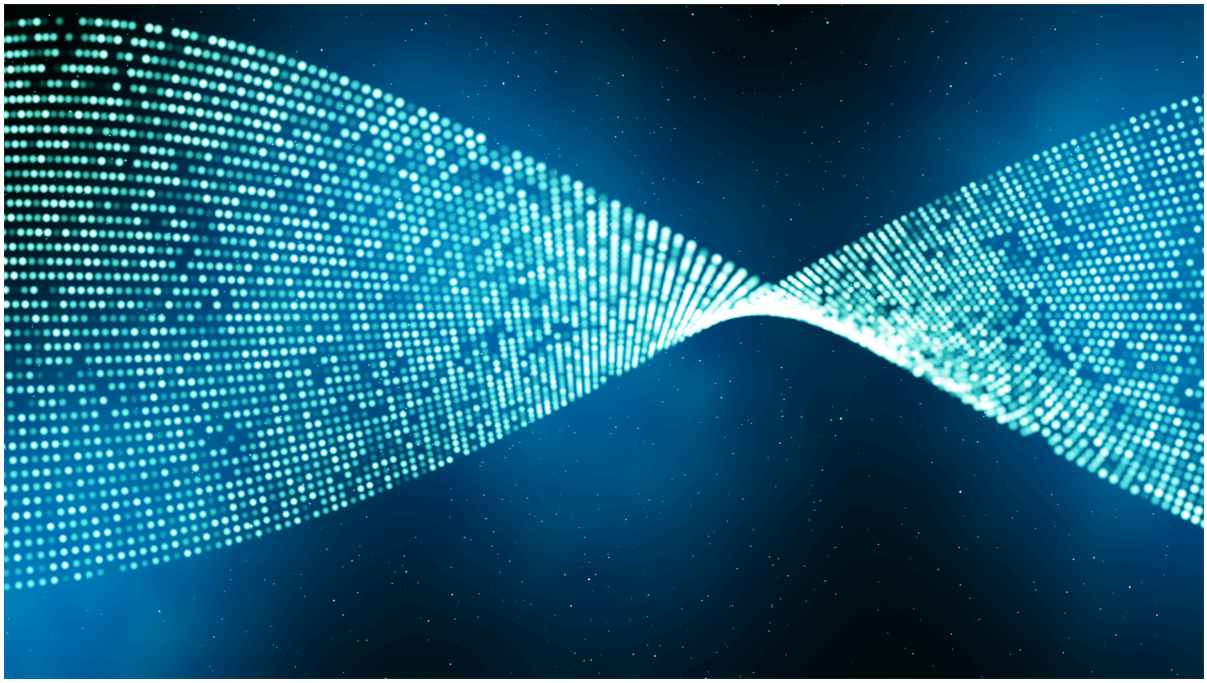
PROVECTIS

Guía para la Protección de Datos Personales

Lo que cada empresa debe resolver antes de diciembre de 2026



Introducción

El 1 de diciembre de este año termina el período de adecuación de la Ley 21.719, la reforma más profunda a la protección de datos personales en la historia de Chile. Publicada el 13 de diciembre de 2024, la ley reemplaza un marco que llevaba más de dos décadas sin capacidad real de fiscalización y alinea a Chile con los estándares del GDPR europeo.

El cambio immplica que desde esa fecha:

- Nace la **Agencia de Protección de Datos Personales (APDP)**, con facultades para investigar de oficio, fiscalizar, multar, suspender tratamientos de datos y publicar las sanciones en un registro nacional.

- Las multas pasan de un máximo histórico de 50 UTM a un rango de **hasta 20.000 UTM** (sobre $1.400 millones de pesos), con agravantes por reincidencia que pueden triplicar el monto o alcanzar un porcentaje de los ingresos anuales.

- Las obligaciones dejan de ser declarativas: la empresa debe poder **demostrar** su cumplimiento con documentación, procesos y medidas técnicas verificables.

Esta guía resume en lenguaje de gestión qué exige la ley, cuánto arriesga tu empresa y los 10 requisitos concretos que deben estar resueltos antes de diciembre. Al final encontrarás un autodiagnóstico de 5 minutos y un plan de trabajo sugerido para los meses que quedan.

