Protección de datos personales



Autonomía digital en la era de la información

Sebastián Bozzo Hauri

Dykinson, S.L.

Protección de datos personales

Autonomía digital en la era de la información*

* En la preparación de este libro se utilizaron herramientas de inteligencia artificial generativa (LLM) como apoyo para la organización de materiales, revisión de estilo, detección de inconsistencias formales y mejora de la claridad expositiva. Estas herramientas no fueron utilizadas como fuente de conocimiento ni como sustituto del análisis, investigación o juicio profesional del autor.

Este libro ha sido sometido a evaluación por pares y aprobado por nuestro Consejo Editorial
Para mayor información, véase www.dykinson.com/quienes_somos

© Copyright by
Los autores
Madrid, noviembre de 2026
Santiago de Chile, noviembre de 2026

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid
Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69
e-mail: info@dykinson.com

http://www.dykinson.es
http://www.dykinson.com

ISBN impreso: 978-956-417-214-9
ISBN digital: 978-956-417-220-0

Maquetación:
Ediciones Universidad Autónoma de Chile
http://ediciones.uautonoma.cl
ediciones@uautonoma.cl



IA Y DERECHO PRIVADO EUROPEO
MÓDULO JEAN MONNET
Universidad Autónoma de Chile



Cofinanciado por el programa Erasmus+ de la Unión Europea

Módulo Jean Monnet
IA y Derecho Privado Europeo

Protección de datos personales

Autonomía digital en la era de la información

Sebastián Bozzo Hauri

Colaboración en contenido: Paula Rodríguez

DUC IN ALTUM
UA
UNIVERSIDAD AUTÓNOMA DE CHILE

Dykinson, S.L.

Contenido

11 **Introducción**

15 **¿Qué protege la ley? Descubriendo cómo y cuándo se aplican las reglas sobre datos personales**

15 ¿Qué dice esta norma constitucional?

17 ¿Por qué importa proteger tus datos personales? El propósito de la ley

19 ¿Quién tiene derecho a la protección de sus datos? Conociendo el alcance de la ley

20 Términos clave para entender la ley

22 ¿Por qué esta ley es importante en tu día a día?

23 Entender la ley es el primer paso para protegerte

25 **¿A quién protege esta ley? Objeto y alcance de la protección de datos personales**

26 ¿Se aplica esta ley fuera de Chile? Alcance territorial de la protección de datos

27 ¿Qué significa todo esto? Glosario básico para entender la Ley de Protección de Datos Personales

33 **Protegiendo tu información: principios claves y ejemplos prácticos**

34 ¿Cuáles son estos principios fundamentales?

43 **Tu permiso importa. Entendiendo el consentimiento en el uso de datos personales**

44 Consentimiento libre, informado y específico

48 Consentimiento previo e inequívoco

49 Revocar el consentimiento: tú decides cuándo parar
50 Cuidado con los consentimientos forzados
50 ¿Quién tiene que demostrar que tú consentiste?
56 Consentimiento de niños, niñas y adolescentes: ¿quién decide sobre sus datos personales?
63 ¿Sabías que no siempre se necesita tu permiso? Casos en que se pueden usar tus datos sin consentimiento

67 **Protege tu privacidad: descubre tus derechos sobre datos personales**
68 Derechos sobre tus datos personales
71 ¿Qué pasa si el titular de los derechos fallece? Derechos en caso de fallecimiento del titular

75 **Un vistazo más profundo a tus derechos sobre los datos personales**
75 Sobre el derecho de acceso
82 Sobre el derecho de rectificación
84 Derecho de supresión
86 Derecho de oposición

107 **Quien maneja tus datos debe respetar las reglas**
107 ¿Qué debe hacer quien maneja tus datos? Obligaciones clave del responsable según la ley
111 Deber de secreto o confidencialidad
114 «Tu información, tus reglas»: lo que toda persona debe saber sobre la transparencia en el uso de sus datos personales
119 ¿Por qué tu privacidad debería estar asegurada desde el inicio?
122 Cuidar los datos no es opcional: medidas de seguridad obligatorias
126 ¿Qué hacer cuando ocurre una vulneración de seguridad?
131 Medidas a la medida: cómo se ajustan los estándares de seguridad y transparencia en el tratamiento de datos

135 **Cómo ejercer tus derechos sobre tus datos**
135 Ejercicio ante el responsable de datos
136 Responsables de datos no constituidos en Chile
136 Mecanismos para ejercer los derechos
137 Gratuidad en el ejercicio de los derechos
138 Supervisión de la Agencia de Protección de Datos

138 Tus derechos en acción: paso a paso para ejercerlos
139 Presentación de la solicitud
144 Protegiendo tus datos: cómo reclamar si no se cumplen las reglas

157 **¿Pueden las instituciones públicas usar nuestros datos? ¿Cuándo?**
161 ¿Cómo deben usar tus datos los servicios públicos?
169 Ejercicio de los derechos del titular y procedimientos
172 Regulación especial para el tratamiento de datos sensibles en situaciones críticas
176 Tratamiento de datos sobre infracciones: reglas, límites y confidencialidad

179 **La Agencia de Protección de Datos Personales: una aliada en el cuidado de tu privacidad**
179 ¿Quién protege tus datos cuando estos se usan mal?
179 ¿Qué es la APDP?
180 ¿Cómo está organizada la APDP?

185 **Protección de datos en la Unión Europea**
186 ¿Quieres saber cómo se protegen tus datos en la Unión Europea?
186 ¿Por qué es importante proteger nuestros datos?
187 ¿Qué ley protege nuestros datos en la UE?
188 ¿Qué otras reglas complementan al RGPD?
188 ¿Qué pasa cuando nuestros datos se transfieren a otros países?
189 ¿Cómo nos afecta en la vida diaria?
189 Conclusión

193 **Conclusiones**

199 **Respuestas correctas**

209 **Bibliografía**

Introducción

En esta era, cada clic, cada búsqueda en línea, cada compra digital y cada imagen compartida deja una huella. Esa huella se compone de datos personales: fragmentos de nuestra identidad que, si bien parecen inofensivos, pueden ser utilizados —muchas veces lo son— con fines que van más allá de nuestro conocimiento o consentimiento. Frente a esta realidad, el derecho a la protección de datos personales ya no es un tema reservado a especialistas ni a grandes corporaciones. Es una necesidad cotidiana y un derecho fundamental de toda persona.

Protección de datos personales. Autonomía digital en la era de la información nace para convertirse en una herramienta de divulgación científica-jurídica accesible para todos. Está escrito en un lenguaje claro e incluye ejemplos prácticos, datos útiles, casos reales y secciones para aplicar lo aprendido. No se requiere formación jurídica para comprenderlo, pero sí interés por defender aquello que nos define como individuos: nuestra privacidad, nuestra información, nuestra autonomía.

Consideramos que este libro es urgente y necesario, ¿por qué? Porque en Chile, el acceso a Internet ha alcanzado cifras históricas. Según la Décima Encuesta de Acceso, Usos y Usuarios de Internet de 2023, un 94,3% de los hogares declara tener acceso a esta red y más del 50% de las zonas rurales declara estar conectado gracias a tecnologías móviles (Subtel, 1 de marzo de 2024). Internet se ha transformado en un servicio básico que habilita derechos como salud, educación y trabajo. Sin embargo, mientras crece el acceso, los

riesgos se incrementan. Cada conexión es una puerta abierta al tratamiento —y potencial abuso— de nuestros datos personales. Como consumidores digitales, estamos expuestos de manera permanente a ser objeto de vigilancia, segmentación y manipulación por parte de perfiles automatizados, muchas veces sin saberlo.[1]

Protección de datos personales se construye a partir del marco normativo que hoy regula la protección de datos personales en Chile: la Ley 19.628 sobre Protección de la Vida Privada, en su versión modificada por la Ley 21.719, cuya entrada en vigor está prevista para el 1 de diciembre de 2026.

La reforma introducida por esta segunda ley representa un cambio profundo en la forma en que se conciben y protegen los datos personales, pues incorpora nuevos derechos personales y mayores

1 En este sentido Pino (2025) quien señala en términos similares que: la protección de los datos personales —y, en particular, frente al tratamiento masivo de información— constituye una exigencia estructural del Estado Constitucional de Derecho cuando se pretende resguardar la democracia y la autonomía individual. El uso intensivo de datos por parte de actores tanto públicos como privados se configura como una herramienta de alto impacto político, capaz de incidir en la formación de la opinión pública, orientar decisiones de consumo y moldear conductas sociales, incluso en relación con la aceptación de determinados marcos morales. Si bien la regulación no elimina esta capacidad de influencia, sí contribuye a acotarla y, sobre todo, a hacerla visible, lo que resulta esencial frente a su tensión con los principios democráticos.

En este contexto, resulta clave comprender que la democracia se funda en la autonomía, la cual posee una dimensión simultáneamente individual y relacional. La autonomía implica la capacidad de autodeterminación, pero esta solo adquiere pleno sentido en interacción con otros, quienes pueden influir o interferir en las decisiones personales. Por ello, desde una perspectiva jurídica, la autonomía debe entenderse también como una cualidad que se define en función del grado de interferencia posible sobre cada individuo.

Así, las nociones de democracia, autonomía y Estado Constitucional de Derecho se articulan de manera estrecha, permitiendo una reflexión crítica y propositiva. El análisis busca evidenciar un riesgo que afecta tanto a la esfera individual como colectiva en materia de protección de datos, abordándolo desde una perspectiva política y democrática. Asimismo, pretende contribuir a relevar la relevancia de esta problemática y a ampliar los marcos de comprensión de quienes intervienen en su regulación y aplicación: juristas, diseñadores de políticas públicas, órganos jurisdiccionales y la ciudadanía en general.

responsabilidades para quienes recolectan, usan o almacenan información personal.

Este libro busca empoderarte. Que sepas que tus datos personales no son una moneda de cambio. Que no puedes —ni debes— entregarlos como si fueran el precio por usar una app, por acceder a una red social o por suscribirte a un servicio. Porque proteger tus datos es proteger tu libertad, tu dignidad y tu identidad.

En los capítulos que siguen, revisaremos los principales aspectos que todo ciudadano debe conocer:

* ¿Qué protege realmente la ley de datos personales?
* ¿A quién protege y en qué situaciones se aplica?
* ¿Cuáles son los principios que rigen su tratamiento?
* ¿Qué derechos tienes como titular de datos y cómo ejercerlos?
* ¿Qué obligaciones tienen quienes manejan tus datos?
* ¿Qué pasa con los consentimientos forzados o genéricos?
* ¿Cómo puedes actuar ante una filtración o mal uso de tu información?
* ¿Qué rol cumple la nueva Agencia de Protección de Datos Personales?
* ¿Cómo se regula este derecho en la Unión Europea y qué podemos aprender de ella?

Este recorrido busca informarte y ayudarte a tomar el control. Porque la brecha digital no se cierra solo con conectividad, sino también con educación y conciencia sobre nuestros derechos en el entorno digital. Porque ser ciudadano en la era de la información exige más que estar conectados: exige estar empoderados.

Bienvenidos a este viaje hacia la autonomía digital. Aquí empieza tu defensa informada de uno de los bienes más preciados del siglo XXI: tus datos personales.



¿Qué protege la ley? Descubriendo cómo y cuándo se aplican las reglas sobre datos personales

En Chile existe una ley que protege tu información personal y regula cómo esta puede ser utilizada. Se trata de la Ley de Protección de Datos Personales (LPDP), que garantiza que nadie puede usar tus datos sin cumplir ciertas reglas. Este derecho está reconocido en la Constitución en su artículo 19, N°4, el cual establece que todas las personas tienen derecho a la protección de su vida privada y de su información personal.[2]

¿Qué dice esta norma constitucional?

El artículo 19, N.° 4, de la Constitución Política de la República sostiene: El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos perso-

2 Contreras, Drago y Violler (2025: p. 3) señalan que: «En el año 2018, se consagró explícitamente en la Constitución el derecho a la protección de datos personales, también conocido como autodeterminación informativa. Fue incorporado por una reforma constitucional a través de la Ley 21.096». Como señalan los autores, apoyados en lo indicado por la jurisprudencia de Tribunal Constitucional STS, Roles N.° 1732 y N.° 1800 y por la doctrina (Banda (2000: pp. 55-70) y Nogueira (2005: pp. 449-479) antes de este reconocimiento expreso, el derecho a la protección de datos personales se había entendido como parte del contenido iusfundamentalmente protegido del derecho al respeto y protección de la vida privada, establecido en el artículo 19 N.° 4 de la Constitución.

nales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.[3]

En otras palabras, nuestra información no puede ser utilizada de cualquier forma; esta debe ser tratada de manera justa, transparente y respetuosa. En efecto, siguiendo a Donoso y Reusser[4] Si la protección de datos personales ha pasado a ser reconocida como un derecho fundamental, corresponde entonces precisar cuál es su alcance, quiénes pueden ejercerlo y sobre quiénes recaen los deberes correlativos. En cuanto a su contenido, este derecho se traduce en una facultad de control y disposición sobre los datos personales, que permite a cada persona decidir qué información entregar a terceros —ya sea al Estado o a particulares— y también determinar qué datos pueden ser recopilados por ellos. Del mismo modo, este derecho habilita al individuo para conocer quién posee sus datos y, en su caso, oponerse a su conservación o utilización.

Los titulares de este derecho son todas las personas naturales, sin distinción entre nacionales y extranjeras. Por su parte, los obligados son tanto personas naturales como personas jurídicas de derecho privado, así como también los órganos del Estado, siempre que realicen operaciones de tratamiento de datos personales.

---

3 Contreras (2020) señala que: Sin embargo, la reforma constitucional de 2018 marca un punto de inflexión al reconocer la autodeterminación informativa como un derecho fundamental autónomo, distinto —aunque relacionado— del derecho a la vida privada. Este reconocimiento no solo explicita una protección que antes se entendía implícita, sino que redefine el contenido del derecho, poniendo el acento en la capacidad de las personas para ejercer un control efectivo sobre sus datos personales, con independencia de que estos se encuentren en ámbitos más o menos privados.

En este sentido, la autodeterminación informativa se configura como el derecho de toda persona a decidir sobre la recopilación, uso, tratamiento y destino de su información personal, expresión directa del principio de dignidad humana y del libre desarrollo de la personalidad. Tal como lo destaca la doctrina constitucional y la experiencia comparada, este derecho busca evitar la instrumentalización de las personas mediante el tratamiento indiscriminado de sus datos, afirmando que la información personal pertenece a la esfera de control de su titular y no puede ser utilizada sin límites ni justificación jurídica suficiente.

4 Donoso y otros (2022).

Tratándose del Estado, sus deberes no se agotan en el mero respeto de las normas y principios en la materia. Además, debe adoptar todas las medidas necesarias para garantizar la vigencia efectiva de este derecho, lo que supone implementar disposiciones legislativas, reglamentarias y organizativas que hagan posible el ejercicio real de las facultades de control y disposición que corresponden a cada persona sobre su información personal.

En esa línea, y conforme a los estándares internacionales, la plena eficacia de este derecho constitucional no se alcanza únicamente mediante la dictación de leyes que reconozcan principios y derechos generalmente aceptados. También resulta indispensable establecer una autoridad independiente encargada de velar por su cumplimiento efectivo, junto con un sistema sancionatorio suficientemente disuasivo frente a la infracción de las reglas de protección de datos.

¿Por qué importa proteger tus datos personales? El propósito de la ley

En la era digital, tus datos personales son más valiosos que nunca. Información como tu nombre, dirección, historial médico o incluso tus preferencias en línea puede ser utilizada tanto para fines legítimos como para actividades no deseadas si no está adecuadamente protegida. Por eso, la Ley de Protección de Datos Personales establece reglas para garantizar que quienes manejan esta información lo hagan de manera responsable, respetando tu privacidad y tu derecho a decidir sobre tus propios datos.

Proteger tus datos personales no se trata solo de evitar que estos lleguen a las manos equivocadas. También significa asegurarte de que sean tratados de manera justa, transparente y con un propósito legítimo. La ley impone límites y obligaciones a las organizaciones que manejan esta información, asegurando que solo se use con tu consentimiento y que puedas acceder a ella para corregir, actualizar o eliminar lo que consideres necesario.

Este nuevo cuerpo legislativo regula todo el proceso de tratamiento de datos, desde su recolección hasta su almacenamiento, pasando por su uso, transmisión y eliminación. Lo que significa que cualquier entidad que maneje datos personales debe seguir

reglas claras y respetar los derechos de las personas a quienes pertenecen estos datos. No solo se protege la privacidad, sino que también se establecen límites y responsabilidades para quienes administran esta información.[5]

Pero ¿qué significa, exactamente, *tratamiento de datos personales*?[6] [7] Se refiere a toda acción que involucre datos personales, ya sea de forma manual o automatizada.

En un mundo donde la información se ha convertido en un recurso muy valioso, conocer y ejercer tus derechos sobre tus datos personales es clave para mantener tu privacidad y prevenir posibles riesgos.

---

5 Zaror (2025: p.117) señala en este sentido que: «El responsable debe desplegar un marco integral de gober-nanza de la información al interior de la compañía que combine una inversión adecuada en tecnología, capacitación de las personas e implementación de procesos. El primer asunto escapa del ámbito de este artículo, el segundo es parte de este proceso de divulgación y el tercero, los procesos, son aquellos actos que la organización tendrá que poner en marcha para el cumplimiento de las obligaciones que implica el tratamiento de datos personales.

Para hacer este abordaje hay distintos enfoques. El primero apunta a una implementación total, el segundo, a una implementación progresiva que permita implementar tareas inmediatas y urgentes. Lo cierto es que, sin perjuicio de la obligatoriedad de todas las reglas, cada empresa debe hacer una evaluación de sus capacidades humanas y económicas para hacer frente al desafío».

6 La Ley 19.628 sobre Protección de la Vida Privada (Chile), en su artículo 2 letra o), define el tratamiento de datos personales como cualquier operación o conjunto de operaciones o procedimientos técnicos, automatizados o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

7 La Ley 19.628 sobre Protección de la Vida Privada (Chile), en su artículo 2 letra o), define el tratamiento de datos personales como cualquier operación o conjunto de operaciones o procedimientos técnicos, automatizados o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

¿Quién tiene derecho a la protección de sus datos? Conociendo el alcance de la ley

Antes de entrar en los detalles técnicos, es importante entender cuándo y cómo esta ley entra en juego, pues su alcance define en qué situaciones tus datos personales están protegidos y qué deben hacer las personas o las empresas que los manejan para cumplir con ella.

En términos generales, esta ley aplica a todas las personas y empresas (tanto públicas como privadas) que manejan, en Chile, datos personales. Es decir, cualquier persona o entidad que recoja, almacene o utilice tu información debe seguir las reglas.

Sin embargo, existen algunas excepciones importantes a su ámbito de aplicación.

En primer lugar, no son aplicables sus normas al tratamiento de datos que efectúen las personas naturales en el marco de sus actividades personales o domésticas. Esto se refiere a situaciones de la vida privada, sin fines comerciales ni profesionales. Por ejemplo, si una persona guarda los números de teléfono de sus contactos en su teléfono celular, comparte fotos familiares por mensajería instantánea o mantiene una agenda personal con direcciones y cumpleaños, ese tratamiento de datos queda fuera del ámbito de la ley.

En segundo lugar, la ley tampoco se aplica al tratamiento de datos personales vinculado al ejercicio de la *libertad de expresión y de información*, derecho que se encuentra protegido por la Constitución. Esto incluye, por ejemplo, el trabajo periodístico y las actividades de los medios de comunicación. Así, un medio puede recopilar y difundir información sobre personas, incluidas figuras públicas, cuando ello tenga por finalidad informar u opinar.

No obstante, esta excepción *no es absoluta*. Si los mismos datos recopilados con fines informativos se utilizan posteriormente para otros objetivos, como publicidad, marketing o ventas, el tratamiento sí queda sujeto a la ley. Por ejemplo, si un medio de comunicación utiliza los datos obtenidos en un reportaje para elaborar bases de datos comerciales o para vender información a terceros, deberá cumplir con las exigencias legales, como contar con una base de licitud para ese uso.

Estas reglas buscan mantener un equilibrio entre la protección de la vida privada de las personas y el resguardo de derechos fundamentales como la libertad de expresión y de información.

Además, la ley también establece normas sobre su aplicación en diferentes situaciones geográficas. Se aplica en los siguientes casos:[8]

* cuando la persona o empresa que maneja los datos está ubicada en Chile,
* cuando el tratamiento de datos se realiza en nombre de una entidad establecida en Chile, aunque quien lo haga esté fuera del país, y
* cuando los datos se manejan fuera de Chile, pero afectan a personas que se encuentran en el país. Por ejemplo, cuando se ofrecen servicios a estas personas o se monitorea su comportamiento.

Este último punto es muy importante porque vivimos en un mundo globalizado y digital, donde las fronteras ya no son un límite. Esto significa que, si una empresa de otro país maneja tus datos y te afecta, aunque la empresa esté fuera de Chile tiene que cumplir con las reglas de la ley chilena.

Términos clave para entender la ley

Para comprender cómo funciona la Ley de Protección de Datos Personales, es importante conocer algunos términos básicos. Estos conceptos te ayudarán a entender mejor tus derechos y cómo se manejan tus datos:

* *Dato personal*:[9] cualquier información que permita identificarte, ya sea directamente (nombre o RUT) o indirectamente (dirección, correo electrónico o historial de compras). Con la expre-

8 Contreras y otros (2025: p. 24) distingue además el caso de la aplicación de la ley por disposición de un contrato o del derecho internacional. Esta regla de extraterritorialidad remite a otras fuentes del derecho que disponga la aplicación de la ley chilena. En primer lugar, el contrato puede fijar que se aplicará la ley chilena en materia de tratamientos de datos. En segundo lugar, reglas de derecho internacional, como tratados, acuerdos o convenciones.

9 La Ley 19.628 en su artículo 2 letra g), define a los datos personales sensibles, como aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

sión «cualquier información», el legislador quiere decir que el concepto *datos personales* debe entenderse en su sentido más amplio posible (Contreras y otros, 2025).

- *Datos personales sensibles:*[10] información privada y delicada como tu estado de salud, creencias religiosas, orientación sexual o antecedentes penales. Estos datos tienen una protección especial porque pueden afectar tu privacidad de manera significativa.
- *Responsable del tratamiento:* es la persona, empresa o entidad que decide cómo y por qué se usan tus datos personales. Es quien tiene la obligación de manejarlos de manera segura y respetando la ley.
- *Anonimización:* proceso irreversible en el que tu información personal se transforma de tal manera que nadie pueda identificarte. Una vez que un dato ha sido anonimizado, no se puede volver a relacionar contigo (Romeo, 2021).
- *Seudonimización:*[11] forma de proteger tus datos reemplazando tu identidad con un código o alias. A diferencia de la anonimización, aquí sí existe la posibilidad de volver a vincular la información contigo, pero solo si se tiene acceso a ciertos datos adicionales protegidos (Tosoni, 2020).

En este sentido, siguiendo la doctrina SCANIA,[12] un mismo dato puede estar seudonimizado para el responsable del tratamiento,

---

10 La ley 19.628 en su artículo 2 letra ñ) define al titular de datos o titular, como persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

11 La *doctrina SCANIA* se construye a partir de la jurisprudencia del Tribunal de Justicia de la Unión Europea, en particular del caso *Patrick Breyer vs. Bundesrepublik Deutschland* (asunto C-582/14), y del criterio de identificabilidad relativa desarrollado en el considerando 26 del Reglamento (UE) 2016/679 (RGPD), conforme al cual un dato puede constituir dato personal para un sujeto que dispone de medios razonables de identificación, pero no necesariamente para un tercero que carece de ellos.

12 La *doctrina SCANIA* se construye a partir de la jurisprudencia del Tribunal de Justicia de la Unión Europea, en particular del caso *Patrick Breyer vs. Bundesrepublik Deutschland* (asunto C-582/14), y del criterio de identificabilidad relativa desarrollado en el considerando 26 del Reglamento (UE) 2016/679 (RGPD), conforme al cual un dato puede constituir dato personal para un sujeto que dispone de medios razonables de identificación, pero no necesariamente para un tercero que carece de ellos.

quien conserva los medios para identificar a la persona y, al mismo tiempo, considerarse anonimizado para un tercero o encargado que no tiene acceso a esa información adicional.

Ahora bien, es importante tener presente que un dato seudonimizado sigue siendo un dato personal, por lo que su tratamiento debe cumplir con todos los principios y obligaciones establecidos en la Ley de Protección de Datos Personales. En cambio, los datos verdaderamente anonimizados, al no permitir la identificación directa ni indirecta de una persona, pueden ser tratados libremente, pues quedan fuera del ámbito de aplicación de la normativa de protección de datos.

¿Por qué esta ley es importante en tu día a día?

Vivimos en un mundo donde cada vez más actividades se realizan en línea: compras, redes sociales, trámites bancarios y hasta la inscripción en servicios básicos. En todas estas interacciones estás compartiendo tus datos personales, muchas veces sin darte cuenta.

La Ley de Protección de Datos Personales es clave porque establece reglas claras sobre cómo deben ser tratados estos datos, garantizando que se usen de manera segura y con respeto a tu privacidad.

Por ejemplo, las empresas que ofrecen servicios en línea deben cumplir con esta normativa, incluso si se ubican fuera de Chile, mientras manejen datos de personas que viven en el país. Esto significa que tienes derechos que puedes ejercer en cualquier momento, como solicitar que se eliminen o corrijan tus datos si no están siendo manejados correctamente.

Comprender esta ley no solo es importante para las empresas y las instituciones, sino para cualquier persona. Conocer tus derechos te permite tomar decisiones informadas sobre qué información compartes y cómo proteger tu privacidad en un mundo cada vez más digital.

Imagina que te registras en una tienda *online* para comprar un producto y, sin darte cuenta, la empresa comparte tu información con terceros sin tu consentimiento. De repente empiezas a recibir correos, llamadas y mensajes promocionales de otras empresas con las que nunca tuviste contacto.

Pues bien, gracias a la Ley de Protección de Datos Personales puedes exigir que la empresa elimine tu información, deje de compartirla sin autorización y, en algunos casos, incluso podrías presentar una denuncia si hubo un uso indebido de ella.

Este tipo de situaciones ocurren a diario. Hoy, la existencia de esta ley garantiza que puedas tener control sobre tu información y decidir quién puede utilizarla y para qué.

Entender la ley es el primer paso para protegerte

Esta ley de protección de datos busca establecer un equilibrio entre el avance tecnológico, las necesidades comerciales y el derecho de las personas a la privacidad. Conocer su alcance y aplicación es clave para garantizar que nuestros datos sean tratados de forma segura y responsable, ya sea por empresas, instituciones públicas o cualquier otra organización que los utilice en su actividad cotidiana.



Caso práctico

Una empresa de marketing digital en España ofrece sus servicios a clientes en Chile. Esta empresa recopila datos personales de usuarios chilenos para crear campañas personalizadas.

¿Debe esta empresa cumplir con la ley chilena de protección de datos personales, a pesar de estar ubicada fuera de Chile? ¿Por qué? Fundamente su respuesta en la normativa legal aplicable.



Apliquemos lo aprendido

1. ¿Cuál es el objeto principal de la Ley de Protección de Datos Personales en Chile?

a. Regular el comercio electrónico

b. Regular la protección y el tratamiento de datos personales

c. Regular las telecomunicaciones

2. ¿Qué implica el *ámbito de aplicación territorial* de la ley?

a. Que la ley solo se aplica en Santiago

b. Que la ley solo se aplica dentro del territorio nacional, sin excepciones

c. Que la ley se aplica a cualquier tratamiento de datos personales que afecte a titulares en Chile, incluso si se realiza fuera del país

3. ¿Cuál de los siguientes es un ejemplo de dato personal?

a. El clima de una ciudad

b. El número de cédula de identidad de una persona

c. El nombre de una empresa

4. ¿Qué es la *anonimización* de datos personales?

a. Proceso de destrucción del vínculo entre el dato y el titular

b. Proceso de encriptar datos personales

c. Proceso de compartir datos personales de forma anónima

5. ¿Qué entidad es responsable de decidir sobre los fines y medios del tratamiento de datos personales?

a. El titular de los datos

b. El encargado de los datos

c. El responsable del tratamiento

¿A quién protege esta ley? Objeto y alcance de la protección de datos personales

El artículo 1 nos señala que la presente ley tiene por objeto regular la forma y las condiciones en las que se efectúa el tratamiento y la protección de los datos personales de personas naturales, en conformidad al artículo 19, N.° 4, de la Constitución Política.

Todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos[13], debe respetar los derechos y libertades de las personas y quedará sujeto a las disposiciones de esta ley.

13 Como señala Abusleme (2025) hasta antes de la reforma la inexistencia de normas precisas para el tratamiento de datos personales, junto con la carencia de una adecuada estructura de gobernanza en esta materia, ha dado lugar a zonas de incertidumbre y vacíos interpretativos. Frente a ello, los órganos públicos han procurado suplir estas deficiencias mediante la suscripción de convenios de colaboración, la elaboración de protocolos, la emisión de oficios y, en términos generales, a través de un incremento de la burocracia. Este escenario ha operado como un obstáculo histórico para avanzar hacia un Estado verdaderamente interoperable.

No obstante, el nuevo marco normativo introduce una mejora sustantiva al dotar al sector público de herramientas jurídicas más definidas, lo que debiera permitir un flujo de datos más seguro. Ello, a su vez, facilita la optimización de los servicios dirigidos a la ciudadanía, fortalece la eficiencia y eficacia en la gestión pública, y posibilita el diseño, implementación y evaluación de políticas públicas sustentadas en el uso de datos e información.

El régimen de tratamiento y protección de datos establecidos en esta ley no se aplicará al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19, N.° 12, de la Constitución Política de la República. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a opinar e informar.

¿Se aplica esta ley fuera de Chile? Alcance territorial de la protección de datos

Conforme el artículo 1 bis las disposiciones de la presente ley se aplicarán al tratamiento de datos personales que se realice bajo cualquiera de las siguientes circunstancias:

* Cuando el responsable o mandatario esté establecido o constituido en territorio nacional.
* Cuando el mandatario, con independencia de su lugar de establecimiento o constitución, realice las operaciones de tratamiento de datos personales a nombre de un responsable establecido o constituido en territorio nacional.
* Cuando el responsable o mandatario no se encuentren establecidos en el territorio nacional pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a titulares que se encuentren en Chile, independientemente de si a estos se les requiere un pago, o a monitorear el comportamiento de titulares que se encuentran en territorio nacional, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento.

La presente ley también se aplicará al tratamiento de datos personales que sea realizado por un responsable al que, no estando establecido en territorio nacional, le resulte aplicable la legislación nacional a causa de un contrato o del derecho internacional.

¿Qué significa todo esto? Glosario básico para entender la Ley de Protección de Datos Personales

El artículo 2 señala que, para los efectos de esta ley, se entenderá por:

* *Almacenamiento de datos:* conservación o custodia de datos en un registro o base de datos.
* *Bloqueo de datos:* suspensión temporal de cualquier operación de tratamiento de los datos almacenados.
* *Comunicación de datos personales:* dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos.
* *Dato caduco:* dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.
* *Dato personal:* cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Para determinar si una persona es identificable deberán considerarse todos los medios y factores objetivos que razonablemente se podrían usar para dicha identificación en el momento del tratamiento.
* *Datos personales sensibles:* tendrán esta condición aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad que revelen el origen étnico-racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud y al perfil biológico humano,

los datos biométricos[14], y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

- *Eliminación o cancelación de datos:* destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
- *Fuentes de acceso público:* todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley. El tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de esta ley.
- *Organismos públicos:* autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política de la República y aquellos comprendidos en el inciso segundo del artículo 1 de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- *Anonimización:* procedimiento irreversible en virtud del cual un dato personal no puede vincularse o asociarse a una persona determinada ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.
- *Seudonimización:* tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y or-

14 Para entender este tipo de datos revisar lo señalado por Maulén (2025) quien indica que en general provienen de servicios de seguridad, defensa y servicios de inteligencia. Son cantidades de datos generados por lectores biométricos como escáneres de retina, escáneres de huellas digitales, o lectores de cada de ADN. El propósito de estos datos es proporcionar mecanismos de seguridad y suelen estar custodiados por los ministerios de defensa y departamentos de inteligencia.

ganizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.

* *Base de datos personales:* conjunto organizado de datos personales, cualquiera sea la finalidad, forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar su tratamiento.
* *Responsable de datos o responsable:* toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.
* *Titular de datos o titular:* persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.
* *Tratamiento de datos:* cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.
* *Consentimiento:* toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada a través de una declaración o una clara acción afirmativa, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen.
* *Derecho de acceso:* derecho del titular de datos a solicitar y obtener del responsable, confirmación acerca de si sus datos personales están siendo tratados por él, acceder a ellos en su caso y a la información prevista en esta ley.
* *Derecho de rectificación:* derecho del titular de datos a solicitar y obtener del responsable, que modifique o complete sus datos personales cuando están siendo tratados por él y sean inexactos, desactualizados o incompletos.
* *Derecho de supresión:* derecho del titular de datos a solicitar y obtener del responsable, que suprima o elimine sus datos personales, de acuerdo con las causales previstas en la ley.
* *Derecho de oposición:* derecho del titular de datos a solicitar y obtener del responsable, que no se lleve a cabo un tratamiento de

datos determinado, de conformidad a las causales previstas en la ley.

