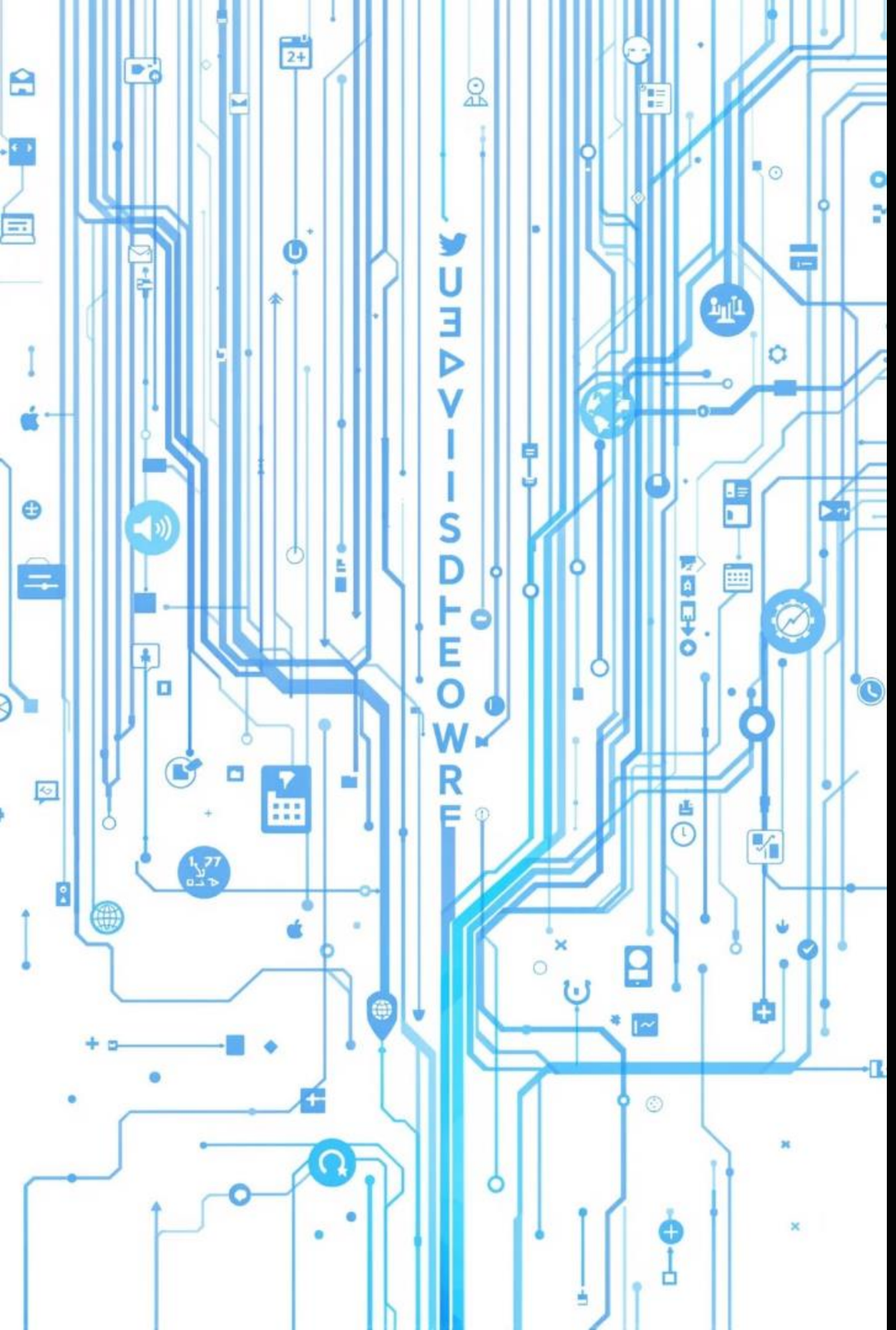
GA-ABOGADOS

Protección de Datos en la Relación con Clientes y Proveedores

Seminario Protección de Datos en la Empresa
Cámara de Comercio de Santiago

Raúl Arrieta Cortés



¿Qué entendemos por recolección y tratamiento de datos?

Recolección

Toda obtención de datos personales, sea directa o indirecta, que permita identificar a una persona natural.

