TEXTO CONSOLIDADO

Artículo 1º.-

La presente ley tiene por objeto regular el tratamiento legítimo, controlado e informado de los datos personales que realicen las personas naturales o jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los derechos y libertades de las personas, en particular, el derecho a la privacidad en relación con el tratamiento de sus datos.

DEFINICIONES

Artículo 2º.-

Para los efectos de esta ley se entenderá por:

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos personales: dar a conocer, de cualquier forma, datos personales a personas distintas del titular de datos, sean identificadas o identificables, sin llegar a cederlos. Las comunicaciones que realice el responsable de datos deberán contener información exacta, completa, actualizada y veraz del titular.

d) Dato caduco, el 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.

e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

“f) Dato personal: cualquier información vinculada a una persona natural identificada o identificable a través de medios que puedan ser razonablemente utilizados.

“g) Datos personales sensibles: aquellos datos que se refieren a las características físicas o morales de las personas, tales como origen racial, ideologías, afiliaciones políticas, creencias o convicciones religiosas o filosóficas, estados de salud físicos o psíquicos, orientación sexual, identidad de género, identidad genética y biomédica.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

“i) Fuentes de acceso público: Todos aquellos registros o bases de datos personales, computacionales o manuales, públicos o privados, cuyo acceso o consulta pueda ser efectuada por cualquier persona sin existir restricciones legales para su acceso o utilización. No se consideran fuentes de acceso público aquellos registros o bases de datos que contengan información obtenida en forma ilegítima o en contravención a esta ley.

j) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

k) Proceso de disociación o anonimización: procedimiento en virtud del cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Se entenderá que un dato es anonimizado o irreversiblemente disociado cuando se trata de un dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gasto y trabajo desproporcionados.

“l) Registro o base de datos personales: conjunto organizado de datos personales, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar el tratamiento de ellos.

“m) Responsable de datos: persona natural o jurídica, pública o privada, a quien compete decidir acerca del tratamiento de datos personales, con independencia de si estos son tratados directa o indirectamente por él y de su localización.

n) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

“ñ) 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 en cualquier forma datos de carácter personal.

o) Consentimiento: toda manifestación de voluntad libre, inequívoca e informada, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de sus datos personales.

p) Derecho de acceso: derecho del titular de datos para solicitar y obtener directamente del responsable de datos toda la información que tiene respecto de su persona.

q) Derecho de rectificación: derecho del titular de datos para solicitar y obtener del responsable de datos que modifique, complete o actualice los datos incorporados en su base de datos que sean erróneos, inexactos, equívocos o incompletos.

r) Derecho de cancelación: derecho del titular de datos que se ejerce en contra del responsable de datos para que éste suprima o elimine sus datos personales de conformidad a lo señalado en esta ley.

s) Derecho de oposición: derecho del titular de datos que se ejerce en contra del responsable de datos que tiene por objeto impedir que se lleve a cabo la recolección o el tratamiento de sus datos personales de acuerdo a las causales que se establecen en la presente ley.

t) Registro Nacional de Responsables de Datos: registro nacional de carácter público, administrado por la Dirección Nacional de Protección de Datos, en el que deberán inscribirse las personas naturales o jurídicas, que posean bases de datos personales o realicen tratamiento de datos personales de acuerdo a la presente ley.

Artículo 3°.-

Principios. El tratamiento de los datos personales se regirá por los siguientes principios:

a) Principio de legitimidad. El tratamiento de datos personales sólo puede realizarse cuando el titular otorgue su consentimiento o lo autorice la ley.

b) Principio de finalidad. El tratamiento de datos personales debe limitarse al cumplimiento de finalidades legítimas, determinadas e informadas al titular al momento de la recolección.

En aplicación de este principio, no se pueden recolectar o tratar datos personales con una finalidad distinta de la informada, salvo que el titular otorgue nuevamente su consentimiento, los datos provengan de fuentes de acceso público, así lo disponga la ley o se traten exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones.

c) Principio de proporcionalidad. El tratamiento de datos personales debe limitarse a aquellos que resulten necesarios, pertinentes y no excesivos en relación con las finalidades para las cuales hayan sido obtenidos.

Los datos deben ser conservados y almacenados el tiempo necesario para el cumplimiento de las finalidades que habilitaron su recolección o tratamiento, luego de lo cual deberán ser cancelados o anonimizados.

d) Principio de calidad. Los datos personales que sean objeto de tratamiento deberán ser precisos, actualizados y completos en relación con las finalidades informadas al momento de su recolección, debiendo el responsable de datos adoptar las medidas necesarias con este objeto.

e) Principio de responsabilidad. El Responsable de datos deberá adoptar las medidas necesarias para cumplir con los principios, requisitos y obligaciones que impone esta ley para el tratamiento de datos personales, debiendo mantener el resguardo e integridad de los datos o registros, independientemente de su localización o de si estos son tratados directamente por él o a través de un tercero. El responsable de datos será civilmente responsable de los daños que cause debido al incumplimiento de este principio.

f) Principio de seguridad. Los datos personales deberán ser tratados por el responsable garantizando niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado y contra su pérdida, filtración, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas que persigan la confidencialidad, integridad, disponibilidad y resiliencia de los datos, acorde al estado de la técnica y el costo de implementación de estas medidas, en relación con los riesgos y la naturaleza de los datos que serán objeto del tratamiento. En las medidas que adopte el responsable deberá considerar análisis de riesgos, evaluar fórmulas de mitigación y adoptar estándares de seguridad iguales o superiores a los que mantenga para el manejo de su propia información.

g) Principio de información. El responsable de datos deberá mantener sus políticas sobre recolección y tratamiento de datos personales permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.”.

**TÍTULO I: DE LOS DERECHOS DEL TITULAR DE DATOS PERSONALES**

**Artículo 4.- Derechos del titular de datos**

Toda persona, actuando por sí o a través de su representante legal o mandatario, según corresponda, tiene derecho a acceder, rectificar, cancelar y oponerse a la recolección o al tratamiento de sus datos personales, de conformidad a la presente ley.

Los derechos de acceso, rectificación, cancelación y oposición son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención. El ejercicio de estos derechos será siempre gratuito.

En caso de fallecimiento del titular de datos, el ejercicio de sus derechos y acciones se transmiten a sus herederos.

**Artículo 5.- Derecho de acceso.**

El titular de datos tiene derecho a solicitar y obtener del responsable de datos información completa, actualizada y fidedigna respecto a si sus datos personales son o no objeto de tratamiento, y en caso de serlos tiene derecho a ser informado sobre:

a) Los datos personales que son o serán objeto de tratamiento, y su origen.

b) La finalidad o finalidades específicas para las cuales los datos serán tratados.

c) Las personas o categorías de personas u organismos a quienes potencialmente se les podría comunicar y/o ceder los datos personales.

d) El período de tiempo durante el cual los datos personales serán almacenados.

**Artículo 6.- Derecho de rectificación y cancelación**

El titular de datos tiene derecho a solicitar y obtener del responsable de datos la rectificación y/o la cancelación de sus datos personales. La rectificación procederá cuando los datos del titular sean inexactos, erróneos, incompletos o equívocos. La cancelación o eliminación se realizará cuando los datos personales del titular resulten innecesarios o excesivos en relación a la finalidad para la cual serán tratados.

La rectificación y/o la cancelación deberán realizarse por el responsable en el más breve plazo. Serán públicas o deberán difundirse, cuando lo requiera el titular. La rectificación y/o cancelación de datos podrán ser totales o parciales, según corresponda.

El titular tiene derecho a solicitar y obtener del responsable el bloqueo de los datos, en tanto se efectúa la rectificación o cancelación de los mismos.

Las solicitudes de rectificación y/o cancelación se sujetarán al procedimiento establecido en el artículo 10.

Con todo, la cancelación no procederá cuando los datos personales deban ser conservados durante el período de tiempo que determine la ley o cuando afecten la ejecución o cumplimiento de un contrato en que sea parte el titular.

Los datos cancelados no podrán ser objeto de ningún tipo de tratamiento.

**Artículo 7.- Derecho de Oposición**

El titular de datos tiene derecho a oponerse ante el responsable al tratamiento de sus datos personales, en los siguientes casos:

a) Cuando el tratamiento carece de legitimidad.

b) Cuando se trate de un dato caduco.

c) Cuando el titular de datos hubiere fallecido, salvo las excepciones dispuestas en la ley.

d) Cuando el tratamiento de datos sea utilizado con fines de publicidad o marketing.

e) Cuando se realice tratamiento automatizado de sus datos personales y se adopten decisiones que impliquen una valoración, evaluación o predicción de su comportamiento realizada únicamente en base a este tipo de tratamiento.

f) Cuando el tratamiento de los datos cause un perjuicio arbitrario o ilícito al titular.

Acogida la solicitud de oposición, el responsable de datos deberá cesar en las operaciones de tratamiento y procederá a la cancelación de los datos.

En los casos que no se requiera el consentimiento del titular de datos conforme al artículo 12, éste no podrá oponerse a su tratamiento.