* *Derecho a la portabilidad de los datos personales:* derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos. El titular tendrá derecho a que sus datos personales se transmitan directamente de responsable a responsable cuando sea posible según criterios técnicos.
* *Cesión de datos personales:* transferencia de datos personales por parte del responsable de datos a otro responsable de datos.
* *Elaboración de perfiles:* toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural.
* *Tercero mandatario o encargado:* persona natural o jurídica que trata datos personales por cuenta del responsable de datos.[15]
* *Agencia:* la Agencia de Protección de Datos Personales.
* *Registro Nacional de Sanciones y Cumplimiento:* registro nacional de carácter público administrado por la Agencia que consigna los modelos certificados de prevención, los responsables de datos que los hayan adoptado y las sanciones que se hayan impuesto a los responsables de datos que hayan infringido la ley.

15 Una vez que una entidad es reconocida como «encargado del tratamiento», se le aplican las disposiciones de responsabilidad contenidas en el artículo 15 bis, que regula el tratamiento de datos personales realizado por un tercero en calidad de mandatario o encargado. Estas reglas exigen la existencia de un contrato entre el responsable del tratamiento y el encargado. Asimismo, el encargado queda sujeto a obligaciones específicas, como el deber de confidencialidad o secreto (artículo 14 bis), la implementación de medidas de seguridad adecuadas (artículo 14 quinquies) y el cumplimiento de los distintos niveles de seguridad según lo indicado en el inciso primero del artículo 14 septies.



Apliquemos lo aprendido

1. ¿Qué se entiende por dato personal según esta ley?

a. Cualquier información que identifique a una empresa

b. Información vinculada a una persona natural identificada o identificable

c. Datos estadísticos sin nombre asociado

2. ¿Qué diferencia a un dato personal sensible de uno común?

a. Su uso solo está permitido en redes sociales

b. Se refiere a opiniones personales sin valor legal

c. Corresponde a categorías específicas de datos definidas expresamente por la ley, como datos de salud, biométricos u opiniones políticas

3. ¿Qué significa anonimización?

a. Proteger los datos con contraseña

b. Usar los datos para hacer publicidad

c. Hacer que un dato ya no pueda asociarse a una persona

4. ¿Con qué derecho cuenta una persona para saber si una empresa está usando sus datos?

a. Derecho a la portabilidad

b. Derecho de oposición

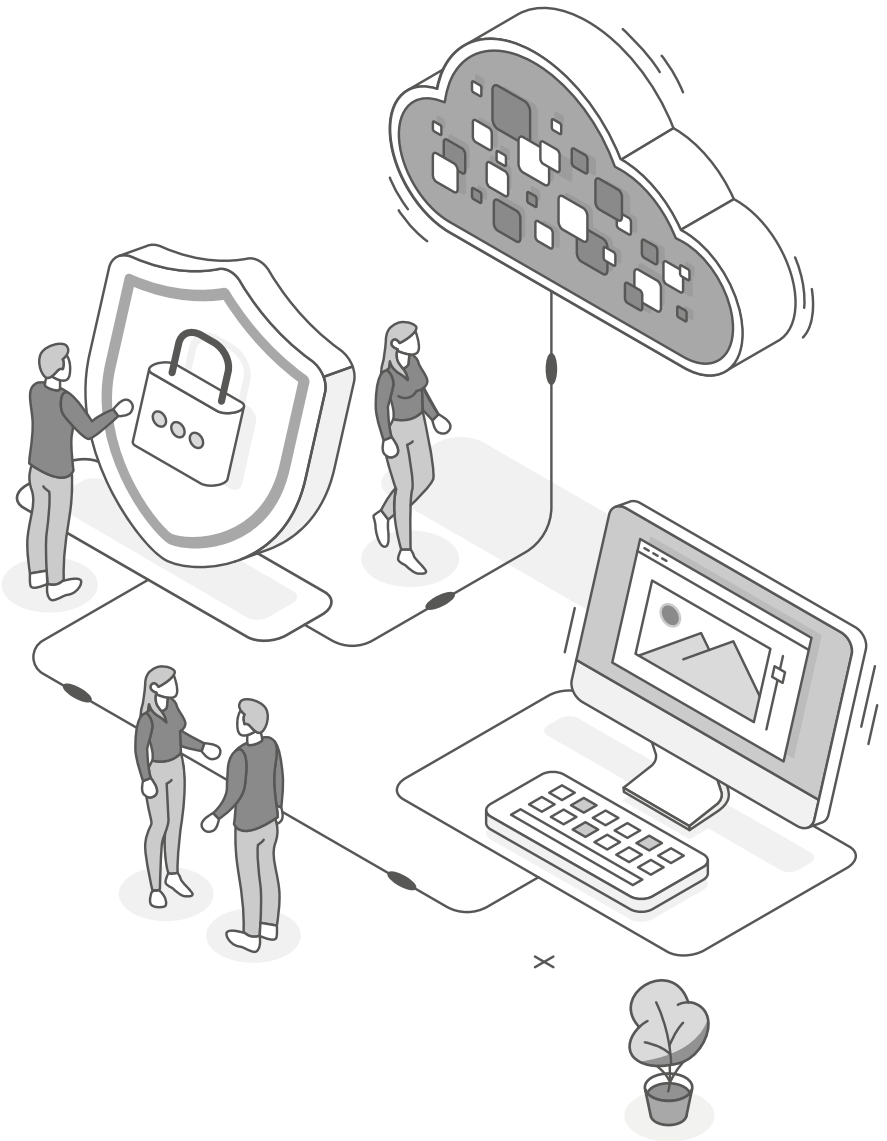
c. Derecho de acceso

5. ¿Qué se entiende por comunicación de datos personales?

a. Es lo mismo que la cesión de datos

b. El tratamiento automatizado de datos sin informar al titular

c. Dar a conocer datos a un tercero sin transferirlos o cederlos formalmente



Protegiendo tu información: principios claves y ejemplos prácticos

En la era digital, proteger nuestra información personal es más importante que nunca. Cada vez que compartimos datos en línea, ya sea al hacer compras, registrarnos en un sitio *web* o incluso al interactuar en redes sociales, estamos exponiendo información que puede ser valiosa o sensible. Por eso, es fundamental conocer los principios que guían la protección de nuestros datos, tal como lo establece la ley.

Como señala Garrido y Sáenz (2025: p 23) «La regulación de la protección de datos personales está compuesta de una serie de principios informadores que constituyen verdaderas reglas para el tratamiento de los datos personales. A diferencia de otras materias, donde los principios pueden resultar definiciones abstractas, en materia de protección de datos los principios son claros y relativamente pacíficos, al no existir interpretaciones demasiado disímiles en legislaciones compara-das. Podríamos afirmar que los principios en materia de protección de datos constituyen el espíritu de la normativa, que colabora en la interpretación de la misma en sede especializada, pero con un contenido claro y específico».

En este capítulo, exploraremos de manera sencilla y clara los principios claves que te ayudarán a entender cómo se deben manejar tus datos personales. También revisaremos ejemplos prácticos para que puedas aplicar estos conocimientos en tu vida diaria y proteger tu privacidad de manera efectiva.

¿Cuáles son estos principios fundamentales?

Estos principios se encuentran regulados en el artículo 3:

Principios de licitud y lealtad

Los datos personales solo pueden tratarse de manera lícita y leal. El responsable deberá ser capaz de acreditar la licitud del tratamiento de datos personales que realiza.[16]

Explicación: este principio establece que los datos personales deben manejarse de manera legal y justa. En términos simples, esto significa que todo tratamiento de datos debe estar amparado en una base legal de licitud. La más conocida es el consentimiento de la persona titular de los datos, pero no es la única. La ley también permite tratar datos personales sin consentimiento en ciertos casos, como cuando el tratamiento es necesario para cumplir una obligación legal, ejecutar un contrato, proteger intereses vitales de la persona o cuando existe un interés legítimo debidamente justificado, entre otros supuestos previstos por la ley.

Además, el principio de lealtad implica que los datos no pueden obtenerse ni utilizarse de forma engañosa o desleal. Las personas deben saber cómo y por qué se usan sus datos, mientras que el responsable debe actuar de manera transparente y ser capaz de demostrar que cumple con todas las reglas establecidas por la normativa de protección de datos.

Ejemplo: imagina que una empresa de marketing digital quiere enviar promociones por correo electrónico. Para hacerlo de manera correcta, debe contar con una base legal que autorice ese tratamiento de datos. En muchos casos, esto implicará que las personas hayan otorgado un consentimiento previo, libre, informado y voluntario para recibir ese tipo de comunicaciones.

Sin embargo, dependiendo de las circunstancias, la ley puede permitir el envío de comunicaciones comerciales sobre la base de otra base de licitud, como la existencia de una relación contractual previa o un interés legítimo debidamente justificado, siempre que se

16 Como señala De Terwangne (2020), el principio de licitud no es otra cosa que establecer que el tratamiento de datos personales debe realizarse cumpliendo con todos los requisitos establecidos en la Constitución y las leyes. En este mismo sentido Troncoso (2021).

respeten los derechos de las personas y se les otorgue la posibilidad de oponerse.

En cualquier caso, la empresa no puede utilizar esos correos electrónicos para fines distintos de aquellos que justificaron su obtención, como venderlos a terceros o enviar publicidad no relacionada. De este modo, se respeta el principio de licitud y lealtad, asegurando que la información de las personas se utilice de forma justa y transparente.

Principio de finalidad

Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. Su tratamiento debe limitarse al cumplimiento de estos fines. En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; que exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta, siempre que se enmarque dentro de los fines del contrato o sea coherente con las tratativas o negociaciones previas a su celebración; que el titular otorgue nuevamente su consentimiento, y cuando lo disponga la ley.[17]

Explicación: significa que los datos personales solo pueden ser recopilados y usados para un propósito específico, legítimo y claramente informado desde el inicio. Además, no se pueden utilizar para otros fines sin el consentimiento del titular, a menos que la ley lo permita o que el nuevo uso sea compatible con el propósito original.

Ejemplo: un hospital recopila datos de salud de sus pacientes para ofrecer un diagnóstico médico. No podría, sin el consentimiento del paciente, utilizar esos datos para fines comerciales, como vender productos de salud.

---

17 En Chile, este principio es considerado en el ámbito financiero. En este sentido señala Bozzo (2020: p. 111) que «La Ley 20.575 tuvo como objetivo establecer el principio de finalidad en el tratamiento de datos personales. De esta manera, se busca otorgar protección a las personas, evitando que sus antecedentes comerciales sean utilizados para un fin distinto que el de la evaluación de riesgo en el proceso de otorgamiento de un crédito». También Reyes (2016).

Principio de proporcionalidad

Según la ley, los datos personales que se traten deben limitarse estrictamente a aquellos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.[18] Además, estos pueden ser conservados por el periodo de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley. Un lapso mayor requiere autorización legal o consentimiento del titular.

Explicación: este principio establece que los datos personales que se recojan deben ser estrictamente los necesarios, adecuados y pertinentes para cumplir con los fines específicos para los cuales fueron recolectados. En otras palabras, no se deben pedir ni tratar más datos de los que realmente se necesitan para cumplir con ese propósito.

Además, los datos personales solo pueden ser guardados por el tiempo que sea necesario para cumplir con esos fines. Una vez cumplido el objetivo, los datos deben ser eliminados o anonimizados. Sin embargo, si la ley establece excepciones o si el titular de los datos otorga su consentimiento para un uso adicional, los datos podrían conservarse por más tiempo.

Ejemplo: imagina que un banco te pide tu número de teléfono y tu dirección para gestionar tu cuenta y enviarte información importante. Eso tiene sentido, ya que esos datos son necesarios para la comunicación. Pero si el banco te pidiera cosas como tus preferencias alimentarias, eso no tendría sentido, ya que no tiene nada que ver con la gestión de tu cuenta bancaria. El banco solo debería pedir la información que realmente necesita para el propósito específico de sus servicios.

Principio de calidad

Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.[19]

---

18 Este principio se encuentra consagrado en la Ley 19.628, modificada por la Ley 21.719.

19 Anguita (2007).

Explicación: este principio establece que los datos personales deben ser exactos, completos, actuales y pertinentes para los fines específicos para los cuales se recogen, lo que significa que, si una empresa recopila datos de una persona, debe asegurarse de que esos datos sean precisos y estén actualizados. Además, los datos deben ser relevantes y apropiados para el propósito que se persigue.

Ejemplo: una universidad cuenta con los datos de contacto de sus estudiantes. Si un estudiante actualiza su dirección, la universidad debe corregir estos datos en sus sistemas para asegurarse de que las comunicaciones lleguen al lugar correcto.

Principio de responsabilidad

Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios contenidos en este artículo, también de las obligaciones y deberes de conformidad a la ley.

Explicación: este principio establece que las personas o entidades que tratan datos personales responden legalmente por el incumplimiento de la ley. En otras palabras, si el tratamiento de datos no respeta los principios, deberes u obligaciones legales, el responsable deberá asumir las consecuencias jurídicas que correspondan.

No se trata de un deber general de demostrar de forma permanente que se cumple la ley, sino de una regla que atribuye responsabilidad jurídica a quien realiza el tratamiento cuando se produce una infracción a la normativa de protección de datos.

Ejemplo: si una empresa trata datos personales sin respetar las reglas legales, por ejemplo, sin contar con una base de licitud o vulnerando los derechos de las personas, será responsable de ese incumplimiento y podrá enfrentar las sanciones que establezca la ley.

Principio de seguridad

En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser

apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.[20]

Explicación: este principio establece que quienes tratan datos personales deben adoptar medidas de seguridad técnicas y organizativas adecuadas para protegerlos frente a accesos no autorizados, pérdida, filtración, daño accidental o destrucción. Estas medidas no son genéricas, sino que deben definirse considerando el tipo de tratamiento que se realiza, la naturaleza de los datos y el nivel de riesgo que dicho tratamiento implica.

Además, este principio se vincula directamente con la obligación legal del responsable del tratamiento de implementar medidas de seguridad acordes con el estado de la técnica, lo que implica utilizar soluciones actualizadas y razonables según el desarrollo tecnológico disponible, sin exigir estándares imposibles, pero sí adecuados y eficaces.

En términos simples, es como poner a los datos una cerradura fuerte, junto a reglas claras sobre quién puede acceder a ellos y cómo deben manejarse, asegurando que la protección sea efectiva y proporcional a la importancia de la información tratada.

Ejemplo: una clínica médica utiliza sistemas encriptados para almacenar los historiales médicos de sus pacientes, garantizando que solo el personal autorizado pueda acceder a esta información sensible.

Principio de transparencia e información

El responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece esta ley, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales, las que además deberán estar accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.[21] El responsable debe adoptar las medidas adecuadas y

20 Como señalan Contreras y otros (2025: p. 55), «La reforma a la Ley 19.628 incluyó expresamente un principio de seguridad, a diferencia del texto original de la ley, en donde existían escasas referencias y medidas de seguridad de la información».

21 El Reglamento General de Protección de Datos (GDPR) establece el principio de transparencia en su artículo 5(1)(a). Luego, este se desarrolla más específicamente en los artículos 12 al 14, que describen las obligaciones del responsable del tratamiento. Además,

oportunas para facilitar al titular el acceso a toda la información que señala esta ley, así como cualquier otra comunicación relativa al tratamiento que realiza.

Explicación: este principio asegura que quienes manejan datos personales sean completamente transparentes con las personas a quienes pertenecen esos datos. Deben proporcionarles toda la información necesaria sobre cómo se usan sus datos, de manera clara y fácil de entender. Esto incluye detalles como las políticas de privacidad y cualquier otra práctica relacionada con su tratamiento. Además, toda esta información debe estar disponible para que las personas puedan acceder a ella en cualquier momento, de forma gratuita y sin complicaciones, para que puedan ejercer sus derechos de manera informada.

Ejemplo: cuando compras algo en un sitio *web*, este debe explicarte claramente cómo usará tu información. Por ejemplo, debe contarte qué datos recopila (como tu nombre o dirección de envío) y para qué los necesitan (enviarte tu pedido). Esta información debe estar escrita en una política de privacidad que sea fácil de leer y que puedas encontrar fácilmente en el sitio *web*.

Principio de confidencialidad:

El responsable de datos personales y quienes tengan acceso a ellos deberán guardar confidencialidad acerca de estos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.[22]

Explicación: las personas que tienen acceso a tus datos deben tratarlos con total privacidad. Esto significa que no pueden compar-

el considerando 39 del reglamento detalla el sentido y alcance de este principio.

22 Como señalan Contreras y otros (2025: p. 58), «Este principio impone un estándar de diligencia y cuidado al responsable del tratamiento de datos personales. La confidencialidad tiene por objeto proteger los datos contra el acceso no autorizado y contra el tratamiento no autorizado. Por lo tanto, el responsable del tratamiento también debe aplicar medidas técnicas y organizativas para garantizar que los datos personales no se divulguen, se pirateen o se pierdan. La confidencialidad busca excluir que personas no autorizadas tengan acceso a los datos y se extiende después de concluida la relación con el titular de los datos».

tirlos con nadie ni usarlos de manera inapropiada. Incluso si ya no estás en contacto con ellos, siguen siendo responsables de mantener la confidencialidad de tu información.

Ejemplo: imagina que un contador tiene acceso a tus datos financieros. Aunque ya no trabajes con él, sigue siendo su obligación mantener en secreto toda la información a la que tuvo acceso, como si fuera un compromiso que nunca termina.



Casos prácticos

☛ Principio de licitud y lealtad

Una empresa que desarrolla aplicaciones móviles está creando una nueva app que recopila datos sobre la ubicación de los usuarios para ofrecerles recomendaciones personalizadas. Sin embargo, la empresa decide usar esta información para hacer un análisis de mercado y vender los resultados a otras empresas, sin informar a los usuarios ni pedirles permiso.

¿Está la empresa cumpliendo con las reglas sobre el uso de datos personales?

☛ Principio de licitud y lealtad

Una aplicación de *fitness* recopila información sobre los hábitos de ejercicio y la salud de sus usuarios para personalizar las recomendaciones. Sin embargo, en su política de privacidad solo menciona que los datos se usan para mejorar la experiencia del usuario, pero no explica con suficiente claridad si esos datos también se usarán para compartirlos con socios comerciales o para otros fines. Además, la política de privacidad no está fácilmente accesible dentro de la aplicación.

¿Está la aplicación cumpliendo con el principio de transparencia e información sobre el uso de los datos personales?



Apliquemos lo aprendido

1. ¿Qué establece el principio de licitud y lealtad en el tratamiento de datos personales?

a. Que los datos pueden ser tratados de cualquier manera siempre que beneficien a la empresa

b. Que los datos personales deben ser tratados de manera lícita y leal, respetando la normativa vigente

c. Que los datos personales deben ser compartidos entre todas las empresas de un mismo sector

2. ¿Qué implica el principio de finalidad en el tratamiento de datos?

a. Que los datos pueden ser usados para cualquier propósito después de su recolección

b. Que los datos deben recolectarse para fines específicos, explícitos y legítimos, y que no deben usarse para otros fines sin consentimiento

c. Que los datos personales no deben ser eliminados nunca

3. Según el principio de proporcionalidad, los datos personales deben ser:

a. Lo más completos posibles, sin importar su relevancia

b. Limitados a lo que es necesario, adecuado y pertinente para el propósito del tratamiento

c. Almacenados indefinidamente para cualquier uso futuro

4. El principio de seguridad en el tratamiento de datos personales se refiere a:

a. Hacer copias de seguridad de los datos en una nube pública

b. Implementar medidas adecuadas para proteger los datos contra accesos no autorizados y daños

c. Compartir datos personales solo en redes seguras



Apliquemos lo aprendido

5. El principio de transparencia e información exige que:

a. El responsable mantenga en secreto cómo se tratan los datos

b. Se proporcione al titular de los datos información clara y accesible sobre el tratamiento de sus datos

c. Los datos personales sean tratados únicamente por el titular

Tu permiso importa. Entendiendo el consentimiento en el uso de datos personales

¿Sabías que cada vez que compartes tu correo en un sitio *web* o aceptas los términos de una app, estás autorizando que tus datos personales sean usados?

En Chile, la regla general es clara: tus datos solo pueden ser tratados si tú lo autorizas. Ese permiso se llama *consentimiento*.

Esto significa que el consentimiento es la base principal que permite a una empresa, institución o persona utilizar tu información personal. Solo en casos específicos establecidos por la ley se puede tratar datos sin tu autorización.

Pero ese permiso no puede pedirse de cualquier manera. La ley exige que sea:

* libre,
* informado,
* específico respecto de su finalidad y
* otorgado de forma previa e inequívoca.

En esta sección te explicamos, de manera simple y con ejemplos cotidianos, qué significa realmente dar consentimiento, cuándo es válido y cuándo… no lo es.

Consentimiento libre, informado y específico

Consentimiento libre

Para que tu consentimiento sea válido, debes darlo *voluntariamente*, sin que nadie te obligue ni te engañe. También es clave que sepas exactamente para qué se van a usar tus datos. No basta con que aceptes «términos y condiciones» sin leer: te deben decir con claridad qué harán con tu información y con qué fin.

Ejemplo: imagina que compras ropa en una tienda *online*. Al registrarte, te preguntan si pueden enviarte promociones a tu correo. Te explican qué tipo de promociones recibirás y con qué frecuencia. Solo si tú aceptas explícitamente, estarán cumpliendo con esta regla.

¿Qué pasa con el consentimiento cuando firmamos un contrato?

Cuando aceptamos un contrato o usamos un servicio, a veces nos piden autorizar el uso de nuestros datos personales. Pero no siempre ese consentimiento es válido, sobre todo si sentimos que nos obligan a darlo para poder acceder al servicio.

La ley chilena dice que se presume que ese consentimiento no es libre si el uso de los datos no es necesario para cumplir el contrato. En otras palabras: si la empresa no necesita realmente esos datos para prestarte el servicio, no puede aprovechar ese momento para pedir tu consentimiento y usar tus datos con otros fines.



¿Sabías que puedes revocar tu consentimiento en cualquier momento, incluso si firmaste un contrato?
Siempre que el uso de tus datos no sea indispensable para el servicio contratado, tienes derecho a decir «ya no quiero» y que dejen de usar tus datos para esa finalidad. ¡No necesitas dar explicaciones!



Siempre revisa si la empresa te da la opción de *aceptar solo lo necesario para que funcione el servicio*. Si no puedes usarlo a menos que aceptes todo (incluido el uso de tus datos con fines publicitarios, por ejemplo), puede que estén abusando de tu consentimiento. En tal caso puedes reclamar ante la Agencia de Protección de Datos Personales.

Por ejemplo, si contratas un curso *online* y la empresa te pide acceso a tu ubicación o contactos, algo que no tiene nada que ver con el curso, eso sería forzarte a aceptar condiciones que no corresponden.

Esto evita lo que se llama «atar el consentimiento al contrato», es decir, hacerte creer que, si no aceptas que usen tus datos, no podrás acceder al servicio. La ley busca protegerte de esa práctica injusta.

Además, se aclara que el consentimiento y el contrato son cosas distintas, por lo tanto, no pueden mezclarse. Si una empresa quiere tus datos para algo que no es esencial al servicio, tiene que pedirte el permiso por separado. De la misma forma, tú puedes decidir con libertad (Rodríguez, 2023: p. 56).

Existe una excepción: cuando un servicio es gratis y lo único que la empresa pide a cambio es tu consentimiento para usar tus datos. Por ejemplo, una aplicación gratuita que funciona gracias a la información que recolecta de sus usuarios. En ese caso sí se permite que el consentimiento sea parte del trato, porque es la forma en que la empresa "cobra" por el servicio.

Consentimiento informado

Cuando una empresa, colegio, aplicación o servicio quiere usar tus datos personales, no basta con que te pida permiso: ese permiso debe ser informado. Es decir, debes saber claramente qué estás autorizando.

Esto significa que no puedes dar un consentimiento si no entiendes qué van a hacer con tus datos. Para que el consentimiento sea realmente informado, la ley exige que se te entregue, al menos, estos datos básicos:

* Quién es el responsable del tratamiento de tus datos (por ejemplo, el nombre de la empresa o institución).
* Para qué quiere usar tus datos (finalidad del tratamiento).
* Qué tipo de datos va a tratar (nombre, correo, ubicación, huella, etc.).
* Que tienes derecho a retirar tu consentimiento cuando quieras.
* Si habrá o no decisiones automáticas con tus datos, como sistemas de inteligencia artificial que tomen decisiones sin intervención humana.

Toda esta información debe estar escrita de forma clara y fácil de entender. Nada de «letra chica» ni lenguaje enredado.

Además, la ley exige que puedas dar o quitar tu consentimiento de forma rápida, confiable, gratuita y cuando quieras. Puedes hacerlo por escrito, en papel o en formato digital (por ejemplo, una opción dentro de una app o sitio *web*).

Ejemplo: Descargas una app para hacer ejercicio. Antes de empezar, te pide permiso para usar tu nombre, tu edad y tu ubicación para sugerirte rutinas. Pero también te pide acceso a tus contactos



Antes de aceptar, busca una sección llamada Política de Privacidad o Términos y Condiciones. Si no entiendes lo que dice o no se presenta una forma clara de revocar tu consentimiento, mejor no lo entregues. Estás en tu derecho de pedir que te lo expliquen de forma clara.

y fotos. Si no te explican por qué quieren esa información ni qué harán con ella, no es un consentimiento informado. Tampoco lo es si no puedes retirar ese permiso más adelante.

Consentimiento específico en cuanto a su finalidad

Cuando te piden permiso para usar tus datos personales, no basta con que digas «sí» de forma general. Para que ese consentimiento sea válido, debes saber exactamente para qué se usarán tus datos. Es decir, la empresa o institución debe decirte claramente cuál es el objetivo del tratamiento. Esto se llama *finalidad del tratamiento* y es clave para proteger tu derecho a decidir qué se hace con tu información. La ley chilena exige que:

* el uso de tus datos sea legal y justo (principio de licitud y lealtad),
* te digan específicamente para qué usarán tus datos (principio de finalidad) y
* no te mezclen cosas: deben separar el consentimiento para usar tus datos del consentimiento para aceptar los términos y condiciones del servicio.

Por ejemplo, no pueden pedirte que aceptes todo en un solo clic sin explicarte si usarán tus datos para enviarte publicidad, compartirlos con terceros o entrenar sistemas de inteligencia artificial.



Antes de aceptar cualquier consentimiento, fíjate si puedes elegir entre distintos usos de tus datos. Si no hay opción y todo viene «amarrado», es probable que estén tratando de que aceptes más de lo que deberías. ¡Tienes derecho a decidir por separado cada finalidad!



Caso práctico

Te inscribes en una tienda *online* para comprar ropa. Al registrarte, aparece un mensaje que dice: «Al crear esta cuenta, aceptas los términos y autorizas el uso de tus datos personales». Sin embargo, no se explica qué datos, ni para qué fines, ni con quién los compartirán.

Este consentimiento no es válido porque es genérico. Tú no sabes qué estás permitiendo realmente.

En cambio, si te dicen:

- vamos a usar tu nombre y correo para enviarte actualizaciones de tu pedido;
- con tu permiso, también podemos enviarte promociones, y
- puedes aceptar solo lo primero y rechazar lo segundo.

Entonces sí estás ante un consentimiento válido y específico.

Consentimiento previo e inequívoco

Para que alguien use tus datos, debe contar con tu permiso. Y ese permiso debe ser *claro e inequívoco*, es decir, no debe dejar dudas sobre tu intención.

Previo significa justamente eso: el consentimiento debe otorgarse antes de que se inicie el tratamiento de los datos. Una empresa no puede usar tu información primero y pedirte autorización después para «regularizar» la situación. El consentimiento no legitima tratamientos realizados con anterioridad.

Puedes darlo de forma verbal, por escrito, haciendo clic en una casilla o usando algún otro medio que refleje tu voluntad.



Caso práctico

En un formulario *online*, hay una casilla vacía que dice «Quiero recibir el boletín». Si tú la marcas, estás dando un consentimiento claro y previo. Pero si la casilla ya viene marcada por defecto, eso *no* se considera válido.

Tampoco sería válido que la empresa te enviara publicidad primero y luego te pidiera aceptar el tratamiento de tus datos.



Un consentimiento no puede ser *obligatorio*

Si una empresa te dice que «debes aceptar el uso de tus datos» para algo que no es esencial, está infringiendo la ley. El consentimiento debe ser libre, es decir, no debe ser impuesto como condición. Además, debe otorgarse antes de que los datos comiencen a ser utilizados.

Revocar el consentimiento: tú decides cuándo parar

Tienes derecho a *cambiar de opinión*. Puedes retirar tu consentimiento en cualquier momento, sin un porqué. La forma para retirar tu consentimiento debe ser tan simple como lo fue darlo: rápida, gratuita y accesible.



Caso práctico

Si estás suscrito a un boletín informativo, cada correo que recibas debe incluir un enlace para cancelar la suscripción. Con un solo clic, debieses dejar de recibir esos correos.



No todo clic es consentimiento
Marcar una casilla preseleccionada o simplemente navegar por una *web* no equivale a dar consentimiento. La ley exige un *acto afirmativo claro*. Esto protege a las personas de consentimientos «por omisión».

Cuidado con los consentimientos forzados

La ley establece algo muy importante: si una empresa te pide tu consentimiento para usar tus datos como parte de un contrato o servicio, y ese consentimiento no es realmente necesario para cumplir tal contrato o servicio, se presume que ese consentimiento no fue otorgado libremente.

Esto no significa que automáticamente sea inválido, significa que la ley desconfía de ese consentimiento, porque podría estar condicionado o impuesto.

En otras palabras, no deberían exigirte autorizar el uso de datos que no son esenciales para el servicio que estás contratando.

¿Quién tiene que demostrar que tú consentiste?

No eres tú quien tiene que probar que diste permiso. *La responsabilidad es de quien trata tus datos*. Esa persona o entidad debe poder



Caso práctico

Si te inscribes en un gimnasio, necesitan tus datos básicos para celebrar el contrato (nombre, identificación, medio de pago). Pero si como condición para inscribirte te exigen autorización para publicar tus fotos en redes sociales, ese consentimiento sería cuestionable, porque tu imagen no es necesaria para que puedas hacer uso del gimnasio. En ese caso, la ley presume que no fue otorgado libremente.



La carga de la prueba es de quien trata los datos

Si hay dudas sobre si diste tu consentimiento o si este fue libre y válido, quien trató tus datos debe demostrar que actuó conforme a la ley.

La ley no exige que tú pruebes que no consentiste; corresponde al responsable acreditar que el consentimiento existió y que fue otorgado de manera libre, informada y específica.

demostrar que obtuvo tu consentimiento de forma válida y que usó tus datos de manera legal, leal y transparente.

En caso de un reclamo o una investigación, el responsable del tratamiento debe tener registros o pruebas suficientes para justificar que actuó conforme a la ley.



Puedes solicitar que se te explique todo lo que harán con tus datos, antes de decir que sí. Tienes derecho a preguntar: ¿qué datos me piden?, ¿para qué los usarán?, ¿los compartirán con terceros?, ¿por cuánto tiempo los guardarán? Si tus dudas no son aclaradas, mejor no firmes ni aceptes.



Caso práctico

¿Puede Juan revocar su consentimiento? Asesoría para una pyme

Contexto general

La empresa Marketing Plus, dedicada al marketing digital para pymes, recopila datos personales de sus clientes con el fin de enviar promociones y ofertas personalizadas. Para esto, incluye una cláusula en sus contratos de servicio que regula el uso de estos datos.

La cláusula en cuestión

Cuando Juan contrató los servicios de Marketing Plus, firmó un contrato que incluía esta cláusula: «El cliente autoriza expresamente a Marketing Plus para recopilar, almacenar y utilizar sus datos personales para el envío de promociones y ofertas relacionadas con nuestros servicios. La autorización incluye el tratamiento automatizado de datos y la elaboración de perfiles para personalizar las ofertas y comunicaciones. Esta autorización se concede de forma *irrevocable* y se mantendrá vigente durante toda la relación contractual».

El conflicto

Con el tiempo, Juan empezó a recibir mensajes publicitarios personalizados. Al revisar la cláusula, se dio cuenta de que no entendía bien cómo se usaban sus datos ni en qué consistía exactamente esa personalización. Decidió entonces revocar su consentimiento, enviando un correo a la dirección indicada por la empresa. Sin embargo, no recibió respuesta ni confirmación, lo que lo llevó a presentar una queja.

Tu rol: asesorar y proponer mejoras

Ponte en el lugar de una persona experta o interesada en el ámbito jurídico y la protección de datos. Imagina que la empresa Marketing Plus te solicita orientación para revisar la validez de la cláusula de consentimiento incluida en sus contratos y mejorar su política de tratamiento de datos personales.

Tu desafío es doble:

- *Evaluar la legalidad de la cláusula,* especialmente si cumple con los requisitos de consentimiento establecidos en la legislación vigente.
- *Recomendar cómo actuar frente a la solicitud de Juan,* considerando buenas prácticas en protección de datos y el principio de respeto al titular.

Guía para tu análisis

1. Resumen del caso

- Expón brevemente la situación: ¿qué ocurrió con Juan?, ¿cuál es el problema principal?

