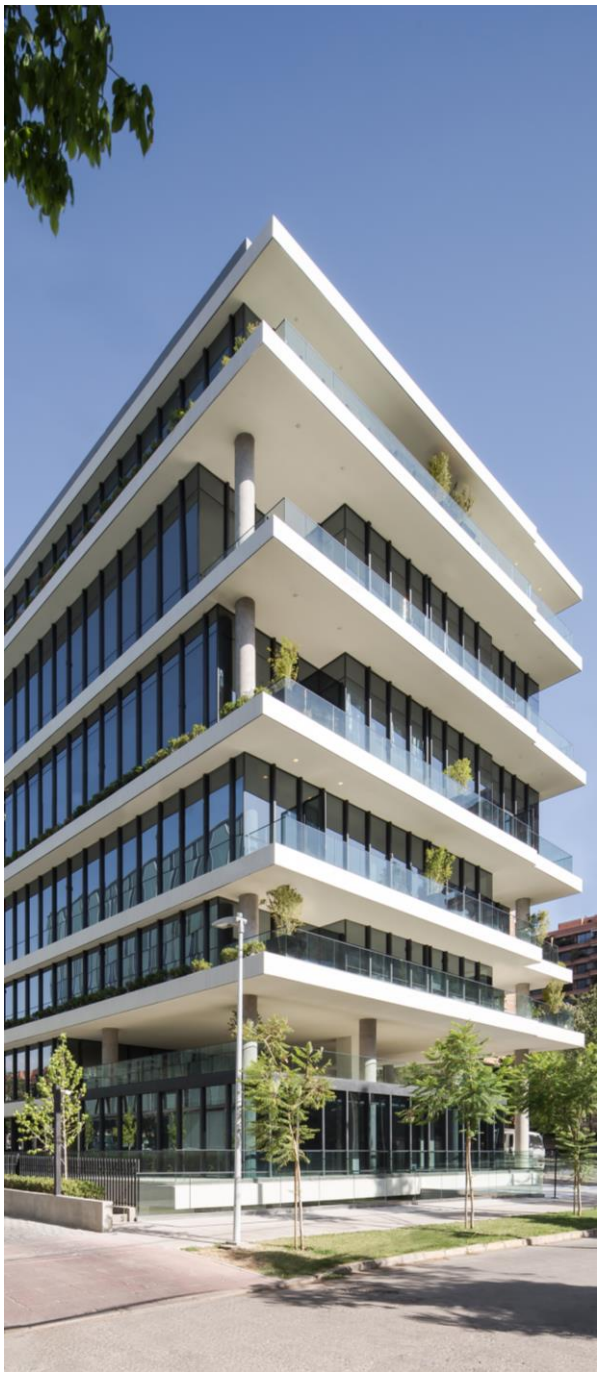
CUATRECASAS

Proyecto de Ley de Datos Personales: principales cambios y desafíos para las empresas

Chile – Legal Flash

Agosto 2024



Con fecha 26 de agosto de 2024, el Congreso Nacional aprobó el Proyecto de Ley de Datos personales (el "Proyecto"), y se encuentra pendiente de ser despachado a control preventivo de constitucionalidad ante el Tribunal Constitucional, último trámite antes de su posterior promulgación y publicación en el Diario Oficial, para convertirse en ley.

- El Proyecto modificará sustancialmente la regulación chilena vigente en materia de datos personales, actualizando y modernizando el marco normativo e institucional, adecuándolo a las recomendaciones de la OCDE y alcanzando los estándares del Reglamento General Europeo de Protección de Datos.
- El Proyecto creará la nueva Agencia de Protección de Datos Personales (la "**Agencia**"). Esta entidad tendrá varias atribuciones, entre ellas emitir normativas, supervisar su cumplimiento, sancionar infracciones, atender solicitudes y reclamos de los titulares de datos, certificar y registrar modelos de prevención y programas de cumplimiento, y gestionar el Registro Nacional de Sanciones y Cumplimiento

El Proyecto de Ley de Datos Personales introduce importantes modificaciones a la ley Nº 19.628, sobre protección de la vida privada, y con ello, significativas implicancias para el ámbito privado. Regulación que entrará en vigencia luego de **dos años de la publicación del Proyecto en el Diario Oficial**.