**Artículo 8°.- Derecho de portabilidad**

El titular de datos tiene derecho a recuperar sus datos personales de manera estructurada y en un formato legible, cuando concurran las siguientes circunstancias:

a) Haber entregado sus datos personales directamente al responsable de datos.

b) Sus datos han sido procesados de manera automatizada.

c) Sus datos han sido tratados con su consentimiento previo o en relación a un contrato en el que son parte el titular y el responsable de datos.

Este derecho se ejercerá por el titular ante el responsable de datos, quien deberá utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para su ejercicio.

El responsable deberá comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos y especificar las características técnicas para llevar a cabo esta operación y la naturaleza interoperable entre los sistemas.

La Dirección Nacional de Protección de Datos establecerá los medios, requisitos y procedimientos necesarios para el ejercicio de este derecho por parte del titular.

**Artículo 9.- Forma y medios de ejercer los derechos del titular de datos**

El responsable de datos deberá implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza los derechos previstos en esta ley en forma expedita, ágil y eficaz.

Los medios dispuestos por el responsable de datos deberán ser sencillos en su operación.

Los derechos reconocidos en esta ley serán ejercidos por el titular de datos, en forma personal o debidamente representado, ante el responsable de datos. Si los datos se encuentran en un registro o base de datos que es administrada o tratada por diversos responsables, el titular podrá ejercer sus derechos ante cualquiera de ellos.

**Artículo 10°.- Procedimiento ante el responsable de datos.**

Con el objeto de ejercer sus derechos de acceso, rectificación, cancelación y oposición, el titular de datos deberá presentar una solicitud ante el responsable en forma escrita o a través de un medio electrónico dispuesto para tal efecto. La solicitud o el medio electrónico deberán contener, a lo menos, las siguientes menciones o aplicaciones:

a) Identificación del titular y de su domicilio o medio electrónico apto para comunicar la respuesta a la solicitud.

b) Autenticación de la identidad del titular o de su representante legal o mandatario.

c) Identificación de los datos personales respecto de los cuales se ejerce alguno de los derechos señalados. Cuando se trate de solicitudes de rectificación, el titular de datos deberá indicar las modificaciones precisas que se deben realizar y acompañar, en su caso, la documentación o antecedentes que las sustente. En el caso del derecho de acceso, bastará una descripción general de los datos.

d) Cualquier otro elemento o documento que facilite la localización de los datos personales.

Recibida la solicitud, el responsable de datos deberá pronunciarse sobre el requerimiento y proceder a dar acceso, rectificar, cancelar, bloquear o cesar en el tratamiento de los datos requeridos por el titular, dentro del plazo de 10 días hábiles contado desde la fecha de ingreso del requerimiento.

El responsable de datos deberá responder por escrito al titular al domicilio o al medio electrónico fijado por éste. Cuando la respuesta se entregue por medios electrónicos, el responsable deberá almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y contenido íntegro, la identidad del remitente y el destinatario de la misma.

En caso de denegación total o parcial de la solicitud, el responsable de datos deberá fundamentar su decisión, indicando la causa invocada y los antecedentes que la justifican. En la misma oportunidad, el responsable deberá señalar al titular que dispone de un plazo de 10 días hábiles para formular una reclamación ante la Dirección Nacional de Protección de Datos, de acuerdo al procedimiento establecido en el artículo 48 de esta ley.

Transcurrido el plazo de 10 días hábiles al que hace referencia el inciso segundo sin que haya respuesta por parte del responsable de datos, el titular podrá formular una reclamación ante la Dirección Nacional de Protección de Datos en los mismos términos del inciso anterior.”.

**TÍTULO II: De la utilización y tratamiento de los datos personales y de categorías especiales de datos**

**Párrafo Primero**

**Del consentimiento del titular, de las obligaciones del responsable y del tratamiento de datos personales**

**Artículo 11.- Regla general.**

El tratamiento de datos personales sólo podrá efectuarse cuando el titular de los mismos exprese su consentimiento en forma previa, inequívoca, libre e informada. También se podrán tratar datos personales cuando la ley expresamente lo autorice, sin el consentimiento de su titular.

El consentimiento del titular podrá ser expreso o tácito. Será expreso, cuando la voluntad se manifieste en forma verbal, escrita o por cualquier medio electrónico idóneo que dé cuenta en forma fidedigna de su otorgamiento. El consentimiento será tácito, cuando habiéndose puesto a disposición del titular una solicitud de autorización para la recolección o tratamiento de datos, éste no manifiesta su oposición.

Con todo, el consentimiento deberá ser específico en cuanto a su finalidad.

El titular de datos podrá revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento. La revocación del consentimiento no tendrá efectos retroactivos.

Los medios utilizados para el otorgamiento o la revocación del consentimiento deberán ser expeditos, accesibles y gratuitos para el titular de datos.

**Artículo 12.- excepciones al consentimiento**

No se requerirá el consentimiento previo del titular de datos en los siguientes casos:

a) Si los datos han sido recolectados de una fuente de acceso público.

b) Si el tratamiento de datos es necesario para la ejecución o cumplimiento de una obligación legal, de un contrato o una relación jurídica aceptada por el titular, debiendo limitarse a la finalidad específica que le dio origen.

c) Si el tratamiento de los datos personales se realiza exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones.

d) Si el tratamiento lo autoriza la ley.

Con todo, en estos casos el tratamiento de datos que se realice siempre deberá cumplir con los principios de legitimidad, calidad, seguridad, responsabilidad e información establecidos en esta ley.

**Artículo 13: obligaciones de los responsables de datos**

Los responsables de datos, sin perjuicio de las demás disposiciones previstas en esta ley y sus reglamentos, tendrán las siguientes obligaciones:

a) Contar y poner a disposición, de manera expedita y gratuita, cuando le sean requeridos, los antecedentes que acrediten la legitimidad del tratamiento de los datos personales que realice.

b) Asegurar que los datos personales han sido recolectados y tratados para fines explícitos, específicos y legítimos.

c) Comunicar, transmitir o ceder, en conformidad a las disposiciones de esta ley, información veraz, completa, exacta y actualizada de los datos personales o bases de datos que sean objeto de tratamiento.

d) Adoptar y mantener los estándares o condiciones mínimas de control, seguridad y resguardo para proteger los datos personales y evitar su acceso o tratamiento no autorizados.

e) Cumplir con los principios para el tratamiento de datos previstos en esta ley.

**Artículo 14. Deber de reserva y confidencialidad**

Los responsables de datos y las personas encargadas del tratamiento de datos están obligados a mantener reserva o confidencialidad sobre los datos personales que traten, cuando estos provengan o hayan sido recolectados de fuentes no accesibles al público. Esta obligación subsistirá aún después de concluida la relación con el titular o con el responsable de datos, según corresponda.

La obligación de reserva o confidencialidad establecida en el inciso anterior es sin perjuicio de la comunicación o cesión de datos que se realice de conformidad a lo dispuesto en esta ley, del deber de informar el origen de los datos personales objeto de tratamiento o el en caso de requerimiento de información hecho por la autoridad competente en el ejercicio de sus facultades legales.

**Artículo 14 bis.- Deber de información y transparencia**.

Los responsables de datos deberán mantener permanentemente a disposición del público en su sitio Web o en cualquier otro medio de información equivalente, sus políticas sobre tratamiento de datos personales, debiendo proporcionar al menos la siguiente información:

a) La política de tratamiento de datos personales que haya adoptado, la fecha y versión de la misma.

b) La identidad del responsable de datos y de las personas encargadas del tratamiento de datos.

c) La finalidad del tratamiento de datos personales que realiza o pretende realizar.

d) Los nombres, categorías o tipos de base de datos que administra.

e) El domicilio y/o la dirección de correo electrónico a la cual se le notificarán las solicitudes de acceso, rectificación, cancelación y oposición de los titulares.

f) Los potenciales destinatarios a los que se prevé comunicar y/o ceder los datos personales que trate.

g) El tipo de medidas de seguridad adoptadas para proteger las bases de datos que administra.

h) Cualquier otro antecedente relevante que permita informar de mejor manera respecto de la forma en que realiza el tratamiento de datos personales.

**Artículo 14 ter.- Deber de adoptar medidas de seguridad**

El responsable de datos y las personas encargadas del tratamiento de datos personales deberán disponer las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en la presente ley, considerando el estado de la técnica actual y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con naturaleza de los datos personales tratados.

Para estos efectos, el responsable de datos y las personas encargadas del tratamiento deberán realizar análisis de los riesgos a los que están sometidos los datos objeto de tratamiento y adoptar las medidas técnicas y organizativas para precaver y mitigar los efectos negativos que puedan provocar los incidentes de seguridad.

Si la información y los sistemas que opera el responsable de datos tienen distintos niveles de criticidad, se deberán adoptar las medidas de seguridad que correspondan al nivel más alto.

Ante la ocurrencia de un incidente, corresponderá al responsable de datos acreditar la existencia y funcionamiento de las medidas de seguridad adoptadas en función de los niveles de criticidad y de acuerdo a la tecnología disponible.

