PC **PrivacyCheck**
BY SWELL

TOOLKIT DESCARGABLE

MarTech Compliance para Ley 21.719

Una guía práctica para revisar, ordenar y corregir el ecosistema de marketing digital de tu empresa antes del 1 de diciembre de 2026 — sitio web, formularios, publicidad, CRM, email y proveedores.

privacycheck.cl

Versión 1.0 · Julio 2026

Cómo usar este Toolkit

Este documento reúne, en un solo lugar, las revisiones más importantes que tu equipo de marketing puede hacer hoy para reducir su exposición frente a la Ley 21.719 — sin necesidad de un abogado para empezar.

La Ley 21.719 de Protección de Datos Personales entra en plena vigencia el **1 de diciembre de 2026**. Para la mayoría de las empresas chilenas, el riesgo real no vive en un contrato mal redactado — vive en las herramientas que marketing usa todos los días: el sitio web, los formularios de captación, los píxeles de publicidad, el CRM, las plataformas de email y los proveedores de tecnología (MarTech).

Este Toolkit está organizado en **6 áreas**, las mismas que evalúa el diagnóstico automatizado de PrivacyCheck. Cada área incluye una checklist de revisión concreta y un ángulo táctico sobre qué priorizar primero.

1. Revisa cada área con la persona de tu equipo que administra esa herramienta (marketing, growth, IT o el proveedor externo).
2. Marca cada punto de la checklist como resuelto, pendiente o "no aplica" — no necesitas resolverlo todo en un día.
3. Prioriza los puntos marcados como **crítico**: son los que concentran el mayor riesgo de infracción grave o gravísima.
4. Si necesitas ayuda para implementar cualquier punto, **PrivacyCheck** puede acompañarte — siempre dentro del ámbito de marketing digital.

Alcance de este Toolkit. El contenido de este documento cubre exclusivamente el ecosistema de marketing digital de tu empresa. La Ley 21.719 también aplica a otras áreas —recursos humanos, seguridad de la información, contratos societarios, gobierno de datos a nivel de directorio— que quedan fuera del alcance de PrivacyCheck y de este Toolkit. Para esas materias, tu empresa debe contar con asesoría especializada en el área correspondiente. Este documento es contenido educativo general y no constituye asesoría legal ni un diagnóstico personalizado.

ÁREA 1 DE 6

1 Sitio web

> Tu sitio es la primera línea de cumplimiento visible. Es también lo primero que revisa cualquier fiscalización o auditoría: política de privacidad, gestión de cookies y transparencia sobre qué datos capturas y para qué.

- **Política de Privacidad publicada y actualizada** conforme a la Ley 21.719 — no una versión heredada de la Ley 19.628 sin actualizar.
- **Banner de cookies que bloquea scripts** hasta que el usuario da su consentimiento — no solo un aviso informativo que no impide la carga.
- **Opciones granulares de consentimiento** por categoría de cookie (necesarias, analíticas, publicitarias), no un solo botón "Aceptar todo".
- Los textos de privacidad especifican **propósito, base legal y encargados del tratamiento** de forma concreta, no genérica.
- Existe un **canal claro para ejercer derechos ARCOP** (acceso, rectificación, cancelación, oposición, portabilidad) visible desde el sitio.

Prioriza esto primero: si tu banner de cookies no bloquea scripts antes del consentimiento, cada visita a tu sitio es una transferencia de datos sin base legal. Es el punto más rápido de corregir y el que más reduce exposición de inmediato.

ÁREA 2 DE 6

2 Formularios

> Cada formulario que captura un nombre, email o teléfono es un punto de tratamiento de datos. Sin un consentimiento válido y documentado en el momento de la captura, cada envío es un riesgo acumulado.

- **Checkbox de consentimiento explícito** en cada formulario de contacto, cotización o registro — nunca premarcado.
- El texto del consentimiento está **en el punto de captura**, no solo como un link genérico en el footer.
- Existe un **mecanismo simple de revocación** del consentimiento, tan fácil como otorgarlo.
- Los formularios que capturan **datos sensibles** (salud, situación socioeconómica, etc.) tienen consentimiento específico y separado.
- Se documenta **cuándo y cómo** se obtuvo el consentimiento de cada contacto (fecha, formulario, versión de la política vigente).

Prioriza esto primero: audita primero los formularios con más tráfico (landing pages de campañas activas). Son los que generan volumen de datos nuevo cada semana.