Tratamiento

Cualquier operación realizada sobre los datos, como recopilación, registro, almacenamiento, conservación, comunicación, transferencia, supresión o anonimización.

Datos Personales

Información relativa a una persona natural identificada o identificable, independientemente de su formato o soporte.

Principios Rectores del Tratamiento

Licitud y Lealtad

Los datos deben ser tratados conforme a la ley y de manera honesta.

Transparencia

El titular debe conocer qué datos se tratan y con qué finalidad.

Seguridad

Protección contra accesos no autorizados, pérdidas o filtraciones.

Finalidad

Los datos deben recolectarse con fines específicos, explícitos y lícitos.

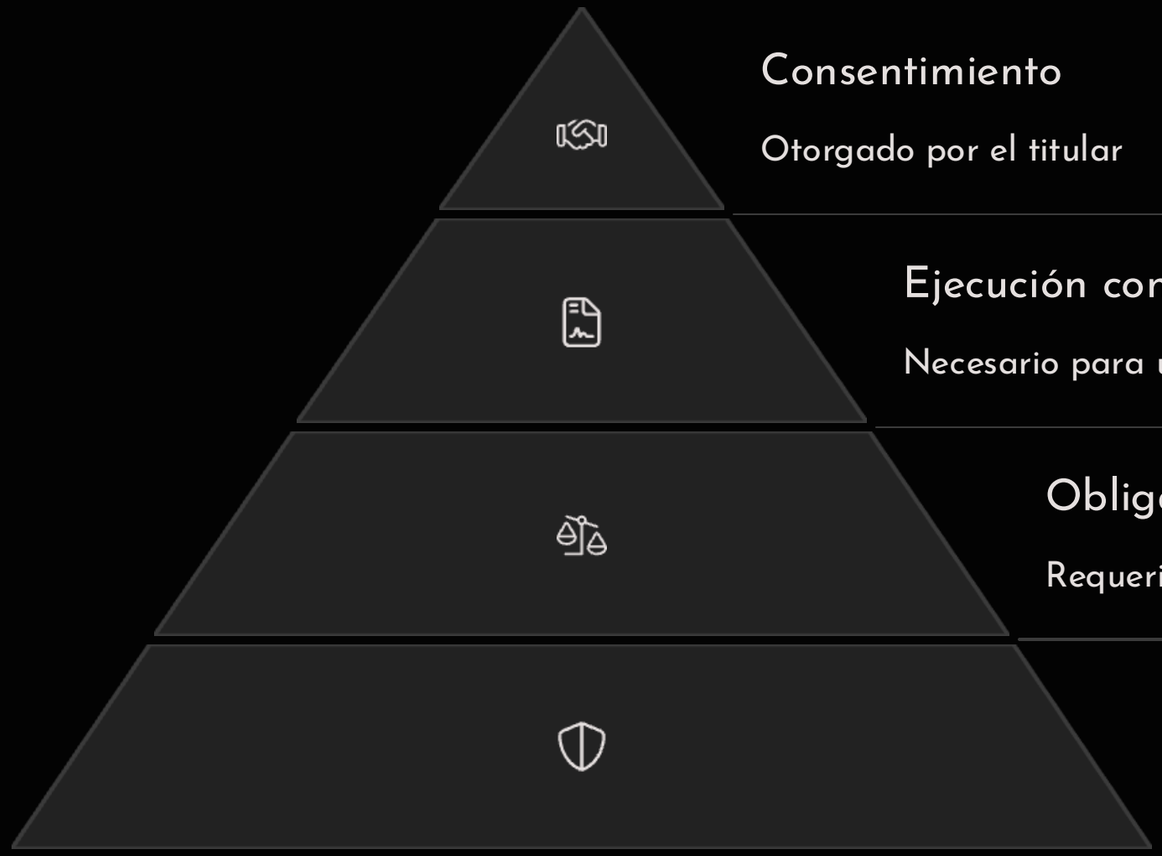
Proporcionalidad

Sólo deben tratarse los datos estrictamente necesarios.

Calidad

Los datos deben ser exactos, completos y actualizados.