En caso de controversia judicial, corresponderá al responsable de datos acreditar la existencia y funcionamiento de las medidas de seguridad adoptadas en función de los niveles de criticidad y de acuerdo a la tecnología disponible.

Un reglamento del Ministerio de Hacienda y suscrito además por el Ministro de Economía, Fomento y Turismo y el Ministro Secretario General de la Presidencia, especificará los estándares o condiciones mínimas de control, seguridad y resguardo que se deberán observar por el responsable de datos y las personas encargadas del tratamiento, considerando el análisis de riesgo y el de criticidad, estableciendo estándares y medidas diferenciadas para las empresas señaladas en el inciso segundo del artículo segundo de la Ley N° 20.416.

**Artículo 14 quáter.- Deber de reportar las vulneraciones a las medidas de seguridad**

Los responsables de datos y las personas encargadas de su tratamiento deberán reportar a la Dirección Nacional de Protección de Datos, 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 o la comunicación o acceso no autorizados a dichos datos.

Cuando dichas vulneraciones se refieran a datos personales sensibles, el responsable también deberá efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, individualizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se realizará a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.

Asimismo, los responsables de datos y las personas encargadas de su tratamiento deberán registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

**Artículo 15.- Cesión de bases de datos personales**

Se podrá ceder todo o parte de los registros o bases de datos que disponga el responsable de datos, cuando la cesión sea necesaria para cumplir con los fines o funciones del responsable o cedente y/o del cesionario.

La cesión requiere el consentimiento previo del titular de datos. El consentimiento del titular y las excepciones a éste se sujetarán a las reglas establecidas en los artículos 12 y 13 de esta ley.

En caso que el consentimiento otorgado por el titular al momento de realizarse la recolección de los datos no haya considerado la cesión de los mismos, deberá recabarse antes de que ésta se produzca, considerándose para todos los efectos legales como una nueva operación de tratamiento.

El consentimiento que otorgue el titular deberá considerar la información necesaria que le permita conocer la finalidad a la cual serán destinados los datos en caso de cesión o el tipo de actividades de aquel a quien se le pretenden ceder.

La cesión de datos deberá constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberán individualizar a las partes, los registros o bases de datos que son objeto de la cesión, las finalidades previstas para el tratamiento de datos y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario.

El tratamiento de los datos personales cedidos deberá realizarse por el cesionario de conformidad a las finalidades establecidas en el contrato de cesión.

Una vez perfeccionada la cesión, el cesionario de la base de datos adquirirá la condición de responsable de datos para todos los efectos legales, respecto de los registros o bases de datos que fueron objeto de la cesión. El cedente, por su parte, también mantendrá la calidad de responsable de datos.

Si se verifica la cesión sin contar con el consentimiento del titular siendo éste necesario o no se le informa acerca de la finalidad a la cual serán destinados los registros cedidos o el tipo de actividades que desarrolla el cesionario, la cesión será considerada nula para todos los efectos legales, debiendo el cesionario cancelar todos los registros recibidos, sin perjuicio de las responsabilidades legales que correspondan.

En caso que los datos personales sean cedidos previa disociación de los mismos, no le serán aplicables las reglas señaladas en este artículo, considerando que por efecto de dicho procedimiento estos datos dejan de tener la aptitud de identificar a una persona.

**Artículo 15 bis.- Tratamiento de datos por parte de un tercero.**

El responsable de datos podrá efectuar el tratamiento de datos en forma directa o a través de un tercero.

En este último caso, el tercero realizará el tratamiento de datos personales conforme al encargo y a las instrucciones del responsable de datos, quedándole prohibido su tratamiento, comunicación, cesión o entrega para un objeto distinto del convenido con el responsable.

Si el tercero trata, comunica, cede o entrega los datos o registros con un objeto distinto del encargo convenido o a una persona distinta del responsable, será considerado como responsable de datos para todos los efectos legales, debiendo responder solidariamente por las infracciones y los perjuicios en que hubiere incurrido, sin perjuicio de las responsabilidades contractuales que le correspondan frente al responsable de datos.

Cumplida la prestación del servicio de tratamiento por parte del tercero, los datos deberán ser cancelados.

**Artículo 15 ter.- Tratamiento automatizado de datos.-**

El responsable de datos podrá establecer un procedimiento automatizado de tratamiento y de transmisión de datos personales, siempre que se cautelen los derechos del titular y el tratamiento guarde relación con las tareas y finalidades de las personas o entidades participantes.

El titular de datos podrá solicitar al responsable que le asegure que ninguna decisión que le pueda afectar de manera significativa se adopte exclusivamente basada en el procesamiento automatizado de sus datos, sin perjuicio del ejercicio del derecho establecido en la letra e) del artículo 7 de esta ley.

La Dirección Nacional de Protección de Datos velará por el cumplimiento de los principios y estándares en materia de tratamiento automatizado de datos.

Esta disposición no será aplicable cuando se transmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios internacionales vigentes.

**Párrafo Segundo: Del tratamiento de datos personales sensibles**

**Artículo 16.- Tratamiento de datos personales sensibles.**

El tratamiento de datos personales sensibles sólo podrá realizarse con el consentimiento expreso, previo, inequívoco y específico del titular de datos, su representante legal o mandatario, según corresponda, otorgado a través de un medio escrito o tecnológico idóneo que dé cuenta de manera fidedigna de su otorgamiento o cuando la ley expresamente lo autorice.

Los datos personales sensibles sólo podrán ser almacenados cuando sea indispensable para el cumplimiento de los fines para los cuales fueron recolectados o están siendo tratados, y deberán mantenerse por el tiempo estrictamente necesario para cumplir estos fines.

Los datos personales sensibles no podrán ser objeto de cesión.

**Artículo 16 bis.- Datos relativos a la salud.**

Sin perjuicio del cumplimiento de lo dispuesto en el artículo anterior, los datos personales relativos a la salud sólo podrán ser objeto de tratamiento en los siguientes casos:

a) Cuando exista urgencia médica o sanitaria.

b) Para la prevención o promoción de la salud.

c) Para realizar un diagnóstico médico.

d) Para calificar el grado de dependencia de una persona.

e) Para la determinación de tratamientos médicos, siempre que dichos tratamientos se realicen por establecimientos de salud públicos o privados o por un profesional de la salud titular del secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

f) Cuando sean utilizados con fines estadísticos, científicos y de estudios o de investigaciones que atiendan a un interés público o al desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera.

Excepcionalmente no será necesario el consentimiento previo del titular de datos para la recolección o el tratamiento de datos personales relativos a su salud, cuando ello resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona o cuando el titular se encuentre física o jurídicamente impedido para otorgar su consentimiento. Una vez que cese el impedimento, el responsable de datos deberá informar detalladamente al titular de los datos relativos a la salud que fueron tratados y las operaciones realizadas con ellos.

**Artículo 16 ter.- Datos biométricos**

Los responsables de datos que deseen utilizar o tratar datos biométricos, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz, además de cumplir con las reglas establecidas en el artículo 16, deberán proporcionar al titular la siguiente información específica:

a) La identificación del sistema biométrico que utilizarán.

b) La finalidad para la cual los datos recolectados por el sistema biométrico serán utilizados.

c) La forma en que se garantiza la exactitud de los datos biométricos recolectados y el vínculo entre el titular y sus datos personales.

d) El período durante el cual los datos biométricos serán almacenados y el procedimiento que se utilizará para cancelarlos, una vez que haya transcurrido dicho período.

e) La forma en la cual el titular de datos podrá ejercer sus derechos.

Un reglamento regulará la forma y los procedimientos que se deberán utilizar para la implementación de los sistemas biométricos.

Si la utilización de los sistemas biométricos se realiza con la exclusiva finalidad de comprobar la identidad de una persona de manera tal de que no se pueda volver a construir el elemento biométrico a partir del dispositivo que lo contiene, no se requerirá cumplir con lo dispuesto en los incisos precedentes.

**Artículo 16 quáter.- Datos genéticos y protéomicos humanos**

Los responsables de datos, además de cumplir con los requisitos generales para el tratamiento de datos sensibles, sólo podrán realizar tratamiento de datos genéticos y proteómicos para los siguientes fines:

a) Realizar diagnósticos médicos.

b) Prestar asistencia sanitaria.

c) Realizar investigaciones médicas u otras formas de investigación científica, incluidos los estudios epidemeológicos, los estudios de carácter antropológico o arqueológico y de medicina forense.

d) Cumplir resoluciones judiciales recaídas en procesos civiles, de familia o penales.

Queda prohibido el uso, tratamiento, publicación, distribución y cesión de los datos genéticos y protéomicos y las muestras biológicas asociados a una persona identificada o identificable, incluido el almacenamiento del material biológico que pueda recolectarse en el ámbito laboral, educativo, social o de seguros, salvo que la ley expresamente lo autorice en casos calificados.

Los prestadores institucionales de salud, sean estos públicos o privados, que necesiten tratar datos genéticos dentro del marco de las funciones que les señala el Código Sanitario, la ley Nº 20.120 y su normativa complementaria, deberán guardar los más altos niveles de seguridad de dicha información y de las muestras biológicas a partir de las cuales pueda recolectarse.