Importante: esta guía es material informativo y no constituye asesoría legal. Para decisiones de cumplimiento específicas, consulta con tu asesor jurídico.

La ley en tres pilares

1. Reglas nuevas para tratar datos. La ley define qué es un dato personal y establece seis bases legales que legitiman su tratamiento: consentimiento, contrato, obligación legal, interés vital, interés público e interés legítimo. Tratar datos sin una base legal es infracción grave. Los datos sensibles (salud, biometría, origen étnico, afiliación sindical, datos de menores, entre otros) tienen condiciones reforzadas.

2. Derechos exigibles para las personas. Los titulares de datos —tus clientes, trabajadores y proveedores— pueden ejercer los derechos conocidos como **ARCO+**: Acceso, Rectificación, Cancelación (supresión), Oposición, más Portabilidad y Bloqueo. Tu empresa debe tener un canal habilitado para recibir estas solicitudes y responderlas dentro del plazo legal (30 días corridos).

3. Una autoridad con dientes. La APDP puede fiscalizar de oficio o por denuncia, aplicar multas, ordenar la suspensión del tratamiento de datos por hasta 30 días, prohibirlo de forma temporal o definitiva, y publicar la sanción en el **Registro Nacional de Sanciones**, visible por 5 años. Para una empresa que vende a otras empresas, aparecer en ese registro tiene un costo comercial que puede superar a la multa.

¿A quién aplica y cuánto arriesga tu empresa?

Aplica a toda persona natural o jurídica, pública o privada, que trate datos personales en Chile. No hay excepción por tamaño ni por rubro: si tu empresa tiene una base de clientes, una nómina de trabajadores o un CRM, está dentro del alcance.

Régimen de multas

Tipo de infracción	Multa máxima	Ejemplos de conducta
Leve	Amonestación escrita o hasta **5.000 UTM**	Incumplimientos formales y deberes de información
Grave	Hasta **10.000 UTM**	Tratar datos sin base legal, no responder solicitudes ARCO+, vulnerar obligaciones de seguridad
Gravísima	Hasta **20.000 UTM**	Tratamiento fraudulento, uso indebido de datos sensibles, obstrucción a la fiscalización

Agravante de reincidencia: si la empresa vuelve a infringir dentro de 5 años, la multa puede triplicarse (hasta 60.000 UTM) o, para empresas que no califican como de menor tamaño según la Ley 20.416, calcularse como el **2% de los ingresos anuales** (reincidencia grave) o el **4%** (gravísima), lo que resulte mayor.

Atenuante clave: contar con un **modelo de prevención de infracciones** certificado opera como atenuante relevante. El cumplimiento proactivo, además de reducir el riesgo, se está convirtiendo en requisito en licitaciones y contratos B2B.

Referencia: al valor UTM vigente, 20.000 UTM superan los $1.400 millones de pesos chilenos.

Los 10 requisitos que exigirá la ley 21.719

Gobierno del dato

1. Inventario de datos: el Registro de Actividades de Tratamiento (RAT)

Es el punto de partida de todo lo demás: un documento estructurado que identifica, por cada tratamiento, qué categorías de datos maneja la empresa, de qué titulares, con qué finalidad, bajo qué base legal, quién accede, dónde se almacenan y por cuánto tiempo. Sin inventario no hay forma de demostrar cumplimiento. Pregunta de control: ¿Podrías listar hoy todos los sistemas de tu empresa que contienen datos personales, incluyendo planillas y herramientas SaaS?

2. Base legal para cada tratamiento

Cada uso de datos personales debe apoyarse en una de las seis bases legales. El error típico del midmarket: bases de prospectos acumuladas por años "por si acaso", sin consentimiento ni interés legítimo documentado. Tratar datos sin base legal es infracción grave.

3. Canal y proceso para derechos ARCO+

Un correo o formulario visible donde las personas puedan ejercer sus derechos, y un proceso interno con responsable, registro y plazo de respuesta de 30 días. No basta la casilla: si la solicitud llega y nadie la gestiona, la infracción es la misma.

4. Deberes de información y política de privacidad

La política de privacidad del sitio web y los avisos al momento de recolectar datos deben reflejar la realidad: qué se recopila, para qué, con quién se comparte, cuánto tiempo se conserva y cómo ejercer derechos. Una política genérica copiada de otro sitio es un incumplimiento formal a la vista de cualquier fiscalización.

