

GUÍA PRÁCTICA PARA EMPRESAS · CHILE

Cumplir la Ley 21.719 con IA *on-premise.*

Qué exige la nueva ley de protección de datos personales, qué cambia el 1 de diciembre de 2026, y un checklist concreto para implementar inteligencia artificial sin que tus datos salgan del país.

1. Qué cambia con la Ley 21.719

La Ley 21.719, publicada en diciembre de 2024, moderniza por completo el régimen chileno de protección de datos personales (que databa de 1999) y lo alinea con estándares internacionales como el RGPD europeo. Entra en **plena vigencia el 1 de diciembre de 2026**, y trae tres cambios estructurales:

- **Una autoridad fiscalizadora con dientes:** se crea la Agencia de Protección de Datos Personales, con facultades para fiscalizar, sancionar y ordenar medidas correctivas.
- **Notificación obligatoria de brechas:** las vulneraciones de seguridad deben reportarse a la Agencia "por los medios más expeditos posibles y sin dilaciones indebidas" (el estándar operativo de referencia en la industria: 72 horas). Si afectan datos sensibles, de menores de 14 años o de carácter económico-financiero, también hay que comunicarlas a los titulares.
- **Multas significativas:** las infracciones se clasifican en leves, graves y gravísimas, con multas de hasta 5.000, 10.000 y 20.000 UTM respectivamente (arts. 34 bis a 34 quáter). En caso de reincidencia, para empresas de mayor tamaño, la multa puede llegar al 2% (graves) o 4% (gravísimas) de los ingresos anuales.

La lectura de negocio: hasta ahora, incumplir la normativa de datos en Chile casi no tenía costo. Desde diciembre de 2026, el costo es concreto, alto y fiscalizable. Los sectores que manejan datos sensibles —banca, salud, minería, sector público— ya están exigiendo cumplimiento demostrable a sus proveedores.

2. Los conceptos que tienes que dominar

CONCEPTO	QUÉ SIGNIFICA EN LA PRÁCTICA
Dato personal	Cualquier información vinculada o vinculable a una persona identificada o identificable: nombre, RUT, correo, ubicación, imagen de cámara, voz, historial de compra.
Dato sensible	Salud, perfil biológico humano, datos biométricos, origen étnico o racial, afiliación política o sindical, situación socioeconómica, creencias, vida sexual, orientación sexual e identidad de género. Régimen reforzado: por regla general exigen consentimiento expreso, y varias categorías tienen reglas propias (arts. 16 bis a 16 sexies: salud, biometría, menores, geolocalización).
Responsable	Quien decide sobre el tratamiento: tu empresa. La responsabilidad no se externaliza con el proveedor de nube o de IA.
Encargado	Quien trata datos por cuenta del responsable (un proveedor). Necesita contrato que regule el encargo y medidas de seguridad.
Base de licitud	Todo tratamiento necesita fundamento: consentimiento, contrato, obligación legal o interés legítimo. "Los tenemos en la base" no es una base.
Derechos del titular	Acceso, rectificación, supresión, oposición y portabilidad, más la revocación del consentimiento. Debes poder responderlos en plazos legales.
Transferencia internacional	Enviar datos fuera de Chile —incluido almacenarlos en una nube extranjera— solo procede hacia países con nivel adecuado de protección o con garantías específicas.

3. Por qué la IA complica el cumplimiento

Los proyectos de IA concentran los riesgos de la ley en un solo lugar:

- **Volumen y sensibilidad:** los modelos se alimentan de datos operativos masivos — video de cámaras, documentos, historiales — que casi siempre contienen datos personales, y a menudo sensibles.
- **Nube extranjera por defecto:** la mayoría de las plataformas de IA procesan en data centers fuera de Chile. Cada inferencia puede ser una transferencia internacional de datos que debes poder justificar.
- **Trazabilidad difusa:** si no puedes decir dónde se procesó un dato, quién accedió y con qué base, no puedes demostrar cumplimiento — y la carga de demostrar es tuya.
- **Terceros encadenados:** proveedor de nube, proveedor de modelo, integrador: cada eslabón es un encargado que necesita contrato y garantías.

La alternativa estructural: desplegar la IA on-premise —cómputo y almacenamiento en infraestructura local, dentro de Chile— elimina de raíz la transferencia internacional, reduce los encargados a un mínimo contratable y deja la trazabilidad bajo tu control directo. El cumplimiento deja de ser una promesa del proveedor y pasa a ser una propiedad de la arquitectura.

4. Checklist: IA que cumple la ley

Gobernanza del dato

- ☐ **Inventario de datos:** mapea qué datos personales tratas, dónde viven, con qué base de licitud y quién accede.
- ☐ **Clasificación de sensibilidad:** identifica los datos sensibles (salud, biometría, video con personas) y dales régimen reforzado.
- ☐ **Contratos de encargo:** todo proveedor que toque datos personales necesita contrato de encargado con medidas de seguridad verificables.

Arquitectura

- ☐ **Cómputo y almacenamiento en Chile:** para datos sensibles o críticos, procesa on-premise o en infraestructura local; evita que el dato cruce la frontera.
- ☐ **Control de acceso:** privilegios mínimos, autenticación fuerte y registro de quién accede a qué.
- ☐ **Trazabilidad auditable:** logs de procesamiento e inferencia que permitan reconstruir qué se hizo con cada dato.
- ☐ **Cifrado en tránsito y en reposo,** con llaves bajo tu control.

Operación

- **Procedimiento de derechos:** canal y plazos definidos para responder acceso, rectificación, supresión, oposición y portabilidad.
- **Plan de respuesta a brechas:** detección, contención y notificación a la autoridad con el estándar de 72 horas como referencia.
- **Retención limitada:** define cuánto tiempo conservas cada categoría de dato y elimina automáticamente al vencer.
- **Evaluación de impacto:** para tratamientos de alto riesgo (video-analítica, datos de salud), documenta una evaluación previa.

5. Cómo lo resuelve Refracta

Refracta es una plataforma de procesamiento y visualización de datos con IA que se usa por web y que, cuando el dato es sensible o regulado, **puede instalarse completa dentro de tu propia infraestructura**: el dato se procesa en GPU y se guarda en tus servidores, sin salir de tu empresa ni del país.

- **El dato no sale del país:** en el modo on-premise, cómputo y almacenamiento quedan en tu data center — la transferencia internacional simplemente no ocurre.
- **Control de acceso real:** usuarios y roles definidos por tu organización, con permisos por módulo y por acción, y registro de quién ve qué.
- **La IA redacta, nunca calcula:** los números salen del motor de cálculo; el modelo de lenguaje solo los traduce. Si el servicio de IA no está disponible, la plataforma muestra un texto determinista — nunca una cifra inventada.
- **Cumplimiento sin sacrificar valor:** indicadores, segmentos y proyecciones navegables por tu equipo — el dato protegido sigue siendo dato útil.

Siguiente paso: agenda una demo con tus datos en refracta.tribucorp.cl/#demo o escríbenos a info@tribucorp.cl. Te mostramos tu información procesada y visualizada, sin que salga de Chile.