Con su entrada en vigencia, las empresas se verán enfrentadas a considerables desafíos, debiendo adaptarse a las exigencias que establece el Proyecto. Por lo mismo, durante este tiempo de vacancia, se espera y recomienda que el sector privado se anticipe y tome las medidas necesarias para dar cumplimiento al nuevo estándar normativo. Proponemos analizar la necesidad de ejecutar, entre otras, las siguientes:

- **Diagnosticar** la situación de la empresa en materia de datos personales, lo que conllevará recopilar y analizar la información sobre los tratamientos de datos que lleva a cabo la compañía, el tipo de datos que recoge y trata, las bases de datos que posee, las finalidades del tratamiento, los procedimientos de recolección de los datos, analizando y revisando los modelos de cláusulas utilizados, tanto respecto de trabajadores, proveedores, clientes, u otros terceros, las políticas y protocolos de privacidad y seguridad, entre otros.
- **Implementar** acciones tendientes a fomentar dentro de la empresa una cultura y conciencia en torno a la protección de los datos personales.
- **Implementar** un registro de actividades de tratamiento.
- **Adaptar** las políticas de privacidad a los contenidos mínimos en materia de información.
- **Implementar** sistemas y procedimientos para dar respuesta y garantizar que los titulares puedan ejercer sus derechos de acceso, rectificación, supresión, bloqueo, oposición y portabilidad.
- **Implementar** medidas organizativas y técnicas que permitan cumplir con los estándares de la protección desde el diseño y por defecto.
- **Implementar** medidas organizativas y técnicas de seguridad apropiadas al tratamiento realizado y a la realidad de la compañía.
- **Adaptar** las prácticas de transferencia internacional de datos a los nuevos requerimientos del Proyecto.
- **Efectuar** las evaluaciones de impacto de privacidad, cuando la actividad de tratamiento, de forma previa, lo amerite.

- **Adaptar** la documentación contractual suscrita con terceros que accedan a datos personales, ya sea como encargados o responsables.
- **Adoptar** políticas internas y mecanismos de reportes hacia autoridades.
- **Adoptar** un modelo de prevención de infracciones consistente en un programa de cumplimiento o designar a un delegado de protección de datos personales.

Lo anterior, no obsta a la necesidad de implementar otras medidas, mecanismos o políticas internas, o ajustar las ya tomadas, para efectos de dar cumplimiento al Reglamento que debe dictarse en virtud del Proyecto y a las interpretaciones de la normativa e instrucciones y normas generales y obligatorias que la Agencia pudiera dictar, en el ejercicio de su competencia.

Antes de señalar las principales modificaciones introducidas por el Proyecto, es importante considerar las siguientes definiciones establecidas en el mismo:

- **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.
- **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 de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.

I. Definición del ámbito de aplicación territorial de la normativa

El Proyecto precisa y define que la normativa se aplicará no solo a aquél responsable o mandatario establecido o constituido en Chile, sino que establece, de forma inequívoca una aplicación **extraterritorial** de la Ley sobre Protección de Datos Personales cuando, por ejemplo, **(i)** el mandatario no se encuentre en Chile pero realice operaciones de tratamiento de datos a nombre de un responsable establecido o constituido en Chile, o **(ii)** cuando el responsable o mandatario no

se encuentren establecidos en Chile, pero sus operaciones de tratamiento de datos personales estén destinadas a ofrecer bienes o servicios a personas que se encuentren en Chile o a monitorear el comportamiento de titulares que se encuentran en el territorio nacional.

En el caso de responsables personas jurídicas no constituidas en Chile, éste deberá señalar por escrito, ante la Agencia, un correo electrónico u otro medio de comunicación equivalente de una persona natural o jurídica capaz de actuar en su nombre, para los efectos de que **(i)** el titular pueda ejercer sus derechos y comunicarse con el responsable, y **(ii)** se le practiquen válidamente las comunicaciones y notificaciones administrativas que disponga la ley.