2. Revisión de la cláusula contractual

- ¿Proporciona información clara sobre el uso de los datos personales?
- ¿Explica en qué consiste el tratamiento automatizado y la elaboración de perfiles?

- ¿Permite al cliente revocar su consentimiento de forma sencilla y sin trabas?
- ¿Qué significa que la autorización sea *irrevocable*? ¿Es compatible con la ley?

3. Revisión del procedimiento de revocación

- ¿Es efectivo el canal ofrecido (correo electrónico)?
- ¿Qué debería haber hecho la empresa tras recibir la solicitud de Juan?
- ¿Cómo puede mejorarse el sistema de gestión de solicitudes para garantizar una respuesta adecuada?

4. Propuesta de mejoras

- Reformula la cláusula contractual para hacerla más clara, transparente y conforme a la ley.
- Sugiere medios alternativos y más eficaces para la revocación del consentimiento.
- Destaca la importancia de *respetar los derechos del titular* y mantener la confianza de los clientes.



Apliquemos lo aprendido 1

1. ¿Qué condiciones debe cumplir el consentimiento para que sea válido legalmente?

a. Ser libre, informado y específico

b. Ser libre y secreto

c. Ser general e implícito

2. Si una empresa pide tu consentimiento para usar tus datos en un contrato donde no lo necesita realmente, ¿qué podemos concluir?

a. Que el consentimiento es válido

b. Que el consentimiento no fue libremente otorgado

c. Que el consentimiento no se puede revocar

3. ¿Cómo debe manifestarse el consentimiento para que no haya dudas de tu intención?

a. Hablando por teléfono

b. De forma clara, por cualquier medio que demuestre tu voluntad

c. De manera automática al usar un sitio *web*

4. Si entregaste tu consentimiento, ¿puedes cambiar de opinión más adelante?

a. No, una vez dado no se puede cambiar

b. Sí, pero solo si tienes una buena razón

c. Sí, en cualquier momento y sin tener que dar una explicación

5. ¿Quién tiene que demostrar que tu consentimiento fue válido?

a. Tú mismo

b. La persona o empresa que trata tus datos

c. La Agencia de Protección de Datos

Consentimiento de niños, niñas y adolescentes: ¿quién decide sobre sus datos personales?

En un mundo digital donde niños, niñas y adolescentes comparten cada vez más información en redes sociales, videojuegos, plataformas educativas y aplicaciones, es fundamental entender cómo la ley chilena protege sus datos personales. ¿Pueden, los menores de edad, dar su consentimiento? ¿Necesitan la autorización de un adulto? ¿Qué pasa si quieren revocar ese permiso?

En este capítulo te explicamos de manera sencilla quién puede consentir el tratamiento de datos personales de menores de edad en Chile, cómo funciona este consentimiento, qué prácticas son recomendadas para proteger su privacidad y qué hacer en caso de problemas. Además, te mostraremos ejemplos reales y situaciones cotidianas para que puedas aplicar estos conocimientos fácilmente.

¿Qué dice la ley sobre el consentimiento de menores?

La ley establece que, por regla general, ningún dato personal puede ser tratado sin consentimiento, y que este debe ser libre, informado, previo y específico (art. 12). Esto significa que nadie puede usar tu información sin que tú lo sepas y autorices. Pero cuando se trata de niños, niñas o adolescentes, la ley exige mayores cuidados.

¿Por qué? Porque está en juego el interés superior del menor y su autonomía progresiva. La ley entiende que, a medida que crecen, los menores ganan capacidad para tomar decisiones sobre su propia vida, incluida la protección de sus datos (Ravetllat y Pinochet, 2015: pp. 903-934 y Lansdown, 2005: p. 3).

¿A qué edad pueden consentir los menores?

La ley chilena establece distintas reglas según la edad del menor y el tipo de dato:

Edad	Tipo de dato	¿Quién debe dar el consentimiento?
Menores de 14 años	Ordinarios o sensibles	Los padres, tutores o quien tenga el cuidado personal del menor
14 a 15 años	Datos ordinarios	El/la adolescente puede consentir por sí mismo/a

Edad	Tipo de dato	¿Quién debe dar el consentimiento?
14 a 15 años	Datos sensibles (salud, orientación sexual, etc.)	Lo consienten los representantes legales
16 a 17 años	Cualquier dato	El/la adolescente puede consentir directamente, igual que un adulto



Son datos que revelan aspectos íntimos (salud, ideología, orientación sexual, religión, etc.) y requieren una protección más estricta.

¿Qué requisitos debe cumplir ese consentimiento?

Cuando se trata de datos sensibles como información sobre salud, creencias religiosas, afiliación sindical y orientación sexual, entre otros, la ley exige un estándar más alto de protección.

El consentimiento debe cumplir con los siguientes requisitos:

* *Debe ser previo*, es decir, otorgado antes de que comience el tratamiento.
* *Debe ser específico*, indicando claramente para qué se utilizarán los datos.
* *Debe ser expreso*, lo que significa que debe manifestarse de forma clara y directa, sin ambigüedades.
* Puede otorgarse mediante una declaración *escrita, verbal o por un medio tecnológico equivalente*, pero siempre debe existir una manifestación explícita de voluntad.
* *Es revocable* en cualquier momento, utilizando medios similares a los empleados para otorgarlo.
* El responsable del tratamiento debe *conservar prueba del consentimiento*. Si no puede demostrar que lo obtuvo válidamente, se presume que no contó con autorización.

Buenas prácticas para proteger los datos de menores

Padres y apoderados

* Leer bien las políticas de privacidad antes de aceptar.
* Pedir copia del consentimiento otorgado.
* Conversar con el menor sobre el alcance de la autorización, con un lenguaje que él o ella pueda comprender.

Colegios, talleres y clubes

* Designar a un encargado de protección de datos.
* Solicitar autorizaciones separadas para actividades específicas (como redes sociales o difusión institucional).
* Recolectar los datos estrictamente necesarios.

Plataformas digitales y apps

* Verificar la edad de los usuarios.
* Pedir consentimiento de los adultos responsables cuando se trate de menores de 14 años.
* Ofrecer controles parentales, opciones de revocación fácil y configuraciones de privacidad estrictas por defecto.

¿Cuándo NO se necesita consentimiento?

Aunque el consentimiento es la regla general, la ley establece diversas situaciones en las que se pueden tratar datos personales, incluso datos sensibles, sin pedir autorización previa al titular.[23]

23 Conforme a los artículos 13, 16 y 16 bis de la Ley 19.628 (modificada por la Ley 21.719), el tratamiento de datos personales sin consentimiento es lícito, entre otros casos, cuando: (i) se trate de datos económicos, financieros, bancarios o comerciales en conformidad al Título III; (ii) sea necesario para el cumplimiento de una obligación legal; (iii) sea necesario para la celebración o ejecución de un contrato o medidas precontractuales; (iv) responda a intereses legítimos del responsable o de un tercero, siempre que no se afecten los derechos del titular; (v) sea necesario para la formulación, ejercicio o defensa de derechos ante tribunales u órganos administrativos; (vi) el titular haya hecho manifiestamente públicos sus datos sensibles; (vii) se trate de tratamiento efectuado por personas jurídicas sin fines de lucro respecto de sus miembros, bajo las condiciones

Por ejemplo:

* Cuando es necesario para proteger la vida o la salud de una persona (como en una emergencia médica).
* Cuando el tratamiento es exigido por la ley o por una resolución judicial.
* Cuando es indispensable para ejecutar un contrato.
* Cuando existe un interés legítimo que no afecta los derechos del titular.
* En ciertos casos de interés público, salud pública o investigación científica, siempre que se cumplan los requisitos legales.

Estas situaciones no eliminan la protección de los datos, pero permiten su tratamiento bajo condiciones estrictas.

¿Qué hacer si hay una filtración o un mal uso de datos?

Si los datos personales de un menor (especialmente menores de 14 años) se ven comprometidos por una filtración o acceso no autorizado, el responsable debe:

* informar a la Agencia de Protección de Datos Personales y
* notificar a los representantes del menor, usando un lenguaje claro y accesible.

legales; (viii) resulte indispensable para salvaguardar la vida o integridad del titular; (ix) en casos de alerta sanitaria; (x) con fines históricos, estadísticos o científicos de interés público, previa anonimización; (xi) para fines de medicina preventiva, laboral o gestión de sistemas sanitarios; (xii) cuando la ley autorice expresamente el tratamiento. En todos los casos, el responsable debe acreditar la licitud del tratamiento.



Caso práctico

¿Puedo subir a una página web la foto del acto de graduación?

Un colegio quiere publicar en su página *web* fotos de la ceremonia de graduación.

¿Qué debe hacer?

- Si los estudiantes son menores de 14 años, debe pedir consentimiento a los padres.
- Si tienen 16 o 17 años, puede pedir el consentimiento directamente a los estudiantes.
- Publicar solo lo necesario, evitar etiquetar o identificar individualmente y configurar la *web* para que no aparezcan las imágenes en motores de búsqueda.
- Guardar constancia del consentimiento y permitir su revocación fácil.

Claves para recordar

La edad sí importa:

- Si el menor tiene menos de 14 años, no puede consentir por sí solo. El consentimiento debe ser otorgado por sus padres, tutores o quien tenga su cuidado personal.
- Entre 14 y 15 años, el/la adolescente puede consentir por sí mismo/a solo para datos personales ordinarios (como nombre o dirección), pero no para datos sensibles (como información médica o religiosa).
- Desde los 16 años, el/la adolescente puede consentir plenamente para todo tipo de datos, igual que una persona adulta.

Todo consentimiento es revocable:

- No importa si fue otorgado por un adulto o por el propio adolescente: puede retirarse en cualquier momento, sin necesidad de justificar la decisión.
- El proceso para revocar debe ser tan simple como el de otorgar el consentimiento.

Sin prueba no hay consentimiento:

- El responsable del tratamiento (por ejemplo, un colegio, una app o una empresa) debe guardar un registro verificable del consentimiento.
- Si no puede demostrarlo, se presume que nunca obtuvo autorización válida.

Menos es más (en protección de datos):

- Mientras menos datos se recolecten, menos riesgos existen para la privacidad del menor.
- Solo deben recopilarse los datos estrictamente necesarios para cumplir con el objetivo declarado (esto se llama *principio de minimización*).



Apliquemos lo aprendido 2

1. ¿Quién debe dar el consentimiento para tratar los datos personales de un niño o niña menor de 14 años?

a. El propio niño o niña

b. El profesor o profesora a cargo

c. Sus padres, tutores o quien ejerza el cuidado personal

2. Una adolescente de 15 años quiere compartir su información médica en una app de salud, ¿puede consentir por sí sola?

a. Sí, siempre que sea mayor de 13 años

b. No, sus padres o tutores deben dar el consentimiento

c. Sí, si lo hace por medios electrónicos

3. ¿Cuál de las siguientes características NO es parte de un consentimiento válido según la ley chilena?

a. Que sea informado

b. Que sea irrevocable

c. Que sea específico

4. ¿Cuál es una buena práctica recomendada para los colegios cuando manejan datos personales de menores?

a. Pedir una autorización general para todo el año

b. Publicar fotos sin consentimiento si es una actividad institucional

c. Designar a una persona encargada de protección de datos

¿Sabías que no siempre se necesita tu permiso? Casos en que se pueden usar tus datos sin consentimiento

¿Pueden usar tus datos sin pedirte permiso? Sí, pero solo en estos casos

Aunque lo más común es que las empresas y organizaciones necesiten tu consentimiento para tratar tus datos personales, la ley también establece algunas excepciones. El artículo 13 de la Ley de Protección de Datos explica que en ciertas situaciones *sí se pueden usar tus datos sin tu autorización previa*, siempre que se cumplan requisitos muy específicos.

Te lo explicamos punto por punto, con ejemplos concretos para que sea más fácil de entender.

Obligaciones económicas, financieras, bancarias o comerciales

Un banco revisa tu historial de pagos antes de decidir si aprobará tu crédito.

¿Por qué es legal sin tu consentimiento?

Porque la ley permite el tratamiento de datos relacionados con tus obligaciones económicas, financieras, bancarias o comerciales como tu comportamiento de pago cuando se realiza conforme a las reglas establecidas en la propia ley.

Esto significa que las entidades pueden analizar información sobre el cumplimiento o incumplimiento de deudas para efectos de evaluación crediticia y análisis de riesgo financiero. No se trata de cualquier dato económico general, sino específicamente de antecedentes vinculados a tus obligaciones y su cumplimiento.

Cumplimiento de obligaciones legales

Una empresa informa a la autoridad tributaria sobre los sueldos de sus trabajadores.

¿Por qué es legal?

Porque está cumpliendo con una obligación que impone la ley. En estos casos, la empresa no necesita tu consentimiento, ya que está actuando conforme a una norma legal específica.

Ejecución de un contrato o medidas precontractuales

Compras algo en línea y entregas tu dirección para que te lo envíen.
¿Por qué es legal?
Porque esos datos son esenciales para cumplir el contrato (entregarte el producto). También aplica si, antes de firmar un contrato, tú mismo solicitaste ciertas gestiones.

Intereses legítimos del responsable o de terceros

Una tienda en línea personaliza las ofertas que te muestra basándose en tu navegación.
¿Por qué es legal?
Porque la empresa tiene un interés legítimo en mejorar tu experiencia como cliente o en promover sus productos.

Sin embargo, este tratamiento solo es válido si, al comparar ambos intereses, el interés de la empresa no prevalece de manera desproporcionada sobre tus derechos y libertades. En otras palabras, debe existir un equilibrio: si el uso de tus datos afecta gravemente tu privacidad o tus derechos, el interés empresarial no puede imponerse.

Además, siempre tienes derecho a ser informado sobre qué datos se están usando y cuál es el interés legítimo que justifica ese tratamiento.

Defensa o ejercicio de derechos legales

Una empresa usa tus datos como prueba en un juicio.
¿Por qué es legal?
Porque los necesita para defenderse o presentar pruebas ante un tribunal u organismo público. En estos casos, la ley autoriza el uso sin necesidad de consentimiento.



Aunque en estos casos *no se pide tu permiso, el responsable siempre debe justificar legalmente el uso de tus datos*. Esto significa que no pueden tratar tu información personal de forma arbitraria: deben estar amparados en la ley y respetar tus derechos.



Caso práctico

¿Está bien usar tus datos así?

Servicios Financieros Beta es una pequeña empresa que otorga préstamos personales. Para saber si una persona puede acceder a un préstamo, la empresa revisa datos como el sueldo, el historial de pagos anteriores y la situación económica general del cliente.

En su contrato, la empresa incluye una cláusula que dice lo siguiente: "El cliente autoriza a Servicios Financieros Beta a tratar sus datos personales, incluidos datos financieros y económicos, con el fin de evaluar su capacidad de pago y ofrecer productos personalizados. El tratamiento de datos se realizará conforme a las leyes vigentes y sin necesidad de recabar el consentimiento explícito del cliente cada vez que se realice dicho tratamiento, debido a la naturaleza contractual de los servicios".

Resuelve:

Lee con atención la cláusula y responde estas preguntas o reflexiona en grupo:

1. ¿Crees que es razonable que la empresa use estos datos sin pedir permiso cada vez? ¿Por qué?
2. ¿Consideras que esta cláusula respeta tus derechos como persona? ¿Qué te genera al leerla?
3. Si tú fueras quien firma este contrato, ¿qué pedirías que se aclare o modifique?
4. ¿Qué recomendaciones le harías a la empresa para que informe mejor a las personas sobre el uso de sus datos?



Apliquemos lo aprendido 3

1. ¿Cuándo se pueden usar tus datos personales sin permiso en temas financieros o comerciales?

a. Cuando no logran contactarte

b. Cuando tus datos se usan para ofrecerte publicidad

c. Cuando se ajustan a la ley y están relacionados con tu situación económica, financiera, bancaria o comercial

2. ¿En qué caso una empresa puede usar tus datos sin pedirte permiso por una obligación legal?

a. Si tú no dices nada en contra

b. Cuando la empresa cree que es conveniente

c. Cuando una ley lo exige y es necesario para cumplirla

3. ¿Cuándo es válido usar tus datos para cumplir un contrato que firmaste (o estás por firmar)?

a. Siempre se debe pedir tu permiso

b. Cuando es necesario para cumplir el contrato o gestionar algo que tú pediste antes de firmarlo

c. Solo si se usan datos anónimos

4. Si una empresa usa tus datos porque tiene un "interés legítimo", ¿qué debe hacer?

a. No contar nada para evitar problemas

b. Explicarte claramente por qué usa tus datos y cuál es ese interés

c. Guardar la mayor cantidad de datos posible

5. ¿Cuándo se pueden usar tus datos como parte de una defensa legal o juicio?

a. Solo si el juicio es internacional

b. Cuando los datos son necesarios para defender un derecho o presentar pruebas en un tribunal u organismo público

c. Solo si tú das permiso para usar tus datos en un juicio

Capítulo 5

Protege tu privacidad: descubre tus derechos sobre datos personales

Cada vez que usamos Internet, llenamos un formulario o realizamos una compra en línea, compartimos información sobre nosotros. Nuestro nombre, dirección, número de teléfono o incluso nuestras preferencias pueden quedar almacenadas en bases de datos de empresas, instituciones públicas o plataformas digitales. Pero ¿qué derechos tenemos sobre esos datos?

En Chile, la Ley de Protección de Datos Personales reconoce una serie de derechos que permiten a cada persona mantener el control sobre su información.[24] Estos derechos son fundamentales, lo que significa que nadie puede quitárnoslos ni hacer que renunciemos a ellos mediante un contrato o acuerdo. Gracias a estos mecanismos, podemos exigir que nuestros datos sean corregidos, eliminados o utilizados solo de manera adecuada.

En este capítulo, exploraremos cuáles son estos derechos, cómo ejercerlos y por qué son tan importantes en un mundo donde la información se ha convertido en uno de los bienes más valiosos.

24 Uno de los cambios más relevantes introducidos por la reforma a la Ley de Protección de Datos Personales es la considerable expansión de los derechos reconocidos a los titulares, tanto en términos del número de derechos que pueden ejercer sobre su información personal como en la profundidad normativa con que estos están regulados. Antes de la reforma de 2024, la Ley 19.628 contemplaba de manera limitada solo cuatro derechos fundamentales: acceso, rectificación, cancelación y oposición, comúnmente conocidos en la doctrina como «Derechos ARCO». En este sentido, Jijena (1992), Corral (2001b); Cerda (2003) y Anguita (2007).

Derechos sobre tus datos personales

El artículo 4 establece los derechos que cualquier persona tiene sobre sus datos personales. Estos son:

* *Acceso:* confirmar si una persona o entidad está tratando sus datos personales y, en caso afirmativo, poder acceder a ellos para conocer qué información se maneja y con qué finalidad.
* *Rectificación:* corregir información incorrecta o desactualizada.
* *Supresión:* pedir que se eliminen sus datos cuando ya no sean necesarios o si se usaron sin su consentimiento.
* *Oposición:* oponerse, en los casos que establece la ley, a que sus datos personales sean tratados, incluyendo el derecho a oponerse a decisiones que se adopten únicamente mediante tratamientos automatizados que puedan afectarle.
* *Portabilidad:* solicitar una copia de sus datos personales en un formato estructurado y de uso común, que permita recibirlos directamente y, si lo desea, transferirlos a otra persona o entidad.
* *Bloqueo:* restringir temporalmente el uso de sus datos.

Estos derechos son personales, intransferibles e irrenunciables, lo que significa que nadie puede renunciar a ellos ni venderlos. Tampoco pueden ser limitados por un contrato o acuerdo.

Ahora analicemos los derechos que tienes sobre tus datos.

Derecho de acceso

Este derecho te permite saber si alguien (una empresa, una institución o cualquier entidad) tiene información tuya, para qué la está usando y con quién la está compartiendo. Es como abrir una ventana por la que mirar qué datos tuyos están almacenados y cómo los manejan.

***Ejemplo**:* Imagina que tienes una cuenta en un banco y te preguntas qué datos tienen sobre ti. Puedes pedirles un informe detallado donde te digan qué información guardan, cómo la usan y si la han compartido con otras entidades, como aseguradoras o burós de crédito. Así, tienes claridad y control sobre tu información.

Derecho de rectificación

Si tus datos personales están incorrectos, desactualizados o tienen errores, puedes pedir que sean corregidos. Este derecho garantiza que la información que tienen sobre ti sea siempre precisa y refleje tu situación actual.

Ejemplo: Imagina que cambiaste de casa y notas que tu empleador mantiene en sus registros tu dirección antigua. Para evitar problemas con correspondencia o documentos oficiales, puedes solicitar que actualicen tu información con tu nueva dirección.

Derecho de supresión (o «derecho al olvido»)

Si ya no quieres que una empresa o institución siga guardando tus datos personales, puedes pedir que los eliminen. Este derecho conocido como derecho de supresión procede, por ejemplo, cuando la información ya no es necesaria para el propósito con el que fue recopilada o cuando entregaste tu consentimiento y luego decides retirarlo.[25]

Ejemplo: Imagina que decides dejar de usar una red social y quieres que desaparezca tu información, como fotos y publicaciones. Puedes solicitar la eliminación de tu cuenta y de los datos asociados a ella, siempre que no exista una obligación legal u otra base que justifique su conservación[26].

---

25 La Ley 19.628, modificada por la Ley 21.719, regula de manera específica las hipótesis en que procede el derecho de supresión. Entre ellas se encuentran, por ejemplo: cuando los datos hayan dejado de ser necesarios para la finalidad que motivó su tratamiento, cuando el titular haya revocado su consentimiento y no exista otra base legal que justifique el tratamiento, cuando los datos hayan sido tratados ilícitamente o cuando deban suprimirse para dar cumplimiento a una obligación legal. El ejercicio de este derecho se encuentra sujeto a las limitaciones y excepciones establecidas en la ley. Sobre el derecho al olvido ver Reusser (2021).

26 Sobre la justificación de este derecho Reusser (2021) reflexiona indicando que el planteamiento de una eventual "amenaza" puede comprenderse mejor si se observa la lógica que estructura nuestras relaciones sociales. En efecto, la vida en comunidad descansa, en parte, en nuestras limitaciones como seres humanos: con el paso del tiempo, la memoria se debilita, los recuerdos —incluso los más intensos— se difuminan y, progresivamente, dejamos de reprocharnos errores o agravios del pasado.

Esta misma racionalidad se replica en el ámbito jurídico. El derecho incorpora mecanismos institucionales de olvido: las deudas prescriben, las ofertas caducan, los plazos

Derecho de oposición

Tienes el derecho de decir «no quiero que usen mis datos para esto» en ciertas situaciones previstas por la ley. Por ejemplo, si una empresa está usando tu información para enviarte publicidad sin tu consentimiento, puedes pedir que dejen de hacerlo.

Ejemplo: Imagina que empiezas a recibir correos y mensajes de una tienda con ofertas en las que no estás interesado. Si no diste tu consentimiento para recibir esa publicidad, puedes solicitar que eliminen tus datos de su lista y dejen de enviarte promociones.[27]

Derecho de portabilidad

Este derecho te permite recibir tus datos personales en un formato fácil de leer y de usar, junto a la posibilidad de transferirlos a otro responsable sin problemas. Es como pedir una copia de tu información para llevártela y usarla donde tú decidas.

---

se extinguen y, en ciertos casos, se conceden amnistías. En otras palabras, el ordenamiento jurídico reconoce que, transcurrido un tiempo razonable, ciertos hechos deben perder relevancia, incluso por mandato legal.

¿La razón? Una necesidad básica de convivencia. Resultaría inviable sostener vínculos sociales si todo error, falta o acierto quedara permanentemente presente: desde omisiones cotidianas hasta conductas reprochables ocurridas décadas atrás. Como se ha señalado, la vida humana requiere del olvido para ser posible.

Sin embargo, este equilibrio se ve tensionado en el contexto de la digitalización. Los medios de comunicación, particularmente en su versión digital, han alterado esta lógica al mantener disponibles en línea hechos, imágenes y opiniones que habían desaparecido de la memoria colectiva e individual. Así, el pasado se reactiva constantemente, como si hubiese ocurrido recientemente, erosionando la posibilidad de cierre y reconciliación. Este fenómeno —potenciado por la indexación de contenidos en motores de búsqueda— genera una suerte de permanencia indefinida de la información, donde aquello que debía ser olvidado permanece accesible, desafiando los límites tradicionales entre memoria, tiempo y derecho.

27 El derecho de oposición procede en las hipótesis establecidas por la Ley 19.628, modificada por la Ley 21.719. Entre ellas se encuentra, por ejemplo, el tratamiento de datos con fines de mercadotecnia o publicidad directa. Asimismo, puede ejercerse cuando el tratamiento se base en el interés legítimo del responsable y existan motivos fundados y legítimos del titular relacionados con su situación particular. Su ejercicio se encuentra sujeto a las condiciones y excepciones establecidas en la ley.

Ejemplo: Imagina que usas una plataforma de música en *streaming* y tienes varias listas de reproducción que te gustan. Si decides cambiar a otro servicio, puedes solicitar que se te entreguen tus listas y preferencias para que puedas llevarlas y transferirlas fácilmente al nuevo servicio sin perder nada de lo que habías creado.

Derecho de bloqueo

Es el derecho a solicitar que tus datos personales sean bloqueados temporalmente, es decir, que se suspenda su tratamiento mientras se resuelve la tramitación de una solicitud relacionada con otros derechos, como la rectificación, supresión u oposición.
De esta manera, se evita que los datos sigan siendo utilizados mientras se aclara la situación.

Ejemplo: Imagina que encuentras un error en tu informe de crédito que afecta tu puntuación. Puedes solicitar la rectificación de ese dato y pedir que sea bloqueado temporalmente mientras se revisa tu solicitud. De esta manera, se suspende su tratamiento hasta que se determine si la información es correcta o no.

¿Qué pasa si el titular de los derechos fallece? Derechos en caso de fallecimiento del titular

En caso de fallecimiento, los derechos del titular pueden ser ejercidos por sus herederos, permitiéndoles acceder, rectificar o suprimir los datos del fallecido. Sin embargo, si el titular fallecido prohibió expresamente el acceso o la modificación de sus datos antes de morir, los herederos no podrán ejercer estos derechos, salvo que una ley establezca lo contrario.

Ejemplo: Si una persona fallecida dejó instrucciones claras de que sus datos médicos no sean accesibles después de su muerte, los herederos no podrán acceder a esa información.



Caso práctico

Gestión de los datos de un titular fallecido

Juan falleció y dejó explícito en su testamento que no quería que sus correos electrónicos fueran accesibles para nadie después de su muerte. Sin embargo, su hija quiere acceder a estos correos para resolver asuntos pendientes.

¿Puede la hija de Juan acceder legalmente a sus correos electrónicos?

Resolución

Si Juan dejó instrucciones claras en su testamento para que sus correos electrónicos no fueran accesibles después de su fallecimiento, la hija no podrá acceder a esa información. La voluntad del titular fallecido, en este caso, debe ser respetada. Los herederos solo podrán acceder a los datos si no hay instrucciones contrarias y si la ley lo permite, lo cual generalmente no es el caso cuando se trata de datos privados, como los correos electrónicos.



Apliquemos lo aprendido

1. ¿Cuál de los siguientes derechos NO puede ser ejercido por los herederos del titular de los datos en caso de que el titular haya prohibido expresamente el acceso a sus datos?

a. Derecho de acceso

b. Derecho de oposición

c. Ninguno de los anteriores

2. En caso de fallecimiento del titular, los herederos pueden ejercer los derechos sobre los datos personales del fallecido salvo que:

a. El titular haya expresamente prohibido el acceso o modificación de sus datos

b. Los datos sean irrelevantes para los herederos

c. No exista relación directa entre los datos y el patrimonio del fallecido

3. El derecho de portabilidad permite al titular:

a. Bloquear temporalmente sus datos

b. Obtener una copia de sus datos personales en un formato estructurado y de uso común, junto con solicitar su transferencia a otro responsable cuando sea técnicamente posible

c. Solicitar la eliminación de sus datos personales



Un vistazo más profundo a tus derechos sobre los datos personales

Sobre el derecho de acceso

Imagina que un desconocido tiene acceso a tu información personal: nombre, dirección, historial de compras, incluso detalles sobre tu vida digital. Ahora pregúntate: ¿sabes quién tiene tus datos y para qué los está usando? En un mundo donde la información es poder, conocer y ejercer nuestros derechos sobre los datos personales se ha vuelto más importante que nunca.

El derecho de acceso es una herramienta esencial para proteger nuestra privacidad.[28] Nos permite preguntar a las empresas, organismos públicos y otras entidades qué datos tienen sobre nosotros, de dónde los obtuvieron, con quién los comparten y cuánto tiempo los conservarán. Pero ¿cómo funciona realmente este derecho? ¿Qué podemos exigir y qué limitaciones existen?

En este capítulo exploraremos a fondo el derecho de acceso, desglosando cada uno de sus elementos de manera sencilla y con ejemplos

28 Contreras y otros (2025: p. 85) señalan, en este sentido, que «el derecho de acceso opera como un verdadero "derecho llave", puesto que facilita el ejercicio de los otros derechos del titular y hasta cierto punto opera como condición necesaria para el ejercicio de estos, bajo el entendido que el titular no podrá ejercer sus derechos si no conoce quién está procesando sus datos personales y bajo qué condiciones». También lo reconoce en este sentido el Tribunal de Justicia de la Unión Europea en su sentencia de 7 de mayo de 2009, asunto C-533/07.

prácticos para que puedas entender cómo ejercerlo en tu vida cotidiana. Porque cuando se trata de nuestros datos personales, la información no solo es un derecho, sino también nuestra mejor defensa.

Tu derecho a saber: protección de tus datos personales

El artículo 5 de la Ley de Protección de Datos Personales explica el derecho de acceso, el cual concede a cualquier persona a saber si sus datos personales están siendo utilizados y, en caso afirmativo, acceder a información detallada sobre cómo y por qué se están usando esos datos. Esto incluye conocer los datos que se están procesando, su origen, los fines del tratamiento, con quién se comparten y cuánto tiempo se mantendrán, junto a detalles sobre el tratamiento automatizado. Sin embargo, este derecho puede limitarse si alguna ley lo impide expresamente.

¿Qué información se puede solicitar?

Si una persona ejerce su derecho de acceso, el responsable debe entregarle la siguiente información:

- *Los datos en sí y su origen:* qué datos tiene la empresa o institución y de dónde los obtuvo.
- *El propósito del uso de los datos:* para qué se están utilizando.
- *Quién recibe los datos:* si los datos han sido compartidos con alguien más, la persona puede saber con quién. Puede pedir información general (por ejemplo, «se comparten con bancos») o detalles específicos (los nombres de las entidades que los han recibido).
- *Tiempo de uso*: cuánto tiempo se almacenarán y utilizarán los datos.
- *Intereses legítimos del responsable:* si los datos se están usando con base en una justificación especial establecida en la ley (artículo 13, letra d), se debe explicar cuál es esa justificación.
- *Cómo funcionan los procesos automatizados:* si los datos están siendo tratados mediante decisiones automatizadas (por ejemplo, inteligencia artificial o algoritmos), se debe explicar cómo funciona esa lógica.

Ahora analicemos los distintos puntos de este artículo

Los datos tratados y su origen

El titular tiene derecho a saber qué datos específicos están siendo utilizados por la entidad responsable. Esto incluye cualquier tipo de dato personal, como nombre, dirección y número de teléfono, entre otros. Además, el titular tiene derecho a saber de dónde provienen esos datos, es decir, si fueron proporcionados directamente por él (cuando se rellena un formulario, por ejemplo) o si se obtuvieron de otras fuentes (por ejemplo, bases de datos públicas o información obtenida de otras empresas).

Ejemplo: Si una persona se registra en una tienda en línea, tiene derecho a saber qué datos personales tiene la tienda sobre ella (nombre, dirección, historial de compras) y si esos datos fueron proporcionados directamente por ella o si fueron obtenidos a partir de alguna otra fuente, como una compra anterior.

La finalidad o las finalidades del tratamiento

El titular tiene derecho a saber para qué se están utilizando sus datos. Esto significa que la entidad responsable debe explicar claramente el propósito del tratamiento. Los datos no pueden ser usados para fines distintos a los que fueron originalmente informados al titular.

Ejemplo: Si una empresa recoge el correo electrónico de una persona para enviarle promociones, esa es la finalidad del tratamiento. Si luego la empresa empieza a usar ese correo para enviarle información no relacionada, como encuestas o publicidad de terceros, estaría violando este derecho.

Las categorías, clases o tipos de destinatarios, o bien, la identidad de cada destinatario, en caso de solicitarlo así el titular, a los que se les hayan comunicado o cedido los datos o se prevea hacerlo

El titular tiene derecho a saber a quién se ha enviado sus datos personales o a quién se prevé que se enviarán en el futuro. Esto incluye tanto a las empresas o personas con las que se comparte la información como el tipo de entidad (por ejemplo, proveedores, servicios de publicidad, organismos gubernamentales, etc.).

Ejemplo: Si una empresa comparte la información de sus clientes con una agencia de publicidad, el titular tiene derecho a saber qué empresa o persona tiene acceso a esos datos y para qué propósito. Si la empresa tiene planes de compartir esos datos con un socio futuro, también debe informarlo.

