usas y a quién se los comunicas.
- **Rectificación**
  Derecho a corregir datos incorrectos o incompletos.
- **Supresión**
  Eliminar los datos cuando ya no corresponde tratarlos.
- **Oposición**
  Negarse a que se traten sus datos en ciertos casos.
- **Portabilidad**
  Recibir sus datos en un formato que otro sistema pueda usar.
- **Bloqueo**
  Suspender el tratamiento mientras se resuelve una solicitud.

Los dos roles que define la ley

Entender estos roles es clave para saber dónde está tu responsabilidad:

Responsable del tratamiento

Quien decide para qué se usan los datos y da las instrucciones (fines y medios). Son, generalmente, las empresas que contratan un servicio. Por ejemplo, una empresa que publica un aviso de empleo y decide qué datos pide a los postulantes, para qué los usa y por cuánto tiempo los guarda.

Encargado del tratamiento

Quien procesa esos datos siguiendo esas instrucciones, como un mandatario. Ese rol lo cumplen plataformas como, por ejemplo Plutto y Buk.

La normativa no acepta la excusa de que un tercero realizó algo y yo no tuve nada que ver, porque finalmente el responsable soy yo dentro de toda esta cadena productiva.

Jaime Henríquez, Asociado en Propiedad Intelectual y Tecnología de la Información, Carey

Para Webinar Ley de Datos Personales

Bases de Licitud

Las bases de licitud son las razones que la ley reconoce como válidas para poder tratar datos personales. Esta ley cambia las reglas sobre cuándo puedes tratar datos:

- Que un dato sea público ya no basta por sí solo, ahora hay que documentar por qué tratas cada dato.
- El consentimiento sigue valiendo, pero reforzado: libre, expreso y escrito.
- Aparece el cumplimiento de un deber legal, cuando la propia ley autoriza un determinado tratamiento de datos.
- El interés legítimo: tratar datos como por ejemplo, la prevención de fraude, siempre informando al público y cumpliendo con los demás requisitos legales.

Recomendación

Antes de tratar un dato, pregúntate con qué base lo haces (consentimiento, contrato, deber legal, interés legítimo) y déjalo documentado. La ley te va a pedir justificar el porqué de cada dato.

Qué pasa con los proveedores

Ya vimos qué exige la ley en general, pero gran parte de los datos personales de una empresa los tratan sus proveedores, y quien contrata sigue siendo responsable de cómo un tercero trata los datos. Por eso, elegir y controlar bien a tus proveedores pasa a ser parte central del cumplimiento.

No saco nada con tener un contrato con cláusulas robustas, si no refleja la realidad de mi modelo de negocio y mis riesgos concretos. **El contrato tiene que ser un reflejo de una realidad concreta.**

José Ignacio Mercado, Director Grupo de Protección de Datos y Tecnología, Carey

Para Webinar Ley de Datos Personales

La responsabilidad no se traspasa

Cuando contratas a un proveedor para que trate datos por ti, estás externalizando una actividad que sigue siendo tuya. Sacas de tu control inmediato algo de lo que, ante la ley, sigues respondiendo. Por eso, saber en quién delegas esa función, y qué hace exactamente con tus datos, es parte central de gestionar tu riesgo.

El contrato, una pieza clave

Si la ley te hace responsable de lo que hace tu proveedor, el contrato es donde eso se ordena: define qué puede hacer cada parte con los datos y es la evidencia que muestras si la Agencia pregunta. Revisa el que ya tienes y ajústalo.

Qué debe incluir el contrato

En el contrato se deberá establecer:

- Objeto del encargo
- Duración del mismo
- Finalidad del tratamiento
- Tipo de datos personales tratados
- Categorías de titulares a quienes conciernen los datos
- Derechos y obligaciones de las partes

Perspectiva colaboradores:

Los datos que viven dentro de la empresa

Dentro de la empresa hay datos personales que solemos dar por cubiertos con el contrato de trabajo, y un grupo que casi siempre queda fuera del radar: los postulantes. Así impacta la ley en la gestión de personas dentro del proceso de selección.

Un proceso de selección concentra más riesgo del que parece, por tres razones principales:

1. **El efecto multiplicador**
   Al abrir una vacante, recibes decenas o cientos de personas entregándote sus datos. Ese volumen, por sí solo, ya es algo que hay que cuidar.

2. **Los datos se dispersan**
   Un mismo currículum pasa por RR.HH., una psicóloga externa y jefatura, y termina repartido en computadores, correos y planillas. Sin estructura, es casi imposible saber dónde está cada dato.

3. **Es un proceso público**
   A diferencia de tus procesos internos, un reclutamiento está a la vista de todos, incluida la futura Agencia. Basta simular una postulación para ver cómo trata los datos toda tu organización.

Todo esto se vuelve tangible cuando el proceso termina y un postulante pide borrar sus datos. Si están dispersos en diferentes lugares, no sabes ni dónde buscarlos. Y las solicitudes de supresión ya están llegando.

Cuando el proceso termina y el postulante exige que se borren sus datos, ¿a dónde los voy a buscar? Ese es un gran problema.

Lorena Cantergiani, Sr. Information Security Engineer, Buk

Para Webinar Ley de Datos Personales

La solución práctica:

Colaboradores - Información centralizada

El problema de fondo no es tener muchos datos, es tenerlos desordenados. Por eso la solución parte por centralizar toda la información de un proceso en un solo sistema, en vez de dejarla repartida en correos y planillas.

En la práctica: 4 puntos para mitigar el riesgo

Minimiza la exposición

Centraliza la información de postulación (o de cualquier proceso que maneje datos) en un solo sistema. Menos dispersión, más control.