II. Incorporación de principios

El Proyecto innova e incluye los siguientes principios por los cuales se debe regir el tratamiento de los datos personales (los "**Principios**"):

- **Principios de licitud y lealtad:** el responsable deberá ser siempre capaz de acreditar la licitud del tratamiento que realiza.
- **Principio de finalidad:** los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. No se podrán tratar los datos con fines distintos a los informados al momento de la recolección, salvo concurra alguna de las excepciones establecidas en la normativa.
- **Principio de proporcionalidad:** el tratamiento debe limitarse estrictamente a aquello que resulte necesario, adecuado y pertinente en relación con los fines del tratamiento. Los datos pueden ser conservados sólo por el período 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 normativa).
- **Principio de calidad:** los datos personales deben ser exactos, completos, actuales y pertinentes.
- **Principio de responsabilidad:** quienes realicen tratamiento de datos personales serán legalmente responsables del cumplimiento de los Principios y de las obligaciones y deberes de conformidad a la normativa.
- **Principio de seguridad:** el responsable debe garantizar estándares adecuados de seguridad, protegiendo los datos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción.
- **Principio de transparencia e información:** el responsable debe entregar al titular de los datos toda la información que sea necesaria para el ejercicio de sus derechos, incluyendo

las políticas y las prácticas sobre el tratamiento de los datos personales, las que deberán encontrarse permanentemente accesibles y a disposición de cualquier interesado.

- **Principio de confidencialidad:** el responsable de datos personales y quienes tengan acceso a los datos deberán guardar secreto acerca de los mismos.

III. Reforzamiento de los derechos de los titulares e incorporación del derecho a la portabilidad

El Proyecto establece que todo titular de datos personales tendrá los derechos personales, intransferibles e irrenunciables, que se señalan a continuación. Los mismos, no podrán ser limitados por ningún acto o convención y deberán ser solicitados ante el responsable del tratamiento.

En virtud de la nueva normativa, será una obligación del responsable, implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil, eficaz y sencilla. Recibida la solicitud, el responsable deberá acusar recibo de ella y pronunciarse a más tardar dentro de los 30 días corridos siguientes a la fecha de ingreso de la solicitud. Este plazo podrá ser prorrogado, por una sola vez, hasta por 30 días adicionales.

- **Derecho de Acceso:** obtener confirmación acerca de si los datos del titular están siendo tratados por el responsable y, en tal caso, acceder a dichos datos y a cierta información, entre la que se encuentra: **a)** Los datos tratados y su origen; **b)** Las finalidades del tratamiento; **c)** Las categorías, clases o tipos de destinatarios; y **d)** El período de tiempo durante el cual los datos serán tratados.
- **Derecho de Rectificación:** obtener la rectificación de los datos personales cuando sean inexactos, desactualizados o incompletos.
- **Derecho de Supresión:** obtener del responsable, la eliminación de sus datos personales, entre otros, en los siguientes casos: **a)** Cuando los datos no resulten necesarios en relación con los fines del tratamiento; **b)** Cuando el titular haya revocado su consentimiento para el tratamiento y éste no tenga otro fundamento legal**; c)** Cuando los datos hayan sido obtenidos o tratados ilícitamente; y **d)** Cuando los datos deban suprimirse para el cumplimiento de una sentencia judicial, de una resolución de la autoridad de protección de datos o de una obligación legal.

  Sin perjuicio de lo anterior, el Proyecto establece ciertas causales en virtud de las cuales el responsable podrá denegar el ejercicio de este derecho. Entre éstas, cuando el tratamiento sea necesario: **(i)** para el cumplimiento de una obligación legal o la ejecución

de un contrato suscrito entre el titular y el responsable; **y (ii)** para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.

- **Derecho de Oposición:** oponerse a que se realice un tratamiento específico o determinado de los datos personales, en los siguientes casos: **a)** Cuando la base de licitud del tratamiento sea la satisfacción de intereses legítimos del responsable. El responsable deberá dejar de tratar los datos personales, **salvo** que **(i)** acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o **(ii)** para la formulación, el ejercicio o la defensa de reclamaciones; **b)** Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, incluida la elaboración de perfiles; y **c)** Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no existe otro fundamento legal para su tratamiento.

  Asimismo, el titular de datos tiene derecho oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente. Lo anterior, no se aplicará en los siguientes casos: **(i)** cuando la decisión sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable; **(ii)** cuando exista consentimiento previo y expreso del titular; y **(iii)** cuando lo permita la ley.

- **Derecho de Portabilidad:** recibir una copia de los datos personales que el titular haya facilitado al responsable, en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias: **a)** El tratamiento se realice en forma automatizada, y **b)** el tratamiento esté basado en el consentimiento del titular.

- **Derecho de Bloqueo:** solicitar la suspensión temporal de cualquier operación de tratamiento cuando formule una solicitud de rectificación, supresión u oposición, mientras dicha solicitud no se resuelva.