El periodo de tiempo durante el cual los datos serán tratados

El titular tiene derecho a saber durante cuánto tiempo se mantendrán sus datos personales en poder de la entidad responsable. Esto asegura que los datos no se retengan por más tiempo del necesario. En algunas situaciones, los datos pueden ser eliminados o anonimizados después de cierto lapso, dependiendo de la finalidad del tratamiento.

Ejemplo: Si una persona se inscribe en una suscripción mensual a una revista, la empresa debe indicarle cuánto tiempo mantendrá sus datos, ya sea hasta que se cancele la suscripción o si se mantienen por algún tiempo adicional para fines de marketing.

Los intereses legítimos del responsable (cuando el tratamiento se base en lo dispuesto en el artículo 1 3, letra d)

Cuando el tratamiento de datos se basa en intereses legítimos (por ejemplo, el interés de la empresa en mejorar sus productos o servicios), el titular tiene derecho a saber qué intereses son esos. Es decir, la empresa debe justificar por qué el tratamiento de los datos es necesario para sus intereses, sin que afecte negativamente los derechos y libertades del titular.

Ejemplo: Una empresa que utiliza los datos de contacto de sus clientes para mejorar su servicio debe explicar qué intereses tiene en ese tratamiento, como la mejora del servicio al cliente o la optimización de sus procesos. Si el interés legítimo de la empresa es contactar a los clientes para obtener comentarios sobre su experiencia, debe ser claro en cuanto a ello.

Información significativa sobre la lógica aplicada en el caso de que el responsable realice tratamiento de datos de conformidad con el artículo 8 bis de esta ley

Este punto se refiere a los casos en los que el tratamiento de datos se realiza a través de medios automáticos, como algoritmos o sistemas de inteligencia artificial. Si la empresa toma decisiones sobre el titular basándose en estos procesos automáticos, el titular tiene derecho a saber cómo se aplican esos procesos, qué criterios se utilizan y qué consecuencias pueden tener para él.[29]

Ejemplo: Si un banco usa un sistema automático para decidir la aprobación o el rechazo de un crédito, el titular tiene derecho a saber qué criterios utiliza el sistema (por ejemplo, historial crediticio, ingresos, etc.) y cómo puede afectar esa decisión a su acceso al crédito.

29 El grado de detalle con que el responsable debe explicar el funcionamiento técnico de un sistema automatizado o algorítmico ha sido ampliamente discutido en el contexto europeo. Esta controversia surge, por un lado, porque muchos algoritmos están protegidos por derechos de propiedad intelectual, lo que implica que revelar su código fuente podría afectar negativamente los intereses económicos de sus desarrolladores. Por otro lado, en algunos casos resulta técnicamente complejo, incluso para quienes administran sistemas avanzados —como los basados en inteligencia artificial generativa—, identificar con precisión las inferencias o correlaciones que el sistema ha realizado para arribar a un determinado resultado. En este sentido ver Veale y Edwards (2018: pp. 398-404).



Caso práctico

Derecho de acceso

Situación:

Una empresa de tecnología usa un sistema de inteligencia artificial (IA) para analizar el comportamiento de sus usuarios y mejorar sus servicios. Este sistema recopila mucha información personal, como ubicación, historial de navegación y preferencias de compra, pero no explica cómo utiliza estos datos ni por qué toma ciertas decisiones, como las recomendaciones de productos o los ajustes en los precios.

Un usuario preocupado por la privacidad de sus datos pide a la empresa que le proporcione acceso a toda la información personal que ha sido procesada, así como una explicación detallada de cómo la IA usa esos datos para tomar decisiones que le afectan.

Sin embargo, la empresa responde con un resumen general de los datos recolectados y da una explicación vaga sobre la IA, diciendo que la lógica que usa es demasiado compleja y privada para compartirla.

¿Está la empresa cumpliendo con sus obligaciones bajo el artículo 5 de la Ley de Protección de Datos Personales en Chile? ¿Qué acciones puede tomar el usuario si considera que la respuesta de la empresa es insuficiente?



Apliquemos lo aprendido 1

1. ¿Qué derecho tiene el titular de los datos personales, según el artículo 5 de la Ley de Protección de Datos Personales?

a. Derecho a ser informado sobre el uso de sus datos, pero no a acceder a ellos

b. Derecho a solicitar acceso y conocer qué datos están siendo tratados, su origen y cómo se utilizan

c. Derecho a eliminar sus datos sin saber qué tratamiento reciben

2. Según el artículo 5, ¿qué información tiene el titular derecho a conocer respecto a los destinatarios de sus datos personales?

a. La cantidad exacta de destinatarios a los que se les pueden ceder los datos

b. Las categorías de destinatarios o su identidad, si así lo solicita el titular

c. Solo si los destinatarios son entidades gubernamentales

3. ¿Qué aspecto debe especificar la empresa cuando el tratamiento de datos se basa en «intereses legítimos» del responsable, según el artículo 5?

a. Que la empresa puede usar los datos para cualquier fin que considere necesario

b. Que los datos serán utilizados solo para mejorar los servicios sin necesidad de justificación

c. Que la empresa debe explicar qué intereses legítimos tiene para tratar los datos y cómo no afectan los derechos del titular

Sobre el derecho de rectificación

¿Alguna vez te has encontrado con información incorrecta sobre ti en una base de datos? Por ejemplo, una dirección mal escrita, un error en tu nombre o antecedentes laborales que no te corresponden. En la era digital, donde nuestros datos personales circulan constantemente, es fundamental mantener el control sobre ellos.

Uno de los derechos más importantes, en este contexto, es el derecho de rectificación, pues permite solicitar la corrección de cualquier dato personal que sea inexacto o esté incompleto o desactualizado. Gracias a este derecho puedes exigir que se actualice la información que manejan empresas, instituciones o plataformas digitales para que refleje de forma veraz tu realidad.

En definitiva, el derecho de rectificación permite al titular solicitar al responsable del tratamiento que corrija o complete sus datos personales cuando estos sean incorrectos, estén desactualizados o resulten incompletos. Para que proceda, debe existir una inexactitud material o un error verificable en la información registrada; no basta con que el titular discrepe subjetivamente del contenido del dato. Por ejemplo, no podría exigirse la modificación de un diagnóstico médico únicamente porque la persona considera que el profesional se equivocó, si dicho diagnóstico fue emitido conforme a criterios técnicos.

Este derecho tiene como finalidad concretar el principio de calidad, el cual exige que los datos personales sean precisos, completos, actualizados y adecuados en función de su origen y los objetivos para los cuales se recogen y utilizan.[30]

¿Qué pasa con los datos corregidos?

Si los datos ya fueron compartidos con otras personas o entidades, el responsable *debe avisarles* para que también corrijan la información. Sin embargo, hay dos excepciones donde esto no ocurre:

---

30 En el ámbito europeo, el artículo 16 del GPDR concede a los titulares el derecho a exigir que en el registro de datos que se busca rectificar se deje una indicación o anotación de que este impugna la exactitud de la información, mientras se encuentra pendiente la decisión final. Sin embargo, este elemento no fue incorporado en la nueva ley chilena.

* Cuando es *imposible* comunicar la rectificación (por ejemplo, si la entidad ya no existe).
* Cuando avisarles implica un *esfuerzo desproporcionado* (por ejemplo, si los datos se compartieron con miles de destinatarios y no hay una forma práctica de notificarlos).

¿Se pueden seguir usando los datos incorrectos?

No. Una vez que se haya corregido la información, *no se pueden volver a usar los datos antiguos o erróneos*.



Caso práctico

Imagina que un banco tiene registrado un número de teléfono equivocado en la cuenta de un cliente. Como resultado, el cliente no recibe notificaciones importantes sobre su estado financiero. En este caso, la persona puede ejercer su derecho de rectificación y pedirle al banco que corrija el número.

Además, si el banco ha compartido ese dato erróneo con otra entidad (por ejemplo, una empresa de cobranza), también debe notificarles la corrección, a menos que esto sea extremadamente difícil o imposible de hacer.

Recomendación:

Este derecho es especialmente útil cuando la información es incorrecta o está incompleta, ya que permite modificarla sin eliminarla. Esto es importante en situaciones donde los datos deben seguir siendo utilizados por razones legales o contractuales, como en registros bancarios o antecedentes laborales.

Derecho de supresión

El artículo 7 regula el *derecho de supresión*, también conocido como «derecho al olvido». Permite a las personas solicitar la eliminación de sus datos personales cuando ya no son necesarios, cuando se usaron sin autorización o cuando su tratamiento ya no tiene un fundamento legal válido.

Sin embargo, hay excepciones. No siempre es posible borrar los datos si existen razones de interés público o legal que exijan su conservación.

¿Cuándo puedes solicitar que se borren tus datos?

Tienes derecho a solicitar que eliminen tus datos personales en estas situaciones:

* *Cuando ya no son necesarios:* si dieron tus datos para algo en específico y ese motivo ya no existe, deberían borrarlos.
* *Cuando cambiaste de opinión:* si tus datos estaban siendo tratados porque tú lo autorizaste, puedes retirar ese consentimiento y solicitar su eliminación, siempre que no exista otra base legal que justifique su conservación.
* *Cuando los obtuvieron de forma ilegal:* si alguien recopiló o usó tus datos sin tu autorización o sin cumplir la ley.
* *Cuando están desactualizados o caducaron:* por ejemplo, si ya no tienen valor porque el tiempo pasó y la información ya no es relevante.
* *Cuando existe una orden para eliminarlos:* si un juez, una autoridad de protección de datos o una ley dice que deben ser borrados.
* *Cuando te opones a su uso:* si decides que no quieres que sigan tratando tus datos y no hay una razón legal que lo justifique.

¿Cuándo NO pueden borrar tus datos?

Hay algunas excepciones en las que no se podrá eliminar tus datos, incluso si lo pides:

* *Si afecta la libertad de expresión o información:* no se puede borrar datos que sean necesarios para informar o ejercer la libertad de opinión.

* *Si la ley o un contrato lo exige:* por ejemplo, si una empresa debe conservarlos por ley o porque forman parte de un contrato vigente.
* *Si son necesarios para el Estado o el interés público:* como registros usados por el gobierno o por entidades públicas.
* *Si se necesitan para proteger la salud pública:* en casos donde la información es clave para la seguridad sanitaria de la población.
* *Si sirven para investigaciones o estadísticas:* datos usados en estudios históricos, científicos o estadísticos en beneficio de la sociedad.
* *Si se necesitan para un juicio o reclamación legal:* si alguien está usando esos datos para defenderse o presentar una demanda.



Caso práctico

Un usuario de una red social decide eliminar su cuenta y solicita que todos sus datos sean borrados. Si no existe ninguna obligación legal que requiera conservar esa información (como registros de transacciones comerciales), la plataforma debe eliminar los datos personales del usuario.

En cambio, si una persona quiere eliminar su historial de deudas en una entidad financiera, es probable que no pueda hacerlo si esa información debe conservarse por obligación legal.

Recomendación:

este derecho es útil cuando los datos personales ya no tienen un propósito legítimo o fueron utilizados de manera indebida. Sin embargo, antes de solicitar la eliminación, es importante verificar si existen razones legales o de interés público que justifiquen su conservación.

Derecho de oposición

Conforme indica el artículo 8, el derecho de oposición te permite decir «no quiero que usen mis datos personales» en ciertas situaciones. Básicamente, puedes solicitar que una empresa o institución deje de tratar tu información si no tienes obligación de permitirlo.[31]

¿Cuándo puedes oponerte?

- Si el único motivo para usar tus datos es que a la empresa le conviene. A veces, las empresas procesan datos porque dicen que tienen un «interés legítimo». Si este es el único fundamento para tratar tu información, puedes pedir que la dejen de usar.

  Excepción: Si la empresa puede demostrar que tiene razones más importantes que tu derecho a la privacidad o si necesita los datos para una demanda legal, entonces podrá seguir usándolos.
- Si están usando tus datos para enviarte publicidad o promociones. Puedes oponerte a recibir anuncios, correos promocionales o cualquier otra estrategia de marketing que use tu información personal.
- Si tomaron tus datos de una fuente pública y no hay otra razón legal para usarlos. Por ejemplo, si alguien sacó tu información de un directorio público, pero no tiene una justificación válida para procesarla.

---

31 La forma en que se concibe el derecho de oposición en la nueva ley chilena presenta diferencias significativas respecto del enfoque adoptado por el Reglamento General de Protección de Datos (GDPR) en Europa. En este último, el titular puede oponerse al tratamiento de sus datos personales por razones vinculadas a su situación particular. No obstante, el responsable del tratamiento tiene la posibilidad de justificar su actuar si logra acreditar la existencia de motivos legítimos imperiosos que prevalezcan sobre los derechos, intereses y libertades del titular, o bien si el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones (ver Arenas [2021: p. 1707]). En contraste, la ley chilena establece un catálogo cerrado de situaciones en las que el titular puede ejercer el derecho de oposición, sin contemplar la posibilidad de que el responsable contrarreste dicha oposición argumentando un interés superior, salvo en el caso específico del literal a), que trata precisamente sobre los tratamientos basados en el interés legítimo como fundamento de licitud.

¿Cuándo NO puedes oponerte?

No puedes ejercer este derecho si los datos se están usando para:

- investigación científica o histórica (como estudios médicos o sociológicos),
- estadísticas importantes para la sociedad (por ejemplo, censos o encuestas nacionales), o
- funciones del Estado o actividades de interés público (por ejemplo, si una institución gubernamental necesita los datos para cumplir con su labor).



Caso práctico

Una persona recibe correos electrónicos de una empresa con promociones y ofertas sin haber dado su consentimiento. Puede ejercer su derecho de oposición y exigir que la empresa deje de utilizar sus datos para fines de marketing. La empresa deberá detener el envío de estos mensajes, salvo que pueda demostrar que existen razones legítimas para continuar con el tratamiento.

En cambio, si una entidad pública está utilizando datos personales para una investigación estadística sobre salud pública, el titular no podrá oponerse, ya que estos datos son necesarios para el interés general.

Recomendación:

El derecho de oposición es útil cuando una persona quiere evitar que sus datos sean utilizados para fines específicos, como publicidad o marketing, o cuando considera que el tratamiento de su información no está justificado. Para ejercerlo, es recomendable contactar directamente al responsable del tratamiento y solicitar el cese del uso de los datos.



Apliquemos lo aprendido 2

1. ¿Cuál de los siguientes derechos permite al titular solicitar la eliminación de sus datos personales cuando ya no son necesarios para los fines del tratamiento?

a. Derecho de rectificación

b. Derecho de supresión

c. Derecho de oposición

2. Si un titular de datos descubre que su dirección está incorrecta en los registros de una empresa, ¿qué derecho debería ejercer?

a. Derecho de supresión

b. Derecho de acceso

c. Derecho de rectificación

3. ¿En qué caso no procede la supresión de datos personales?

a. Cuando los datos son inexactos

b. Cuando los datos son necesarios para cumplir una obligación legal

c. Cuando el titular revoca su consentimiento

4. El derecho de oposición es más adecuado en situaciones donde:

a. Los datos se han vuelto irrelevantes

b. El tratamiento se basa en intereses legítimos del responsable

c. Los datos necesitan ser rectificados

5. ¿Qué ocurre después de que los datos personales han sido rectificados?

a. Se eliminan inmediatamente

b. Se comunican las rectificaciones a las entidades que los recibieron, salvo imposibilidad o esfuerzo desproporcionado

c. Se bloquean temporalmente

6. ¿Qué acción puede tomar un titular si se opone al tratamiento de sus datos para fines de marketing directo?

a. Solicitar la rectificación de sus datos

b. Exigir la supresión inmediata de sus datos

c. Oponerse al tratamiento de sus datos y solicitar que cese.

7. ¿En qué circunstancia puede un responsable continuar tratando los datos a pesar de la oposición del titular?

a. Cuando el titular ha revocado su consentimiento

b. Cuando el tratamiento es necesario para el cumplimiento de un contrato

c. Cuando el tratamiento es con fines de marketing directo

8. ¿Cuál de los siguientes derechos se aplica cuando el titular desea que se dejen de utilizar sus datos para un fin específico, como el marketing?

a. Derecho de rectificación

b. Derecho de acceso

c. Derecho de oposición

9. ¿Qué derecho permite al titular corregir datos personales inexactos?

a. Derecho de oposición

b. Derecho de acceso

c. Derecho de rectificación

10. ¿Qué sucede si un titular se opone al tratamiento de sus datos y el responsable no puede demostrar motivos legítimos para continuar el tratamiento?

a. El responsable debe rectificar los datos

b. El responsable debe suspender el tratamiento

c. El titular debe ejercer su derecho de supresión

Tabla 1. Cuadro comparativo entre los derechos de rectificación y oposición

	Derecho de rectificación	Derecho de oposición
¿Qué permite?	Corregir o actualizar datos personales que sean incorrectos, estén desactualizados o estén incompletos.	Impedir o detener el tratamiento de datos personales en casos específicos, como marketing o tratamiento basado en intereses legítimos.
Objetivo	Garantizar que la información personal sea precisa y adecuada para su uso.	Proteger la privacidad del titular y evitar el uso de sus datos para fines no deseados.
¿Cuándo se aplica?	Cuando los datos almacenados por una empresa o entidad contienen errores o no están actualizados.	Cuando el titular no desea que sus datos sean utilizados para determinados fines, como publicidad o estudios de mercado.
Ejemplo 1	Un cliente nota que su dirección está mal escrita en los registros de una tienda online y solicita la corrección.	Un usuario recibe correos promocionales sin haberlos solicitado y pide que se detenga el envío.
Ejemplo 2	Un empleado se da cuenta de que su número de teléfono en los registros de la empresa es incorrecto y pide que se actualice.	Un banco utiliza los datos de un cliente para analizar su perfil de consumo, mientras que este solicita que dejen de hacerlo.
Recomendación de uso	Se debe utilizar cuando el problema es la inexactitud de los datos y esto puede afectar la comunicación o la prestación de un servicio.	Se recomienda utilizar cuando el titular desea impedir el uso de sus datos para fines que considera innecesarios o no justificados.
Base legal	Se fundamenta en la necesidad de que los datos sean exactos y actualizados para garantizar su uso correcto.	Se basa en el derecho del titular a decidir sobre el uso de su información personal y proteger su privacidad.
Obligación del responsable	Corregir los datos inexactos y, si es necesario, notificar a quienes hayan recibido la información errónea.	Dejar de tratar los datos del titular para los fines indicados, salvo que existan razones legítimas para continuar.
Impacto en el tratamiento de datos	Una vez corregidos los datos, el responsable no podrá seguir usando la información incorrecta.	Si se acepta la oposición, el tratamiento de los datos para ese fin debe cesar inmediatamente.
Beneficio a largo plazo	Mejora la precisión de la información, asegurando una gestión eficiente de los datos.	Protege al titular del uso indebido de su información personal y refuerza su derecho a la privacidad.



Caso práctico

Valoración de derechos

El cliente de una compañía de seguros descubre que su dirección está registrada de forma incorrecta en la base de datos de la empresa. Al mismo tiempo, se entera de que la compañía ha actualizado su política de privacidad y ahora utiliza los datos de los clientes para estudios de marketing y análisis de mercado. No está de acuerdo con esto y quiere tomar medidas para corregir su información y evitar el uso de sus datos con estos fines.

¿Qué derechos puede ejercer el cliente para corregir su información y evitar que sus datos sean utilizados para marketing? ¿En qué orden debería hacerlo?

Conclusión:

Gracias a estos derechos, el cliente puede asegurarse de que su información personal sea precisa y, al mismo tiempo, proteger su privacidad, evitando que sus datos sean utilizados sin su consentimiento para fines comerciales.

Tabla 2. Cuadro comparativo entre los derechos de oposición y supresión de datos personales

	Derecho de oposición	Derecho de supresión
¿Qué permite?	Permite al titular rechazar el tratamiento de sus datos personales en ciertos casos, por ejemplo, cuando se usan para marketing o basados en intereses legítimos del responsable.	Permite al titular solicitar la eliminación de sus datos personales cuando ya no son necesarios, cuando ha retirado su consentimiento o cuando se han tratado de manera ilegal.
Objetivo	Evitar que los datos sean utilizados para fines que el titular considera innecesarios, inapropiados o perjudiciales.	Garantizar que los datos del titular sean eliminados cuando ya no haya una justificación legal para conservarlos.
¿Cuándo se aplica?	Cuando el titular no desea que sus datos sean utilizados para fines específicos, como publicidad, o cuando considera que el tratamiento no está debidamente justificado.	Cuando los datos han cumplido su propósito, el titular retira su consentimiento o el tratamiento de los datos es ilegal.
Ejemplo práctico 1	Un cliente rechaza que una empresa de telecomunicaciones use sus datos para ofrecer promociones que no ha solicitado.	Un usuario de una red social solicita la eliminación de su cuenta y toda la información relacionada.
Ejemplo práctico 2	Un paciente se opone a que sus datos médicos sean utilizados en estudios de mercado por una farmacéutica, ya que considera que su información debe ser confidencial.	Un exempleado pide que su información personal sea eliminada de los registros de su antigua empresa, puesto que ya no es necesaria.
Recomendación de uso	Se recomienda usar cuando el titular quiere impedir que sus datos sean utilizados para un propósito en particular, sin que se eliminen completamente.	Se recomienda cuando el titular quiere asegurarse de que sus datos sean eliminados de manera definitiva.
Base legal	Basado en el derecho del titular a controlar el uso de su información personal y oponerse a tratamientos no deseados.	Basado en la protección de la privacidad, asegurando que los datos no sean retenidos innecesariamente o sin justificación.
Obligación del responsable	Detener el uso de los datos para los fines a los que el titular se opone, salvo que existan razones legales para continuar.	Eliminar los datos personales, salvo que exista una obligación Legal que justifique su conservación.

Tabla 2. (Continuación)

	Derecho de oposición	Derecho de supresión
Impacto en el tratamiento de datos	Si se acepta la oposición, el tratamiento de los datos para esos fines debe cesar de inmediato, a menos que haya una justificación legal para continuar.	Una vez eliminados, el responsable no puede seguir tratando los datos ni almacenarlos de forma accesible.
Beneficio a largo plazo	Protege al titular del uso indebido de su información y fortalece su derecho a decidir sobre el tratamiento de sus datos.	Reduce el riesgo de que los datos sean utilizados en el futuro sin consentimiento, mejorando la protección de la privacidad.



Caso práctico

Valoración de derechos

Un cliente de una tienda en línea descubre que la empresa está utilizando su historial de compras para enviarle recomendaciones de productos y ofertas personalizadas. Al principio, no le molestaba, pero ahora siente que esto invade su privacidad y quiere que la tienda deje de usar sus datos con ese propósito. Además, está considerando eliminar su cuenta y que todos sus datos personales sean borrados por completo.

¿Qué derecho puede ejercer el cliente para dejar de recibir recomendaciones y ofertas? ¿Qué derecho debe ejercer si decide eliminar su cuenta y toda su información de la tienda?

Conclusión:

Este caso muestra la importancia de que los usuarios conozcan y ejerzan sus derechos sobre sus datos personales. Gracias a los derechos de oposición y supresión, el cliente puede decidir cómo se utilizan sus datos y proteger su privacidad. Las empresas, por su parte, deben respetar estas solicitudes y garantizar un manejo transparente de la información personal.

«Cuando los algoritmos deciden por ti»

Hoy, muchas decisiones no son tomadas por personas, sino por computadoras. Por ejemplo, cuando una app te recomienda una película o cuando un banco decide si te aprueba un crédito, es probable que estén usando tus datos personales y un sistema automatizado para llegar a esa conclusión. Pero ¿qué pasa si esa decisión no es justa o no estás de acuerdo con ella?

El artículo 8 bis habla justamente de esto. Este artículo te da el derecho a decir "no" a las decisiones que se tomen únicamente de forma automática, especialmente si esas decisiones pueden afectar de manera importante tu trabajo, tu economía o tu vida personal.[32]

Sin embargo, existen excepciones. Por ejemplo, si estás firmando un contrato y es necesario usar un sistema automatizado para procesarlo o si tú mismo das tu permiso explícito, estas decisiones sí pueden llevarse a cabo. Pero, en todos los casos, las empresas o instituciones tienen la obligación de asegurarse de que tus derechos estén protegidos. Esto significa que deben informarte claramente, darte la posibilidad de opinar, explicarte cómo se tomó la decisión y permitirte pedir una revisión si no estás de acuerdo.

En resumen, este artículo busca equilibrar el uso de la tecnología con tus derechos. Porque, al final del día, tú deberías tener el control sobre cómo se usan tus datos y cómo te afectan las decisiones que se toman con ellos.

Concepto de decisiones individuales automatizadas y elaboración de perfiles

Decisiones individuales automatizadas: Imagina que una computadora toma una decisión sobre ti sin que una persona la revise o intervenga de manera real en el proceso. Por ejemplo, que un sistema automático determine si te aprueban un crédito, si accedes a un beneficio o si continuas en un proceso de selección laboral.

Hablamos de *decisiones automatizadas* cuando el sistema actúa con un grado relevante de autonomía respecto de una persona y la decisión produce efectos jurídicos o afecta de manera significativa tu situación.

---

32 Esta norma se basa en el artículo 22 del GPDR, con el objeto de enfrentar los desafíos que representa el uso de algoritmos y la implementación de sistemas de IA.

Aunque pueden ser rápidas y eficientes, este tipo de decisiones pueden influir de forma importante en tu vida, por lo que la ley establece garantías especiales para asegurar que se utilicen de manera justa, transparente y con posibilidad de revisión.

Elaboración de perfiles: ¿Alguna vez te has preguntado cómo las redes sociales saben qué publicaciones mostrarte o cómo las tiendas en línea te recomiendan productos que parecen hechos para ti?

Esto se debe a la *elaboración de perfiles*. Básicamente, es cuando las empresas usan tus datos (como lo que te gusta, cómo te comportas o tu situación económica) para crear una «ficha» sobre ti, que les ayuda a tomar decisiones más informadas, pero también puede generar preocupaciones, como que te traten de manera injusta o que usen tu información de forma que no te sientes cómodo.[33]

Excepciones al derecho a oponerse

El derecho consagrado en el artículo 8 bis de la Ley 21.719 permite oponerse y no ser objeto de decisiones automatizadas que te afecten significativamente o te produzcan efectos jurídicos, pero no opera de forma absoluta. El mismo artículo establece tres casos de excepción, en los que estas decisiones pueden seguir aplicándose legalmente, aun cuando el titular no esté de acuerdo:[34]

---

33 Como señala Contreras y otros (2025: p. 103): «El encabezado del artículo 8 bis —al igual que el artículo 22 del GDPR— señala que aplica tanto para las decisiones basadas en el tratamiento automatizado de datos personales como para la elaboración de perfiles. Sin embargo, como correctamente ha señalado Medina, *mutatis mutandis*, el artículo 8 bis no regula el tratamiento de datos, sino que la toma de decisiones basadas en el tratamiento automatizado de datos. La creación de perfiles necesariamente implica el tratamiento automatizado de datos personales, pero no necesariamente implica la toma de una decisión». «Sin embargo, para efectos prácticos, la elaboración de perfiles queda sujeta a la misma prohibición general contenida en el artículo 8 bis, y solo podrán ser realizadas si concurre alguna de las circunstancias contenidas en el inciso 2 del mismo artículo».

34 Algunos autores señalan que el artículo 8 bis puede entenderse tanto como un derecho que el titular puede ejercer de forma autónoma como una prohibición condicionada del uso de decisiones automatizadas que afecten significativamente al titular, ya que el artículo ordena que estas decisiones solo se adopten si se verifica alguna de sus excepciones. Ese matiz es objeto de interpretación doctrinal y de futura orientación jurisprudencial o regulatoria. Sobre el debate doctrinal respecto de si el artículo 8 bis consagra

- *Cuando es necesario para cumplir un contrato:* Si estás haciendo un trato con una empresa (por ejemplo, solicitando un préstamo) y se necesita usar un sistema automatizado para evaluar tu solicitud, no puedes oponerte. Esto responde a que la decisión automatizada es parte esencial del proceso.
- *Cuando tú das tu permiso:* Si en algún momento aceptas de manera clara y explícita que tus datos se usen para tomar decisiones automatizadas, no podrás oponerte después. Eso sí, tu consentimiento debe cumplir con las reglas que establece la ley.
- *Cuando la ley lo permite:* En algunos casos, la misma ley autoriza el uso de decisiones automatizadas, siempre asegurando que tus derechos estén protegidos. Por ejemplo, si el gobierno usa un sistema automatizado para evaluar quiénes pueden recibir un subsidio, esto estaría permitido si la ley lo respalda.

En resumen, aunque tienes derecho a oponerte a las decisiones automatizadas, existen situaciones en las que estas decisiones son necesarias o están permitidas. Lo importante es que siempre se respeten tus derechos y que se te informe claramente sobre cómo se usan tus datos.

Derechos adicionales del titular en caso de decisiones automatizadas

Aunque en algunos casos se permiten las decisiones automatizadas, las empresas o instituciones tienen la obligación de proteger tus derechos. Esto significa que, incluso cuando usen sistemas automatizados, cuentas con varias herramientas para asegurarte de que todo sea justo y transparente. Estos son tus derechos:

- *Derecho a la información y transparencia:* Las empresas deben explicarte que van a usar tus datos en un proceso automatizado y cómo funciona ese proceso. No pueden tomar decisiones a escondidas; tienes derecho a saber qué están haciendo con tu información.

---

un derecho subjetivo del titular o configura una prohibición general condicionada a determinadas excepciones. Véase Viollier y Contreras (2026).

- *Derecho a obtener una explicación:* Si una decisión automatizada te afecta, puedes pedir que te expliquen cómo se llegó a esa conclusión. La explicación debe ser clara y fácil de entender, no llena de tecnicismos.[35]
- *Intervención humana:* Si una decisión automatizada te afecta de manera importante, puedes pedir que una persona la revise. Esto es especialmente útil si crees que la computadora se equivocó o si no estás de acuerdo con el resultado.
- *Expresar tu punto de vista:* Tienes derecho a dar tu opinión sobre la decisión automatizada. Si algo no te parece justo o tienes preocupaciones al respecto, puedes decirlo y pedir que esto sea tomado en cuenta.
- *Derecho a solicitar una revisión:* Si no estás de acuerdo con la decisión que tomó el sistema automatizado, puedes pedir su revisión. Esto podría implicar que una persona intervenga y reevalúe la decisión para asegurarse de que sea justa.

---

35 Sobre el alcance del derecho a obtener una explicación frente a decisiones automatizadas, resulta especialmente relevante la Sentencia del Tribunal de Justicia de la Unión Europea de 27 de febrero de 2025, asunto Dun & Bradstreet Austria (C-203/22).

En este caso, una persona fue rechazada para contratar un servicio telefónico debido a un perfil de solvencia (*credit score*) generado mediante un sistema automatizado. Al ejercer su derecho de acceso conforme al artículo 15 del Reglamento General de Protección de Datos (RGPD), solicitó conocer qué datos se habían utilizado y cómo funcionaba la lógica del sistema que determinó el resultado.

El Tribunal estableció que el responsable del tratamiento no puede limitarse a entregar explicaciones genéricas. Debe proporcionar información clara, comprensible y concreta sobre los criterios utilizados y sobre cómo los datos personales influyeron en el resultado. No es necesario revelar el algoritmo completo, pero sí explicar el procedimiento de forma inteligible.

Además, señaló que la alegación de secreto comercial no puede justificar una negativa absoluta a entregar información. Si existe conflicto entre derechos, debe realizarse una ponderación caso a caso.

Aunque el asunto no era laboral, su doctrina es plenamente aplicable a decisiones automatizadas en el ámbito del empleo, reforzando el derecho de las personas a comprender, cuestionar y eventualmente impugnar decisiones adoptadas mediante sistemas de inteligencia artificial.

En resumen, aunque las decisiones automatizadas pueden ser útiles, tú tienes el poder de asegurarte de que se usen de manera responsable y respetando tus derechos. ¡No estás solo frente a la tecnología!



Caso práctico

Decisiones automatizadas en la evaluación de créditos

María quiere pedir un préstamo en un banco para hacer unas reparaciones en su casa. Sin embargo, al enviar su solicitud, recibe una respuesta automática diciendo que su préstamo fue rechazado. El banco usó un sistema computarizado que analizó su historial crediticio y decidió negarle el préstamo sin que una persona lo revisara. María sospecha que el sistema usó información desactualizada sobre sus finanzas, como un antiguo préstamo que ya pagó, y no está de acuerdo con la decisión.

¿Puede María oponerse a esta decisión automatizada y pedir que una persona revise su caso?

¿Por qué esto es importante?

Este caso muestra cómo las decisiones automatizadas pueden afectar a las personas en situaciones importantes, como obtener un préstamo. Pero también demuestra que, gracias a la ley, tú tienes herramientas para defender tus derechos y asegurarte de que las decisiones sean justas y transparentes.