En el caso de datos genéticos recolectados con motivo de proyectos de investigación o estudios, estos deberán ser disociados en forma previa a su publicación.

**Párrafo Tercero: Del tratamiento de datos especiales**

**Artículo 16 quinquies.- Datos personales relativos a los niños, niñas y adolescentes.**

El tratamiento de los datos personales de los niños, niñas y adolescentes deberá realizarse atendiendo al interés superior de estos y al respeto de su autonomía progresiva.

Sólo se podrán tratar los datos personales de los niños y niñas cuando sea indispensable para su identificación, en caso de urgencia médica o sanitaria o para el otorgamiento de un beneficio, debiendo contar con el consentimiento previo, expreso y específico de quien ejerza su cuidado personal o cuando lo autorice la ley.

Los datos personales de los adolescentes, salvo los datos personales sensibles, se podrán tratar de acuerdo a las normas de autorización previstas para los adultos. Los datos personales sensibles sólo se podrán tratar con el consentimiento previo, expreso y específico de quien ejerza su cuidado personal o en los casos que autoriza la ley.

Para los efectos de esta ley se consideran adolescentes a los mayores de catorce y menores de dieciocho años.

Será obligación de los establecimientos educacionales y de quienes ejerzan el cuidado personal del niño, niña o adolescente velar por la protección de la información personal de aquellos.

**Artículo 16 sexies.- Datos con fines históricos, estadísticos, científicos y de estudios o investigaciones.**

Las personas naturales o jurídicas que recolecten o traten datos personales con fines históricos, estadísticos, científicos y de estudios o de investigaciones, deberán asegurar que han adoptado todas las medidas de calidad y seguridad necesarias con el objeto de resguardar que los datos que recolecten o traten se utilicen exclusivamente para tales fines. En estos casos, los datos podrán ser almacenados y utilizados por un período indeterminado de tiempo.

La Dirección Nacional de Protección de Datos evaluará la pertinencia y suficiencia de las medidas de calidad y seguridad adoptadas por el responsable, instruyendo las modificaciones o refuerzos necesarios con el objeto de asegurar la custodia y protección de la información.

Los registros o bases de datos que se recolecten o traten exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones, sólo podrán ser cedidos cuando el responsable de datos sea una persona jurídica. La cesión sólo se podrá realizar a otra entidad o a una persona natural, siempre que los utilice con los mismos fines. El cedente deberá asegurarse que el cesionario adopte medidas de calidad y seguridad iguales o superiores a las adoptadas por él.

Asimismo, los responsables de datos y las personas encargadas del tratamiento deberán asegurar que los datos personales no sean utilizados para adoptar decisiones, medidas o acciones en perjuicio del titular de datos.

Los responsables de datos que hayan tratado datos personales exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones, podrán efectuar publicaciones con los resultados y análisis obtenidos como producto del tratamiento realizado, debiendo previamente adoptar todas las medidas necesarias con el objeto de evitar que los titulares de estos datos sean identificados o identificables.

**Artículo 16 septies.- Datos de tráfico electrónico**

Los datos de tráfico electrónico serán tratados y almacenados con el solo propósito de transmitir una comunicación y deberán ser cancelados o irrevocablemente disociados, cuando ya no se necesiten para el propósito por el cual fueron recibidos o capturados. Con todo, los datos de tráfico necesarios para la facturación de los servicios y pagos de interconexiones podrán ser tratados hasta la expiración del plazo durante el cual pueda impugnarse la factura o exigirse el pago.

El proveedor de servicios de telecomunicaciones electrónicas deberá adoptar las medidas técnicas y de gestión para preservar la seguridad de sus servicios. En caso que exista un riesgo de vulneración de seguridad de la red, el proveedor de un servicio de telecomunicaciones electrónicas deberá informar a quien utilice su servicio sobre dicho riesgo, detallando sus características y posibles repercusiones en el sistema del usuario.

Los proveedores de servicios de telecomunicaciones electrónicas que se ocupen de la facturación o de la gestión de tráfico de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de telecomunicaciones electrónicas o de la prestación de un servicio con valor añadido, deberán limitar el tratamiento a lo necesario para realizar dichas actividades.

**Artículo 16 octies.- Datos de localización**

Sólo podrán ser objeto de tratamiento los datos de localización, previo consentimiento del titular o si estos son anonimizados.

El responsable y/o proveedor del servicio deberá informar a los titulares, usuarios y/o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y si los datos se transmitirán a un tercero para la prestación de un servicio con valor añadido. El proveedor del servicio deberá ofrecer a los titulares, usuarios y/o abonados la posibilidad de revocar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico.”.

**Título III: De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial**

**Artículo 17.**

Los responsables de los registros o bases de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas el Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios, y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentren con alguna modalidad pendiente.

También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura.

Las entidades responsables que administren bases de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el período de cesantía que afecte al deudor.

Para estos efectos, la Administradora de Fondos de Cesantía comunicará los datos de sus beneficiarios al Boletín de Informaciones Comerciales sólo mientras subsistan sus beneficios para los efectos de que éste bloquee la información concerniente a tales personas.

Sin embargo, las personas que no estén incorporadas al seguro de cesantía deberán acreditar dicha condición ante el Boletín de Informaciones Comerciales, acompañando el finiquito extendido en forma legal o, si existiese controversia, con el acta de comparecencia ante la Inspección del Trabajo, para los efectos de impetrar este derecho por tres meses renovable hasta por una vez. Para que opere dicha renovación se deberá adjuntar una declaración jurada del deudor en la que manifieste que mantiene su condición de cesante.

El bloqueo de datos será sin costo para el deudor.

No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral.

No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral.

Los artículos 1º, 2º y 3º transitorios de la LEY 19812, publicada el 13.06.2002, establecen en

relación con el presente artículo, lo siguiente:

**"Artículo 1° transitorio.-** Los responsables de los registros o bancos de datos personales que traten información señalada en el artículo 17 de la ley N° 19.628 no podrán comunicarla cuando se refiera a obligaciones que, a la fecha de publicación de esta ley, hayan sido pagadas o se hayan extinguido por otro modo legal.

Asimismo, no podrán comunicar los datos relativos a esas obligaciones que se hayan hecho exigibles antes del 1º de mayo de 2002 y se encuentren impagas, siempre que el total de obligaciones impagas del titular que comunique el registro o base de datos a la fecha de publicación de esta ley sea inferior a $2.000.000 por concepto de capital, excluyendo intereses, reajustes y cualquier otro rubro.

En el caso de los incisos anteriores, tampoco podrá proporcionarse información al titular de los datos, ni comunicarse el hecho de que éste haya sido beneficiado con esas disposiciones.

**Artículo 2º transitorio.-** Los responsables de los registros o bases de datos personales que comuniquen información sobre las obligaciones a que se refiere el artículo 17 de la ley Nº 19.628 eliminarán todos los datos relacionados con créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios.

**Artículo 3º transitorio**.- Los deudores del Banco del Estado de Chile que al 30 de septiembre de 1999 obtuvieron créditos en el marco del programa de créditos para establecimiento por cuenta propia de chilenos retornados y que hayan optado, dentro del plazo establecido, a los beneficios que les otorga la ley Nº 19.740, una vez aclarada la morosidad y previa solicitud, serán borrados definitivamente del o los registros históricos que existan sobre los documentos señalados en el artículo 17.".

**Artículo 18**

En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal.

Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes.

**Artículo 19**

El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente.

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o base de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación a la base de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de conformidad a lo dispuesto en el Título VII de esta ley.

**Título IV: Del tratamiento de datos por los organismos públicos**

**Artículo 20.- Tratamiento de datos por parte de organismos públicos.**

El tratamiento de datos personales por parte de los organismos públicos se realizará para el cumplimiento de sus funciones, dentro del ámbito de sus competencias y, de conformidad a las normas especiales que se establecen en sus leyes respectivas, a las disposiciones previstas en este Título y a las demás normas señaladas en esta ley, en cuanto les sean aplicables. En esas condiciones, los organismos públicos actuarán como responsables de datos y no requerirán el consentimiento del titular para efectuar el tratamiento de sus datos personales.

**Artículo 21.- Principios aplicables al tratamiento de datos por organismos públicos.**

El tratamiento de datos personales por parte de los organismos públicos se regirá por los principios establecidos en el artículo 3 de la presente ley, en todo aquello que les sean aplicables, y por los principios de coordinación, eficiencia, transparencia y publicidad.

En virtud del principio de coordinación, los organismos públicos deben propender a un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y reiteración de requerimientos de información o documentos a los titulares de datos personales. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites, tanto entre los organismos del Estado como para los trámites y gestiones que realicen los titulares de la información. De acuerdo con los principios de transparencia y publicidad, los organismos públicos deben dar acceso a la información que tengan a su disposición, resguardando los derechos de las personas que pudieran verse afectadas por ello, de conformidad con lo establecido en el artículo 20 de la ley N° 20.285, sobre acceso a la información pública.