IV. Se incorporan nuevas fuentes de licitud para el tratamiento de datos personales

Como regla general para el tratamiento de los datos, el consentimiento seguirá teniendo un papel fundamental en cuanto base de licitud. En virtud del Proyecto, se establece que este consentimiento debe ser libre, informado y específico en cuanto a su finalidad o finalidades. Asimismo, el consentimiento debe manifestarse en forma previa y de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico o equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular. Lo anterior, presentará un gran desafío

para las empresas, a efectos de analizar la forma en que están recogiendo el consentimiento de los titulares. En especial, será interesante ver cómo la Agencia dota de contenido el concepto de "consentimiento libre".

El consentimiento es revocable por el titular, sin efectos retroactivos.

La carga de prueba para acreditar que se cuenta con el consentimiento corresponde al responsable. Lo mismo ocurre respecto a que el tratamiento de datos ha sido realizado en forma lícita, leal y transparente.

De forma adicional al consentimiento, el Proyecto incorpora **nuevas fuentes de licitud** en virtud de las cuales no se requerirá el consentimiento del titular para tratar los datos. Estas son las siguientes:

- Cuando el tratamiento sea **necesario para la ejecución o el cumplimiento de una obligación legal** o lo disponga la ley.
- Cuando el tratamiento de datos sea **necesario para la celebración o ejecución de un contrato** entre el titular y el responsable, **o para la ejecución de medidas precontractuales** adoptadas a solicitud del titular.
- Cuando el tratamiento sea necesario para la **satisfacción de intereses legítimos del responsable o de un tercero**, siempre que con ello no se afecten los derechos y libertades del titular.
- Cuando el tratamiento de datos sea **necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia u órganos públicos**.

V. Se refuerzan, aumentan y dotan de contenido las obligaciones y deberes del responsable del tratamiento de los datos

Dentro de las obligaciones y deberes más destacados que se establecen como de carga del responsable, podemos mencionar que se han incluido las siguientes en virtud del Proyecto:

- Facilitar y **mantener permanentemente a disposición del público**, en su sitio web o en cualquier otro medio de información equivalente, cierta información relacionada con:
  a) La política de tratamiento de datos personales adoptada.
  b) La individualización del responsable de datos.
  c) Las categorías, clases o tipos de datos que trata el responsable y las bases de legitimidad del tratamiento de los datos.
  d) Los destinatarios a los que se prevé comunicar o ceder los datos.
  e) las finalidades de los tratamientos que realiza.
  f) La política y las medidas de seguridad adoptadas.

g) Los derechos de los titulares, ya sea ante el responsable como ante la Agencia.
h) La transferencia de datos personales a un tercer país u organización internacional.
i) El periodo durante el que se conservarán los datos personales.
j) La existencia de decisiones automatizadas, incluida la elaboración de perfiles. En tales casos, se debe incluir información significativa sobre la lógica aplicada, así como las consecuencias previstas de dicho tratamiento para el titular.

- Aplicar **medidas técnicas y organizativas adecuadas desde el diseño con anterioridad y durante** el tratamiento de los datos personales. Asimismo, el responsable de datos deberá aplicar medidas técnicas y organizativas para garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales específicos y estrictamente necesarios para dicha actividad.
- Adoptar las **medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo**.
- **Reportar a la Agencia por los medios más expeditos posibles y sin dilaciones indebidas**, las **vulneraciones a las medidas de seguridad** que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares. Cuando las vulneraciones se refieran a datos personales sensibles, datos relativos a niños menores de 14 años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos.
- Realizar una **evaluación de impacto en protección de datos personales** o DPIA, por sus siglas en inglés, cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, previo al inicio de las operaciones del tratamiento. El Proyecto establece algunas causales en virtud de las cuales siempre se requerirá el DPIA, e.g., cuando se realice un tratamiento masivo de datos, o cuando se realice una evaluación sistemática y exhaustiva de aspectos personales de los titulares, basadas en tratamiento o decisiones automatizadas que produzcan en efectos jurídicos significativos en los titulares. Esto no obsta, a la facultad de la Agencia de poder determinar casos adicionales en que será necesario realizar un DPIA.