Apliquemos lo aprendido 3

1. Qué es una decisión individual automatizada según el artículo 8 bis?

a. Una decisión tomada únicamente por una persona

b. Una decisión tomada sin intervención humana, basada únicamente en el tratamiento automatizado de datos personales

c. Una decisión tomada por una autoridad

2. ¿Cuándo NO puede el titular oponerse a una decisión automatizada según el artículo 8 Bis?

a. Cuando la decisión es necesaria para la ejecución de un contrato

b. Cuando la decisión se basa en la satisfacción de intereses legítimos

c. Siempre puede oponerse, sin excepciones

3. ¿Qué derecho adicional tiene el titular cuando se toma una decisión automatizada que lo afecta significativamente?

a. Solicitar la supresión de sus datos

b. Solicitar la intervención humana y una explicación

c. Solicitar la elaboración de un nuevo perfil

4. ¿En qué caso se permite la elaboración de perfiles sin el derecho de oposición?

a. Cuando la decisión afecta positivamente al titular

b. Cuando hay consentimiento previo y expreso del titular

c. Cuando la empresa considera que la elaboración de perfiles es necesaria para su negocio

5. ¿Qué debe hacer el responsable del tratamiento cuando utiliza decisiones automatizadas?

a. Simplemente notificar al titular de los datos

b. Adoptar medidas que aseguren el derecho a la información, transparencia y la posibilidad de intervención humana

c. Eliminar los datos después de cada decisión

El derecho de bloqueo: pausar el uso de tus datos personales

El derecho de bloqueo (regulado en el artículo 8 Ter.) es como poner «pausa» en el uso de tus datos personales. Imagina que has pedido a una empresa que corrija o elimine tu información, pero mientras esperas a que resuelvan tu solicitud, no quieres que sigan usando tus datos. Este derecho te permite pedir que se suspendan temporalmente las operaciones con tus datos hasta que tu caso sea resuelto.

En otras palabras, si has solicitado que corrijan, eliminen o dejen de usar tus datos, el bloqueo asegura que, mientras tanto, nadie los use. Es una forma de protegerte y evitar que sigan usando información incorrecta o que no quieres que se utilice.



Caso práctico

Derecho de bloqueo

A) Imagina que eres cliente de una compañía de teléfono y te das cuenta de que tienen mal registrado tu correo electrónico. Les pides que lo corrijan, pero mientras tanto, no quieres que sigan enviándote facturas o comunicaciones a esa dirección equivocada. Con el derecho de bloqueo, puedes solicitar que dejen de usar tus datos temporalmente hasta que arreglen el error. Así evitas problemas como facturas pérdidas o información confidencial enviada al lugar incorrecto.

Alternativa a la eliminación

El derecho de bloqueo también es útil si no quieres que tus datos sean eliminados por completo, pero tampoco quieres que los sigan usando. Por ejemplo, si estás en desacuerdo con la forma en que una empresa usa tu información, pero no quieres borrar todo, puedes pedir que «congelen» el uso de tus datos mientras se resuelve

tu solicitud. Durante este tiempo, tus datos se guardan, pero no se pueden usar.

¿Por qué es importante este derecho?
El derecho de bloqueo es una herramienta poderosa para proteger tu información personal. Te da control sobre cómo y cuándo se usan tus datos, especialmente cuando estás en proceso de corregir algo o de oponerte a su uso. Es como tener un botón de "pausa" para tu privacidad.

***

B) Imagina que usas una plataforma de *streaming*, como Netflix o Spotify, y te das cuenta de que tu historial de reproducción tiene errores. Por ejemplo, aparecen películas o canciones que nunca viste o escuchaste. Esto afecta las recomendaciones que recibes, sugiriéndote contenido que no te interesa. Decides solicitar que tu historial sea corregido, pero mientras tanto no quieres que sigan usando esos datos incorrectos para recomendarte cosas. Entonces solicitas que «bloqueen» temporalmente el uso de tu historial hasta que sea arreglado.

¿Qué derecho está usando el usuario y cómo le ayuda?



Apliquemos lo aprendido 4

1. ¿En qué situación puede el titular de los datos ejercer el derecho de bloqueo del tratamiento?

a. Cuando presenta una solicitud de rectificación, supresión u oposición

b. Cuando desea eliminar permanentemente sus datos

c. Cuando la empresa requiere verificar su identidad

2. ¿Qué implica el ejercicio del derecho de bloqueo?

a. La eliminación inmediata de los datos

b. La suspensión temporal del tratamiento de los datos mientras se resuelve una solicitud

c. El acceso permanente a los datos

3. El derecho de bloqueo ¿implica la eliminación de los datos personales?

a. Sí, siempre que se solicite

b. No, solo implica la suspensión temporal del tratamiento

c. Solo si el titular lo solicita explícitamente

4. ¿En qué casos puede el titular ejercer el derecho de bloqueo como alternativa a la supresión?

a. En cualquier caso

b. Cuando los datos son tratados automáticamente

c. En los casos mencionados en el artículo 7

5. El derecho de bloqueo ¿afecta el almacenamiento de los datos?

a. Sí, impide que se almacenen los datos

b. No, solo detiene el tratamiento temporal de los datos mientras se resuelve la solicitud

c. Depende del tipo de datos tratados

El derecho a llevarte tus datos: portabilidad

El derecho a la portabilidad (artículo 9) constituye la llave para tus datos personales. Te permite pedir una copia de tu información en formato digital y fácil de usar, para que puedas llevártela a otra empresa o servicio sin problemas. Es especialmente útil cuando quieres cambiar de proveedor, como pasarte de una compañía de teléfono a otra o de una red social a una nueva plataforma.

Este derecho aplica cuando:

* Tus datos se procesan de forma automatizada (es decir, con sistemas computarizados).
* Tú diste tu consentimiento para que usen tus datos.

En otras palabras, la portabilidad te da control sobre tu información y facilita que cambies de servicio sin perder tiempo ni datos.



Caso práctico

Derecho a la portabilidad

A) Imagina que usas una red social y decides cambiarte a otra plataforma. En lugar de empezar desde cero, puedes solicitar que te envíen tu perfil, tu lista de contactos y tus fotos en un formato que la nueva plataforma pueda usar. Así, no pierdes tu información y el cambio es mucho más sencillo.

Transferencia directa entre empresas

En algunos casos, tus datos pueden transferirse directamente de una empresa a otra, siempre que sea técnicamente posible. Por ejemplo, si cambias de proveedor de Internet, puedes solicitar que tus datos (como tu historial de pagos o tus preferencias) se envíen automáticamente al nuevo proveedor.

Portabilidad sin eliminar tus datos

Es importante saber que, al ejercer tu derecho a la portabilidad, tus datos no se eliminan automáticamente de la empresa original. Solo se borrarán si tú lo pides de forma explícita. Esto te permite conservar tus datos en ambos lugares si así lo prefieres.

***

B) Ana quiere cambiar de proveedor de almacenamiento en la nube. Le pide a su proveedor actual que transfiera todos sus archivos y datos personales al nuevo proveedor en un formato que pueda usar fácilmente. Además, le solicita que eliminen sus datos de su sistema una vez que se complete la transferencia.

¿Qué derechos está ejerciendo Ana y qué debe hacer el proveedor?

¿Por qué es importante este derecho?

El derecho a la portabilidad te da libertad y control sobre tus datos personales. Te permite cambiar de servicios sin perder tu información y asegura que las empresas no te «aten» a sus plataformas solo porque es difícil llevarte tus datos. ¡Es como tener la libertad de moverte con tus pertenencias digitales a donde quieras!



Apliquemos lo aprendido 5

1. ¿Qué permite el derecho a la portabilidad de los datos personales?

a. Obtener una copia de los datos en un formato estructurado y transferirlos a otro responsable

b. Eliminar automáticamente los datos del primer responsable

c. Cambiar el formato de los datos sin consentimiento

2. ¿Qué condición es necesaria para ejercer el derecho a la portabilidad?

a. Que los datos sean inexactos

b. Que el tratamiento se base en el consentimiento del titular

c. Que los datos sean eliminados después de la transferencia

3. ¿El derecho de portabilidad implica la supresión automática de los datos del primer responsable?

a. Sí, siempre que se transfieran los datos

b. No, salvo que el titular lo solicite explícitamente

c. Solo si los datos son incorrectos

4. ¿En qué formato deben entregarse los datos al ejercer el derecho de portabilidad?

a. En cualquier formato

b. En un formato electrónico, estructurado y de uso común

c. En formato impreso

5. ¿Qué debe hacer el responsable si el titular solicita la transferencia directa de sus datos a otro responsable?

a. Rechazar la solicitud si no es técnicamente posible

b. Hacerlo en un formato incompatible

c. Facilitar la transferencia si es técnicamente posible



Quien maneja tus datos debe respetar las reglas

¿Qué debe hacer quien maneja tus datos? Obligaciones clave del responsable según la ley

El artículo 14 de la Ley de Protección de Datos Personales establece las reglas que deben seguir las personas o empresas que usan tus datos personales. Estas obligaciones están pensadas para proteger tu información y asegurarte que esta se use de manera segura y legal. A continuación, te explicamos de forma sencilla qué debe hacer el responsable del tratamiento de tus datos.

Debe explicarte por qué y cómo usa tus datos

Quien usa tus datos tiene que decirte con claridad para qué los va a usar y demostrar que lo está haciendo legalmente. Además, si tú lo pides, debe entregarte esa información sin demora.

Ejemplo: Si una tienda *online* quiere enviarte promociones por correo electrónico, debe explicarte que tiene tu permiso o que existe una norma que le permite hacerlo.

Debe obtener tus datos de forma legal y con un objetivo claro

Solo se pueden recoger tus datos de fuentes legales y usarse para un fin específico y legítimo, que se te haya informado previamente.

Ejemplo: Si compras un producto y das tu dirección, la empresa puede usar esa información para enviarte el pedido, pero no para inscribirte en un concurso sin tu consentimiento.

Debe asegurarse de que tus datos sean correctos y estén actualizados si los comparte

Si entrega tus datos a otra empresa o entidad, debe revisar que la información sea verdadera, completa y esté actualizada.

Ejemplo: Si una empresa comparte tus datos con una agencia de cobranza, debe verificar que la deuda existe y que los datos sean correctos.

Debe eliminar o anonimizar tus datos cuando ya no los necesite

Si tus datos fueron entregados para cotizar un servicio o producto y luego no se concreta nada, tus datos deben borrarse o transformarse para que no puedas ser identificado.

Ejemplo: Si pides la cotización de un crédito y no aceptas la oferta, tus datos no deben seguir guardados sin motivo.

Debe cumplir con todos los principios de la ley

Esto incluye cuidar la confidencialidad de tus datos, protegerlos para que no se filtren y garantizar transparencia en su uso.



¿Y si la empresa está fuera de Chile?
Aunque la empresa no tenga oficina en Chile, si trata datos de personas que viven aquí, debe tener un correo electrónico u otro medio de contacto válido para que puedas hacer tus consultas o reclamo.



Caso práctico

¿Qué pasa con mis datos personales?

María solicitó un préstamo a una empresa financiera que presta servicios en Chile, aunque su oficina principal está en otro país. Lamentablemente, le rechazaron el préstamo. Al intentar saber por qué, María pidió información sobre cómo se usaron sus datos personales, pero la empresa nunca le respondió.

María sospecha que usaron información desactualizada sobre su situación financiera para tomar la decisión, como datos de deudas antiguas que ya están pagadas. Además, se dio cuenta de que la empresa nunca le entregó un correo electrónico ni otro medio para contactarlos desde Chile.



Para reflexionar y responder

- Si la empresa usó datos que ya no están actualizados, ¿qué debería haber hecho con esa información?
- Cuando una empresa que no tiene oficina en Chile presta servicios a personas que viven en el país, ¿qué medio de contacto debería entregar para recibir consultas o reclamos?
- ¿Qué podría hacer María si quiere saber cuáles de sus datos fueron utilizados y cómo los usaron para tomar esa decisión?



Apliquemos lo aprendido 1

1. Cuando una empresa comparte tus datos con otra, ¿qué es lo que primero debe asegurarse?

a. Que la otra empresa tenga buenas referencias

b. Que los datos que comparte sean correctos y estén actualizados

c. Que el titular siempre dé su permiso por escrito

2. ¿Qué debe hacer una empresa con tus datos si ya no los necesita para el motivo por el que los pidió?

a. Guardarlos por si acaso

b. Borrarlos o convertirlos en anónimos para que no te identifiquen

c. Enviarlos a una base de datos del gobierno

3. Si una empresa está fuera de Chile, pero usa datos de personas que viven aquí, ¿qué debe hacer?

a. Tener un teléfono chileno disponible

b. Publicar su dirección en Internet

c. Dar un correo electrónico u otro medio para que la gente pueda contactarla

4. Cuando una empresa recolecta datos personales, ¿qué debe garantizar?

a. Que los datos se mantengan en secreto por diez años

b. Que los datos provengan de fuentes legales y se usen para fines claros

c. Que los pueda usar como quiera

5. ¿Qué principio debe seguir una empresa cuando entrega tus datos a otra?

a. Solo el principio de confidencialidad

b. El principio de transparencia

c. El principio de exactitud y actualización, para que los datos estén correctos

Deber de secreto o confidencialidad

El artículo 14 bis señala que toda persona o institución que maneje tus datos personales tiene la obligación de mantenerlos en secreto o bajo confidencialidad, es decir, no puede compartirlos con otros sin tu permiso, a menos que tú los hayas hecho públicos.

En la práctica, ¿qué significa esto?

Si entregaste tu información personal a una empresa o institución (como tu nombre, dirección, historial financiero o de salud), esa información debe mantenerse protegida, incluso después de que termines tu relación con esa empresa. Por ejemplo, si cerraste una cuenta bancaria, ese banco no puede divulgar tu información.

¿Y si la información se obtuvo desde fuentes públicas?

Aunque algunos datos estén disponibles públicamente (como tu nombre en una red social o en un registro público), si una empresa los organiza, cruza o complementa con otros datos para sacar conclusiones, también está obligada a mantenerlos confidenciales.

¿Hay excepciones?

Sí. Esta obligación no impide que se entreguen datos si la ley lo exige o si tú, como titular de los datos, pides acceder a ellos o saber de dónde los obtuvieron.

¿Y las personas que trabajan con esos datos?

La empresa que trata los datos debe asegurarse de que sus empleados y las empresas externas que colaboran con ella también respeten el deber de confidencialidad. Esta obligación subsiste incluso después de terminada la relación laboral o contractual.

Esto significa que quien haya tenido acceso a datos personales no puede divulgarlos ni utilizarlos para otros fines, aunque ya no trabaje para esa organización.



Caso práctico

A) Imagina que postulas a un crédito en una tienda. Entregas tus datos personales y luego decides no tomar el crédito. Aun así, la tienda debe seguir protegiendo tu información y no puede usarla ni compartirla sin tu consentimiento, incluso si ya no eres su cliente.

B) Una clínica dental recolecta y almacena datos personales y médicos de sus pacientes. Sofía, una paciente habitual, deja de atenderse allí y cambia de prestador de salud. A los meses, descubre que la clínica compartió su historial odontológico con una empresa de marketing sin su autorización, con el fin de ofrecerle tratamientos estéticos. Indignada, Sofía presenta una queja por vulneración de la confidencialidad.



Para reflexionar y responder

- ¿Qué deber incumplió la clínica al compartir los datos de Sofía sin su consentimiento, considerando que ya no existía una relación activa entre ambas partes?
- ¿Continúa vigente el deber de confidencialidad, aunque Sofía ya no sea paciente?
- ¿Qué medidas debería haber adoptado la clínica respecto a sus empleados o a las empresas externas que trataron los datos?



Apliquemos lo aprendido 2

1. ¿Cuándo termina la obligación de guardar secreto sobre los datos personales?

a. Cuando la empresa lo decida

b. Nunca, sigue vigente incluso después de que termine la relación con la persona

c. Cuando se firma un nuevo contrato

2. Si una empresa combina datos públicos con datos personales, ¿qué debe hacer?

a. No tiene que hacer nada

b. Debe seguir respetando el deber de confidencialidad

c. Tiene que eliminar esos datos

3. ¿Quiénes deben cumplir con el deber de confidencialidad?

a. La empresa y todas las personas que trabajen con esos datos

b. Solo los trabajadores directos de la empresa

c. Solo empresas externas contratadas

4. Si una persona hizo públicos sus datos personales (por ejemplo, en redes sociales), ¿la empresa todavía debe guardarlos en secreto?

a. Sí, siempre

b. No, si los datos fueron publicados por la persona misma, no se aplica el deber de secreto

c. Tiene que borrar esos datos

5. ¿Puede la empresa entregar información confidencial si la ley lo exige?

a. Sí, si la ley lo pide, debe hacerlo

b. No, nunca

c. Solo si tiene permiso del dueño de los datos

«Tu información, tus reglas»: lo que toda persona debe saber sobre la transparencia en el uso de sus datos personales

Cuando entregamos nuestros datos personales a una empresa o institución, tenemos derecho a saber qué harán con ellos. Para proteger ese derecho, la ley exige en su artículo 14 Ter que quienes manejan datos (los llamados *responsables del tratamiento*) entreguen información clara, fácil de entender y accesible para todos.

Esta información debe estar disponible públicamente, por ejemplo, en el sitio *web* de la empresa para que cualquier persona pueda saber cómo se recopilan, usan y protegen sus datos.

Aquí te explicamos, paso a paso, qué debe informar toda empresa o institución que trate tus datos personales.

Política de tratamiento de datos

La empresa debe publicar su política de privacidad, indicando claramente cómo maneja los datos personales, en qué fecha fue publicada y si ha sido modificada.

Ejemplo: una tienda *online* debe tener una sección donde explique cómo usa la información de sus clientes y actualizar esa política cada vez que cambie algo.

¿Quién es el responsable?

Debe decirse claramente quién es la persona o entidad a cargo de los datos, quién la representa legalmente y, si existe, quién se encarga de evitar malas prácticas.

Ejemplo: una empresa de telecomunicaciones debe publicar el nombre y los datos de contacto del encargado de datos personales.

Cómo contactar

Debe haber al menos un medio de contacto disponible, como un correo electrónico o un formulario *web*, para que cualquier persona pueda ejercer sus derechos sobre sus datos.

Ejemplo: un banco debería ofrecer un número o correo donde los clientes puedan preguntar por su información o pedir correcciones.

¿Qué datos se recopilan y para qué?

La empresa debe informar qué tipo de datos personales recoge (como nombre, dirección, correo o información financiera) y para qué los usa (enviar publicidad, procesar compras o mejorar servicios).

Ejemplo: una red social debe contar que recolecta información como tu historial de navegación para personalizar los anuncios que ves.

¿Qué tan seguros están tus datos?

Deben explicarse las medidas de seguridad que se usan para proteger tus datos, como sistemas de cifrado, contraseñas robustas o verificación en dos pasos.

Ejemplo: una aplicación de salud podría decir que protege tu información médica usando cifrado y autenticación biométrica.

Tus derechos como titular de datos

Debes saber qué derechos tienes y cómo ejercerlos. Por ejemplo, puedes pedir acceso a tus datos, corregirlos, eliminarlos o incluso oponerte a su uso. También puedes solicitar que te los entreguen para llevarlos a otra empresa (portabilidad).

Ejemplo: un servicio de almacenamiento en la nube debe explicar cómo puedes descargar tus archivos o pedir que se borren definitivamente.

Transferencias de datos al extranjero

Si tus datos serán enviados a otro país u organización internacional, se debe explicar si ese destino ofrece suficiente protección o qué garantías existen para cuidar tu información.

Ejemplo: una empresa que guarda datos en servidores ubicados fuera del país debe indicar si esa transferencia cumple con las leyes de protección de datos.



Caso práctico

Juan y la app misteriosa

Juan usa una aplicación de mensajería para comunicarse con sus amigos. Con el tiempo, nota algunas cosas preocupantes:

- La app recolecta su información de contacto y cómo la usa.
- No hay una política clara que explique qué hacen con sus datos.
- No encuentra ningún correo, teléfono o formulario para hacer preguntas.
- Descubre que sus datos se envían a otro país, pero nunca le dijeron si ese país los protege bien o si existía alguna garantía.



Para reflexionar y responder

- ¿Qué cosas debería hacer la aplicación para cumplir con las reglas del artículo 14 ter? Pista: piensa en lo que debe informar una empresa sobre el uso de datos personales, su política, responsables, contacto, medidas de seguridad y transferencias internacionales.
- Si la aplicación no da a Juan información clara sobre sus datos, ¿qué derechos tiene él como usuario? Pista: piensa en el derecho a saber, a corregir, a oponerse, a pedir que borren sus datos y otros derechos parecidos.
- ¿Qué puede hacer Juan si siente que sus derechos fueron pasados por alto o no respetados? Pista: recuerda que puede hacer reclamos ante una autoridad o pedir ayuda si cree que no se está cumpliendo la ley.



Apliquemos lo aprendido 3

1. ¿Qué debe incluir la empresa o institución en su política de tratamiento de datos personales?

a. Solo el nombre de la empresa

b. La política completa, con la fecha y versión actualizada.

c. Solo la fecha en que se creó la política

2. ¿Qué forma de contacto debe entregar el responsable de los datos personales?

a. Solo un número de teléfono

b. Un correo electrónico o un formulario fácil de usar

c. La dirección tributaria de la empresa

3. ¿Qué debe mencionar la empresa sobre las medidas de seguridad que usa para proteger tus datos?

a. El nombre del jefe de seguridad

b. Un resumen del personal que trabaja en seguridad

c. Las medidas técnicas que usa, como el cifrado o autenticación

4. Si una empresa no respeta tus datos personales, ¿qué puedes hacer como titular?

a. Presentar un reclamo ante la autoridad correspondiente

b. Reclamar solo ante la empresa, sin otras opciones

c. Exigir que le pongan una multa directamente

5. Si la empresa envía tus datos a otro país, ¿qué debe hacer?

a. Informar a la autoridad de protección de datos solamente

b. Informar si ese país protege bien los datos o si hay garantías especiales

c. Transferirlos sin decir nada

¿Por qué tu privacidad debería estar asegurada desde el inicio?

El artículo 14 quáter establece una regla fundamental para quienes manejan datos personales: la protección de los datos no puede ser algo improvisado o que se agrega al final del proceso. Debe estar presente desde el principio y en cada etapa del tratamiento de la información.

Privacidad desde el diseño

La ley exige que las medidas de seguridad estén pensadas e incorporadas desde el momento en que se comienza a crear un sistema o servicio, no después. Esto significa que la protección de los datos debe ser parte del diseño mismo.

Ejemplo: si una empresa desarrolla una plataforma de pagos en línea, debe incorporar protocolos de cifrado desde el inicio, para proteger la información financiera de los usuarios desde el primer momento.

Privacidad por defecto

El artículo señala que, por defecto, solo deben tratarse los datos personales que sean estrictamente necesarios. Es decir, si una persona no cambia ninguna configuración, su información igual debe estar protegida.

Ejemplo: una red social que solicita información para registrarse debería pedir solo lo básico (como nombre y correo electrónico), sin requerir datos adicionales como ubicación o intereses, a menos que el usuario decida entregarlos voluntariamente.

Evaluación de riesgos

El responsable de los datos también debe considerar los riesgos que pueden surgir durante el tratamiento, como accesos no autorizados, filtraciones o pérdidas de información. Por eso, es importante analizar estos peligros y tomar decisiones preventivas.

Ejemplo: una empresa que gestiona datos bancarios debería evaluar periódicamente si su sistema tiene vulnerabilidades que podrían ser explotadas por ciberataques.



Caso práctico

Y los datos, ¿para qué?

Una empresa que se dedica al análisis de datos desarrolla un nuevo sistema para recolectar información de sus usuarios. Este sistema recopila nombres, correos electrónicos, ubicación y hábitos de navegación. Aunque la mayoría de estos datos no son estrictamente necesarios para el objetivo principal del servicio, la empresa los recolecta «por si acaso», pensando en usarlos para análisis futuros. Además, no se diseñaron medidas de seguridad desde el inicio del desarrollo del sistema.



Para reflexionar y responder

- ¿Qué principios o deberes está incumpliendo esta empresa al recolectar más datos de los necesarios? Pista: piensa en la idea de «minimización de datos» y «protección por defecto».
- ¿Qué medidas debería haber considerado la empresa desde el momento en que diseñó su sistema, para cumplir con la normativa de protección de datos? Pista: considera el principio de «protección desde el diseño» y cómo se pueden evitar riesgos desde el principio.



Apliquemos lo aprendido 4

1. ¿Qué significa proteger los datos «desde el diseño»?

a. Incorporar medidas de seguridad desde el principio, al momento de crear el sistema

b. Esperar a que ocurra un problema para empezar a proteger los datos

c. Diseñar sin pensar en seguridad y agregarla después

2. ¿Qué busca la protección «por defecto»?

a. Permitir recolectar toda la información posible, por si acaso

b. Asegurar que solo se usen los datos realmente necesarios

c. Guardar muchos datos por si se necesitan en el futuro

3. ¿En qué momento deben aplicarse las medidas de protección de datos?

a. Solo si ocurre una filtración o incidente

b. Desde el momento en que se empieza a diseñar el sistema y durante todo su uso

c. Solo cuando el titular de los datos lo solicita

4. ¿Qué aspectos debe tener en cuenta el responsable al aplicar medidas de seguridad?

a. Solo cuánto cuesta implementarlas

b. El tipo de datos, el contexto en que se usan y los riesgos que podrían surgir

c. Solo cuántas personas entregaron sus datos

5. Si una empresa recolecta más datos de los necesarios, ¿qué debería hacer?

a. Guardarlos, por si en el futuro los necesita

b. Reducir la cantidad de datos recolectados y eliminar los que no son necesarios

c. Guardarlos para posibles nuevos usos

Cuidar los datos no es opcional: medidas de seguridad obligatorias

El artículo 14 quinquies establece que toda persona o empresa que trate datos personales tiene la obligación legal de protegerlos adecuadamente. No basta con tener buenas intenciones: se deben implementar medidas concretas que eviten la pérdida, filtración o el uso no autorizado de la información.

Estas medidas deben ser proporcionales y adecuadas al riesgo. Para determinar cuáles son exigibles, la ley ordena considerar diversos factores, como el estado actual de la técnica, los costos de aplicación, la naturaleza de los datos, el contexto del tratamiento y la gravedad del daño que podría producirse en caso de una vulneración.

Esto significa que no todas las organizaciones están obligadas a implementar exactamente las mismas herramientas de seguridad. Por ejemplo, una gran empresa que maneja datos financieros o de salud deberá adoptar estándares más robustos que una pequeña empresa que trata información menos sensible. Sin embargo, en todos los casos existe un deber mínimo e ineludible de protección.

¿Qué significa proteger los datos?

El artículo destaca que las medidas de seguridad deben asegurar:

* Confidencialidad: solo las personas autorizadas deben tener acceso a los datos.
* Integridad: la información no debe ser modificada sin control.
* Disponibilidad: los datos deben estar accesibles cuando se necesiten.
* Resiliencia: los sistemas deben ser capaces de resistir y recuperarse frente a fallos o ataques.

¿Qué tipo de medidas deben adoptarse?

La ley no se limita a decir que los datos deben protegerse: exige que el responsable implemente medidas concretas que aseguren un nivel de seguridad adecuado al riesgo. Y agrega algo importante: estas medidas deben incluir, al menos, ciertas acciones básicas, sin perjuicio de que, en algunos casos, sea necesario adoptar otras adicionales.

Entre esas medidas mínimas se encuentran:

* *Seudonimización y cifrado:* técnicas que dificultan identificar directamente a una persona, haciendo más difícil que terceros usen los datos de forma indebida.
* *Protección contra accesos no autorizados:* asegurar que solo quienes tienen permisos puedan ver o modificar los datos.
* *Planes de recuperación rápida:* si hay una falla técnica o un ciberataque, se debe poder restaurar el sistema y recuperar los datos lo antes posible.
* *Controles periódicos:* no basta con implementar medidas una vez. Hay que evaluarlas regularmente para confirmar que siguen siendo eficaces.

Estas exigencias constituyen un piso mínimo de protección. Dependiendo del tipo de datos y del nivel de riesgo involucrado, puede ser necesario adoptar medidas adicionales.



Una clínica médica que almacena historias clínicas electrónicas debe:

- cifrar la información para que no pueda ser leída si es robada,
- hacer copias de seguridad automáticas,
- tener planes de acción en caso de que sus servidores fallen o sufran un ataque informático, y
- revisar constantemente su sistema para detectar posibles vulnerabilidades.



Caso práctico

¿Medidas de seguridad suficientes?

Una empresa de *software* que almacena datos de tarjetas de crédito de sus clientes sufre un ciberataque, durante el cual se accedió temporalmente a la base de datos y algunos registros fueron modificados sin autorización. Aunque la empresa tenía medidas de seguridad, no ha revisado ni actualizado sus sistemas de verificación desde hace cinco años. A raíz del incidente, varios clientes presentan una queja ante la Agencia de Protección de Datos.



Para reflexionar y responder

- ¿Cumplió la empresa con su obligación de adoptar medidas de seguridad, según lo establecido en el artículo 14 quinquies? Explica tu respuesta considerando si las medidas fueron adecuadas, actualizadas y proporcionales al riesgo.
- ¿Qué acciones concretas podría haber tomado la empresa para evitar o reducir el impacto del acceso no autorizado? Menciona medidas técnicas u organizativas que habrían sido útiles, según lo que establece la norma.
- Redacta una recomendación breve para la empresa sobre cómo puede mejorar su política de seguridad de datos. Incluye la importancia de revisar periódicamente sus sistemas y adaptarse al nivel de riesgo.



Apliquemos lo aprendido 5

1. de seguridad que exige el artículo 14 quinquies?

a. Ahorrar en los costos del sistema

b. Proteger los datos asegurando su confidencialidad, integridad y disponibilidad

c. Recolectar la mayor cantidad de datos posible

2. Si ocurre un problema técnico o físico que afecta los datos personales, ¿qué se debe hacer?

a. No hacer nada si el daño no parece grave

b. Recuperar el acceso a los datos lo antes posible

c. Solo avisar a las personas directamente afectadas

3. ¿Cuál de estas técnicas ayuda a mejorar la seguridad de los datos personales?

a. Compartir los datos en un formato fácil de leer

b. Usar cifrado para proteger la información

c. Cambiar constantemente los datos, aunque no sea necesario

4. ¿Cómo puede el responsable asegurarse de que las medidas de seguridad sigan funcionando bien, pese al tiempo transcurrido?

a. Contratando más personal para el área de datos

b. Haciendo revisiones y pruebas periódicas de seguridad

c. Guardando los datos en un lugar distinto cada vez

5. ¿Qué tipo de datos necesita una protección especial, según este artículo?

a. Información usada para publicidad

b. Datos personales de niños y niñas menores de 14 años

c. Preferencias de compra y consumo

¿Qué hacer cuando ocurre una vulneración de seguridad?

El artículo 14 sexies regula qué debe hacer una organización cuando se produce una vulneración de las medidas de seguridad que protegen los datos personales.

No se trata solo de «filtraciones». La norma incluye cualquier incidente que provoque:

* la destrucción de datos,
* su filtración,
* su pérdida,
* su alteración accidental o ilícita, o
* el acceso o la comunicación no autorizada.

Pero no toda vulneración debe reportarse. La obligación surge cuando el incidente genera un riesgo razonable para los derechos y libertades de las personas.

Notificación a la Agencia de Protección de Datos

Cuando exista ese riesgo razonable, el responsable debe informar a la Agencia por los medios más expeditos posible y sin dilaciones indebidas.

Pero no basta con avisar: debe registrar formalmente la comunicación, dejando constancia de:

* la naturaleza del incidente,
* sus efectos,
* las categorías de datos afectadas,
* el número aproximado de titulares involucrados y
* las medidas adoptadas para enfrentar el problema y evitar que vuelva a ocurrir.

¿Cuándo debe informarse también a los titulares?

La ley establece una regla especial. Si la vulneración afecta:

* datos personales sensibles,
* datos de niños y niñas menores de 14 años o

* datos relativos a obligaciones económicas, financieras, bancarias o comerciales, el responsable también debe comunicar el incidente directamente a los titulares afectados (o a sus representantes, cuando corresponda).

Esta comunicación debe:

* usar un lenguaje claro y sencillo,
* especificar qué datos fueron afectados,
* explicar las posibles consecuencias e
* indicar qué medidas se han adoptado para solucionar o mitigar el problema.

La notificación debe realizarse a cada titular afectado. Solo si ello no es posible, puede reemplazarse por la publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.



Caso práctico

Si una institución financiera sufre un acceso no autorizado a una base de datos que contiene información sobre deudas o historial comercial y existe un riesgo razonable para los derechos de las personas, deberá:

- informar sin demora a la Agencia,
- registrar formalmente el incidente y
- comunicar directamente a cada persona afectada, explicando qué ocurrió y qué medidas puede adoptar para protegerse.



Importante
Estas obligaciones no reemplazan otros deberes de información que puedan existir en leyes especiales. Si otra normativa exige avisos adicionales, también deberán cumplirse.



Caso práctico

Vulneración de datos en un colegio privado
Un colegio privado sufrió un ataque a sus servidores, donde se almacenaban los datos personales de los estudiantes, incluidos niños menores de 14 años. Durante el ataque, se expuso información sensible, como direcciones y resultados académicos de los alumnos. La vulneración duró solo unas horas y el colegio decidió no notificar a las familias afectadas, argumentando que el incidente no tuvo consecuencias graves debido a la corta duración del acceso no autorizado.

- Evalúa si el colegio actuó correctamente según el artículo 14 sexies.
- Explica qué deberían haber hecho las autoridades del colegio para cumplir con su deber de reportar la vulneración.
- Elabora una propuesta de cómo el colegio podría mejorar sus protocolos de respuesta ante incidentes de seguridad.