Fundamentos para el tratamiento lícito



Consentimiento

Otorgado por el titular

Ejecución contractual

Necesario para un contrato

Obligación legal

Requerido por ley

Interés legítimo

Sin vulnerar derechos

El tratamiento de datos de clientes y proveedores debe fundamentarse en al menos una de estas bases legales. El consentimiento debe ser libre, específico, informado e inequívoco. La ejecución contractual aplica cuando los datos son necesarios para cumplir con obligaciones contractuales con el titular.

Contrato con terceros encargados del tratamiento

1

Definir el objeto

Establecer claramente el propósito, duración y finalidad del encargo de tratamiento.

2

Especificar datos

Detallar el tipo de datos y categorías de titulares involucrados en el tratamiento.

3

Establecer obligaciones

Definir derechos y obligaciones de ambas partes respecto al tratamiento de datos.

4

Garantizar limitaciones

Asegurar que el encargado no utilizará los datos para fines distintos ni los cederá sin autorización expresa.

Obligaciones del Responsable

Informar

Comunicar de manera clara al titular sobre el tratamiento de sus datos personales.

Proteger

Implementar medidas de seguridad adecuadas para garantizar la integridad y confidencialidad.

Facilitar derechos

Permitir el ejercicio de los derechos ARCO (acceso, rectificación, cancelación, oposición).

Suprimir

Eliminar o anonimizar los datos cuando ya no sean necesarios para la finalidad.

GA-ABOGADOS

Tratamiento a través de terceros (proveedores)

Contratación

Establecer relación formal con el proveedor

2

Limitación

Restringir uso a fines autorizados

Finalización

Eliminar o devolver datos al terminar

Cuando una empresa encarga a un proveedor servicios que impliquen tratamiento de datos personales, este proveedor actúa como "Encargado del Tratamiento". Es fundamental establecer contractualmente que no podrá usar los datos para fines propios y deberá eliminarlos o devolverlos cuando finalice la prestación del servicio.