Los 10 requisitos que exigirá la ley 21.719

Seguridad y continuidad

5. Medidas de seguridad adecuadas al riesgo

La ley obliga a adoptar medidas técnicas y organizativas proporcionales a la naturaleza de los datos y al riesgo del tratamiento: control de accesos, cifrado, segmentación, monitoreo. Vulnerar las obligaciones de seguridad es infracción grave, y la vara no es "hicimos algo", sino "hicimos lo adecuado al riesgo y podemos demostrarlo".

6. Plan de respuesta y notificación de brechas

Si ocurre una vulneración de seguridad que afecte datos personales, la empresa debe notificar a la autoridad sin dilaciones indebidas y, cuando el riesgo lo amerite, también a los titulares afectados. Esto exige dos capacidades que hoy la mayoría del midmarket no tiene: **detectar** el incidente a tiempo y **saber exactamente qué datos fueron comprometidos**. Un plan de respuesta escrito, con roles y tiempos, deja de ser buena práctica y pasa a ser exigencia operativa.

7. Respaldo, retención y eliminación segura

El ciclo de vida del dato completo queda bajo la ley: conservar información solo mientras exista finalidad y base legal, poder recuperarla ante un incidente (integridad y disponibilidad son parte de la seguridad exigida), y eliminarla de forma efectiva cuando corresponda — incluyendo las copias de respaldo, un punto que casi ningún plan de retención contempla. Preguntas de control: ¿Tu último respaldo válido tiene horas o semanas? ¿Puedes acreditar que un dato suprimido desapareció también de los respaldos históricos según tu política de retención?

Los 10 requisitos que exigirá la ley 21.719

Terceros y gobernanza

8. Contratos con encargados de tratamiento (proveedores)

Cuando un tercero accede a datos personales por cuenta de tu empresa (el proveedor del ERP, la plataforma de correo masivo, el datacenter, el partner de soporte) debe existir un contrato que regule ese acceso (DPA, por su sigla en inglés). La brecha más frecuente detectada en diagnósticos de cumplimiento: años usando plataformas SaaS sin haber firmado el DPA del proveedor ni revisado dónde se alojan los datos.

9. Transferencias internacionales con garantías

Si los datos se almacenan o procesan fuera de Chile (nube pública, SaaS con servidores en el extranjero), la transferencia requiere garantías adecuadas. Usar servicios internacionales sin ese resguardo constituye infracción desde el día uno de vigencia. Saber **en qué región geográfica** viven tus datos deja de ser un detalle técnico y pasa a ser una obligación legal.

10. Gobernanza: un responsable con nombre y apellido

La ley no obliga a todas las empresas a designar un Delegado de Protección de Datos, pero sí lo exige en escenarios de mayor riesgo (datos sensibles a gran escala, tratamientos de alto riesgo, o si se adopta un modelo de prevención de infracciones). En la práctica, toda empresa necesita al menos un responsable interno del cumplimiento con mandato real, y aquí aparece la brecha del "Oficial de Datos" que pocas compañías han resuelto: alguien que entienda a la vez el negocio, los procesos y la infraestructura donde los datos viven.

Autodiagnóstico: ¿Dónde está tu empresa hoy?

Responde sí o no. Cada "no" es una brecha con plazo al 1 de diciembre.

1. ¿Existe un inventario actualizado de todos los sistemas y repositorios con datos personales (incluidas planillas y SaaS)?
2. ¿Cada tratamiento tiene identificada su base legal?
3. ¿Hay un canal publicado y un proceso interno para responder solicitudes ARCO+ en 30 días?
4. ¿La política de privacidad refleja la operación real de la empresa?
5. ¿Las medidas de seguridad están documentadas y son proporcionales al riesgo?
6. ¿Existe un plan escrito de respuesta a incidentes con responsables y tiempos de notificación?
7. ¿Los respaldos se prueban periódicamente y existe una política de retención y eliminación que los incluya?
8. ¿Están firmados los contratos de encargo (DPA) con todos los proveedores que acceden a datos?
9. ¿Sabes en qué país o región se alojan los datos de cada plataforma que usas?
10. ¿Hay una persona designada como responsable del cumplimiento, con respaldo de la gerencia?