Apliquemos lo aprendido 6

1. ¿Cuándo debe el responsable notificar una vulneración a las medidas de seguridad?

a. Solo si los datos son de carácter público

b. Cuando existe un riesgo razonable para los derechos de los titulares

c. Si más del 50% de los datos fue afectado

2. ¿Qué debe incluir la notificación de vulneración de datos?

a. Una lista de los empleados responsables del incidente

b. Una descripción detallada de los datos afectados, el número de titulares afectados y las medidas adoptadas para gestionarlo

c. Un resumen general sin especificaciones

3. ¿Qué tipo de datos requieren una notificación especial en caso de vulneración?

a. Datos relacionados con marketing

b. Datos sensibles como salud, menores de edad o datos financieros

c. Datos de acceso público

4. Si no se puede notificar directamente a todos los afectados, ¿qué debe hacer el responsable?

a. Ignorar la notificación

b. Publicar un aviso en un medio de comunicación masivo de alcance nacional

c. Notificar solo a los clientes frecuentes

5. ¿Qué debe hacer el responsable tras la vulneración de seguridad para evitar futuros incidentes?

a. Realizar una evaluación general cada cinco años

b. Implementar nuevas medidas de seguridad y registrarlas

c. Cambiar de empresa de seguridad



Apliquemos lo aprendido 6

6. ¿Qué debe hacer el responsable con respecto a las vulneraciones de seguridad?

a. Solo reportarlas si son graves

b. Registrar las vulneraciones, describir sus efectos y las medidas adoptadas para evitar futuros incidentes

c. Ignorar las vulneraciones menores y no registrarlas

Medidas a la medida: cómo se ajustan los estándares de seguridad y transparencia en el tratamiento de datos

No todas las organizaciones tienen la misma capacidad para proteger datos personales ni manejan la misma cantidad o tipo de información. Por eso, el artículo 14 septies establece que los deberes de seguridad e información (es decir, cómo se protegen los datos y cómo se informa a los titulares) deben adaptarse según las características de cada caso.

¿Qué factores se consideran para esta diferenciación?

Quién trata los datos: No es lo mismo una gran empresa que una persona natural o una microempresa. Las obligaciones se ajustan según el tipo de responsable.

Tamaño de la entidad: Las pequeñas empresas, según la Ley 20.416, tienen menos exigencias que las grandes. La idea es ser razonables y proporcionales.

Tipo y cantidad de datos: Si se manejan datos sensibles (como salud o antecedentes penales) o se trata con grandes volúmenes de información, las medidas de protección deben ser más estrictas.

Para qué se usan los datos: No es lo mismo usar los datos para enviar promociones que para tomar decisiones médicas. La finalidad también importa a la hora de establecer los estándares.

¿Quién decide estos estándares?

La Agencia de Protección de Datos será la encargada de fijar, a través de una *instrucción general*, cuáles son las condiciones mínimas que deben cumplir los distintos tipos de entidades, según los datos que manejen.



Caso práctico

Diferenciación de estándares de cumplimiento

Una microempresa de desarrollo de *software*, con menos de diez empleados, en un inicio recolectaba solo datos básicos de sus clientes (nombre, correo electrónico y número de teléfono) con fines de marketing. Sin embargo, tras lanzar un nuevo sistema de pagos, ha comenzado a recopilar información financiera sensible, como números de tarjetas y registros de compra. Ante esta situación, el dueño de la empresa se pregunta qué nuevas exigencias legales deberá cumplir en materia de seguridad y protección de datos.

- ¿Qué cambios deberá implementar la empresa en su política de protección de datos al comenzar a tratar información financiera?
- ¿Cómo pueden diferir los estándares de cumplimiento entre esta empresa y una gran institución financiera?
- ¿Qué medidas mínimas de seguridad deberían adoptarse, considerando el tipo de datos y el tamaño de la empresa?



Apliquemos lo aprendido 7

1. ¿Cuáles aspectos se toman en cuenta para definir qué tan exigentes deben ser las medidas de seguridad e información que debe aplicar una organización?

a. Solo el tipo de datos que maneja

b. El tamaño de la empresa, el tipo de datos y para qué se usan

c. El rubro en el que trabaja la empresa

2. ¿Quién tiene la responsabilidad de establecer los estándares mínimos de cumplimiento en protección de datos?

a. La Agencia de Protección de Datos

b. El Ministerio de Justicia y Derechos Humanos

c. La Superintendencia de Bancos e Instituciones Financieras

3. ¿Qué ley establece las normas especiales para las empresas de menor tamaño, según lo mencionado en el artículo 14 septies?

a. Ley 18.046 sobre Sociedades Anónimas

b. Ley 20.416 sobre Empresas de Menor Tamaño

c. Ley 19.496 sobre Protección de los Derechos del Consumidor

4. ¿Cuál de estas organizaciones necesita aplicar medidas de seguridad más estrictas, aunque sea pequeña?

a. Una tienda que solo guarda nombres y correos electrónicos

b. Una clínica que almacena historiales médicos

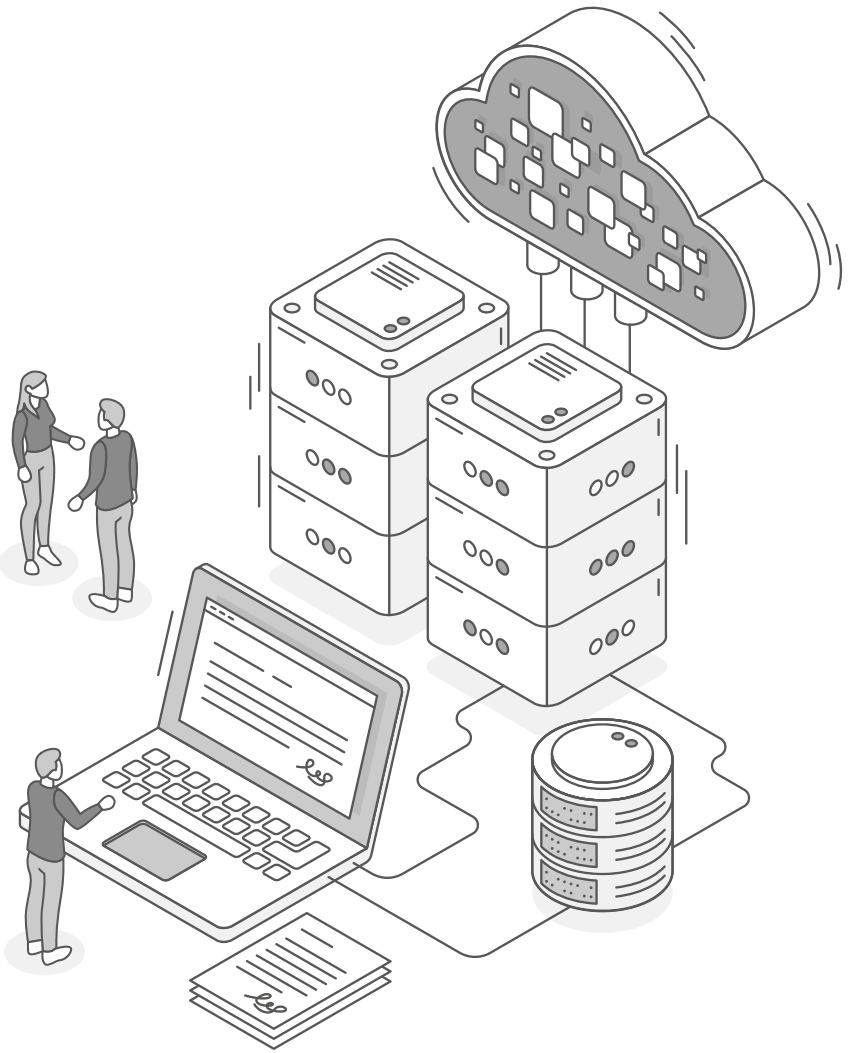
c. Un restaurante que solo recibe reservas *online*

5. ¿Quién está exento de cumplir con los estándares que menciona este artículo?

a. Las microempresas

b. Las grandes empresas

c. Nadie, todas deben cumplir según los factores que les correspondan



Cómo ejercer tus derechos sobre tus datos

El artículo 10 funciona como un manual de instrucciones para ejercer tus derechos sobre tus datos. Aquí se explica cómo y dónde puedes hacer valer tus derechos, por ejemplo, solicitar que corrijan, eliminen o te entreguen tu información personal. Además, establece que las empresas deben facilitarte el proceso, haciéndolo sencillo, rápido y, en la mayoría de los casos, gratuito.

Este artículo también asegura que, si una empresa no está en Chile, debe designar a alguien para que puedas comunicarte con ellos y ejercer tus derechos. En resumen, el artículo 10 te da las herramientas para proteger tus datos de manera fácil y efectiva, sin complicaciones ni costos innecesarios.

Ejercicio ante el responsable de datos

Tú, como titular de tus datos personales, tienes derechos que la ley te garantiza. Estos son:

* Saber qué datos tienen sobre ti (derecho de acceso).
* Solicitar que corrijan información incorrecta (derecho de rectificación).
* Solicitar que eliminen tus datos (derecho de supresión).
* Oponerte a que usen tus datos de ciertas maneras (derecho de oposición).

* Llevarte tus datos a otra empresa o servicio (derecho a la portabilidad).

Para ejercer estos derechos, debes dirigirte directamente al responsable de los datos, es decir, la persona o empresa que decide cómo y para qué se usan tus datos.

Lo bueno es que, si tus datos están en manos de varias empresas, no tienes que contactar a todas por separado. Puedes ejercer tus derechos ante cualquiera de ellas, pues están obligadas a responderte. Esto hace todo más sencillo y evita que tengas que perder tiempo contactando una por una.

¿Por qué esto es importante? Este derecho te ahorra tiempo y esfuerzo. Imagina que tus datos están en varias empresas (un banco, una red social y una tienda en línea, por ejemplo). En lugar de tener que escribirles a todas, puedes elegir una y pedirle que resuelva tu solicitud. ¡Es como tener un «atajo» para proteger tus datos!

Responsables de datos no constituidos en Chile

Si una empresa o persona que usa tus datos no está registrada en Chile (por ejemplo, una red social o una tienda en línea extranjera), la ley exige que tengan un medio de contacto válido y operativo, como un correo electrónico o una plataforma en línea. Esto es para que tú, como titular de los datos, puedas ejercer tus derechos sin problemas, incluso si la empresa está en otro país.

Además, estas empresas deben mantener actualizada su información de contacto, para que siempre puedas comunicarte con ellas. Esto asegura que ni las barreras geográficas ni las barreras legales te impidan proteger tus derechos.

¿Por qué esto es importante? Imagina que usas una app o un servicio extranjero y necesitas que corrijan o eliminen tus datos. Gracias a esta norma, puedes contactarlos fácilmente, sin importar dónde estén. ¡Es como tener un puente que conecta tus derechos con cualquier empresa, sin importar su ubicación!

Mecanismos para ejercer los derechos

La ley exige que las empresas o personas que manejan tus datos personales te ofrezcan herramientas fáciles de usar para que puedas

ejercer tus derechos de manera rápida y sin complicaciones. Esto significa que los sistemas que usen deben ser simples, claros y accesibles.

Por ejemplo, si un banco tiene tus datos, debe ofrecerte una plataforma en línea donde puedas ver tu información, solicitar que la corrijan o incluso pedir que la eliminen. La idea es que no tengas que pasar por trámites engorrosos o enfrentarte a sistemas confusos para proteger tus derechos.

¿Por qué esto es importante? Esta norma asegura que las empresas no pongan barreras tecnológicas o burocráticas que te dificulten ejercer tus derechos. Es como decirles: «si usan mis datos, deben hacerme las cosas fáciles». Así, tú tienes el control sin necesidad de ser un experto en tecnología o trámites.

Gratuidad en el ejercicio de los derechos

Cuando quieras ejercer tus derechos para corregir, eliminar u oponerte al uso de tus datos personales, el camino siempre debe ser gratuito. Lo mismo aplica para el derecho de acceso, es decir, para pedir una copia de tus datos, al menos una vez cada tres meses[36].

Sin embargo, si solicitas acceso a tus datos o quieres llevártelos a otra empresa (derecho a la portabilidad) más de una vez durante ese periodo, la empresa podría cobrarte un monto por los costos directos que le genere procesar tu solicitud. Eso sí, estos costos deben ser razonables y estarán regulados por la Agencia de Protección de Datos, que considerará factores como la cantidad de datos y el tipo de empresa.

¿Por qué esto es importante? Esta norma asegura que puedas ejercer tus derechos sin que te cobren de más, pero también evita que las empresas tengan que asumir costos excesivos si realizas muchas solicitudes en poco tiempo. Es un equilibrio justo que protege tanto tus derechos como los recursos de las empresas.

---

36 Conforme indica Guzmán y otro (2025) «en caso de infracción del deber de gratuidad por parte del responsable, el titular tendrá derecho a ser indemnizado por daño patrimonial y moral, y el responsable también tendrá que eliminar. Modificar o bloquear los datos de acuerdo con lo requerido por el titular o, en su caso, lo ordenado por el tribunal».

Supervisión de la Agencia de Protección de Datos

La Agencia de Protección de Datos es como un «guardián» que asegura el cumplimiento de la ley y que tus derechos sobre tus datos personales sean respetados. Entre sus responsabilidades está:

* dar instrucciones claras sobre cómo las empresas deben calcular los costos si te cobran por acceder a tus datos o llevártelos a otra plataforma y
* supervisar que las empresas tengan sistemas adecuados para que puedas ejercer tus derechos de manera fácil y sin complicaciones.

En resumen, la Agencia está ahí para asegurarse de que las empresas jueguen limpio y tú puedas proteger tus datos sin problemas.

¿Por qué esto es importante? La Agencia actúa como un «árbitro» que garantiza que las reglas se cumplan. Si alguna empresa no respeta tus derechos o te pone trabas, la Agencia está para intervenir y asegurarse de que todo funcione como se debe. ¡Es tu aliada en la protección de tus datos!

Tus derechos en acción: paso a paso para ejercerlos

El artículo 11 funciona como una receta de cocina que te explica cómo ejercer tus derechos sobre tus datos personales. Aquí se detalla el proceso que debes seguir para hacer una solicitud, ya sea para acceder, corregir, eliminar u oponerte al uso de tus datos.

En resumen, este artículo te dice:

* *Cómo presentar una solicitud:* debes hacerlo por escrito, ya sea por correo electrónico, mediante un formulario en línea o a través de un medio electrónico similar.
* *Qué debe incluir tu solicitud:* tu identificación, los datos que quieres modificar o eliminar, y una dirección para recibir la respuesta.
* *Plazos y respuestas:* la empresa tiene 30 días para responderte (con una posible prórroga de otros 30 días). Si no lo hace, puedes reclamar ante la Agencia de Protección de Datos.
* *Bloqueo temporal:* si solicitas corregir, eliminar u oponerte al uso de tus datos, puedes solicitar que se «congelen» temporalmente mientras se resuelve tu solicitud.

Este artículo asegura que las empresas te respondan de manera clara y en un plazo razonable, dándote herramientas para proteger tus datos sin complicaciones.

El artículo 11 ofrece un camino claro para ejercer tus derechos. No importa si quieres saber qué datos tuyos guardan, corregir algo incorrecto o evitar que sigan usando tu información: este artículo te dice cómo hacerlo, paso a paso. ¡Es como tener un mapa para proteger tus datos personales!

Presentación de la solicitud

Si quieres ejercer tus derechos sobre tus datos personales, debes presentar una solicitud por escrito o electrónica a la empresa o persona que los tiene. Esto puede hacerse a través de un correo electrónico, un formulario en línea o cualquier otro medio digital que la empresa tenga disponible. La idea es que quede un registro formal de tu solicitud.

Esta debe incluir lo siguiente:

* *Tu identificación:* es decir, quién eres y, si alguien más está actuando en tu nombre (como un abogado o representante), su identificación también. El objetivo es asegurar que eres tú quien está haciendo la solicitud.
* *Dónde te pueden responder:* debes proporcionar una dirección física, un correo electrónico o algún medio para que la empresa te pueda contactar y darte una respuesta.
* *Qué datos o tratamiento estás cuestionando:* especifica qué datos quieres corregir, eliminar o sobre los cuales te opones. También debes indicar qué derecho estás ejerciendo (por ejemplo, rectificación, supresión, oposición, etc.).

¿Por qué esto es importante? Presentar una solicitud formal asegura que haya un registro claro de lo que estás pidiendo y que la empresa pueda responder de manera adecuada. Es como enviar una carta certificada: sabes que llegó y que hay un seguimiento.

Detalles adicionales en la solicitud

Dependiendo del derecho que quieras ejercer, tu solicitud debe incluir información específica:

* *Rectificación:* si quieres corregir tus datos, debes explicar exactamente qué cambios necesitas y adjuntar documentos que respalden tu solicitud (por ejemplo, un documento de identidad actualizado).
* *Supresión:* si pides que eliminen tus datos, debes indicar el motivo (por ejemplo, que ya no usas el servicio) y, si es necesario, adjuntar documentos que respalden tu petición.
* *Oposición:* si te opones a que sigan usando tus datos, debes explicar brevemente por qué (por ejemplo, que no diste tu consentimiento o que no estás de acuerdo con cómo los usan).

¿Por qué esto es importante? Incluir estos detalles asegura que la empresa entienda exactamente lo que estás pidiendo y pueda actuar de manera correcta. Además, los documentos que adjuntas ayudan a respaldar tu solicitud, evitando malentendidos o retrasos.

Plazo para responder

La empresa o persona que tiene tus datos tiene 30 días para responderte a partir de la fecha en que recibió tu solicitud. En casos excepcionales, este plazo puede extenderse por otros 30 días, pero solo si es realmente necesario.

¿Por qué esto es importante? Este plazo asegura que las empresas no te hagan esperar indefinidamente. Sabes que, en máximo 30 días (o 60 en casos excepcionales), tendrás una respuesta clara sobre tu solicitud.

Forma de la respuesta

La empresa debe responderte por escrito, ya sea por correo electrónico o a la dirección que indicaste en tu solicitud. Además, deben guardar un registro de la respuesta, incluyendo la fecha y el contenido, para que haya pruebas de que cumplieron con su obligación.

¿Por qué esto es importante? Esto garantiza que haya un registro formal de la respuesta, lo que protege tanto a la empresa como a ti. Si hay algún problema, puedes demostrar que hiciste la solicitud y que la empresa te respondió (o no).

En caso de rechazo o falta de respuesta

Si la empresa rechaza tu solicitud (total o parcialmente), debe explicarte por qué y especificar que tienes 30 días hábiles para presentar una queja ante la Agencia de Protección de Datos. Si la empresa no te responde dentro de los 30 días establecidos, puedes ir directamente a la Agencia para que intervenga.

¿Por qué esto es importante? Este punto te ofrece un recurso claro si la empresa no cumple con su obligación. No importa si te rechazan la solicitud o si no te responden: tienes la opción de acudir a la Agencia para que te ayude a resolver el problema.

Bloqueo temporal de datos

Si solicitas corregir, eliminar u oponerte al uso de tus datos, puedes solicitar que se bloqueen temporalmente mientras se resuelve tu solicitud. Esto significa que la empresa no podrá usar tus datos durante ese tiempo, aunque sí podrá guardarlos.

¿Por qué esto es importante? El bloqueo temporal te protege mientras se evalúa tu solicitud. Por ejemplo, si pediste que corrijan un error en tus datos, el bloqueo evita que la empresa siga usando la información incorrecta hasta que se resuelva el problema.



Caso práctico

Reclamo por falta de respuesta

Camila es cliente de una tienda en línea y se dio cuenta de que tienen mal registrada su dirección de entrega. Para evitar problemas, envió una solicitud a través del formulario de contacto de la tienda, pidiendo que corrijan su dirección. Además, les pidió que dejaran de usar sus datos personales para enviarle correos promocionales. Sin embargo, pasaron más de 30 días y Camila no recibió ninguna respuesta. Peor aún, sigue recibiendo correos publicitarios de la tienda.

¿Qué puede hacer Camila para que respeten sus derechos?



Apliquemos lo aprendido 1

1.¿Qué debe incluir una solicitud de rectificación de datos?

a. La solicitud general sin documentación

b. Los cambios precisos solicitados y la documentación que los respalde

c. Solo la identificación del titular

2. ¿Cuál es el plazo máximo de respuesta a una solicitud de datos?

a. 10 días

b. 15 días

c. 30 días

3. ¿Qué debe hacer el responsable si no responde a una solicitud en el plazo establecido?

a. Puede solicitar una extensión de tiempo indefinida

b. Debe notificar a la Agencia de Protección de Datos

c. El titular puede presentar una reclamación directamente ante la Agencia

4. ¿Quién puede presentar una reclamación ante la Agencia?

a. Solo el representante legal del titular

b. Cualquier persona

c. El titular de los datos

5. ¿Qué sucede si el responsable de datos está en el extranjero?

a. No se pueden ejercer los derechos del titular

b. El responsable debe designar un medio de contacto válido en Chile

c. El titular debe presentar la solicitud en persona

6. ¿Qué significa el bloqueo temporal de datos?

a. La eliminación permanente de los datos

b. La suspensión del tratamiento de los datos mientras se resuelve la solicitud

c. La limitación del acceso del titular a sus propios datos

7. ¿Quién regula los costos asociados con la solicitud de datos?

a. El responsable de los datos

b. La Agencia de Protección de Datos

c. El titular de los datos

8. ¿Qué se debe hacer si el responsable no proporciona un medio adecuado para solicitar los derechos?

a. Presentar la solicitud de todos modos y esperar

b. Informar a la Agencia de Protección de Datos

c. No se puede hacer nada

9. ¿Qué garantiza que el responsable haya respondido a la solicitud del titular?

a. Un aviso verbal del responsable

b. La falta de queja del titular

c. El registro de envío y contenido de la respuesta por parte del responsable

10. ¿Cuál es la principal función de la Agencia de Protección de Datos?

a. Proteger los intereses de los responsables

b. Asegurar el cumplimiento de los derechos del titular de los datos

c. Emitir multas

Protegiendo tus datos: cómo reclamar si no se cumplen las reglas

Procedimiento Administrativo de Tutela de Derechos (artículo 41)

Este proceso te permite presentar una reclamación ante la Agencia de Protección de Datos si la empresa o persona que tiene tus datos:

* te negó una solicitud (como corregir o eliminar tus datos) o
* no te respondió en el plazo de 30 días establecido por la ley.

A continuación, te explicamos paso a paso cómo funciona este proceso.

Presentación de la reclamación

Tienes 30 días corridos (que pueden extenderse por otros 30 días) para presentar tu reclamación ante la Agencia. Puedes hacerlo en persona o en línea.

Tu reclamación debe incluir:

* la decisión que estás impugnando (por ejemplo, la negativa de la empresa o su falta de respuesta),
* todos los documentos que respalden tu caso y
* una dirección física o electrónica donde la Agencia pueda contactarte.

Si pediste que eliminen tus datos de una empresa y no recibiste respuesta en 30 días, puedes presentar una reclamación ante la Agencia dentro del siguiente mes.

Suspensión del uso de tus datos

Si lo solicitas, la Agencia puede ordenar que se suspenda temporalmente el uso de tus datos mientras se resuelve tu reclamación. Sin embargo, primero escuchará a la empresa para decidir si es necesario.

Si sospechas que una empresa está usando tus datos para enviarte publicidad sin tu consentimiento, puedes pedir que se suspendan esos envíos hasta que la Agencia resuelva tu caso.

Revisión de la reclamación

La Agencia tiene diez días hábiles para revisar tu reclamación y decidir si cumple con los requisitos necesarios. Si no se pronuncia en ese plazo, se entiende que tu reclamación fue aceptada.

Presentas una reclamación y la Agencia tiene diez días hábiles para decidir si la tramita. Si no lo hace en ese tiempo, tu reclamación sigue adelante.

Notificación a la empresa

La Agencia notifica a la empresa sobre tu reclamación. Luego, esta tiene 30 días corridos (extensibles a 60 días) para responder.

Una empresa recibe la notificación de la Agencia. Tiene 30 días para responder y presentar su versión de los hechos.

Periodo de pruebas

Si hay desacuerdos sobre los hechos, la Agencia abre un periodo de diez días hábiles para que ambas partes presenten pruebas.

Si tú sostienes que la empresa compartió tus datos sin tu consentimiento, pero la empresa lo niega, la Agencia abre un periodo para que ambas instancias presenten pruebas.

Si la empresa acepta tu reclamación, debe presentar pruebas de que está corrigiendo el problema. Luego, tienes diez días para asegurarte de que se respeten tus derechos antes de que la Agencia cierre el caso.

Resolución final

La Agencia tiene hasta seis meses para resolver tu caso. Si no estás de acuerdo con la decisión, tienes 15 días hábiles para impugnarla ante un tribunal.

Si la Agencia no resuelve a tu favor, puedes llevar el caso a la justicia en un plazo de 15 días.



Este procedimiento te ofrece una vía clara para defender tus derechos cuando una empresa no responde o no cumple con la ley. Además, asegura que las empresas rindan cuentas y que tus datos personales estén protegidos.

Procedimiento Administrativo por Infracción de Ley (artículo 42)

Este procedimiento es el que sigue la Agencia de Protección de Datos cuando una empresa o una persona incumple las normas de protección de datos, por ejemplo, usando información personal sin consentimiento o no garantizando la seguridad de los datos. La Agencia tiene la facultad de investigar y, si encuentra una infracción, aplicar sanciones.

A continuación, te explicamos las etapas principales de este proceso.

Inicio del procedimiento

* *¿Cómo comienza?* La Agencia puede iniciar el procedimiento:
  - por su cuenta (de oficio),
  - a partir de la reclamación de un titular de datos o
  - como resultado de una fiscalización o inspección.
* *Certificación del reclamo:* si el proceso comienza por una reclamación, la Agencia debe confirmar que recibió el reclamo.
* *Designación de un funcionario:* se asigna a una persona para que investigue el caso.

Un usuario denuncia que una empresa usó sus datos personales sin su consentimiento. La Agencia inicia el procedimiento y designa a un funcionario para investigar.

Formulación de cargos

* La Agencia debe presentar un documento detallado con los cargos contra la empresa o persona responsable. Este documento explica:
  - los hechos que se consideran una infracción,
  - las normas que se incumplieron y
  - cualquier otro antecedente relevante.
* *Notificación:* los cargos se notifican al responsable por correo electrónico, postal u otro medio electrónico.

La Agencia formula cargos contra una empresa por no proteger adecuadamente los datos de sus clientes, detallando cómo ocurrió el incidente.

Descargos del responsable

* *Plazo:* el responsable tiene 15 días hábiles para presentar sus argumentos y pruebas en defensa. También debe proporcionar una dirección electrónica para futuras notificaciones.
* *Pruebas:* puede presentar cualquier prueba que considere necesaria para defenderse.

La empresa presenta pruebas dentro del plazo para demostrar que ya corrigió los problemas de seguridad y que no hubo mal uso de los datos.

Periodo probatorio

* Si hay desacuerdos sobre los hechos, la Agencia abre un periodo de diez días hábiles para que ambas partes presenten pruebas.
* La Agencia decide si acepta o rechaza las pruebas presentadas. Si las rechaza, debe explicar por qué.

Resolución final

* La Agencia emite una resolución final que debe estar bien fundamentada y responder a todas las defensas presentadas.

* *Sanciones:* si se confirma la infracción, la Agencia puede imponer multas o medidas correctivas, dependiendo de la gravedad del caso.
* *Plazo:* el procedimiento no puede durar más de seis meses desde su inicio.

Recursos y reclamaciones

* Si el responsable no está de acuerdo con la resolución, tiene 15 días hábiles para apelar ante un tribunal.
* Si la Agencia no resuelve en el plazo de seis meses, el titular de datos o el responsable pueden presentar un reclamo por la demora.

La empresa sancionada decide apelar la decisión de la Agencia, argumentando que las pruebas no fueron valoradas correctamente.



Este procedimiento asegura que empresas y personas que manejan datos personales cumplan con la ley. Si no lo hacen, la Agencia puede investigar y aplicar sanciones para proteger tus derechos. Además, garantiza que el proceso sea justo y transparente para todas las partes involucradas.

Esquema del Procedimiento Administrativo por Infracción de Ley

Iniciación del procedimiento

¿Cómo comienza?

- La Agencia puede actuar:
  - por su cuenta (de oficio),
  - por una reclamación de un titular de datos o
  - tras una fiscalización o inspección.
- Si existe una reclamación, se certifica su recepción.
- Se designa a un funcionario para investigar.

Un usuario denuncia que una empresa usó sus datos sin permiso. La Agencia inicia el proceso y asigna a un funcionario para investigar.

Formulación de cargos

- La Agencia describe:
  - los hechos que constituyen la infracción y
  - las normas que se incumplieron.
- Notificación: se informa al responsable por correo electrónico, por correo postal u otro medio.

La Agencia notifica a una empresa que no protegió adecuadamente los datos de sus clientes.

Descargos del responsable

- Plazo: 15 días hábiles para presentar su defensa.
- Qué debe hacer el responsable:
  - presentar pruebas y argumentos, y
  - designar un correo electrónico para futuras notificaciones.

La empresa presenta pruebas de que corrigió los problemas de seguridad.

Periodo probatorio

* ¿Cuándo ocurre?: cuando existe desacuerdos sobre los hechos.
* Plazo: diez días hábiles para presentar pruebas.
* Decisión de la Agencia: puede aceptar o rechazar las pruebas presentadas.

Resolución final

* La Agencia emite una resolución. Esta debe:
  - estar bien fundamentada e
  - incluir sanciones (multas o medidas correctivas) si se confirma la infracción.
* Plazo máximo: seis meses desde el inicio del procedimiento.

Impugnación

* ¿Qué pasa si no estás de acuerdo?: el responsable tiene 15 días hábiles para apelar ante un tribunal.
* ¿Y si la Agencia no resuelve en seis meses?: el titular o el responsable pueden presentar un reclamo por la demora.

La empresa apela la sanción, argumentando que las pruebas no fueron valoradas correctamente.



Apliquemos lo aprendido 2

1. ¿Cómo puede iniciarse el Procedimiento Administrativo por Infracción de Ley?

a. Solo por fiscalización de la Agencia

b. Solo por una reclamación del titular

c. Por fiscalización, de oficio o por reclamación del titular

2. ¿Qué plazo tiene el responsable para presentar sus descargos tras la notificación de cargos?

a. 10 días corridos

b. 20 días hábiles

c. 15 días hábiles

3. ¿En qué casos la Agencia puede abrir un periodo probatorio?

a. Siempre que lo solicite el titular de los datos

b. Cuando existan hechos sustanciales, pertinentes y controvertidos

c. Solo si lo solicita el responsable

4. ¿Qué debe contener la resolución final de la Agencia?

a. Solo la decisión de sancionar o absolver

b. Un resumen de los hechos sin justificación

c. Una declaración de cumplimiento o incumplimiento y las sanciones correspondientes

5. ¿Cuál es el plazo máximo para que la Agencia resuelva un procedimiento sancionatorio?

a. 3 meses

b. 9 meses

c. 6 meses

Procedimiento de Reclamación Judicial

Este procedimiento permite a las personas (ya sean naturales o jurídicas) *impugnar decisiones o resoluciones de la Agencia de Protección de Datos* si las consideran ilegales o injustas. Por ejemplo, si la Agencia emite una resolución que te afecta negativamente y crees que no se ajusta a la ley, puedes llevar el caso a la Corte de Apelaciones para que lo revise.

El objetivo de este proceso es corregir cualquier error o infracción que pueda haberte causado un daño o perjuicio. A continuación, te explicamos las etapas principales y cómo funciona.

Presentación del Reclamo de Ilegalidad

- *¿Quién puede reclamar?* Cualquier persona o empresa que considere que una decisión de la Agencia es ilegal.
- *¿Dónde se presenta el reclamo?* En la Corte de Apelaciones de Santiago o en la Corte de la ciudad donde vive el reclamante.
- *¿Plazo?* se debe presentar dentro de los 15 días hábiles después de recibir la notificación de la resolución.
- *¿Qué debe incluir el reclamo?* La resolución que se está impugnando, las normas que se consideran vulneradas, cómo se produjo la infracción y por qué la decisión perjudica al reclamante.

Una empresa recibe una multa de la Agencia, pero considera que la sanción es injusta porque no se tomaron en cuenta sus pruebas de defensa. En ese caso, puede presentar un reclamo ante la Corte de Apelaciones dentro del plazo establecido.

Revisión de Admisibilidad del Reclamo

La Corte revisa si el reclamo cumple con todos los requisitos. Si no es así, puede declararlo inadmisible.

Si el acto impugnado puede causar un daño grave e irreparable, la Corte puede emitir una *orden de no innovar*, lo que significa que suspende temporalmente la aplicación de la sanción hasta que se resuelva el reclamo.

Si la empresa sancionada no puede pagar la multa sin afectar gravemente su funcionamiento, puede pedir esta suspensión para evitar el pago hasta que se resuelva el caso.

Informe de la Agencia

Si el reclamo es admitido, la Corte pide a la Agencia que explique por qué tomó esa decisión. La Agencia tiene diez días para responder.

La Agencia debe presentar un informe detallando por qué aplicó la multa y qué normas utilizó para justificar su decisión.