**Artículo 22.- Comunicación y cesión de datos.**

Los órganos públicos podrán comunicar, transmitir o ceder los datos personales que contengan sus bases de datos a otros órganos públicos cuando sea necesario para el ejercicio o cumplimiento de las funciones, competencias o atribuciones de cualquiera de dichos órganos. Asimismo, se podrán comunicar o ceder datos personales entre organismos públicos cuando tengan por objeto otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

Para los efectos de poder comunicar o ceder datos personales a terceros, los organismos públicos deberán contar con el consentimiento expreso del titular, obtenido al momento de la recolección. Cuando se trate de comunicar o ceder datos personales en virtud de una solicitud de acceso a la información formulada con arreglo a lo establecido en el artículo 10 de la ley N° 20.285, los organismos públicos deberán contar con el consentimiento del titular obtenido en la oportunidad prevista en el artículo 20 de dicha ley.

En los casos de comunicación o transmisión de datos, el órgano público que efectúa la comunicación será el responsable de datos para los efectos de la presente ley. Cuando se realice una cesión de datos, el órgano cesionario también será considerado como responsable de datos.

Los organismos públicos sólo podrán comunicar datos personales sensibles a otros organismos públicos.

**Artículo 23.- Ejercicio de los derechos por el titular y reclamo de ilegalidad.**

Los titulares de datos podrán ejercer los derechos que le reconoce esta ley ante los organismos públicos que sean responsables de datos. Con todo, el titular no podrá oponerse al tratamiento de datos realizado por un órgano público cuando este último actúa en uso de sus facultades y competencias legales, salvo que el tratamiento sea arbitrario o ilegal.

El ejercicio de los derechos del titular se realizará de acuerdo al procedimiento establecido en la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de la Administración del Estado, dirigiéndose al jefe superior del servicio.

Las personas naturales o jurídicas que se vean afectadas por la resolución de un órgano público, sea que le deniegue el ejercicio de un derecho reconocido por esta ley a un titular de datos o infrinja algún principio, deber u obligación establecido en ella, causándole perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o del domicilio de reclamante, a su elección, de conformidad con las normas dispuestas en el artículo 50 de esta ley. Con todo, el informe a que alude la letra d) del artículo 50 será evacuado por el órgano público requerido.

Sin perjuicio de lo anterior, la Corte de Apelaciones respectiva podrá requerir informe a la Dirección Nacional de Protección de Datos con el objeto de establecer si en las operaciones de tratamiento de datos realizadas por el órgano público, hubo o no infracción a los principios, deberes u obligaciones establecidos en esta ley.

**Artículo 24. Régimen de excepciones**

Las disposiciones del presente Título no se aplicarán en los siguientes casos:

a) Al tratamiento de datos que efectúen organismos públicos que cuenten con datos o bases de datos elaboradas a partir de sistemas de tratamiento cuyo resguardo y privacidad se encuentren protegidos por normas de secreto, confidencialidad o reserva establecidas en sus respectivas leyes.

b) Al tratamiento de datos personales que realicen organismos públicos con ocasión de la ejecución de investigaciones sobre infracciones de carácter penal, ilícitos económicos o el tratamiento de datos para la seguridad de la Nación, la defensa nacional o la mantención del orden público o la seguridad pública.

Sin perjuicio de lo señalado en el inciso anterior, el tratamiento de datos que realicen estos organismos públicos deberá cumplir con los principios de legitimidad, calidad, seguridad y responsabilidad establecidos en esta ley. Asimismo, deberán cumplir con lo establecido en los artículos 14, 14 ter y 14 quáter.

Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. No obstante, siempre podrán comunicar la referida información cuando les sea solicitada por los Tribunales de Justicia u otros organismos públicos dentro del ámbito de sus competencias legales. Los agentes de estos órganos deberán guardar la debida reserva o secreto respecto de esta información.

**Artículo 25: Registro de bases de datos de los órganos públicos**

Los organismos públicos responsables de datos personales deberán registrarse en el registro a que alude el artículo 33. Para tal efecto, el jefe superior del organismo público informará a la Dirección Nacional de Protección de Datos los antecedentes que den cuenta de la naturaleza de los registros o bases de datos que administra el organismo y de sus actualizaciones. Igualmente, informará a la Dirección Nacional cuando, respecto de las mismas bases de datos, existan varios organismos públicos que simultáneamente detenten la calidad de responsables de datos.

Los organismos públicos no deberán registrar las bases de datos que tengan sobre sus funcionarios.

**Artículo 26: reglamento**

Las condiciones y modalidades de comunicación o cesión de datos entre organismos públicos, así como la forma de dar cumplimiento a la obligación de registro establecida en el artículo anterior, serán reguladas por un reglamento dictado por el Ministerio Secretaría General de la Presidencia y suscrito por el Ministro de Hacienda.

**Artículo 27.- Tratamiento de datos personales por parte del Congreso Nacional, el Poder Judicial y los organismos públicos autónomos.**

El Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral, y los demás tribunales especiales creados por ley, deberán sujetarse, en cuanto al tratamiento de los datos personales que realicen en el ámbitos de sus competencias y funciones, a las disposiciones de esta ley aplicables a los organismos públicos, salvo aquellas en las que expresamente se señale lo contrario.

Estos organismos detentarán la calidad de responsables de datos y deberán dictar a través de sus órganos internos las normas necesarias para dar cumplimiento a las disposiciones de la presente ley, pudiendo requerir, para ello, la asistencia técnica de la Dirección Nacional de Protección de Datos.

Los titulares de datos podrán ejercer los derechos que le reconoce esta ley ante estos organismos, de acuerdo a los procedimientos previstos en sus respectivas normas de funcionamiento.

En caso que cualquiera de estos organismos, con excepción del Poder Judicial, deniegue el ejercicio de un derecho reconocido por esta ley a un titular de datos o infrinja algún principio, deber u obligación establecida en ella, causándole perjuicio, el titular de datos o las personas naturales o jurídicas que se vean agraviadas o afectadas por la decisión del organismo, podrán reclamar ante la Corte de Apelaciones respectiva, de conformidad al procedimiento dispuesto en el artículo 50 de esta ley.”.

**Título V: De la transmisión internacional de datos personales**

**Artículo 28.- Regla general.**

La transmisión internacional de datos personales se podrá efectuar por el responsable de datos, a personas o entidades sujetas al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos.

Se entenderá que el ordenamiento jurídico de un país posee un nivel adecuado de protección de datos, cuando éste cumpla con estándares similares o superiores a los fijados en esta ley. La Dirección Nacional de Protección de Datos determinará los países que poseen niveles adecuados de protección de datos.

En aquellos países con legislaciones que no cumplan niveles adecuados de protección de datos, el responsable de datos deberá obtener una autorización previa de la Dirección Nacional de Protección de Datos para efectuar la transmisión de los datos, la que sólo podrá otorgarse si se obtienen las garantías adecuadas.

En cualquier transmisión internacional de datos personales, el responsable de datos deberá tomar en consideración la naturaleza de los datos, la finalidad y duración del tratamiento, las condiciones de seguridad y calidad que ofrezca la persona o entidad a quien se le transfieren, los mecanismos establecidos para el ejercicio de los derechos del titular, los medios de contacto e información y, el régimen de garantías, obligaciones y responsabilidades determinados entre las partes.

La Dirección Nacional de Protección de Datos fiscalizará las operaciones de transmisión internacional de datos, pudiendo formular recomendaciones, adoptar medidas conservativas o en casos calificados, suspender temporalmente el envío de los datos.

**Artículos 29.- Excepciones.**

No se aplicarán los requisitos y el procedimiento previstos en el artículo anterior:

a) Cuando exista consentimiento específico y determinado del titular de datos para la transmisión.

b) Cuando se trate de tratados o convenios que hayan sido ratificados por el Estado chileno y se encuentren vigentes.

c) Cuando se haga con el objeto de prestar o solicitar auxilio judicial internacional.

d) Cuando sea necesario adoptar medidas urgentes en materia sanitaria, para la prevención o diagnóstico de enfermedades, para tratamientos médicos o la gestión de servicios de salud.

e) Cuando tenga por finalidad asegurar un interés público. Tendrá esta consideración la transmisión solicitada por organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el narcotráfico y la administración aduanera en el cumplimiento de sus funciones y competencias.

f) Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.”.

**Título VI: De la Dirección Nacional de Protección de Datos**

**Artículo 30.- Dirección Nacional de Protección de Datos.**

Créase la Dirección Nacional de Protección de Datos, organismo descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección, que se relacionará con el Presidente de la República, a través del Ministerio de Hacienda y estará afecto al Sistema de Alta Dirección Pública.

El domicilio de la Dirección Nacional de Protección de Datos será la ciudad de Santiago, sin perjuicio de los domicilios que pueda establecer en otros lugares del país.

El Director Nacional de Protección de Datos será el Jefe Superior del Servicio.