VI. Se incluye regulación particular en materia de tratamiento de datos a través de un tercero mandatario o encargado

Actualmente, la regulación en materia de tratamiento de datos a través de un mandatario es bastante escueta, remitiéndose a las normas del mandato del Código Civil. En virtud del Proyecto, será

importante para las empresas considerar en sus contratos con proveedores y terceros mandatarios para el tratamiento de datos, entre otros, lo siguiente:

- Si el tercero mandatario o encargado **trata los datos con un objeto distinto del encargo convenido o los cede o entrega sin haber sido autorizado**, se le considerará como responsable de datos para todos los efectos legales, debiendo responder personalmente por las infracciones en que incurra y solidariamente con el responsable de datos por los daños ocasionados, sin perjuicio de las responsabilidades contractuales acordadas entre las partes.
- El tratamiento de datos a través de un tercero mandatario o encargado se regirá por el contrato celebrado entre el responsable y el encargado, con arreglo a la legislación vigente. En el contrato se deberá establecer el objeto del encargo, la duración del mismo, la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de titulares a quienes conciernen los datos, y los derechos y obligaciones de las partes.
- El encargado **no podrá delegar parte o la totalidad del encargo**, salvo que conste una autorización específica y por escrito del responsable.
- El tercero mandatario o encargado deberá cumplir con el **deber de confidencialidad** y con el deber de adoptar medidas de seguridad establecidos en virtud de la normativa. Tratándose de una vulneración a las medidas de seguridad, el tercero o mandatario deberá reportar este hecho al responsable.
- Cumplida la prestación del servicio de tratamiento por parte del tercero mandatario o encargado, los datos que obran en su poder deben ser **suprimidos o devueltos** al responsable de datos, según corresponda.

VII. Incorporación de regulación particular al tratamiento de datos personales sensibles y a otras categorías especiales de datos personales

El tratamiento de los datos personales sensibles sólo puede realizarse cuando el titular a quien conciernen estos datos manifiesta su consentimiento. Sin perjuicio de lo anterior, el Proyecto prevé ciertas causales específicas en virtud de las cuales se considerará lícito el tratamiento de datos personales sensibles, sin el consentimiento del titular. Entre éstas, podemos destacar:

- Cuando el tratamiento de los datos sea **necesario para la formulación, ejercicio o defensa de un derecho** ante los tribunales de justicia o un órgano administrativo.

- Cuando el tratamiento de datos sea **necesario para el ejercicio de derechos y el cumplimiento de obligaciones del responsable o del titular de datos, en el ámbito laboral o de seguridad social**, y se realice dentro del marco de la normativa.
- Cuando el tratamiento de datos personales sensibles lo autorice o mandate expresamente la ley.

El Proyecto también incluye regulación específica relativa a las siguientes categorías de datos personales: **(i)** datos sensibles relativos a la **salud y perfil biológico** humano, **(ii)** datos **biométricos**, **(iii)** datos relativos a los **niños y adolescentes**, **(iv)** datos con **fines históricos, estadísticos, científicos y de estudios o investigaciones**, y **(v)** datos de **geolocalización**.

VIII. Regulación de la transferencia internacional de datos personales

El Proyecto regula por primera vez en nuestro país la transferencia internacional de datos personales. Las empresas deberán revisar sus contratos y políticas de transferencia internacional de datos ya sea con proveedores, asesores, clientes, autoridades o empresas de su mismo grupo, en consideración a los requerimientos establecidos en la normativa y a los criterios que dictará la Agencia en la materia relacionados con los niveles de protección en materia de datos personales de los países receptores y las garantías que se pudieran establecer contractualmente.

Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, las transferencias podrán quedar amparadas en normas corporativas vinculantes previamente aprobadas por la Agencia.

IX. Creación de la Agencia de Protección de Datos Personales}

Esta nueva entidad tendrá entre otras, las siguientes atribuciones:

- **Dictar instrucciones y normas generales** y obligatorias.
- **Aplicar e interpretar** administrativamente las disposiciones legales, reglamentarias y administrativas.
- **Fiscalizar** el cumplimiento de la normativa.
- **Determinar las infracciones e incumplimientos** en que incurran los responsables.

- Ejercer la **potestad sancionadora** sobre las personas naturales o jurídicas que traten datos personales con infracción a la normativa.
- Resolver **las solicitudes y reclamos** que formulen los titulares de datos en contra de los responsables.
- **Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento** y administrar el Registro Nacional de Sanciones y Cumplimiento.