Presentación de Pruebas (periodo probatorio)

Si la Corte lo considera necesario, abre un periodo para que ambas partes presenten pruebas adicionales.

La empresa puede aportar más documentos o testimonios para demostrar que la sanción es injusta, mientras que la Agencia puede presentar evidencia para defender su decisión.

Decisión de la Corte

Una vez revisadas todas las pruebas, la Corte evalúa el caso en una audiencia.

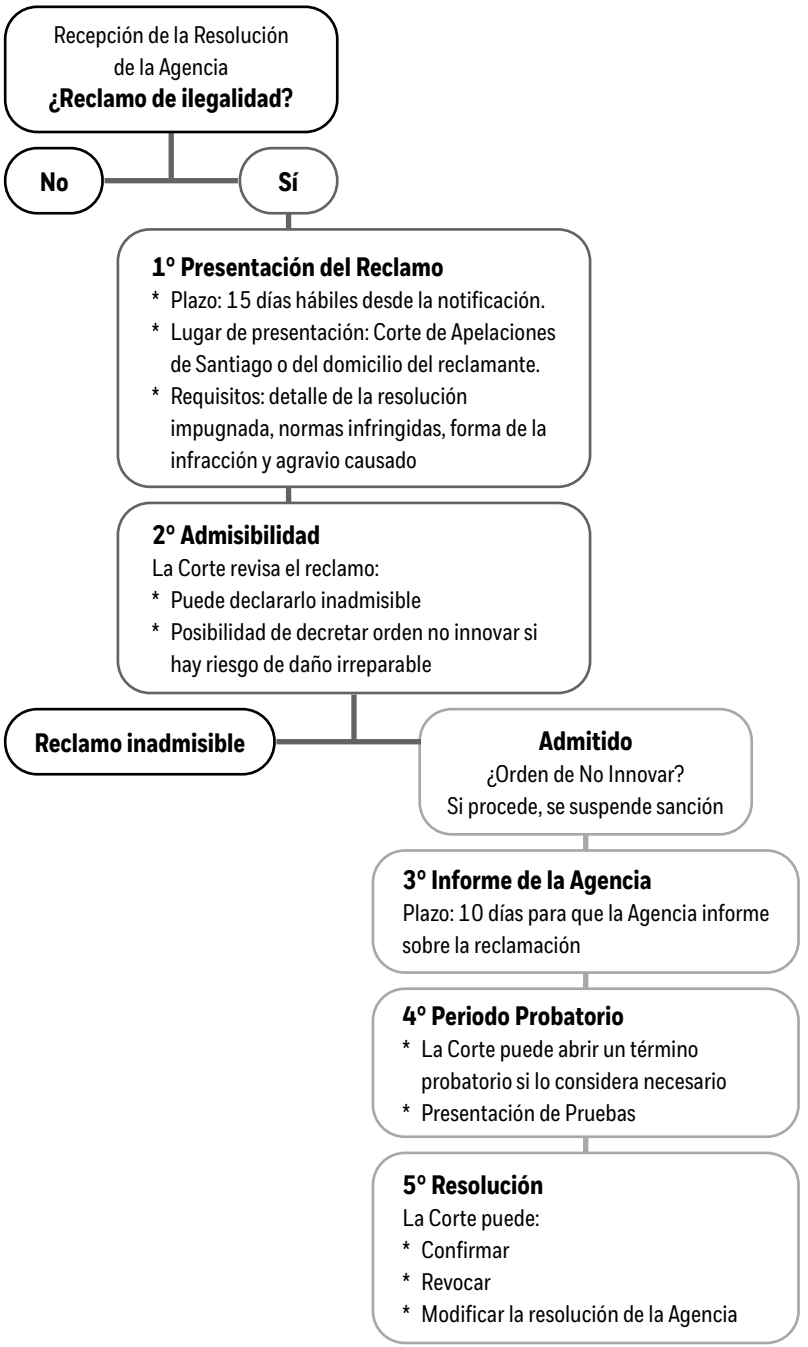
Si da la razón al reclamante, puede ordenar modificar la resolución impugnada o dictar una nueva. En el caso de sanciones, puede confirmar o revocar la multa, determinar si realmente hubo una infracción o mantener, eliminar o cambiar la sanción impuesta.

La Corte puede decidir que la multa impuesta a la empresa fue exagerada y reducirla. Incluso puede eliminarla, si considera que la sanción fue incorrecta.

Normas aplicables en caso de dudas

Si hay algo no regulado específicamente en este proceso, se aplican las normas del Código Orgánico de Tribunales y el Código de Procedimiento Civil.

Figura 1. Procedimiento de reclamación judicial.





Apliquemos lo aprendido 3

1. ¿En qué plazo debe presentarse un reclamo de ilegalidad ante la Corte de Apelaciones?

a. 10 días corridos desde la notificación

b. 20 días hábiles desde la notificación

c. 15 días hábiles desde la notificación

2. ¿Qué puede hacer la Corte si considera que el reclamo de ilegalidad es inadmisible?

a. Declarar inadmisible el reclamo

b. Modificar la resolución impugnada

c. Suspender el procedimiento hasta nueva presentación

3. ¿Qué plazo tiene la Agencia para responder al requerimiento de la Corte?

a. 5 días hábiles

b. 10 días hábiles

c. 15 días corridos

4. ¿Qué sucede si la Corte estima necesario abrir un periodo probatorio?

a. Se fija una nueva audiencia de conciliación

b. Se abre un término probatorio bajo las reglas del Código de Procedimiento Civil

c. Se rechaza automáticamente el reclamo

5. ¿Qué puede decidir la Corte si acoge el reclamo en un procedimiento sancionatorio?

a. Confirmar, revocar o modificar la sanción impuesta

b. Reenviar el caso a la Agencia para nueva evaluación

c. Suspender el acto sin modificar la sanción



¿Pueden las instituciones públicas usar nuestros datos? ¿Cuándo?

El artículo 20 de la Ley de Protección de Datos Personales plantea que los órganos públicos (municipalidades, ministerios, Registro Civil, etc.) pueden tratar datos personales sin necesidad de pedirnos consentimiento, cuando lo hacen para cumplir sus funciones legales y dentro del ámbito de sus competencias.

En otras palabras, no pueden usar nuestros datos «porque sí», sino que deben estar ejerciendo una atribución que la ley les haya otorgado expresamente[37]. Pero hay una distinción importante. Esta regla se refiere a datos personales en general. Si se trata de datos personales sensibles como información sobre salud, creencias religiosas, afiliación sindical, orientación sexual o datos genéticos, se aplican las reglas especiales de los artículos 16 y 16 bis, que establecen requisitos más estrictos y, en algunos casos, exigen consentimiento expreso o una habilitación legal específica.

Es decir, el hecho de ser un órgano público no autoriza automáticamente el tratamiento de cualquier tipo de dato sensible sin cumplir las condiciones adicionales que establece la ley.

37 Moya (2025: p. 40) señala que: «en pocas palabras, si un órgano público necesita tratar datos personales, puede hacerlo en la medida que se ajuste al principio de legalidad. Pero tiene que hacerse responsable de ello (lo cual implica el cumplimiento de numerosos principios y deberes que están reconocidos en el nuevo texto de la Ley 19.628)».

¿Qué significa esto, en palabras simples?

* *Uso permitido si cumple una función legal*: si una institución pública necesita nuestros datos para hacer su trabajo (por ejemplo, pagar subsidios, cobrar impuestos o entregar atención médica), puede tratarlos sin necesidad de que firmemos una autorización.
* *No necesitan consentimiento*: a diferencia de muchas empresas privadas, los órganos públicos pueden tratar datos personales sin pedir permiso cuando actúan dentro de sus competencias legales.

  Sin embargo, si se trata de datos personales sensibles (como información de salud, creencias religiosas o datos genéticos), también deben cumplir las reglas especiales establecidas en los artículos 16 y 16 bis, que exigen mayores resguardos e incluso, en ciertos casos, consentimiento expreso o una habilitación legal específica[38].
* *Igual deben proteger nuestros datos*: aunque no pidan consentimiento, *siguen teniendo la obligación de proteger esa información*, usarla solo para la finalidad que la ley permite y adoptar medidas para evitar filtraciones, accesos indebidos o usos abusivos.

38 Ver Pacheco (2025: p. 108) quien señala: «El tratamiento de los datos personales de salud exige equilibrar el respeto al derecho fundamental a la privacidad con las necesidades de los sistemas de salud para garantizar una atención de calidad y promover el bienestar colectivo. La normativa chilena reconoce la naturaleza sensible de los datos de salud y ha establecido un marco legal robusto que regula su tratamiento bajo estrictos criterios de consentimiento informado o excepciones legales autorizadas para proteger la vida, la salud pública y el interés colectivo. Las recientes reformas, como la ley de interoperabilidad de fichas clínicas y la ley de telemedicina, han actualizado el marco legal para responder a los desafíos de la digitalización del sector salud. Estas iniciativas no solo refuerzan la protección de los derechos de los pacientes, sino que también buscan superar la fragmentación de los registros garantizando la continuidad de la atención y fomentando un sistema de salud más eficiente y transparente. A pesar de estos avances, el desarrollo normativo debe seguir evolucionando para enfrentar desafíos emergentes como la ciberseguridad, el uso secundario de datos para propósitos de investigación y la armonización con estándares internacionales, consolidando así un sistema jurídico que acompañe la transformación digital del sector salud».



El Servicio de Impuestos Internos (SII) necesita conocer nuestros ingresos para calcular los impuestos que debemos pagar. Para eso, recopila información sobre sueldos, empleadores y actividades económicas.

No pide permiso para hacerlo, porque esa función está establecida en la ley. Pero sí debe usar los datos que recopila únicamente para fines tributarios y protegerlos adecuadamente.



Caso práctico

El Departamento de Educación de una municipalidad necesita recolectar información personal de estudiantes de colegios públicos, como nombre, edad y dirección, para coordinar programas de alimentación escolar y entrega de útiles.

Algunos apoderados se molestan porque no fueron consultados y exigen autorización previa.

- ¿Necesitaba, el departamento de educación, pedir consentimiento a las familias para usar estos datos?
- ¿Por qué está permitido que los órganos públicos traten datos personales sin autorización previa?
- ¿Qué obligaciones tienen los funcionarios que manejan esta información, aunque no pidan consentimiento?



Apliquemos lo aprendido 1

1. ¿Cuándo pueden los organismos públicos usar datos personales sin pedir permiso?

a. Solo cuando se trata de datos básicos, como el nombre

b. Cuando lo hacen para cumplir con una función legal dentro de sus competencias

c. Siempre y cuando avisen con una semana de anticipación

2. ¿Qué diferencia a los organismos públicos de una empresa privada al momento de tratar datos personales?

a. Las instituciones públicas no necesitan cuidar los datos

b. Pueden tratar los datos con cualquier fin

c. No necesitan consentimiento si lo hacen para cumplir con su función legal dentro de sus competencias

3. ¿Qué significa que un órgano público sea «responsable de datos»?

a. Que puede compartir la información con otras instituciones

b. Que debe proteger los datos, usarlos correctamente y respetar la ley

c. Que puede eliminar los datos cuando quiera

4. ¿Cuál de estas alternativas constituye un buen ejemplo de tratamiento legal de datos por parte de un órgano público?

a. Un banco que analiza tu historial de compras para ofrecerte una tarjeta

b. El SII usando tus datos para calcular tus impuestos

c. Una tienda en línea usando tu correo para enviarte publicidad

¿Cómo deben usar tus datos los servicios públicos?

El artículo 21 de la Ley de Protección de Datos Personales nos dice cómo deben actuar los organismos del Estado cuando manejan información personal. En resumen: deben hacerlo con responsabilidad, siguiendo principios que aseguren un buen uso de los datos y evitando trámites innecesarios.

1.a. ¿Qué principios deben seguir?

Los servicios públicos deben respetar tanto los principios de esta ley como los principios básicos que guían a toda la Administración del Estado. Los principales son:

- *Coordinación*: las instituciones públicas deben trabajar de forma conjunta para evitar que las personas tengan que entregar la misma información una y otra vez a distintos organismos. Es decir, si ya entregaste tu información a un servicio público, no deberían pedírtela de nuevo para realizar otro trámite. Para eso, los sistemas deben «hablar entre sí»[39].
- *Probidad*: las y los funcionarios públicos deben actuar de manera honesta, ética y transparente al manejar tus datos personales. Esto significa que deben protegerlos y usarlos solo para lo que corresponde.
- *Eficiencia*: se busca que el Estado funcione bien, sin trámites duplicados o pasos innecesarios. El objetivo es que el uso de los datos personales facilite los procesos y evite demoras o complicaciones.

1.b. ¿Qué otras normas deben cumplir?

Además de estos principios, los órganos públicos deben seguir todas las reglas que se aplican a cualquier institución que maneja datos personales, como:

- las definiciones generales de qué son los datos personales (artículo 2),

39 En este sentido ver Seaman (2025)

* las obligaciones del responsable del tratamiento de datos, como seguridad y transparencia (artículos 14 al 15 bis), y
* las reglas sobre derechos de las personas, el tratamiento de datos y las obligaciones legales del Estado en esta materia (artículos de los títulos II, V y VII).



Imagina que necesitas inscribir una propiedad. Para eso, tienes que pasar por el Conservador de Bienes Raíces y el Servicio de Impuestos Internos (SII). En lugar de pedirte los mismos papeles en ambas instituciones, lo ideal es que estos organismos se coordinen, compartan la información entre ellos y tú no tengas que repetir el trámite. Eso es aplicar los principios de coordinación y eficiencia.



Caso práctico

Juan acaba de comprar una propiedad y necesita inscribirla. Para hacerlo, debe entregar su información personal al Registro Civil y al SII. Sin embargo, él ya había dado esos datos al SII en otro trámite anterior. Juan se pregunta si realmente tiene que volver a entregar toda esa información otra vez.

- ¿Cómo debería aplicarse el principio de coordinación en este caso? Explica cómo los organismos públicos deberían trabajar juntos para que Juan no tenga que entregar los mismos datos dos veces.
- ¿Qué tienen que ver los principios de probidad y eficiencia con esta situación? Describe cómo los funcionarios públicos deben actuar con honestidad y buscando simplificar el proceso de Juan.
- ¿Es necesario que el Estado le pida permiso a Juan para usar sus datos en este trámite? Analiza si se requiere su consentimiento y por qué, tomando en cuenta que se trata de un trámite legal.



Apliquemos lo aprendido 2

1. ¿En qué caso un órgano público puede usar tus datos personales sin pedirte permiso?

a. Cuando se trata de datos sensibles

b. Cuando lo necesita para cumplir con sus funciones legales

c. Cuando los usa con fines comerciales

2. ¿Qué principio busca que los organismos públicos trabajen en conjunto para no pedirte los mismos papeles más de una vez?

a. Principio de transparencia

b. Principio de probidad

c. Principio de coordinación

3. ¿Qué artículo de la ley explica las responsabilidades que tienen quienes manejan datos personales, incluyendo los servicios públicos?

a. Artículo 1

b. Artículo 14

c. Artículo 21

4. ¿Qué significa que un servicio público sea «responsable de los datos»?

a. Que puede usarlos libremente

b. Que debe protegerlos y asegurarse de que se usen correctamente

c. Que siempre debe pedir permiso para usarlos

5. ¿Qué tipo de datos puede usar un órgano público sin necesidad de que tú lo autorices?

a. Cualquier dato

b. Solo datos sensibles

c. Datos que necesita para cumplir con sus funciones legales

¿Pueden los órganos públicos compartir datos personales? ¿Cuándo?

El artículo 22 nos dice en qué situaciones los organismos del Estado pueden compartir datos personales, ya sea con otros organismos públicos o con entidades privadas. No pueden hacerlo libremente: deben cumplir con ciertas reglas claras.

Compartir datos entre organismos públicos

Los órganos públicos pueden compartir información entre sí, pero solo si es necesario para que cada uno pueda cumplir con sus funciones legales. Por ejemplo, si un ministerio necesita información de otro organismo para resolver un caso, puede pedirla, pero solo puede usarla para ese fin específico. También pueden compartir datos para facilitar trámites o evitar que una persona tenga que entregar la misma información varias veces.

Por cuánto tiempo pueden conservar los datos

Los datos personales solo deben guardarse el tiempo justo para realizar el trámite o la actividad para la que fueron solicitados. Una vez cumplido ese objetivo, deben ser borrados o anonimizados. Solo se pueden conservar por más tiempo en casos especiales, por ejemplo, para responder reclamos, para realizar controles o para respaldar decisiones importantes tomadas por el órgano público.

Cuando se comparten datos con privados

Para entregar datos personales a empresas o particulares, los organismos públicos necesitan el consentimiento de la persona dueña de esos datos, a menos que la cesión se realice para cumplir funciones de fiscalización o inspección (por ejemplo, revisar si una empresa cumple la ley).

Si alguien pide acceso a información pública según la Ley de Transparencia (Ley 20.285), también se necesita el consentimiento del titular de los datos.

Datos especialmente delicados

Los datos que tienen que ver con infracciones penales, civiles, administrativas o disciplinarias tienen una protección especial. Para esos casos, se deben seguir las reglas del artículo 25 de la ley.

Transparencia y control

Todos los meses, los organismos públicos deben publicar en su sitio web los convenios que han hecho para compartir datos, ya sea con otros organismos del Estado o con privados. Esta obligación será fiscalizada por la Agencia de Protección de Datos.



Imaginemos que el Ministerio de Salud necesita confirmar datos de un ciudadano con el Registro Civil para incluirlo en un programa de salud. En ese caso, puede compartir esa información, pero solo para ese programa. No puede usar esos datos para otros fines ni guardarlos más tiempo del necesario, a menos que tenga una razón legal para hacerlo.



Caso práctico

El Servicio Nacional de Capacitación y Empleo (SENCE) está diseñando un nuevo programa de subsidio al empleo. Para verificar si los postulantes cumplen con los requisitos, necesita acceder a información personal que ya se encuentra en poder de otros organismos, como el Registro Civil (estado civil y domicilio) y el Servicio de Impuestos Internos (situación tributaria). SENCE no cuenta con consentimiento previo de los postulantes, pero argumenta que necesita estos datos para aplicar correctamente el subsidio.

Además, SENCE firma un convenio con una entidad privada para implementar parte del programa y esta entidad solicita acceso a los mismos datos personales para cumplir con sus funciones de apoyo.

- Explica si el SENCE puede solicitar datos personales a otros órganos públicos sin consentimiento del titular. ¿Qué requisitos deben cumplirse para que esta comunicación sea válida, según el artículo 22?
- Analiza si la entidad privada que colabora con SENCE puede acceder a los mismos datos personales sin el consentimiento de los titulares. Justifica tu respuesta con base en el artículo 22.
- Si SENCE almacena los datos personales obtenidos para este programa por más tiempo del que dura el subsidio, ¿en qué casos estaría justificado según la ley? ¿Qué debería hacer con los datos cuando ya no tenga una justificación legal para conservarlos?
- ¿Qué tipo de información relacionada con la cesión de datos personales debe publicar SENCE en su página *web* institucional? ¿Por qué esta exigencia es relevante desde el punto de vista de la transparencia y la protección de datos?



Apliquemos lo aprendido 3

1. ¿En qué caso un órgano público puede usar tus datos personales sin pedirte permiso?

a. Cuando se trata de datos sensibles

b. Cuando lo necesita para cumplir con sus funciones legales

c. Cuando los usa con fines comerciales

2. ¿Qué principio busca que los organismos públicos trabajen en conjunto para no pedirte los mismos papeles más de una vez?

a. Principio de transparencia

b. Principio de probidad

c. Principio de coordinación

3. ¿Qué artículo de la ley explica las responsabilidades que tienen quienes manejan datos personales, incluyendo los servicios públicos?

a. Artículo 1

b. Artículo 14

c. Artículo 21

4. ¿Qué significa que un servicio público sea «responsable de los datos»?

a. Que puede usarlos libremente

b. Que debe protegerlos y asegurarse de que se usen correctamente

c. Que siempre debe pedir permiso para usarlos

5. ¿Qué tipo de datos puede usar un órgano público sin necesidad de que tú lo autorices?

a. Cualquier dato

b. Solo datos sensibles

c. Datos que necesita para cumplir con sus funciones legales

Ejercicio de los derechos del titular y procedimientos

El artículo 23 de la Ley de Protección de Datos Personales establece que toda persona tiene derecho a solicitar ante un órgano público el acceso, la rectificación, la oposición o la supresión de sus datos personales. Sin embargo, también señala que existen ciertas excepciones en las que el organismo puede rechazar la solicitud. En caso de negativa, el titular podrá reclamar ante la Agencia de Protección de Datos Personales.

Este artículo establece que los titulares de datos personales pueden ejercer ante los órganos públicos los siguientes derechos:

* *Acceso*: conocer qué datos personales están siendo tratados por el órgano público.
* *Rectificación*: solicitar la corrección de los datos personales que sean inexactos, estén desactualizados o incompletos.
* *Oposición*: rechazar un tratamiento específico de sus datos cuando este sea contrario a las disposiciones de la ley.
* *Supresión*: pedir la eliminación de sus datos personales en los casos establecidos por la ley, por ejemplo, cuando ya no sean necesarios para los fines que motivaron su tratamiento.

Excepciones

Los organismos públicos pueden rechazar estas solicitudes cuando:

* Su aceptación impida o entorpezca el cumplimiento de funciones fiscalizadoras, investigativas, de protección a víctimas y testigos, o sancionatorias.
* Se vea afectado el carácter secreto de la información, cuando este haya sido establecido por una norma legal.

Procedimiento

Para ejercer estos derechos, el titular debe presentar su solicitud ante el jefe superior del servicio correspondiente, siguiendo el procedimiento establecido en el artículo 11 de esta misma ley.

Si la solicitud es denegada, ya sea de forma expresa o tácita, el titular podrá reclamar ante la Agencia de Protección de Datos Personales, la que resolverá conforme al procedimiento administrativo de tutela de derechos regulado en el artículo 41.



Una persona solicita al Servicio de Impuestos Internos (SII) la eliminación de sus datos personales porque ya no son necesarios para el organismo. Sin embargo, si esos datos están siendo utilizados como parte de una investigación fiscal en curso, el SII puede rechazar la solicitud, ya que su eliminación afectaría el cumplimiento de sus funciones investigativas.



Caso práctico

Un ciudadano presenta una solicitud ante el Ministerio de Desarrollo Social para acceder a un programa de asistencia económica. El Ministerio requiere datos personales de otros organismos públicos para evaluar si el ciudadano cumple con los requisitos. Al consultar los datos del ciudadano con el Servicio de Impuestos Internos (SII), el Ministerio se da cuenta de que los datos están desactualizados. Además, el ciudadano se opone a que el Ministerio utilice su información personal fiscal para la evaluación de su solicitud.

- Explica si el Ministerio puede o no ceder o comunicar los datos del ciudadano al SII sin su consentimiento.
- Evalúa si la oposición del ciudadano es válida o no, de acuerdo con la ley, y cómo debería actuar el Ministerio frente a la solicitud de oposición.
- Analiza si el Ministerio debe suprimir los datos del ciudadano una vez que se ha completado el análisis de su solicitud.



Apliquemos lo aprendido 4

1. ¿Qué derechos puede ejercer un titular frente a un organismo público?

a. Acceso, rectificación, oposición y supresión

b. Acceso únicamente

c. Ninguno, ya que los organismos públicos no tienen que responder

2. ¿Qué puede hacer el titular si un organismo público no responde a su solicitud?

a. Presentar un reclamo ante la Agencia de Protección de Datos

b. Demandar directamente al organismo

c. Nada, no tiene opciones

3. ¿En qué caso puede un organismo público rechazar la solicitud de rectificación de datos?

a. Si afecta una investigación fiscalizadora

b. Si los datos son antiguos

c. Siempre debe aceptar la solicitud

4. ¿Qué debe hacer un organismo público con los datos una vez que se haya cumplido el fin para el que fueron recogidos?

a. Guardarlos indefinidamente

b. Suprimirlos o anonimizarlos

c. Compartirlos con otros organismos

5. ¿A quién debe dirigirse el titular para ejercer sus derechos?

a. Al jefe superior del servicio del organismo público

b. A cualquier funcionario público

c. Directamente a la Agencia

Regulación especial para el tratamiento de datos sensibles en situaciones críticas

El artículo 24 de la Ley de Protección de Datos Personales establece reglas especiales para el tratamiento de datos personales sensibles por parte de los órganos públicos, especialmente cuando estos datos se relacionan con situaciones de gran importancia, como la seguridad pública, la defensa nacional o situaciones de emergencia.

¿Cuándo se pueden tratar estos datos sin necesidad de consentimiento?

El artículo establece tres situaciones en que los datos personales pueden ser tratados sin el permiso del titular:

- *Investigaciones y procesos legales:* cuando se trata de investigar o juzgar delitos, o para proteger a víctimas y testigos.
- *Seguridad nacional:* cuando se trata de temas relacionados con la seguridad de la nación, la defensa del país o la política exterior.
- *Emergencias o catástrofes:* cuando ocurra una emergencia o una catástrofe y se necesiten los datos personales para ayudar a las personas afectadas.

En estos casos no se requiere el consentimiento del titular de los datos, sin embargo, deben tratarse con especial cuidado.

Protección de datos confidenciales

Los datos personales que están protegidos por normas de secreto, reserva o confidencialidad también se manejan bajo estas reglas especiales. Si un organismo público necesita compartir estos datos con otro, debe asegurarse de que el receptor mantenga la misma confidencialidad.

Intercambio de información entre organismos públicos

Los organismos públicos tienen la obligación de intercambiar información entre ellos cuando sea necesario para cumplir con sus funciones legales. Este intercambio debe ser necesario y proporcional, siempre respetando los derechos de las personas.

Rol de la Agencia de Protección de Datos Personales

La Agencia de Protección de Datos Personales tiene la facultad de dar instrucciones específicas sobre cómo se deben aplicar estas reglas y garantizar que se respeten los derechos de las personas. Su objetivo es asegurarse de que las leyes de protección de datos se cumplan correctamente, incluso en situaciones sensibles.



Imagina que hay una investigación en curso sobre un delito grave y la policía necesita compartir información personal de personas involucradas con otros organismos públicos, como la Fiscalía. En este caso, no es necesario pedir el consentimiento de los titulares de los datos. Sin embargo, estos deben ser tratados con mucha cautela, asegurando que solo se usen para el propósito legal permitido y que la confidencialidad se respete en todo momento.



Caso práctico

Durante una investigación por tráfico de drogas, la Policía de Investigaciones solicita al Ministerio de Salud los datos médicos de un sospechoso, ya que podrían aportar antecedentes relevantes. El Ministerio entrega la información, la cual contiene datos sensibles sobre tratamientos psicológicos. Más tarde, un periodista solicita acceso a esos mismos datos alegando interés público.

- ¿Puede el Ministerio de Salud entregar los datos médicos del sospechoso a la Policía en este contexto?
- ¿Está obligado el Ministerio a entregar esos datos al periodista?
- ¿Qué condiciones debe cumplirse para que la cesión de datos sea lícita, según el artículo 24?



Apliquemos lo aprendido 5

1. ¿Qué tipo de datos pueden ser tratados por los órganos públicos bajo el régimen especial de seguridad pública?

a. Datos financieros

b. Datos con fines de investigación penal y protección de víctimas

c. Datos laborales

2. ¿Cuándo puede un órgano público compartir datos personales con otro órgano público?

a. Cuando exista consentimiento del titular

b. Siempre que se realice con fines comerciales

c. Cuando sea necesario para cumplir funciones legales dentro de sus competencias

3. ¿Qué deben garantizar los organismos que reciben datos protegidos por normas de confidencialidad?

a. Mantener los datos en secreto o confidencialidad

b. Publicar los datos en su página *web*

c. Compartir los datos con entidades privadas

4. ¿Cuándo pueden, los datos, ser tratados sin el consentimiento del titular?

a. Solo en investigaciones penales o emergencias

b. En cualquier situación

c. Siempre que haya un contrato entre las partes

5. ¿Qué papel juega la Autoridad de Protección de Datos en la regulación del régimen especial?

a. Ninguno

b. Puede dictar instrucciones para proteger los derechos fundamentales

c. Solo puede actuar en investigaciones penales

Tratamiento de datos sobre infracciones: reglas, límites y confidencialidad

El artículo 25 de la Ley de Protección de Datos Personales establece cómo deben tratarse los datos personales relacionados con infracciones penales, civiles, administrativas y disciplinarias. La idea es proteger la privacidad de las personas y evitar que se exponga su información sin justificación legal.

¿Quién puede tratar estos datos?

Solo los organismos públicos están autorizados a manejar este tipo de información, únicamente cuando sea necesario para cumplir con sus funciones legales y en los casos que la ley lo permite de forma expresa.

¿Qué condiciones deben cumplirse?

Siempre que estos datos se comuniquen o publiquen, deben ser exactos, completos, actualizados y suficientes para el fin que se persigue.

Además, una vez que la acción o sanción prescribe (es decir, ya no tiene efecto legal), los datos no pueden seguir siendo públicos ni compartirse, salvo que una ley diga lo contrario.

¿Cuánto tiempo pueden estar disponibles al público?

Infracciones penales: se aplican los plazos que indica la ley penal.

Infracciones civiles, administrativas y disciplinarias: la información puede ser pública durante cinco años.

¿Qué está prohibido?

Está prohibido el uso masivo de estos datos en registros electrónicos. Es decir, no se pueden recopilar ni usar en grandes cantidades para fines generales, como bases de datos abiertas o comerciales. Hacerlo es una falta gravísima.

¿Hay excepciones?

Sí. Los tribunales de justicia u otros organismos públicos pueden pedir esta información si lo necesitan para cumplir sus funciones legales. Pero incluso en estos casos, deben manejarla con confidencialidad.



Imaginemos que una persona fue sancionada por una infracción administrativa hace cuatro años. Esa información puede estar disponible públicamente. Sin embargo, si han pasado más de cinco años o la sanción ya prescribió, los datos deben dejar de ser públicos. Si un tribunal los necesita, puede solicitarlos, pero no pueden ser compartidos con terceros ni difundidos públicamente.



Caso práctico

Evaluación del tratamiento de datos sobre infracciones

Un ciudadano fue sancionado por una infracción civil hace tres años. Sus datos aún están disponibles en un registro público en línea. La persona solicita que esta información sea eliminada porque considera que la infracción ya prescribió. El organismo público revisa y constata que el plazo de cinco años aún no se cumple.

- ¿Tiene derecho el ciudadano a que se eliminen sus datos antes de que pasen los cinco años?
- ¿Qué debe hacer el órgano público en este caso?
- ¿Qué pasaría si ya hubiesen pasado cinco años desde la infracción?



Apliquemos lo aprendido 6

1. ¿Quiénes pueden tratar datos sobre infracciones penales, civiles, administrativas o disciplinarias?

a. Organismos públicos, dentro de sus funciones legales

b. Empresas privadas

c. Cualquier persona

2. ¿Por cuánto tiempo pueden estar disponibles al público los datos sobre infracciones civiles, administrativas y disciplinarias?

a. Indefinidamente

b. Cinco años

c. Dos años

3. ¿Qué sucede con los datos relacionados con infracciones una vez que la sanción o acción prescribe?

a. Pueden seguir siendo públicos

b. No pueden ser públicos ni compartidos, salvo disposición legal

c. Son eliminados inmediatamente

4. ¿Está permitido el tratamiento masivo de los datos personales contenidos en registros de infracciones?

a. Sí, siempre que haya una justificación

b. No, está prohibido y constituye una infracción gravísima

c. Solo si el titular lo solicita

5. ¿Quiénes pueden acceder a estos datos en situaciones excepcionales?

a. Cualquier ciudadano

b. Tribunales de justicia y organismos públicos dentro de sus competencias

c. Empresas privadas

Capítulo 10

La Agencia de Protección de Datos Personales: una aliada en el cuidado de tu privacidad

¿Quién protege tus datos cuando estos se usan mal?

Imagina que tus datos personales (tu nombre, tu RUT, tus compras *online*, tus hábitos) son piezas que, juntas, forman un rompecabezas que dice quién eres. ¿Qué pasaría si alguien usa esas piezas sin tu permiso o las comparte sin que lo sepas? En Chile, existe una institución pública encargada de que eso no pase: la Agencia de Protección de Datos Personales (APDP)[40].

Este capítulo te ayudará a entender de forma sencilla de qué se trata esta Agencia, cómo funciona, qué puede hacer para protegerte y cómo puedes acudir a ella si sientes que tus datos han sido mal utilizados.

¿Qué es la APDP?

La APDP es una corporación autónoma de derecho público. Esto significa que es una institución pública independiente, con personalidad

40 Como señala Rajevic (2025), se trata, en definitiva, de una verdadera Autoridad Administrativa Independiente —como las denomina el derecho comparado—, que en virtud de esa mayor independencia que garantizan las normas explicadas puede adoptar decisiones sin estar sometida a represalias o consecuencias adversas derivadas del Gobierno, al menos dentro de los límites de lo posible porque, obviamente, este siempre podrá influir, por ejemplo, en la discusión presupuestaria anual.

jurídica y patrimonio propio, creada especialmente para proteger tu privacidad y el correcto uso de tus datos personales.