**Artículo 31.- Funciones y atribuciones.**

La Dirección Nacional de Protección de Datos tendrá las siguientes funciones y atribuciones:

a) Velar por el cumplimiento de la normativa relativa al tratamiento de datos personales y su protección.

b) Dictar instrucciones generales y obligatorias con el objeto que las personas naturales y jurídicas de derecho privado que tratan datos personales, sujeten sus operaciones a los principios y obligaciones establecidos en esta ley.

c) Dictar instrucciones generales y obligatorias con el objeto de operacionalizar las normas que fijan los estándares o condiciones mínimas de control, seguridad y resguardo que se deben observar en el tratamiento de datos por parte del responsable y de las personas encargadas del tratamiento.

d) Dictar, sin perjuicio de las competencias de otros órganos del Estado, orientaciones generales con el objeto que los órganos públicos que tratan datos personales, sujeten sus operaciones a los principios y obligaciones establecidos en esta ley.

e) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial y a los organismos públicos autónomos, para la dictación y ejecución de las políticas y normativa interna que dicten con el objeto de cumplir los principios y obligaciones establecidos en esta ley.

f) Fiscalizar que las operaciones de tratamiento de datos personales sensibles se verifiquen de acuerdo a las reglas establecidas en esta ley.

g) Fiscalizar el cumplimiento de esta ley y sus reglamentos, en especial, lo relativo al ejercicio de los derechos que se le reconocen al titular de datos, el cumplimiento de los principios y estándares en materia de tratamiento automatizado de datos, las operaciones de transmisión internacional de datos y las medidas de calidad y seguridad adoptadas para el tratamiento de datos exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones.

h) Fiscalizar el cumplimiento, el análisis de riesgo y criticidad realizado, las acciones adoptadas para precaver o mitigar efectos negativos y las vulneraciones a las medidas de seguridad.

i) Resolver los reclamos que formulen los titulares de datos por infracción a esta ley y sus reglamentos.

j) Ejercer la potestad sancionadora sobre las personas naturales o jurídicas de derecho privado que recolecten o traten datos de personas con infracción a esta ley e imponer las sanciones establecidas en ella.

k) Establecer las infracciones en que incurra un órgano público a los principios, deberes u obligaciones previstos en esta ley, con ocasión de sus operaciones de tratamiento de datos personales

l) Solicitar a la Contraloría General de la República instruya los procedimientos administrativos competentes con el objeto de establecer las eventuales responsabilidades administrativas del jefe superior de un órgano de la Administración del Estado y/o de sus funcionarios, en caso de infracción a los principios, deberes u obligaciones establecidos en esta ley.

m) Realizar labores de difusión, promoción e información a la ciudadanía sobre el tratamiento y la protección de los datos personales

n) Prestar colaboración o asesoría técnica a los órganos del Estado en la implementación de políticas y acciones relativas al tratamiento y la protección de datos personales, pudiendo para estos efectos celebrar convenios de cooperación y desarrollar programas de asistencia técnica

o) Participar, recibir cooperación y colaborar con organismos públicos nacionales e internacionales, en materias propias de su competencia

p) Solicitar la representación de sus intereses al Consejo de Defensa del Estado de conformidad a la ley

q) Certificar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento

r) Administrar el Registro Nacional de Responsables de Datos

s) Administrar el Registro Nacional de Cumplimiento

t) Realizar todas aquellas funciones que la ley le encomiende especialmente.

**Artículo 32.- Registro Nacional de Responsables de Datos.**

Créase el Registro Nacional de Responsables de Datos, en adelante “el registro”, administrado por la Dirección Nacional de Protección de Datos, en el cual se inscribirán las personas naturales y jurídicas que traten datos personales de conformidad a esta ley.

El registro tendrá carácter público y en él se individualizará al responsable de datos, la finalidad del o los tratamientos que realizan, los registros o bases de datos que administran y la descripción genérica del universo de personas que comprenden.

El responsable de datos deberá registrarse en forma electrónica, proporcionando los antecedentes señalados en el inciso anterior, previo al inicio de sus actividades de recolección o tratamiento, debiendo actualizar los antecedentes del registro cuando se produzcan cambios significativos

**Articulo 33.- Obligación de inscripción en el Registro Nacional de Responsables de Datos.**

Estarán obligados a inscribirse en el registro los responsables de datos siguientes:

a) Los organismos públicos que tratan datos personales para el cumplimiento de las funciones, competencias y atribuciones que les encomienda la ley

b) Los bancos e instituciones financieras supervisadas por la Superintendencia de Bancos e Instituciones Financieras

c) Las personas naturales o jurídicas supervisadas por la Superintendencia de Valores y Seguros

d) Las personas naturales y jurídicas que realicen actividades de comunicación de información, recolección o tratamiento de datos sobre obligaciones de carácter económico financiero, bancario o comercial

e) Las personas naturales y jurídicas que provean servicios de telecomunicaciones e internet

f) Las personas naturales y jurídicas que traten datos personales sensibles

g) Las personas naturales y jurídicas que traten datos personales que por su naturaleza, volumen, objetivos o usos, no tengan una finalidad doméstica. A través de reglamento se determinarán los tipos de registros o bases de datos que se considera tienen una finalidad doméstica y cuyos responsables de datos se encuentran liberados de la obligación de inscribirse en el registro

**Artículo 34.- Del Director de la Dirección Nacional de Protección de Datos.**

La dirección y administración superior de la Dirección Nacional de Protección de Datos estará a cargo de un Director Nacional, nombrado por el Presidente de la República conforme al Sistema de Alta Dirección Pública regulado en el Título VI de la ley N° 19.882.

**Artículo 35.- Incompatibilidades e Inhabilidades**

El desempeño de las labores de director exigirá dedicación exclusiva y será incompatible con el desempeño de todo cargo o servicio, sea o no remunerado, que se preste en el sector privado. No obstante lo anterior, el cargo de director será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales. Del mismo modo, podrá desempeñarse en corporaciones o fundaciones, públicas o privadas, nacionales o extranjeras, siempre que en ellas no perciba remuneración y su desempeño no sea incompatible con sus funciones. Además el cónyuge o conviviente civil del Director y sus parientes hasta el primer grado de consanguinidad no podrán ser director ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

Asimismo, este cargo será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley, como, asimismo, de empresas, sociedades o entidades públicas o privadas en que el Estado, sus empresas, sociedades o instituciones centralizadas o descentralizadas, tengan aportes de capital mayoritario o en igual proporción o, en las mismas condiciones, representación o participación. También será incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

En lo no expresamente regulado en este artículo, se regirá por las normas del párrafo 2° del Título III del decreto con fuerza de ley N° 1-19653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

**Artículo 36.- Post empleo.**

Una vez cesado en el cargo, y por el plazo de seis meses, el ex director nacional no podrá prestar ningún tipo de servicio, sea de forma gratuita o remunerada, ni adquirir participación en la propiedad de entidades respecto de las cuales, dentro de los doce meses anteriores al cese en sus funciones, haya, de forma específica, personal y directa, emitido actos, resoluciones o dictámenes; o intervenido en los procedimientos administrativos, finalizados o no, que produjeron o producirán dichos actos administrativos. La prohibición de que trata este artículo se extiende a aquellas empresas que formen parte del mismo grupo empresarial en los términos del artículo 96 de la ley N° 18.045.

Todo ex director nacional deberá, dentro de los diez días hábiles siguientes al cese en sus funciones, efectuar una declaración jurada en la que individualice las entidades respecto a las cuales haya intervenido en los términos del inciso anterior. Una copia de dicha declaración deberá ser remitida al nuevo director nacional y a la Contraloría General de la República, para su registro.

**Artículo 37.- Del personal.**

El personal de la Dirección Nacional de Protección de Datos estará afecto a las disposiciones de la ley N° 18.834, sobre Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, del Ministerio de Hacienda, de 2004, y, en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, y su legislación complementaria.

Sin perjuicio de lo dispuesto en los incisos precedentes, todo el personal de la Dirección Nacional será de exclusiva confianza del Director Nacional.

**Artículo 38.- Del Patrimonio.**

El patrimonio de la Dirección Nacional de Protección de Datos estará formado por:

a) El aporte que se contemple anualmente en la Ley de Presupuestos

b) Los bienes muebles e inmuebles que se le transfieran o que adquieran a cualquier título y por los frutos de esos mismos bienes

c) Las donaciones que se le hagan, las herencias y legados que acepte, lo que deberá hacer con beneficio de inventario. Dichas asignaciones hereditarias estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten. Las donaciones no requerirán el trámite de insinuación

d) Los aportes de la cooperación internacional

**Artículo 39.- De la administración financiera y fiscalización**

La Dirección Nacional de Protección de Datos deberá cumplir con las normas establecidas en el decreto ley Nº 1.263, de 1975, sobre administración financiera del Estado.

De igual forma, la Dirección Nacional de Protección de Datos estará sometida a la fiscalización de la Contraloría General de la República, en lo que concierne al examen y juzgamiento de sus cuentas.

**Título VII: De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades**

**Párrafo Primero:**

**De las infracciones y sus sanciones**

**Artículo 40.- Responsabilidad.**

Cuando el responsable de datos que es una persona natural o jurídica de derecho privado, infrinja en sus operaciones de recolección, tratamiento, almacenamiento, comunicación o cesión de datos personales, los principios, deberes u obligaciones establecidos en esta ley, será sancionado de conformidad con las normas del presente Título.