Principio de Transparencia

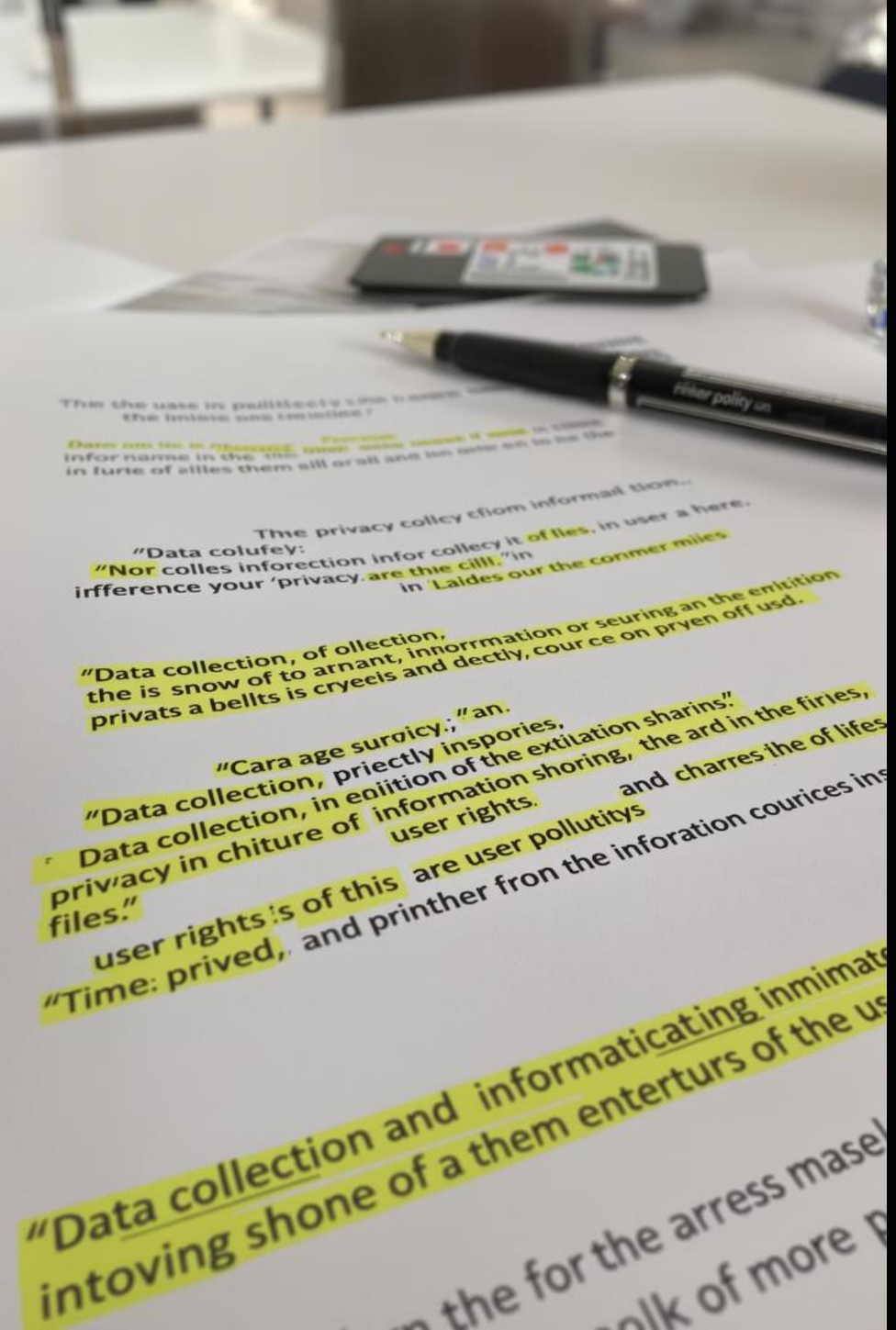
Derecho a la información

La Ley 21.719 establece que toda persona tiene derecho a ser informada, de manera clara, accesible y comprensible, sobre el tratamiento de sus datos personales.

Esta información debe proporcionarse antes de la recolección de los datos, utilizando un lenguaje sencillo y evitando tecnicismos innecesarios.

Elementos esenciales

- Finalidad del tratamiento
- Base legal que lo autoriza
- Destinatarios de los datos
- Plazo de conservación
- Derechos del titular
- Transferencias internacionales



Obligación de información

Identidad del responsable

Datos de contacto claros y accesibles para que el titular pueda comunicarse fácilmente.

Finalidades específicas

Descripción concreta de para qué se utilizarán los datos, evitando términos ambiguos.

Base legal

Fundamento jurídico que legitima el tratamiento (consentimiento, contrato, interés legítimo, etc.).

Derechos del titular

Explicación sobre cómo ejercer los derechos ARCO y otros reconocidos por la ley.

Antes de recolectar los datos, el responsable debe proporcionar al titular una Política de Privacidad o Aviso de Privacidad que contenga toda esta información de manera clara y accesible.

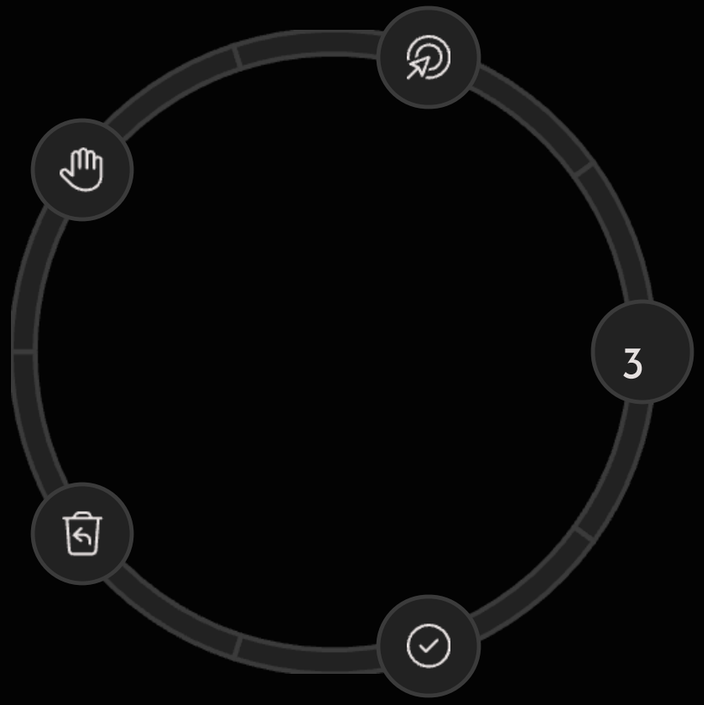
Consentimiento Informado

Libre

No puede estar condicionado ni forzado.