Aunque no depende directamente del Gobierno, se relaciona con el presidente de la República a través del Ministerio de Economía. Su misión principal es garantizar que todas las personas que viven en Chile puedan ejercer su derecho a la vida privada y a la autodeterminación informativa.

Base legal: artículos 30 y siguientes de la nueva Ley de Protección de Datos Personales.

¿Cómo está organizada la APDP?

* *Es autónoma, pero no constitucional.* No está mencionada en la Constitución como el Congreso o la Contraloría General de la República. Por eso, si quiere revisar el uso de datos en instituciones especiales (como el Poder Judicial), necesita autorizaciones particulares.
* *Tiene una dirección colegiada.* Está dirigida por tres consejeros o consejeras, nombrados por el presidente de la República y aprobados por el Senado. Esto busca asegurar un equilibrio político y técnico en su funcionamiento.
* *Independencia y profesionalismo.* Los consejeros duran seis años en su puesto, sin reelección. No pueden trabajar en empresas que usen datos personales. Tampoco pueden tener familiares con intereses en esas empresas.



Si una persona quiere postular como consejero, debe tener experiencia en protección de datos. No basta con ser abogado generalista o político; se necesita saber realmente del tema.



Una ejecutiva de una empresa de marketing digital no puede asumir como consejera de la Agencia, ni siquiera si dejó su cargo antes del nombramiento.

¿Qué puede hacer la APDP?

La Agencia tiene muchas funciones. Estas son algunas de las más importantes, explicadas con ejemplos sencillos:

* *Dictar normas y proponer cambios legales.* Puede establecer reglas obligatorias para instituciones que traten datos personales y sugerir reformas legales. Ejemplo, exige que las apps móviles soliciten consentimiento expreso antes de acceder a tu ubicación.
* *Fiscalizar a quienes manejan tus datos.* Tiene el poder de pedir documentos, hacer visitas y comprobar si se están cumpliendo las normas. Ejemplo, una cadena de tiendas es investigada porque envía correos promocionales a personas que nunca dieron su consentimiento.
* *Interpretar la ley.* Cuando hay dudas sobre cómo entender un artículo o concepto, la APDP puede entregar una interpretación oficial. Ejemplo, aclara que la dirección IP de un computador sí puede ser considerada un dato personal.
* *Aplicar sanciones.* Si detecta incumplimientos, puede iniciar procedimientos y sancionar a los responsables. Ejemplo, multa a una clínica por compartir información médica de una paciente sin su autorización.
* *Educar y colaborar.* Organiza actividades educativas, promueve buenas prácticas y puede firmar convenios con instituciones nacionales e internacionales. Ejemplo, realiza talleres en colegios para enseñar a niños y adolescentes cómo proteger su privacidad digital.



Caso práctico

«Datos al sol»

Felipe, un estudiante de 17 años, descubre que su colegio contrató una aplicación para controlar la asistencia que, además, recolecta información sobre su comportamiento (como si llega tarde o si participa en clases). Esa información fue compartida con una empresa de cursos *online*, sin que Felipe ni sus padres lo autorizaran.

¿Qué puede hacer Felipe?

Felipe puede presentar una reclamación ante la APDP. La Agencia puede:

- investigar al colegio y a la empresa,
- emitir un dictamen que aclare si esos datos son sensibles,
- sancionar a los responsables si hubo infracción y
- proponer nuevas reglas sobre el uso de estas aplicaciones en colegios.

Este caso muestra cómo la APDP puede actuar en defensa de las personas, especialmente de los más jóvenes.



Claves para recordar

- *La APDP es una institución pública independiente*, creada para proteger tus datos y tu privacidad.
- *Está dirigida por un consejo de tres personas*, con experiencia profesional en la materia.
- *Tiene muchas funciones*, como fiscalizar, sancionar, dictar normas y hasta educar.
- *Puedes acudir a ella si piensas que tus datos fueron mal usados*, incluso por colegios, empresas o apps.
- *Promueve la cultura de protección de datos desde edades tempranas*, trabajando con instituciones educativas.



Apliquemos lo aprendido

1.¿Cuál es la naturaleza jurídica de la Agencia de Protección de Datos Personales (APDP)?

a. Subsecretaría del Ministerio de Justicia

b. Corporación autónoma de derecho privado

c. Corporación autónoma de derecho público

2. ¿Quién debe aprobar el nombramiento de los consejeros o consejeras de la APDP?

a. Contraloría General de la República

b. Cámara de Diputados y Diputadas

c. Senado

3. ¿Cuál de las siguientes opciones NO es una función de la APDP?

a. Emitir normas obligatorias para proteger los datos personales

b. Fiscalizar el cumplimiento de la ley

c. Juzgar causas civiles por daños y perjuicios

4. ¿Cuánto dura el cargo de consejero en la APDP?

a. Cuatro años, con posibilidad de reelección

b. Seis años, sin reelección

c. Diez años

Capítulo 11

Protección de datos en la Unión Europea

Actualmente, la circulación de información personal ya no se limita al espacio interno de un solo país. Empresas, plataformas digitales, prestadores de servicios, instituciones educacionales, comercios y organismos de muy diversa naturaleza operan en entornos interconectados, en los que los datos pueden almacenarse, procesarse o compartirse a través de infraestructuras, proveedores o mercados extranjeros. Así, la inclusión de una referencia a la regulación europea en un libro orientado a explicar el régimen chileno de protección de datos personales se justifica por el contexto en que hoy se desarrolla el tratamiento de datos.

En este escenario, quien trata datos personales en Chile no solo debe conocer la normativa nacional que regula su actividad, sino también familiarizarse con los estándares jurídicos que predominan en otros mercados relevantes. Ello resulta especialmente importante cuando una organización chilena presta servicios a usuarios de otros países, utiliza tecnologías desarrolladas en el extranjero, contrata plataformas internacionales o participa en cadenas de prestación de servicios donde intervienen actores sujetos a regulaciones foráneas. Conocer esas reglas permite comprender mejor el entorno en que circulan los datos y actuar con mayor diligencia en su tratamiento.

La regulación europea ocupa en este ámbito un lugar especialmente relevante, porque ha influido de manera decisiva en la construcción de estándares internacionales sobre privacidad, transparencia, seguridad, responsabilidad y derechos de las personas titulares de datos. Su estudio no implica desplazar la centralidad de la ley

chilena, sino complementar su comprensión con un referente normativo que ha orientado buena parte de la evolución contemporánea de esta materia.

Desde esa perspectiva, incorporar una mirada sobre el modelo europeo contribuye a fortalecer una cultura de cumplimiento más amplia, consciente de que tratar datos personales exige no solo respetar la legislación propia, sino también entender las exigencias que pueden provenir de otros espacios regulatorios con los que hoy se interactúa de manera constante. En un entorno digital y globalizado, conocer esos marcos es también una forma de prevenir riesgos, adoptar buenas prácticas y elevar el estándar de protección de las personas.

¿Quieres saber cómo se protegen tus datos en la Unión Europea?

La protección de datos personales es un derecho fundamental en la Unión Europea (UE). En un mundo donde cada vez compartimos más información a través de Internet, es clave conocer qué normas existen para garantizar nuestra privacidad y seguridad. ¿Te has preguntado qué hace la UE para proteger tus datos y cómo te beneficia? En este capítulo, te explicaremos de manera sencilla cómo funciona esta regulación.

¿Por qué es importante proteger nuestros datos?

Cada vez que usamos redes sociales, compramos en línea o suscribimos un servicio, estamos compartiendo datos personales. Sin una regulación adecuada, esta información podría ser utilizada sin nuestro consentimiento. Por eso, la UE ha establecido reglas estrictas para proteger nuestra privacidad y asegurarse de que las empresas y organizaciones manejen nuestros datos de manera segura y responsable.



Imagina que compras ropa en una tienda en línea y al poco tiempo empiezas a recibir correos y anuncios sobre productos similares sin haber dado tu permiso. Gracias al Reglamento General de Protección de Datos (RGPD), puedes exigir que dejen de enviarte publicidad si no diste tu consentimiento.

¿Qué ley protege nuestros datos en la UE?

El Reglamento General de Protección de Datos (RGPD) es la ley de la Unión Europea que regula cómo se recopilan, usan y protegen los datos personales de sus ciudadanos. Su objetivo es garantizar que cualquier empresa u organización que maneje información personal lo haga de forma segura y con transparencia.

Bajo el RGPD, las personas tienen derechos clave, como el acceso a sus datos, la posibilidad de corregirlos, eliminarlos (derecho al olvido) o trasladarlos a otro servicio (portabilidad de datos). Además, exige que las empresas obtengan consentimiento explícito antes de usar la información personal y establece sanciones para quienes no cumplan con estas reglas.

Este reglamento no solo protege a los ciudadanos dentro de la UE, sino que también aplica a empresas de otros países que traten datos de europeos, asegurando un estándar global de privacidad.

El RGPD entró en vigor en 2018. Este reglamento establece reglas claras sobre cómo las empresas deben manejar nuestros datos. Algunos de sus puntos clave son:

* *Transparencia:* debes saber qué datos tuyos se recopilan y para qué los usan.
* *Consentimiento:* no pueden usar tu información sin tu permiso.
* *Derecho al olvido:* puedes solicitar que se eliminen tus datos cuando ya no sean necesarios.
* *Seguridad:* las empresas deben proteger tu información y evitar filtraciones.

* *Multas por incumplimiento:* si una empresa no cumple con estas reglas, puede recibir sanciones millonarias.

¿Qué otras reglas complementan al RGPD?

Además del RGPD, existen otras normativas que refuerzan la protección de datos en situaciones específicas:

* *Protección en el* ámbito *penal:* garantiza que la policía y otras autoridades usen los datos personales de manera responsable.
* *Privacidad en Internet y telecomunicaciones:* regula el uso de información en llamadas, correos electrónicos y mensajes.
* *Protección dentro de la UE:* establece normas para que las instituciones europeas manejen los datos de forma segura.

¿Qué pasa cuando nuestros datos se transfieren a otros países?

Muchas empresas operan a nivel global y necesitan transferir datos a otros países. Para garantizar que tu información esté protegida, la



Si alguna vez creaste una cuenta en una red social y ya no la usas, puedes solicitar que eliminen toda tu información en lugar de que quede almacenada indefinidamente.



Si te llaman de una empresa ofreciéndote un producto sin que hayas dado permiso para que usen tu número, puedes denunciarlo porque vulnera tu privacidad.

UE solo permite transferencias de datos a países que ofrezcan un nivel de seguridad adecuado. Esto ha generado conflictos con Estados Unidos, ya que sus normas de privacidad no cumplen completamente con los estándares europeos.

¿Cómo nos afecta en la vida diaria?

Gracias a estas regulaciones, tienes más control sobre tu información personal. Puedes decidir qué datos compartes, exigir que te informen sobre su uso y pedir que los borren si ya no los necesitas. Además, las empresas deben ser más cuidadosas con la seguridad de la información, lo que reduce riesgos como el robo de identidad o el uso indebido de datos.

Conclusión

La protección de datos en la Unión Europea es un tema fundamental que nos beneficia en nuestra vida diaria. Gracias al Reglamento General de Protección de Datos (RGPD) y otras normativas complementarias, contamos con herramientas para controlar cómo se



Cuando usas un servicio de almacenamiento en la nube con sede en otro país, la empresa debe cumplir con las normas de protección de datos europeas para poder operar en la UE.



Si un banco sufre un ataque informático y se filtran datos de sus clientes, está obligado a informarte de inmediato y tomar medidas para minimizar el daño.

recopila, se usa y se protege nuestra información personal. Esto no solo nos da tranquilidad al navegar en Internet, comprar en línea o usar servicios digitales, sino que también obliga a las empresas a ser más transparentes y responsables con nuestros datos.

En un mundo donde compartimos cada vez más información, estas normas nos aseguran que nuestra privacidad está protegida y que tenemos derechos claros, como acceder a nuestros datos, corregirlos, eliminarlos o incluso trasladarlos a otro servicio. Además, las empresas que no cumplan con estas reglas pueden enfrentar sanciones severas, lo que garantiza que se tomen en serio la seguridad de nuestra información.

En definitiva, la UE ha establecido un estándar alto de protección de datos que no solo nos empodera como ciudadanos, sino que también promueve un manejo más ético y seguro de la información en el ámbito digital. ¡Es un gran paso hacia un mundo en línea más confiable y respetuoso con nuestra privacidad!



Apliquemos lo aprendido

1. ¿Qué es el RGPD?

a. Una red social europea

b. Un reglamento que protege los datos personales en la UE

c. Una ley que regula el comercio electrónico

2. ¿Cuál es uno de los derechos que otorga el RGPD?

a. Derecho a recibir publicidad sin consentimiento.

b. Derecho al olvido (eliminar tus datos)

c. Derecho a compartir datos de otras personas

3. ¿Qué deben hacer las empresas, según el RGPD, antes de usar tus datos personales?

a. Pedir tu consentimiento explícito

b. Usarlos sin informarte

c. Venderlos a otras empresas

4. ¿Qué sucede si una empresa no cumple con el RGPD?

a. Recibe felicitaciones por su gestión

b. Puede ser multada con sanciones millonarias

c. No pasa nada, es solo una recomendación

5. ¿Qué garantiza el RGPD cuando tus datos son transferidos a otros países?

a. Que los países receptores tengan un nivel de seguridad adecuado

b. Que tus datos puedan ser vendidos libremente

c. Que no se apliquen normas de privacidad

6. ¿Qué ejemplo se menciona sobre el uso indebido de datos?

a. Recibir correos publicitarios sin haber dado permiso

b. Ganar un premio por compartir datos

c. Ser invitado a eventos exclusivos



Apliquemos lo aprendido

7. ¿Qué normativa complementa al RGPD en el ámbito penal?

a. Reglas para el uso responsable de datos por parte de la policía

b. Normas para el comercio internacional

c. Leyes sobre redes sociales

8. ¿Qué obligación tiene una empresa si sufre una filtración de datos?

a. No informar a los afectados

b. Informar de inmediato a los clientes y tomar medidas

c. Continuar operando como si nada hubiera pasado

Conclusiones

La vida cotidiana se ha desplazado, con creciente intensidad, hacia entornos digitales que median decisiones personales, relaciones sociales, consumo, educación, salud y trabajo. En ese contexto, los datos personales dejan de ser un elemento accesorio o meramente técnico: se convierten en el «rastro» permanente a partir del cual se describen, clasifican e infieren conductas, preferencias y riesgos. La consecuencia práctica es decisiva: sin un marco de protección claro, exigible y comprensible, las personas quedan expuestas a usos no previstos —o incluso invisibles— de su información, con impactos que pueden proyectarse mucho más allá del momento en que el dato fue entregado.

Desde esta premisa, la reforma introducida por la Ley 21.719 —que modifica la Ley 19.628— representa un giro estructural en el modo de entender el tratamiento de datos en Chile: no se trata solo de actualizar definiciones o agregar obligaciones aisladas, sino de consolidar un sistema que refuerza los derechos de las personas y eleva, correlativamente, los deberes de quienes tratan datos. El texto sitúa este cambio con claridad, destacando que la reforma contempla una entrada en vigor prevista para el 1 de diciembre de 2026 y que su alcance implica responsabilidades más densas para responsables y encargados.

1. Una primera conclusión sustantiva es que el nuevo marco se propone como una regulación de amplio alcance, aplicable tanto a entidades públicas como privadas, articulada desde el estándar constitucional y orientada a ordenar el tratamiento

conforme a condiciones y límites verificables. Ese alcance, además, no se agota en la frontera territorial clásica: el tratamiento puede quedar sometido a la ley incluso cuando ocurre fuera del país, si se ofrecen bienes o servicios a titulares ubicados en Chile o si se monitorea su comportamiento, entre otros supuestos expresamente descritos. Esta proyección extraterritorial confirma una idea central del manuscrito: la protección efectiva requiere acompañar la realidad del ecosistema digital, donde los flujos de datos, servicios y decisiones superan con facilidad los límites geográficos tradicionales.

2. Una segunda conclusión es que la protección se construye desde categorías amplias y, al mismo tiempo, desde una diferenciación normativa relevante. Por un lado, la definición de *dato personal* se formula de modo extenso, atendiendo a la identificabilidad directa o indirecta. Por otro, se reconoce un estatuto especialmente reforzado para los datos sensibles, con referencia a ámbitos particularmente intensos de la vida humana —como salud, datos biométricos, ideología, orientación o identidad—, precisamente porque su tratamiento puede generar riesgos más altos de discriminación, exposición o daño. La consecuencia pedagógica y práctica es clara: el enfoque de cumplimiento no puede reducirse a listas de verificación; exige evaluar qué tipo de datos se tratan, en qué contexto y con qué potencial de afectación.

3. En tercer lugar, el texto permite concluir que los principios del tratamiento adquieren un rol vertebral: operan como criterios de legitimidad y como parámetros para evaluar desviaciones típicas del mundo digital. La licitud y lealtad obligan a tratar datos de manera transparente, evitando engaños o prácticas opacas, y asignan al responsable una carga de acreditación sobre la base que habilita el tratamiento. La finalidad, por su parte, exige que la recolección responda a fines específicos y que no se produzcan reutilizaciones incompatibles sin habilitación. Estas ideas, presentadas como principios, funcionan como una «constitución práctica» del sistema: orientan decisiones organizacionales, modelos de negocio y políticas internas, tanto como

delimitan lo que puede considerarse un uso legítimo de datos en contextos de innovación.

4. En cuarto lugar, el consentimiento se reafirma como un pilar del régimen, pero no como una fórmula vacía ni como un acto ritual. La reforma lo concibe con exigencias de calidad: debe ser libre, específico, inequívoco e informado, expresado mediante declaración o acción afirmativa clara. A la vez, el texto destaca la existencia de supuestos habilitantes distintos del consentimiento —por ejemplo, para proteger vida o salud, por exigencia legal, para la ejecución contractual o por interés legítimo en condiciones acotadas—, lo que muestra un sistema que intenta equilibrar autonomía personal con necesidades sociales e institucionales, bajo parámetros de proporcionalidad. Este equilibrio se vuelve especialmente exigente cuando se trata de datos sensibles, de menores o de categorías que aumentan el riesgo de daño: allí se eleva el estándar y se impone al responsable una obligación de prueba, con la consecuencia de que, si no se acredita la autorización, se presume la ausencia de un consentimiento válido.

5. La quinta conclusión es que la *autonomía digital*, como idea fuerza del libro, se materializa en un catálogo robusto de derechos, irrenunciables y accionables, que amplía el paradigma anterior. Junto a acceso, rectificación y supresión, se reconocen derechos como oposición, portabilidad y bloqueo, ofreciendo al titular herramientas concretas para controlar el ciclo de vida de sus datos y reaccionar frente a tratamientos indebidos. Especial mención merece el bloqueo, por su utilidad práctica: permite suspender el tratamiento mientras se resuelven controversias o solicitudes, evitando que el daño se consolide durante la tramitación. En conjunto, el sistema de derechos no se presenta como una declaración abstracta, sino como una arquitectura de control: saber qué ocurre con los datos, corregir lo incorrecto, detener lo injustificado, eliminar lo improcedente y, cuando corresponda, trasladar la información a otro proveedor o contexto.

6. En sexto lugar, el texto conduce a una conclusión particularmente relevante para la gestión institucional: la protección de

datos no puede ser un «añadido» posterior, sino que debe incorporarse desde el diseño y por defecto. Ello implica planificar el tratamiento de forma preventiva, recolectar solo lo necesario y sostener medidas de seguridad durante todo el ciclo de tratamiento, con una lógica de mejora continua. La seguridad se entiende como una obligación sustantiva vinculada a la confiabilidad del sistema —confidencialidad, integridad, disponibilidad y resiliencia— y no como una mera formalidad documental. El trabajo, además, muestra que el cumplimiento debe adecuarse a factores como tamaño organizacional, volumen y naturaleza de los datos, y finalidades del tratamiento, dejando a la Agencia la fijación de estándares mínimos por vía de instrucción general. Con ello, la protección se vuelve un componente de gobernanza: políticas, controles, roles internos, registros y decisiones de diseño pasan a ser parte de la responsabilidad legal.

7. La séptima conclusión se refiere al tratamiento de incidentes y vulneraciones de seguridad, que el texto aborda con un enfoque institucional y trazable. Se define la vulneración de forma amplia —incluyendo destrucción, pérdida, filtración, alteración o acceso no autorizado— y se activa el deber de notificación cuando exista un riesgo razonable para derechos y libertades de los titulares. Esta obligación se acompaña de deberes de registro y documentación del incidente, exigiendo información sobre su naturaleza, efectos, categorías involucradas, número aproximado de afectados y medidas adoptadas. A ello se suma la obligación de comunicar a los titulares en casos especialmente sensibles (por ejemplo, datos sensibles o de menores), con lenguaje claro y opciones de comunicación masiva si la notificación individual no es posible. En consecuencia, la gestión de incidentes deja de ser un evento meramente técnico: se integra como un deber jurídico de diligencia, transparencia y rendición de cuentas.

8. En octavo lugar, la reforma se consolida mediante institucionalidad especializada. La Agencia de Protección de Datos Personales se describe como una corporación autónoma de derecho público, dotada de una misión de tutela del derecho y

una estructura de dirección colegiada. Su rol resulta crucial no solo por la fiscalización y sanción, sino también por su función interpretativa y formativa, capaz de traducir principios y obligaciones en estándares aplicables, especialmente en ámbitos de alta complejidad técnica. Esta institucionalidad aparece, en el texto, como el puente entre la promesa normativa y la eficacia real: sin un órgano con potestades y capacidades suficientes, los derechos corren el riesgo de quedar como declaraciones difíciles de hacer valer.

9. La novena conclusión se vincula con los procedimientos y vías de tutela. El manuscrito sistematiza el itinerario básico: el ejercicio de derechos comienza ante el responsable, con plazos de respuesta que, en principio, alcanzan 30 días y admiten prórroga; frente a la ausencia de respuesta, se habilita reclamación ante la Agencia. Se contempla, además, una tutela administrativa estructurada ante negativa o silencio, con etapas y plazos definidos. Finalmente, se prevé control judicial mediante reclamación, con una referencia temporal de 15 días hábiles y facultades de la Corte para confirmar, revocar o modificar lo resuelto. El punto central es que la protección no depende de la «buena voluntad» del responsable: se articula una ruta de exigibilidad que aspira a hacer los derechos practicables.

10. La décima y última conclusión es, en cierto sentido, la síntesis del enfoque: la autonomía digital exige una cultura de protección de datos que combine derechos individuales, deberes organizacionales y capacidades institucionales. El texto muestra que la reforma busca instalar un estándar donde el tratamiento de datos sea justificable, proporcional y transparente; donde el titular tenga herramientas reales de control; donde la seguridad se gestione como obligación continua, y donde existan vías efectivas para corregir incumplimientos y reparar impactos. Al mismo tiempo, se recuerda que incluso el Estado, aunque disponga de habilitaciones para tratar datos en el marco de sus funciones, debe hacerlo dentro de los límites de legalidad y finalidad, evitando convertir la excepción en regla.

En definitiva, el capítulo final permite reafirmar la tesis práctica que atraviesa la obra: proteger datos personales no es solo proteger información; es proteger decisiones, oportunidades y dignidad en un entorno donde la vida digital amplifica tanto las ventajas como los riesgos. La reforma, leída desde los principios, los derechos, los deberes de seguridad, la gestión de incidentes, la institucionalidad y los procedimientos, ofrece un camino para transformar la protección de datos en una garantía efectivamente operativa. Su éxito, sin embargo, dependerá de la apropiación social y organizacional de sus estándares: que las personas conozcan y ejerzan sus derechos, que las instituciones diseñen y gobiernen tratamientos responsables, y que la Agencia despliegue una fiscalización e interpretación que vuelva el sistema comprensible, predecible y exigible en la práctica.

Respuestas correctas

Capítulo I

Apliquemos lo aprendido, página 24

1. b

2. c

3. b

4. a

5. c

Capítulo II

Apliquemos lo aprendido, página 31

1. b

2. c

3. c

4. c

5. c

Capítulo III

Apliquemos lo aprendido, página 41

1. b

2. b

3. b

4. b

5. b

Capítulo IV

Apliquemos lo aprendido 1, página 55

1. a

2. b

3. b

4. c

5. b

Apliquemos lo aprendido 2, página 62

1. c

2. b

3. b

4. c

Apliquemos lo aprendido 3, página 66

1. c

2. c

3. b

4. b

5. b

Capítulo V

Apliquemos lo aprendido, página 73

1. c

2. a

3. b

Capítulo VI

Apliquemos lo aprendido 1, página 81

1. b

2. b

3. b

Apliquemos lo aprendido 2, página 88

1. b

2. c

3. b

4. b

5. b

6. c

7. b

8. c

9. c

10. b

Apliquemos lo aprendido 3, página 99

1. b

2. a

3. b

4. b

5. b

Apliquemos lo aprendido 4, página 102

1. a

2. b

3. b

4. c

5. b

Apliquemos lo aprendido 5, página 105

1. a

2. b

3. b

4. b

5. c

Capítulo VII

Apliquemos lo aprendido 1, página 110

1. b

2. b

3. c

4. b

5. c

Apliquemos lo aprendido 2, página 113

1. b

2. b

3. a

4. b

5. a

Apliquemos lo aprendido 3, página 118

1. b

2. b

3. c

4. a

5. b

Apliquemos lo aprendido 4, página 121

1. a

2. b

3. b

4. b

5. b

Apliquemos lo aprendido 5, página 125

1. b

2. b

3. b

4. b

5. b

Apliquemos lo aprendido 6, página 129

1. b

2. b

3. b

4. b

5. b

6. b

Apliquemos lo aprendido 7, página 133

1. b

2. a

3. b

4. c

5. c

Capítulo VIII

Apliquemos lo aprendido 1, página 142

1. b

2. c

3. c

4. c

5. b

6. b

7. b

8. b

9. c

10. b

Apliquemos lo aprendido 2, página 151

1. c

2. c

3. b

4. c

5. c

Apliquemos lo aprendido 3, página 155

1. c

2. a

3. b

4. b

5. a

Capítulo IX

Apliquemos lo aprendido 1, página 160

1. b

2. c

3. b

4. b

Apliquemos lo aprendido 2, página 164

1. b

2. c

3. b

4. b

5. c

Apliquemos lo aprendido 3, página 168

1. b

2. c

3. b

4. b

5. b

Apliquemos lo aprendido 4, página 171

1. a

2. a

3. a

4. b

5. a

Apliquemos lo aprendido 5, página 175

1. b

2. c

3. a

4. a

5. b

Apliquemos lo aprendido 6, página 178

1. a

2. c

3. b

4. b

5. b

Capítulo X

Apliquemos lo aprendido, página 184

1. c

2. d

3. c

4. b

Capítulo XI

Apliquemos lo aprendido, página 191

1. b

2. b

3. a

4. b

5. a

6. a

7. a

8. b

Bibliografía

Abusleme, C. (2025). El diablo está en los detalles: cinco nudos legales de los que depende el éxito de la nueva ley de protección de datos personales en el sector público. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 15-34). Rubicón Editores.

Arenas, M. (2021). El derecho de oposición (comentario al artículo 21 RGPD y al artículo 18 LOPDGDD), en A. Troncoso (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 1701-1723). Civitas—Thomson Reuters.

Anguita, P. (2007). *La protección de datos personales y el derecho a la vida privada: régimen jurídico, jurisprudencia y derecho comparado*. Editorial Jurídica de Chile.

Banda, A. (2000). Manejo de datos personales. Un límite al derecho a la vida privada. *Revista de Derecho (Universidad Austral de Chile), 11*(1), pp 55-70.

Cerda, A. (2003). Autodeterminación informativa y leyes sobre protección de datos. *Revista de Derecho Informático, 3*, pp. 47-75

Bozzo Hauri, S. (2020). Sobreendeudamiento, sistemas de información crediticia y la protección de los datos personales del consumidor en Chile. *Revista de Derecho (Valparaíso), 55*, pp. 99-130

Corral, H. (2001). De los derechos de las personas sobre los responsables de bancos de datos: el habeas data chileno, en J. Wahl

(ed.), *Tratamiento de datos personales y protección de la vida privada. Estudios sobre la Ley 19.628 sobre protección de datos de carácter personal* (pp. 39-57). Ediciones Universidad de los Andes.

Contreras Vásquez, P., Drago Aguirre, M. y Viollier Bonvin, P. (2025). *Compliance y protección de datos personales*, *explicación de la nueva Ley 21.719*. Ediciones Der.

De Terwangne, C. (2020). Article 5. Principles relating to processing of personal data, en Ch. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 309-320). Oxford University Press.

Donoso Abarca, L. y Reusser Monsálvez, C. (2022). *La protección de los datos personales en Chile*. Ediciones DER.

Guzmán Vega, N. y Verdugo Jaña, F. (2025*). La protección y el tratamiento de datos personales*. Editorial Hammurabi.

Lansdown, G. (2005). *The evolving capacities of the child*. UNICET Office of Research–Innocenti.

Nogueira, H. (2005). Autodeterminación informativa y habeas data en Chile e información comparativa, en J. WoIschink (ed.), *Anuario de Derecho Constitucional Latinoamericano 2005* (pp. 449-472). Konrad Adenauer—Stiftung E.V.

Maulén, C. (2025). Desafíos empresariales para negocios basados en datos. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 157-174). Rubicón Editores.

Moya, R. (2025). La autorización legal como base de licitud para el tratamiento de datos personales por parte de los órganos públicos. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 35-54). Rubicón Editores.

Pacheco, J. (2025). Datos personales sobre la salud. Marcos normativos e implicancias para la atención clínica y la toma de decisiones de salud pública. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 97-110). Rubicón Editores.

Pino Pino, F. A. (2025). *Nuevas tendencias regulatorias: tratamiento y protección de datos personales en Chile. Esquema y comentarios prospectivos*. Rubicón Editores.

Rajevic, E. (2025). Estado, datos personales y transparencia: la nueva Agencia chilena de Protección de Datos Personales. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 55-68). Rubicón Editores.

Ravetllat, I. y Pinochet, R. (2015). El interés superior del niño en el marco de la Convención Internacional sobre los Derechos del Niño y su configuración en el derecho civil chileno. *Revista Chilena de Derecho, 42*(3), pp 903-934.

Reyes, P. (2016). Regulación de la protección de datos personales en Chile a la luz de los estándares internacionales. *Revista Derecho y Tecnología, 2*, pp. 187-200

Reusser Monsálvez, C. (2021*). Derecho al olvido: la protección de datos personales como límite a las libertades informativas* (2.ª edición actualizada). Ediciones DER.

Rodríguez, J. F. (2023). *Protección de datos. Estudio conforme al Esquema de Certificación de Delegados de Protección de Datos (AEPD-DPD)*. Tirant lo Blanch.

Romeo, C. M. (2021). Datos personales (comentario al artículo 4.1 RGPD), en A. Troncoso (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 573-589). Civitas—Thomson Reuters.

Santos Morón, M. J. (2020). Tratamiento de datos, sujetos implicados, responsabilidad proactiva, en Asociación de Profesores de Derecho Civil (ed.), *Protección de datos personales* (pp. 23-77). Tirant lo Blanch.

Seaman, L. (2025). Protección de datos personales. El Estado como implementador y el Estado como obligado. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 69-80). Rubicón Editores.

Tosoni, L. y Bygrave, L. (2020). Article 4(2). Processing, en Ch. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 116-122). Oxford University Press.

Troncoso, A. (2021). Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGDD), en A. Troncoso (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 847-907). Civitas—Thomson Reuters.

Veale, M. y Edwards, L. (2018). Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. *Computer Law & Security Review, 34*(2), pp. 398-404.

Viollier, P. y Contreras, P. (2026). Derecho a una explicación en decisiones automatizadas: contrapunto entre el GDPR y la Ley 21.719. *Revista Chilena de Derecho y Ciencia Política, 17*(1), 1–27.

Zaror, D. (2025). Conceptos y obligaciones esenciales para la elaboración de un registro de actividades de tratamiento. En D. Zaror Miralles (ed.), *Expertos en acción: protegiendo datos personales bajo la nueva legislación* (pp. 111-126). Rubicón Editores.

En un mundo cada vez más digitalizado, todos compartimos información personal a diario, desde nuestras fotos en redes sociales hasta nuestras preferencias de compras online. Pero ¿sabías que tienes derechos sobre tus datos? y ¿sabías que puedes ser responsable si estás tratando datos personales de otros de manera incorrecta?

Protección de datos personales. Autonomía digital en la era de la información es una guía práctica y accesible que te ayudará a entender cómo proteger tu privacidad y tomar el control sobre tu información personal. Y si eres responsable en el tratamiento de datos, podrás conocer tus obligaciones en este ámbito.

Este libro te explica, paso a paso, los conceptos clave de la protección de datos, desde los principios fundamentales que inspiran la ley hasta los derechos que tienes como titular de datos y tus obligaciones en caso de que seas responsable en su tratamiento.

Dirigido a quienes deseen entender mejor cómo funciona la protección de sus datos personales, este libro busca empoderarte para que tomes decisiones informadas y seguras en la era digital. Con un lenguaje claro y ejemplos prácticos, *Protección de datos personales* es la herramienta que necesitas para navegar el mundo digital de forma autónoma y con confianza.

¡Tu privacidad y la de otros... están en tus manos!

DUC IN ALTUM
UA
UNIVERSIDAD AUTÓNOMA
DE CHILE