Lectura de resultados:

8-10 sí: Estás en el grupo avanzado, enfoca los meses que quedan en documentar y certificar.

5-7: Hay base, pero las brechas abiertas incluyen probablemente infracciones graves; prioriza seguridad, brechas y DPAs.

0-4: Tu empresa está expuesta. Se requiere un plan de choque inmediato y este es el momento de pedir ayuda externa.

Los 5 errores en Protección de Datos

1. Confundir "tener política de privacidad" con cumplir. La política casi siempre existe, el proceso detrás, casi nunca.

2. Ignorar a los proveedores. El dato viaja a CRMs, plataformas de correo y nubes de terceros sin contrato de encargo. La responsabilidad, en cambio, no viaja: sigue siendo tuya.

3. Tratar el respaldo como un tema aparte del cumplimiento. Disponibilidad, integridad y capacidad de recuperación son parte de las medidas de seguridad exigibles. Un respaldo que no se prueba es una brecha legal, no solo técnica.

4. No poder responder "¿Qué datos fueron afectados?" Ante una brecha, el plazo de notificación corre desde ya. Sin visibilidad de la infraestructura ni clasificación de la información, la respuesta honesta es "no sabemos", la peor respuesta posible frente a la autoridad.

5. Dejarlo para el último trimestre. Levantar el inventario, cerrar contratos con proveedores y desplegar medidas de seguridad toma meses, no semanas. Quien parte en octubre llega a diciembre con papeles, no con cumplimiento integral.

Plan de trabajo sugerido para el segundo semestre 2026

Julio–agosto:

Diagnóstico. Levantar el RAT, aplicar el autodiagnóstico de esta guía, priorizar brechas por severidad (las que constituyen infracción grave primero) y designar al responsable interno.

Septiembre–octubre:

Cierre de brechas estructurales. Firmar DPAs con proveedores, regularizar transferencias internacionales, desplegar o reforzar medidas de seguridad (accesos, cifrado, monitoreo), y establecer la política de retención y eliminación —incluyendo respaldos.

Noviembre:

Operación y evidencia. Probar el plan de respuesta a incidentes con un ejercicio de simulación, probar la recuperación de respaldos, capacitar a los equipos que tratan datos y consolidar la documentación que demuestra cumplimiento.

Diciembre en adelante:

Mejora continua. El 1 de diciembre no termina el trabajo: empieza la fiscalización. Auditorías periódicas, revisión anual del RAT y evaluación del modelo de prevención de infracciones como atenuante y ventaja comercial.

El punto de partida es tu infraestructura

La mayoría de las conversaciones sobre la Ley 21.719 parten por lo legal. Pero cuatro de los diez requisitos de esta guía (seguridad, respuesta a brechas, respaldo y retención, y transferencias internacionales) se resuelven en la infraestructura de TI, no en un documento.

Sin visibilidad de dónde viven los datos, sin respaldos probados y sin capacidad de detección y recuperación, el resto del cumplimiento es papel.

En Provectis ayudamos a empresas del midmarket chileno a resolver exactamente esa capa: soluciones de respaldo On-Premise, Híbrido y BaaS, continuidad operativa y ciberseguridad, diseñadas para que el cumplimiento tenga cimientos técnicos reales.

Diagnóstico de preparación sin costo

Te ofrecemos una sesión de 30 minutos con nuestros especialistas para revisar tu autodiagnóstico de la página 8 y priorizar las brechas técnicas de tu empresa frente a la ley.

Agenda tu diagnóstico aquí

PROVECTIS
www.provectis.cl
info@provectis.cl

Fuentes y nota legal

Este documento fue elaborado por Provectis SpA sobre la base del texto de la Ley 21.719 (Diario Oficial, 13 de diciembre de 2024), que modifica la Ley 19.628 sobre protección de la vida privada, y de análisis públicos de firmas legales y especialistas en cumplimiento chilenos. Los montos en pesos son referenciales y dependen del valor de la UTM vigente al momento de la infracción.

Esta guía tiene fines informativos y no constituye asesoría legal. Provectis recomienda complementar la preparación técnica con asesoría jurídica y tecnológica especializada.