**Artículo 41.- Infracciones.**

Las infracciones a los principios, deberes u obligaciones establecidos en esta ley se califican, atendida su gravedad, en leves, graves y gravísimas.

Serán consideradas infracciones leves las siguientes:

a) El incumplimiento total o parcial del deber de información y transparencia

b) Comunicar, transmitir o ceder datos personales sin dar cumplimiento a los requisitos establecidos en la ley, salvo la falta de consentimiento del titular

c) No disponer de una dirección de correo electrónico o de un medio electrónico equivalente, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos

d) No responder o responder fuera de plazo, las solicitudes formuladas por el titular de conformidad a esta ley

e) No informar o remitir a la Dirección Nacional de Protección de Datos las comunicaciones previstas en esta ley o en sus reglamentos

f) No efectuar la inscripción o las actualizaciones en el Registro Nacional de Responsables de Datos

g) Cometer cualquier otra infracción a los principios, deberes u obligaciones establecidas en esta ley, que no sea calificada como grave o gravísima

Serán consideradas infracciones graves las siguientes:

a) Recolectar o tratar, a sabiendas, datos personales sin contar con el consentimiento previo del titular de datos o sin la habilitación legal correspondiente o tratarlos con una finalidad distinta de aquella para la cual fueron recolectados

b) Comunicar, transmitir o ceder datos personales sin el consentimiento del titular o cederlos para un fin distinto del autorizado por el titular

c) Vulnerar en las operaciones de tratamiento de datos que realice, en forma manifiesta, los principios de calidad, seguridad y responsabilidad

d) Realizar tratamiento de datos personales sensibles y de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley

e) Vulnerar el deber de reserva o confidencialidad establecido en el artículo 14

f) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación u oposición por parte del titular

g) No adoptar las medidas de seguridad que resulten adecuadas, necesarias y oportunas para el tratamiento de datos y que se encuentren previstas en esta ley, en el reglamento respectivo o en las instrucciones generales de la Dirección Nacional de Protección de Datos

h) No efectuar las comunicaciones o no realizar los registros correspondientes en los casos de vulneración de las medidas de seguridad, según lo establecido en el artículo 14 quáter

i) Realizar en forma reiterada operaciones de transmisión internacional de datos en contravención a las normas previstas en esta ley

j) Adoptar, en forma reiterada o manifiestamente, medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones

k) No dar cumplimiento a las instrucciones específicas y directas que le haya impartido la Dirección Nacional de Protección de Datos

Serán consideradas infracciones gravísimas las siguientes:

a) Efectuar tratamiento de datos personales de manera manifiestamente fraudulenta o engañosa y en perjuicio de los titulares de esos datos

b) Comunicar, transmitir o ceder a terceros, a sabiendas, datos personales sensibles sin el consentimiento del titular y en contravención a las normas dispuestas en el Párrafo Segundo del Título II de esta ley

c) Destinar maliciosamente los datos personales recolectados o tratados a una finalidad distinta de la prevista en la ley que autoriza su tratamiento, causando perjuicio o menoscabo al titular

d) Comunicar, transmitir o ceder a terceros, a sabiendas, información no veraz, incompleta, inexacta o desactualizada del titular de datos, ocasionándole perjuicio o menoscabo

e) Vulnerar en forma reiterada el deber de guardar secreto o reserva sobre datos personales sensibles y datos relativos a sanciones penales y/o administrativas

f) No adoptar las medidas de seguridad adecuadas, necesarias y oportunas para el tratamiento de datos personales sensibles previstas en esta ley o establecidas en las instrucciones generales de la Dirección Nacional de Protección de Datos

g) No comunicar oportunamente, habiendo estado en conocimiento de ello y disponiendo de los medios para hacerlo, la vulneración de la medidas de seguridad que puedan afectar la integridad de los datos personales, causando perjuicio a los titulares de los mismos

h) No haber adoptado las medidas adecuadas y suficientes, por falta de diligencia o cuidado, para evitar que en el tratamiento de datos exclusivamente con fines históricos, estadísticos, científicos y de estudios o de investigaciones, se tomen decisiones, medidas o acciones en perjuicio del titular de los datos

**Artículo 42.- Sanciones.**

Las infracciones en que incurran los responsables de datos serán sancionadas de la siguiente forma

1.- Las infracciones leves serán sancionadas con amonestación escrita o multa de 10 a 100 unidades tributarias mensuales

2.- Las infracciones graves serán sancionadas con multa de 101 a 1.000 unidades tributarias mensuales

3.- Las infracciones gravísimas serán sancionadas con multa de 1.001 a 10.000 unidades tributarias mensuales

**Artículo 43.- Determinación del monto de las multas.**

La cuantía de la multa, dentro del rango respectivo asignado para cada tipo de infracción, será determinada teniendo en cuenta los siguientes criterios

a) La conducta realizada por el responsable y la naturaleza de la infracción

b) Si el infractor es persona natural o jurídica

c) En el caso de las empresas se deberá tener en cuenta el monto de las ventas de la empresa infractora conforme a lo dispuesto en la ley Nº 20.416 o el número de trabajadores de la empresa según lo establecido en el artículo 505 bis del Código del Trabajo

d) El perjuicio producido con motivo de la infracción, especialmente el número de titulares de datos que se vieron afectados

e) Los beneficios obtenidos por el responsable a consecuencia de la infracción

f) La conducta anterior del responsable, la reiteración de los hechos y el carácter continuado de la infracción

g) La existencia de circunstancias atenuantes de responsabilidad

En caso que exista reiteración o reincidencia, podrá aplicarse una multa de hasta tres veces el monto señalado en el artículo anterior, según corresponda al tipo de infracción

Se entenderá que hay reiteración o reincidencia, cuando existan dos o más sanciones ejecutoriadas impuestas en virtud de la presente ley en un período inferior a 12 meses

En caso que se verifique la concurrencia de dos o más infracciones de la misma naturaleza, se aplicará la sanción correspondiente a la infracción más grave, estimándose los hechos constitutivos de una sola infracción. Si atendida la naturaleza y gravedad de las infracciones, éstas no pueden estimarse como una sola, se acumularán las sanciones correspondientes a cada una de las infracciones concurrentes.

La Dirección Nacional de Protección de Datos llevará un registro de sanciones en el que se consignará la individualización del infractor y los demás antecedentes de quienes hayan sido objeto de la aplicación de alguna de las sanciones prevista en este Párrafo y la conducta infraccionada

**Artículo 44.- Atenuantes de responsabilidad.**

Se consideran circunstancias atenuantes de responsabilidad las acciones unilaterales y los acuerdos de reparación convenidos entre el responsable y el o los titulares de datos afectados.

Asimismo, constituyen una atenuante de responsabilidad la conducta anterior y la colaboración que preste el responsable de datos en la investigación administrativa que practique la autoridad competente.

Si el infractor detecta que ha cometido o está cometiendo una infracción a los principios, deberes u obligaciones que establece esta ley, podrá autodenunciarse ante la Dirección Nacional de Protección de Datos. En esa misma oportunidad deberá comunicar las medidas adoptadas para el cese de los hechos que originaron la infracción o las medidas de mitigación, según corresponda. La autodenuncia será considerada como una atenuante calificada de responsabilidad

También actuará como una atenuante calificada, cuando el responsable acredite haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento, lo que se verificará con el certificado expedido de acuerdo al artículo 57 de esta ley.

**Artículo 45.- Sanciones accesorias.**

En caso que se impongan multas por infracciones graves o gravísimas reiteradas y existan circunstancias calificadas, la Dirección Nacional de Protección de Datos podrá disponer la suspensión de las operaciones de recolección o tratamiento de datos por parte del responsable de datos, hasta por un término de 30 días.

Durante el período de suspensión, el responsable de datos deberá adoptar las medidas necesarias a objeto de adecuar sus operaciones de tratamiento de datos a las exigencias establecidas en la presente ley, de acuerdo a lo dispuesto en la resolución que ordenó la suspensión.

Si el responsable de datos no da cumplimiento a lo dispuesto en la resolución de suspensión, esta medida se podrá prorrogar por otros 30 días, hasta completar un período máximo de 6 meses de suspensión. De persistir el incumplimiento, el responsable no podrá volver a desarrollar actividades de recolección o tratamiento de datos personales.

**Artículo 46.- Pago de las Multas.**

Las multas impuestas por la Dirección Nacional de Protección de Datos serán comunicadas una vez ejecutoriadas, a la Tesorería General de la República para su cobro y ejecución.

**Artículo 47.- Prescripción.**

Las acciones para sancionar las infracciones descritas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción

Las medidas que se determinen para corregir o sancionar una infracción a la presente ley, prescriben en dos años, contados desde la fecha en que la resolución que establece la medida o impone la sanción quede ejecutoriada.