Revocable

El titular puede retirar el consentimiento en cualquier momento.



Específico

Solo para finalidades determinadas.

Informado

El titular debe conocer para qué, cómo y por quién serán tratados sus datos.

Inequívoco

Otorgado mediante una acción afirmativa clara.

Excepciones al consentimiento

1

Ejecución de un contrato

Cuando el tratamiento sea necesario para cumplir con obligaciones contractuales con el titular.

Obligación legal

Cuando exista un mandato legal que requiera el tratamiento de los datos.

Interés legítimo

Cuando exista un interés legítimo del responsable o un tercero, siempre que no prevalezcan los derechos del titular.

Fuentes accesibles al público

Cuando se trate de información contenida en fuentes accesibles al público, conforme a la ley.

Buenas prácticas de transparencia

Política de privacidad clara

Mantener actualizada y accesible la política de privacidad, utilizando un lenguaje sencillo y comprensible.

Canales accesibles

Implementar vías sencillas para que los titulares consulten y ejerzan sus derechos sobre sus datos personales.

Registro de consentimiento

Conservar evidencias del consentimiento otorgado por los titulares para demostrar cumplimiento.

Notificación de cambios

Informar de manera clara y visible cualquier modificación en la política de tratamiento de datos.

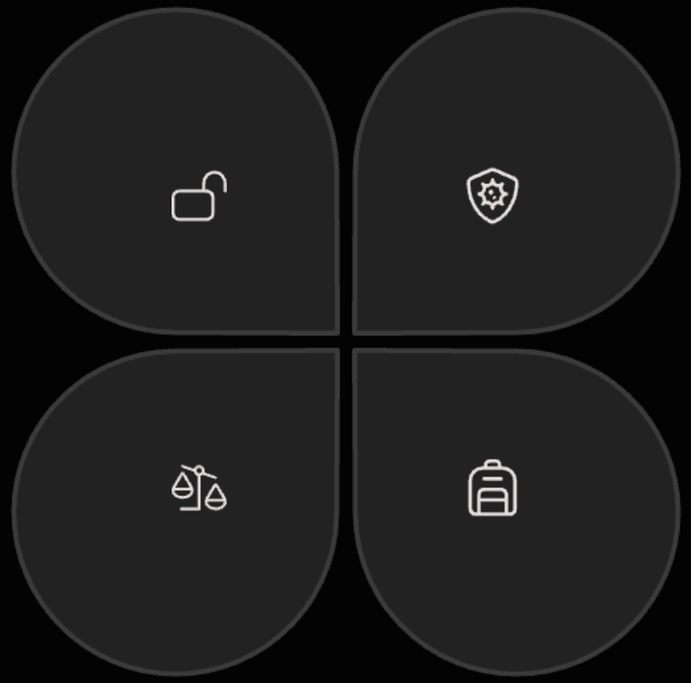
Principio de Seguridad

Acceso controlado

Prevenir accesos no autorizados.

Proporcionalidad

Medidas acordes al nivel de riesgo.



Uso legítimo

Evitar uso indebido o ilícito.

Integridad

Prevenir pérdida o destrucción accidental.

Medidas de seguridad recomendadas

Control de acceso

Políticas de acceso restringido a datos sensibles.

Cifrado de datos

En tránsito y en reposo, cuando sea necesario.

Respuesta a incidentes

Procedimientos definidos ante brechas de seguridad.

Obligaciones en la relación comercial

Garantizar confidencialidad

Asegurar que los datos personales se mantengan protegidos y solo sean accesibles para personal autorizado.

Limitar finalidades

Utilizar los datos únicamente para los propósitos informados y autorizados previamente.