ÁREA 3 DE 6

3 Plataformas Ads

> Meta Pixel, Google Ads y herramientas similares envían datos de comportamiento a servidores en el extranjero. Eso es una transferencia internacional de datos, y requiere acuerdos específicos con esos proveedores.

- Cuentas con un **DPA (Data Processing Agreement) formalizado** con Meta, Google y cualquier otra plataforma de ads que uses.
- El píxel de conversión **se activa después** del consentimiento del usuario, no al cargar la página.
- Tus **bases de remarketing/audiencias personalizadas** tienen origen documentado (no listas históricas sin trazabilidad).
- Revisas periódicamente qué **eventos de conversión** capturan datos personales (email, teléfono) vs. solo comportamiento agregado.
- El equipo de medios sabe qué hacer si una plataforma reporta un **incidente de datos** que involucre tus audiencias.

Prioriza esto primero: revisa el Meta Pixel y el tag de conversión de Google Ads de tus campañas activas — son los que están corriendo hoy y generando el mayor volumen de eventos.

ÁREA 4 DE 6

4 CRM & Bases de datos

> El CRM suele mezclar datos capturados en distintos momentos, con distintos niveles de consentimiento, durante años. Es la fuente más común de datos "sin origen documentado".

- Puedes **trazar, contacto por contacto**, cómo y cuándo se obtuvo el consentimiento inicial.
- Existe un **plazo de conservación definido** para contactos inactivos, con proceso de eliminación o anonimización.
- Identificaste qué **porcentaje de tu base histórica** no tiene origen documentado y tienes un plan para ese segmento.
- El acceso al CRM está **segmentado por rol** — no todo el equipo puede exportar la base completa.
- Existe un proceso definido para **responder solicitudes ARCOP** (acceso, rectificación, cancelación) sobre datos del CRM en un plazo razonable.

Prioriza esto primero: segmenta tu base entre "consentimiento documentado" y "origen desconocido". Ese segundo grupo es tu mayor exposición y el punto de partida de tu propio Registro de Actividades de Tratamiento (RAT).

ÁREA 5 DE 6

5 Email Marketing

> El opt-in de email marketing es de los consentimientos más antiguos y menos documentados en la mayoría de las empresas — muchas listas se armaron antes de que existiera un estándar claro.

- [ ] Cada suscriptor tiene **opt-in documentado** (fecha, formulario u origen de la suscripción).
- [ ] Todo email incluye un **link de baja funcional** que se procesa de inmediato, no en días.
- [ ] Los segmentos de la plataforma de email **no mezclan** contactos con distinto nivel de consentimiento.
- [ ] El proveedor de email marketing (Mailchimp, Klaviyo, HubSpot, etc.) tiene **DPA vigente** como encargado de tratamiento.
- [ ] Existe un proceso para **limpiar contactos inactivos** o sin consentimiento verificable de forma periódica.

Prioriza esto primero: si tienes listas importadas antes de 2024 sin opt-in verificable, ese es tu mayor riesgo — considera una campaña de re-permission antes de seguir enviando.

ÁREA 6 DE 6

6 Proveedores

> Todo proveedor de MarTech que procesa datos personales por tu cuenta —CRM, email, ads, analítica, automatización— es un encargado de tratamiento. Sin contrato adecuado, la responsabilidad recae sobre ti.

- [ ] Tienes un **inventario actualizado** de todos los proveedores MarTech que procesan datos personales de tu empresa.
- [ ] Cada proveedor relevante tiene un **contrato o DPA vigente** que menciona expresamente el tratamiento de datos.
- [ ] Sabes en **qué país** se almacenan los datos que cada proveedor procesa (transferencia internacional).
- [ ] Revisas los **subencargados** de tus proveedores principales (cuarta parte) cuando el contrato lo permite.
- [ ] Tienes un proceso definido para cuando **termina la relación** con un proveedor: qué pasa con los datos que procesó.

Prioriza esto primero: parte por los 3-5 proveedores que concentran más volumen de datos (típicamente CRM, email marketing y la plataforma de analítica). Ahí vive la mayor parte del riesgo contractual.

¿Cuántos de estos puntos tiene tu empresa resueltos?

Este Toolkit te da el mapa. El diagnóstico de PrivacyCheck te da tu propio número: score de riesgo, exposición estimada en CLP y un plan de acción priorizado — con IA, en menos de 5 minutos y sin costo.

Iniciar diagnóstico sin costo →

privacycheck.cl/diagnostico