Avisos de privacidad claros

Que el postulante sepa cómo se tratan sus datos, con una base de licitud definida. En selección no siempre es el consentimiento, muchas veces es un acuerdo precontractual.

Licitud

Solicita solo la información estrictamente necesaria para el proceso. Deja clara tu base de licitud: en selección, lo más apropiado suele ser el contrato y las medidas precontractuales.

Supresión automática

Configura la eliminación de datos cuando se cumplan los plazos que definiste.

El cumplimiento normativo no se logra solo instalando un software, se logra cambiando hábitos. La capacitación constante del equipo de Personas es lo único que transforma una obligación legal en una verdadera cultura de privacidad.

Mientras más estructurada esté la información, más fácil va a ser gestionar cualquier solicitud de derechos o establecer los plazos de supresión de forma automática.

Lorena Cantergiani, Sr. Information Security Engineer, Buk

Para Webinar Ley de Datos Personales

Perspectiva proveedores:

El riesgo que vive fuera de tu empresa

En lo legal quedó claro el qué: la responsabilidad no se traspasa y el contrato importa. Ahora vamos a lo práctico desde adentro de un software, porque tratar estos datos tiene particularidades que conviene entender antes de exigirle algo a un proveedor.

El problema: No todos los datos son iguales

1 **El "dato de la cadena"**

Muchas plataformas tratan datos de una cadena de personas —representantes legales, socios, beneficiarios finales, contactos— con las que no tienes contacto directo y que nunca te entregaron su dato. Ese tipo de dato exige más cuidado.

2 **Tus proveedores ya tratan datos**

Aunque no lo tengas presente, seguramente ya trabajas con software que trata datos personales por ti. Tratarlos no es el problema; el problema es no tener ordenado quién hace qué con ellos.

3 **La cadena sigue: los sub-encargados**

Tu proveedor a su vez se apoya en otros (hosting, correo, soporte, modelos de inteligencia artificial). Ese es el punto que casi nadie mira, si un dato termina en un tercero que ni conoces o incluso en otro país, sigue siendo tu responsabilidad.

Tratar un dato no es malo. Lo importante es tener súper claro y ordenado, por qué y cómo estás haciendo ese tratamiento.

Muchas veces tratamos datos donde ese titular no necesariamente me entregó el dato de manera directa. Y no porque un dato sea de público acceso significa que yo puedo tratarlo.

Felipe Domínguez, COO y Co-Founder de Plutto

Para Webinar Ley de Datos Personales

La solución:

El control tiene que quedar en el responsable, el cliente

No todos los software están preparados para esto. Un buen proveedor te da el control y la flexibilidad de adaptarse a lo que tú definas: hace solo lo que le pediste, ni más ni menos. Si no quieres que un dato se trate, no se toca; y si se trata, se procesa exactamente como tú lo definiste.

Esto es lo que le tienes que poder exigir a tu software:

1 El control lo defines tú

Tú decides qué datos se tratan, qué se busca, cuánto tiempo se guarda y cuándo se borra. Esto debería ser configurable según tu política, no un estándar igual para todos.

> Si un cliente no quiere ir a buscar un dato, el servicio de sowtware tiene que tener la flexibilidad de no ir a buscarlo y nunca tocarlo. Y si lo busca, que se procese exactamente como el cliente lo definió.
>
> **Felipe Domínguez,** COO y Co-Founder de Plutto
> *Para Webinar Ley de Datos Personales*

2 Que puedas responder lo que la ley te va a pedir

La ley les da a las personas derechos sobre sus datos, y tú tienes que poder responder rápido.
Tu software es lo que hace la diferencia entre lograrlo o no:

- **Responder en 30 días (corridos):** Cuando alguien pida ver, corregir o eliminar sus datos, ese es el plazo. Si están repartidos en planillas y correos, el tiempo se te va solo en encontrarlos.
- **Entregar en formato portable:** Si la persona quiere llevarse sus datos, no basta con mandar un PDF, tiene que ser un formato estructurado y de uso común.
- **Avisar una brecha sin demora:** Ante una filtración, tienes que poder explicar qué pasó, qué datos se vieron afectados y a quién.

Nada de esto funciona si tu información vive dispersa. Por eso un buen sistema es lo que te permite cumplir.

Cómo partir:

Las 5 preguntas a tus proveedores críticos

Selecciona los tres proveedores que más datos de personas tratan y ábreles la conversación con estas cinco preguntas. La idea es ordenar qué hace cada uno con tus datos.

1. **Rol y contrato**
   ¿Queda definido el rol de Encargado por escrito, con qué datos trata, para qué, por cuánto tiempo?

2. **Sub-encargados, incluida la IA**
   ¿Tu cadena está declarada, al día, y me avisas cuando cambia?

3. **Trazabilidad y procedencia**
   ¿Me muestra de dónde viene cada dato y quién accedió?

4. **Incidentes**
   Ante una brecha, ¿me explica en simple qué pasó, qué datos se vulneraron y en cuánto me avisa?

5. **Terminación**
   Al terminar la relación, ¿dónde quedan mis datos al irme, cómo los recupero y en qué plazo se eliminan?

¿No sabes cómo abrir la conversación? Copia este correo y envíaselo a tus proveedores críticos.

Para: los 3 proveedores que más datos de personas tocan
Asuntos: Tratamiento de datos personales - proveedores críticos

Hola,
Estamos revisando el tratamiento de datos personales de nuestros proveedores críticos, de cara al 1 de diciembre.
¿Nos pueden responder estas cinco preguntas? [+las 5 preguntas]

Gracias

plutto

Conoce más sobre Plutto

Plataforma para gestionar y evaluar el riesgo de tus proveedores.
Agenda una demo y descúbrela en vivo.

Agendar demo

www.getplutto.com | ventas@getplutto.com