X. Incremento de infracciones y sanciones. Establecimiento de un catálogo de infracciones

El Proyecto establece un régimen general de responsabilidad para los responsables de datos, estableciendo sanciones leves, graves y gravísimas, atendida su gravedad, para quienes infrinjan los Principios y las demás obligaciones y deberes que la normativa les impone.

La acción de la Agencia para perseguir la responsabilidad por las infracciones **prescribe en el plazo de cuatro años desde la ocurrencia del hecho que originó la infracción o desde el día en que la infracción haya cesado**. Estas sanciones se entenderán sin perjuicio de las demás responsabilidades legales, civiles o penales, que pudieran corresponder.

El Proyecto establece que, cuando por unos mismos hechos y fundamentos jurídicos, el infractor pudiese ser sancionado con arreglo a la Ley sobre Protección de Datos Personales y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.

En materia de sanciones y/o fiscalización, será importante ir observando el grado de coordinación que debiera existir entre autoridades como la Comisión para el Mercado Financiero, la Agencia Nacional de Ciberseguridad y, eventualmente, las actuaciones del Servicio Nacional del Consumidor en materia de consumo, aun cuando en virtud del Proyecto se ha eliminado el artículo 15 bis de la Ley No. 19.496 sobre Protección de los Derechos del Consumidor, que otorgaba facultades de fiscalización al SERNAC respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo.

A continuación, incluimos un par de ejemplos sobre las conductas que el Proyecto considerará como sancionables:

- **Infracciones Leves: amonestación escrita o multa de hasta 5.000 UTM.**
  a) Incumplimiento de los deberes y obligaciones de información y transparencia.

b) Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por el titular de datos.
c) Incumplimiento de las instrucciones generales impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima.
d) Cometer cualquier otra infracción a los derechos y obligaciones establecidas en la Ley sobre Protección de Datos Personales, que no sea calificada como una infracción grave o gravísima.

- **Infracciones Graves: multa de hasta 10.000 UTM.**

  a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin un antecedente o fundamento legal que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados.
  b) Comunicar o ceder datos personales, sin el consentimiento del titular, en los casos en que dicho consentimiento sea necesario, o comunicar o ceder los datos para un fin distinto del autorizado.
  c) Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento.
  d) Vulnerar o infringir las obligaciones de seguridad en el tratamiento de los datos personales.

- **Infracciones Gravísimas: multa de hasta 20.000 UTM.**

  a) Efectuar tratamiento de datos personales en forma fraudulenta.
  b) Efectuar tratamiento masivo de datos personales contenidos en registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias, que llevan los organismos públicos, sin contar con autorización legal para ello.
  c) Entregar a sabiendas información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.
  d) Incumplir la obligación de realizar una evaluación de impacto en protección de datos personales.

El Proyecto también regula los criterios que deberá considerar la Agencia **prudencialmente,** al momento de determinar el monto de las multas. Entre éstos se encuentra: **(i)** la **gravedad** de la conducta; **(ii)** la **falta de diligencia** o cuidado; **(iii)** el **perjuicio** producido; **(iv)** el **beneficio** económico obtenido; **(v)** si incluye datos personales **sensibles** o datos personales de **niños y adolescentes**; **(vi)** la **capacidad económica** del infractor; **(vii)** las **sanciones aplicadas con anterioridad** por la Agencia en las mismas circunstancias; y **(viii)** las circunstancias **atenuantes y agravantes** que concurran.

Con respecto a aquellas circunstancias e hipótesis que podrán ser consideradas por la Agencia para agravar o atenuar la pena impuesta, algunos de los ejemplos establecidos, son los siguientes:

- **Atenuantes:**
  - **a)** Las acciones unilaterales de **reparación** y los acuerdos reparatorios convenidos con los titulares afectados.
  - **b)** La **colaboración** que el infractor preste en la investigación.
  - **c)** La **ausencia de sanciones** previas.
  - **d)** La **autodenuncia** ante la Agencia.
  - **e)** Contar con la **certificación** de la Agencia al modelo de prevención de infracciones.