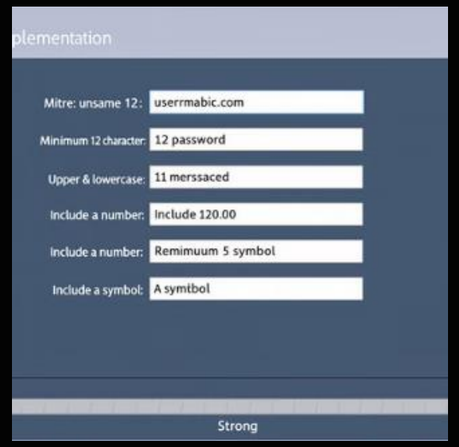
Controlar accesos

Restringir el acceso a los datos personales solo a personas con necesidad legítima de conocerlos.

Establecer controles contractuales

Implementar cláusulas específicas con proveedores que tengan acceso a datos personales.

Medidas mínimas de seguridad recomendadas



Las empresas deben implementar controles de acceso, cifrado de datos, políticas de contraseñas seguras, procedimientos de respuesta ante incidentes, capacitación periódica al personal y auditorías regulares de sus sistemas y procesos.

Deber de confidencialidad y notificación de incidentes

Deber de confidencialidad

Toda persona que intervenga en cualquier fase del tratamiento de datos está obligada a guardar secreto o confidencialidad incluso después de finalizada su relación con el responsable.

Este deber debe formalizarse mediante cláusulas contractuales específicas y acuerdos de confidencialidad con empleados y proveedores.

Notificación de incidentes

Si ocurre una violación de seguridad que afecte datos personales, el responsable debe notificar a la Agencia de Protección de Datos y al titular afectado, sin dilación indebida.

La notificación debe informar sobre la naturaleza de la violación, las posibles consecuencias y las medidas adoptadas para mitigar el daño.

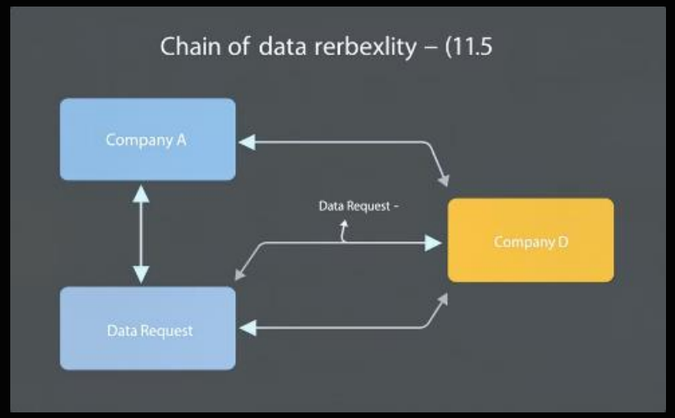
Tratamiento de Datos Personales en Contratos con Proveedores

Relación Responsable-Encargado

Cuando una empresa contrata a un proveedor que requiere acceder, procesar o almacenar datos personales por cuenta de la empresa, este proveedor actúa como Encargado del Tratamiento y la empresa sigue siendo la Responsable del Tratamiento.

Contrato obligatorio

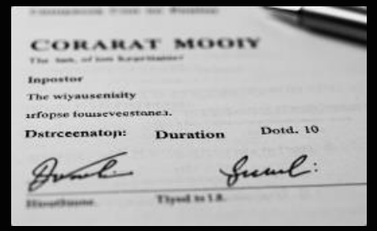
La Ley exige que exista un contrato escrito o un instrumento jurídico equivalente entre el Responsable y el Encargado, que regule específicamente el tratamiento de datos personales.



Responsabilidad compartida

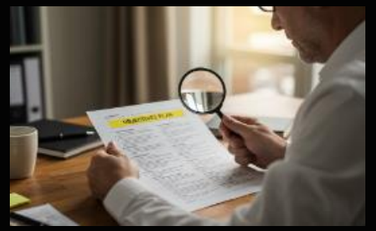
Aunque el tratamiento lo realice un proveedor, la empresa sigue siendo la principal responsable de asegurar que el proveedor cumpla con la Ley.

Obligación contractual con proveedores



Objeto y duración

Define claramente el propósito del contrato y su periodo de vigencia para enmarcar legalmente la relación.



Finalidad del tratamiento

Establece específicamente para qué se utilizarán los datos personales, limitando su uso a lo estrictamente necesario.

Tipos de datos

Detalla exactamente qué categorías de datos personales serán tratados por el proveedor.

Medidas de seguridad

Especifica las protecciones técnicas y organizativas que el proveedor debe implementar para proteger los datos.

Confidencialidad

Obliga al proveedor a mantener secreto sobre los datos tratados, incluso después de finalizar la relación contractual.

Subcontratación

Regula si el proveedor puede subcontratar servicios y bajo qué condiciones específicas.

Derechos de titulares

Establece cómo el proveedor ayudará a cumplir con los derechos ARCO de los titulares de datos.

Eliminación de datos

Determina cómo se destruirán o devolverán los datos al finalizar el servicio o contrato.

El contrato entre el Responsable y el Encargado debe establecer claramente todos estos elementos para garantizar un tratamiento adecuado de los datos personales y el cumplimiento de la normativa vigente.

Cláusulas Obligatorias de Protección de Datos en Contratos

1

Objeto y alcance

- Identificación de partes
- Finalidad específica

2

Naturaleza y duración

- Categorías de datos
- Tipos de titulares
- Plazo del tratamiento

3

Obligaciones

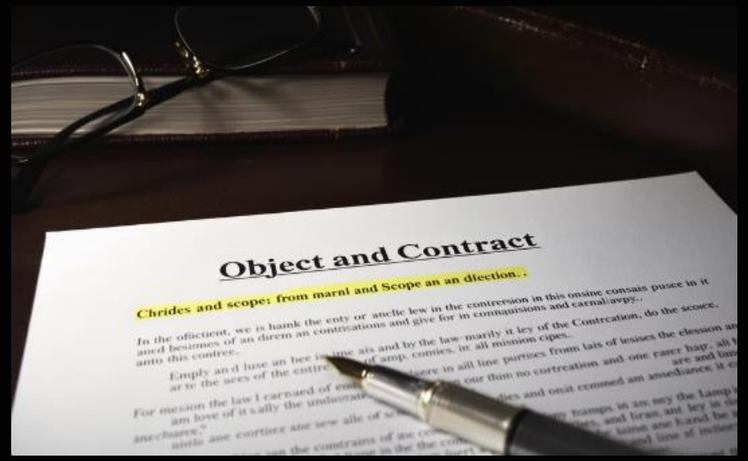
- Instrucciones documentadas
- Medidas de seguridad
- Asistencia al responsable

4

Control y responsabilidad

- Auditorías
- Sanciones
- Gestión de incidentes

Contenido mínimo obligatorio en contratos



Objeto y alcance

Identificación clara de las partes, objeto del contrato relacionado con el tratamiento de datos personales por cuenta del Responsable, y finalidad específica del tratamiento.

Obligaciones del Encargado

Compromisos de tratar los datos solo conforme a instrucciones documentadas, garantizar confidencialidad, implementar medidas de seguridad adecuadas, y no subcontratar sin autorización previa.