- **Agravantes:**
  a) La **reincidencia.** i.e., haber sido sancionado en dos o más ocasiones en los últimos 30 meses. En caso de la ocurrencia de esta agravante, la Agencia podrá aplicar una **multa de hasta tres veces el monto asignado a la infracción** cometida. Asimismo, en caso de que el infractor corresponda a una empresa que no califique como empresa de menor tamaño, si reincide en una infracción de carácter grave o gravísima, la multa podrá alcanzar a la más gravosa entre la recién señalada (tres veces el monto asignado) o hasta el monto correspondiente al **2% o 4% de los ingresos anuales** por ventas y servicios y otras actividades del giro en el último año calendario, según se trate de infracciones graves o gravísimas, respectivamente.
  b) El carácter **continuado** de la infracción.

Ya sean, infracciones leves, graves o gravísimas, la Agencia instruirá las medidas tendientes a subsanar las causales que dieron motivo a la sanción, las que deberán ser adoptadas en un plazo no mayor a 60 días. Si no se cumplieren, la Agencia podrá imponer un **recargo de 50%** a la multa cursada.

Durante los primeros 12 meses luego de la entrada en vigencia de la nueva normativa, en los casos en que proceda alguna sanción para empresas calificadas como de **menor tamaño** la Agencia podrá aplicar como sanción una **amonestación por escrito**.

XI. Responsabilidad del responsable del tratamiento de los datos y establecimiento de la posibilidad de implementar un modelo de prevención de infracciones

El responsable de datos deberá **indemnizar el daño patrimonial y extrapatrimonial que cause a los titulares**, cuando en sus operaciones de tratamiento de datos infrinja los Principios y los derechos y obligaciones establecidos en la Ley sobre Protección de Datos Personales y les cause perjuicio. Las acciones civiles que deriven de una infracción de dicha ley **prescribirán en el plazo**

de cinco años, contados desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva.

Los responsables de datos deberán adoptar acciones destinadas a prevenir la comisión de las infracciones. De igual forma, **los responsables podrán voluntariamente adoptar un modelo de prevención de infracciones** consistente en un programa de cumplimiento.

El programa de cumplimiento deberá contener, entre otros, los siguientes elementos:

- **Designación** de un delegado de protección de datos personales
- La **identificación** del tipo de información que la entidad trata.
- La **identificación** de las actividades o procesos de la entidad en cuyo contexto se genere o incremente el riesgo de comisión de infracciones.
- El **establecimiento** de protocolos, reglas y procedimientos específicos que permitan a las personas dentro de la entidad programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las infracciones.
- **Mecanismos** de reporte interno sobre el cumplimiento de la normativa y mecanismos de reporte a la Agencia para el caso de vulneraciones a las medidas de seguridad.
- **Implementar** sanciones administrativas internas, así como de procedimientos de denuncia o castigo de responsabilidades.

La regulación interna a que dé lugar la implementación del programa, en su caso, deberá ser **incorporada expresamente como una obligación en los contratos de trabajo o de prestación de servicios** de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de ellas, o bien, como una obligación del reglamento interno de orden, higiene y seguridad que regula el Código del Trabajo.

La Agencia será la entidad encargada de certificar que el modelo de prevención de infracciones reúna los requisitos y elementos establecidos en la Ley sobre Protección de Datos Personales y su reglamento (a dictarse) y supervisarlos. Los certificados expedidos por la Agencia tendrán una vigencia de tres años.

Las empresas que no se certifiquen, igualmente podrán designar un delegado de protección de datos.

Las sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, **podrán designar un único delegado de protección de datos, siempre que (i)** todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, y **(ii)** el delegado sea accesible para todas las entidades y establecimientos.

Dentro de las funciones establecidas por la normativa al delegado, se encuentras las siguientes:

- **Informar y asesorar** al responsable de datos.
- **Supervisar** el cumplimiento de la normativa y políticas internas.
- **Preocuparse de la formación** de las personas que participan en las operaciones de tratamiento de datos.
- **Desarrollar** un plan anual de trabajo y rendir cuenta de sus resultados.
- **Resolver** las consultas y solicitudes de los titulares de datos.
- **Cooperar y actuar** como punto de contacto de la Agencia.

Para obtener información adicional sobre el contenido de este documento puede enviar un mensaje a nuestro equipo del *Área de Conocimiento e Innovación* o dirigirse a *aci.informacionjuridica@cuatrecasas.com*.

Contactos:

Josefina Yávar
+5622 889 9900
josefina.yavar@cuatrecasas.com

Isidora Opazo
+5622 889 9900
isidora.opazo@cuatrecasas.com