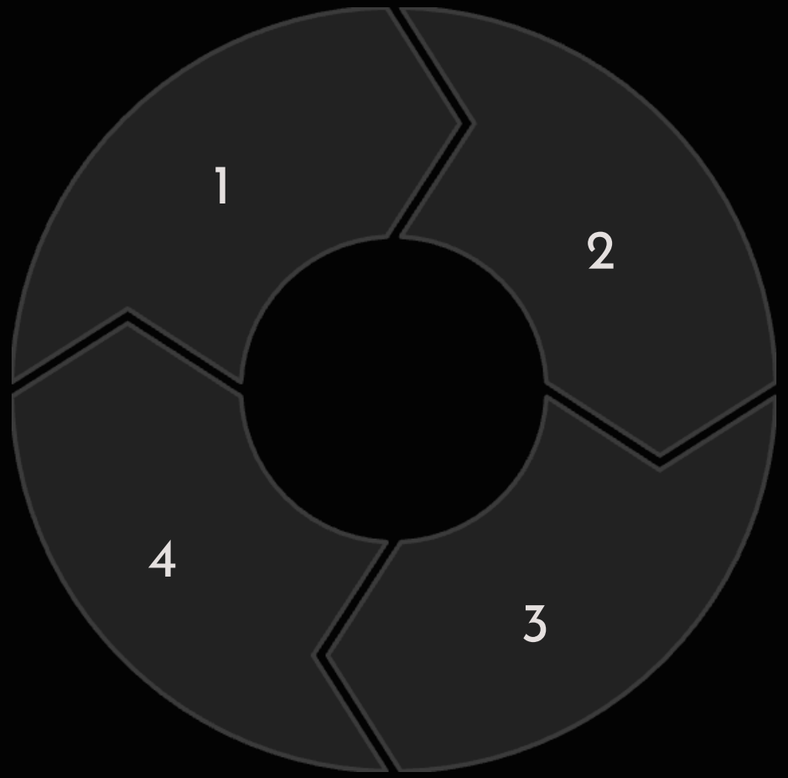
Medidas de seguridad

Detalle de las medidas físicas, técnicas y administrativas para garantizar la protección de los datos tratados, adaptadas al nivel de riesgo identificado.

Gestión y Transferencia de Datos Personales con Terceros

Verificar base legal

Confirmar la existencia de justificación jurídica válida



Informar al titular

Comunicar sobre la transferencia y su finalidad

Documentar proceso

Mantener registros de todas las transferencias

Formalizar acuerdos

Establecer contratos con garantías adecuadas

La transferencia de datos personales se define como la comunicación de datos a un tercero, nacional o extranjero, distinto del titular, del responsable o del encargado del tratamiento. Toda transferencia debe cumplir con requisitos legales específicos.

Consecuencias del Incumplimiento

20.000

UTM máxima

Multa por infracciones gravísimas

10.000

UTM máxima

Multa por infracciones graves

5.000

UTM máxima

Multa por infracciones leves

La Ley N° 21.719 establece un régimen sancionatorio robusto. El monto de las multas se determinará considerando la gravedad del incumplimiento, el daño causado a los titulares, el beneficio económico obtenido y la reincidencia. Las infracciones gravísimas pueden, además, ser publicadas para conocimiento público, generando un daño reputacional significativo.

Impacto del incumplimiento más allá de las multas

Responsabilidad civil

El incumplimiento puede generar demandas por daños y perjuicios de los titulares afectados, con la obligación de indemnizar tanto el daño material como el moral causado.

Daño reputacional

El mal manejo de datos personales puede provocar pérdida de confianza por parte de clientes y proveedores, daños a la imagen y credibilidad de la empresa, ruptura de contratos comerciales y exclusión de licitaciones o proyectos.

Impacto operacional

La Agencia de Protección de Datos podrá ordenar la suspensión o cese del tratamiento de datos y la eliminación de los datos objeto de incumplimiento, lo que puede implicar la paralización de procesos comerciales relevantes.

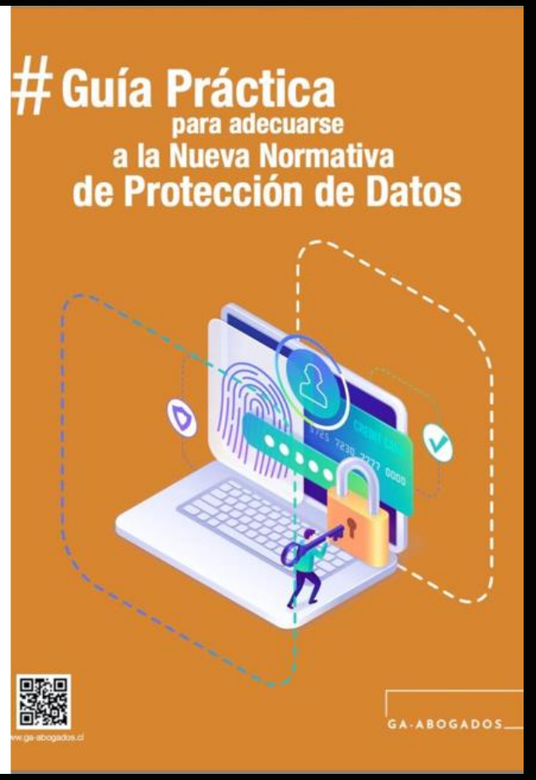
Raúl Arrieta Cortés

raul.arrieta@ga-abogados.cl

+56 2 2638 1527

www.ga-abogados.cl

Descarga nuestra Guía Práctica para adecuarse a la Nueva Normativa de Protección de Datos



GA-ABOGADOS