Las acciones civiles que deriven de una infracción a la presente ley, prescribirán en el plazo de dos años, contados desde que se encuentre ejecutoriada la resolución administrativa o la sentencia judicial, según sea el caso, que imponga la multa respectiva

Párrafo Segundo: De los procedimientos administrativos

**Artículo 48.- Procedimiento de reclamación administrativa.**

El titular podrá presentar una reclamación ante la Dirección Nacional de Protección de Datos, cuando el responsable de datos que sea una persona natural o jurídica de derecho privado, le haya denegado, en forma expresa o tácita, una solicitud de acceso, rectificación, cancelación u oposición.

Asimismo, el titular de datos podrá presentar una reclamación ante la misma Dirección Nacional de Protección de Datos, por actos u omisiones arbitrarias o ilegales del responsable de datos que signifiquen una afectación de los derechos que le reconoce esta ley.

Cualquiera de estas reclamaciones se tramitará conforme a las siguientes reglas

a) El titular deberá presentar su reclamo dentro del plazo de 10 días contado desde que reciba la respuesta negativa del responsable de datos o haya vencido el plazo que disponía el responsable para responder el requerimiento formulado por el titular. Cuando se trate de un acto o de una omisión arbitraria o ilegal del responsable de datos, el plazo se contará desde la ejecución del acto o de la omisión, o desde que el titular haya tomado conocimiento del mismo

b) El reclamo deberá presentarse por escrito, a través de los medios electrónicos dispuestos por la Dirección Nacional de Protección de Datos en su página Web. En el reclamo el titular deberá señalar la decisión impugnada o el acto u omisión en contra del cual se presenta, según corresponda. El titular deberá acompañar todos los antecedentes en que se funda su reclamación. Deberá señalar, también, una dirección de correo electrónico donde se practicarán las notificaciones

c) Recibido el reclamo, la Dirección Nacional de Protección de Datos dispondrá de un plazo de 3 días para determinar si el reclamo cumple con los requisitos establecidos en las letras anteriores. En caso que declare inadmisible la reclamación, la resolución de la Dirección Nacional deberá ser fundada y se notificará al titular

d) Acogido el reclamo a tramitación, la Dirección Nacional de Protección de Datos notificará al responsable de datos, quien dispondrá de un plazo de 10 días para responder la reclamación, acompañando todos los antecedentes que estime pertinentes. Las notificaciones que se practiquen al responsable se realizarán a la dirección de correo electrónico señalada en la letra e) del artículo 14 bis

e) Vencido este plazo, haya o no contestado el responsable de los datos, y sólo si existen hechos sustanciales, pertinentes y controvertidos, se abrirá un término probatorio de 7 días en el cual las partes podrán hacer valer todos los medios de prueba que estimen convenientes

f) El responsable de datos en su respuesta podrá allanarse a la reclamación, en cuyo caso deberá acompañar los antecedentes o testimonios que acrediten esta circunstancia. Verificado lo anterior y notificado el titular de datos, la Dirección Nacional Protección de Datos procederá al archivo de los antecedentes

g) La Dirección Nacional de Protección de Datos tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Podrá, asimismo, instar a las partes a alcanzar un acuerdo

h) La resolución del reclamo deberá dictarse por la Dirección Nacional de Protección de Datos dentro del plazo de 10 días desde recibida la respuesta del responsable de datos o desde el vencimiento de este plazo en caso que no haya respondido, o desde el término del probatorio, según corresponda. La resolución que rechace el reclamo deberá ser fundada

i) En contra de esta resolución sólo procederá el recurso de reposición, el que deberá ser interpuesto dentro del plazo de 3 días contado desde su notificación. La resolución que resuelva el recurso de reposición deberá dictarse en el plazo de 5 días y será reclamable judicialmente dentro del plazo de 15 días, a través del procedimiento establecido en el artículo 50

j) La interposición del reclamo administrativo suspenderá las operaciones de tratamiento de los datos personales que son objeto de la reclamación

Todos los plazos establecidos en este procedimiento serán de días hábiles

**Artículo 49.- Procedimiento sancionatorio.**

La determinación de las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios, deberes u obligaciones establecidas en esta ley y la aplicación de las sanciones correspondientes, se sujetarán a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Dirección Nacional de Protección de Datos

b) La Dirección Nacional de Protección de Datos podrá iniciar un procedimiento sancionatorio como resultado de un proceso de fiscalización o a consecuencia de una reclamación presentada por un titular de datos en virtud del procedimiento establecido en el artículo 48 de esta ley

c) La Dirección deberá presentar una formulación de cargos en contra del responsable de datos en que describa los hechos que configuran la infracción, los principios, deberes u obligaciones incumplidos o vulnerados por el responsable, las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación

d) La formulación de cargos deberá notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra e) del artículo 14 bis y por carta certificada despachada al domicilio registrado ante la Dirección Nacional o aquel en que habitualmente ejerce sus actividades. Las notificaciones se entenderán practicadas a contar del tercer día siguiente al de ingreso de la carta en la oficina de Correos correspondiente al domicilio del notificado

e) El responsable de datos tendrá un plazo de 10 días para presentar sus descargos. En esta oportunidad podrá acompañar todos los antecedentes que estime pertinente para desacreditar los hechos imputados. Junto con los descargos, el responsable deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las comunicaciones y notificaciones

f) Recibidos los descargos o transcurrido el plazo otorgado para ello, el Director Nacional podrá abrir un término probatorio de 7 días, en el caso que existan hechos sustanciales, pertinentes y controvertidos

g) La Dirección Nacional de Protección de Datos dará lugar a las medidas o diligencias probatorias que solicite el responsable en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo deberá fundar su resolución

h) Los hechos investigados y las responsabilidades de los presuntos infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica

i) La Dirección Nacional de Protección de Datos tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución

j) La resolución que ponga fin al procedimiento sancionatorio será fundada y resolverá todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el responsable de datos, y contendrá la declaración de haberse configurado el incumplimiento o vulneración de los principios, deberes u obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que se haya verificado la infracción, en la misma resolución se ponderarán las circunstancias que agravan o atenúan la responsabilidad del infractor y se establecerá la sanción de acuerdo a la gravedad de la infracción. Esta resolución deberá dictarse dentro de los 20 días siguientes desde recibidos los descargos o desde el vencimiento de este plazo en caso que el responsable no haya respondido, o desde el término del probatorio, según corresponda

k) La resolución que ponga fin al procedimiento sancionatorio será fundada y resolverá todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el responsable de datos, y contendrá la declaración de haberse configurado el incumplimiento o vulneración de los principios, deberes u obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que se haya verificado la infracción, en la misma resolución se ponderarán las circunstancias que agravan o atenúan la responsabilidad del infractor y se establecerá la sanción de acuerdo a la gravedad de la infracción. Esta resolución deberá dictarse dentro de los 20 días siguientes desde recibidos los descargos o desde el vencimiento de este plazo en caso que el responsable no haya respondido, o desde el término del probatorio, según corresponda

l) En contra de esta resolución sólo procederá el recurso de reposición que deberá ser interpuesto dentro del plazo de 5 días, contado desde la notificación respectiva. La resolución que resuelva el recurso de reposición deberá dictarse en el plazo de 10 días y será reclamable judicialmente dentro del plazo de 15 días, a través del procedimiento establecido en el artículo siguiente

m) En todo lo no previsto en este artículo se aplicarán supletoriamente y en lo que corresponda la ley Nº 19.880, que establece bases de los procedimientos administrativos que rigen la actuación de los órganos de la Administración del Estado

Todos los plazos establecidos en este procedimiento serán de días hábiles

**Párrafo Tercero: del procedimiento judicial**

**Artículo 50.- Procedimiento de reclamación judicial**

Las personas naturales o jurídicas afectadas por una resolución de la Dirección Nacional de Protección de Datos podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los 15 días siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, finalmente, cuando procediere, las razones por las cuales el acto le perjudica

b) El titular de datos o el responsable de los mismos, según corresponda, podrán hacerse parte en el respectivo reclamo de conformidad a las normas generales

c) La Corte podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente. Asimismo, podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior

d) Recibida la reclamación, la Corte requerirá de informe a la Dirección Nacional de Protección de Datos, concediéndole un plazo de diez días al efecto

e) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil

f) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla

g) Si la Corte da lugar al reclamo, en su sentencia decidirá u ordenará, según sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda

h) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá confirmar la resolución impugnada, desechar la infracción, dejar sin efecto la sanción impuesta o modificarla

i) En todo aquello que no estuviere regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda

Párrafo Cuarto: De la responsabilidad administrativa de los órganos de la Administración del Estado y de sus agentes

**Artículo 51.- Responsabilidad administrativa del jefe superior del órgano público.**

Si un órgano de la Administración del Estado efectúa tratamiento de datos personales con infracción a las normas establecidas en el Título IV de esta ley, el jefe superior de dicho órgano será sancionado con una multa de 20% a 50% de su remuneración mensual.

Si el órgano de la Administración del Estado persiste en la infracción, se le aplicará al jefe superior del órgano el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días.

Las infracciones a los principios, deberes u obligaciones establecidos en esta ley por parte del órgano público, serán determinadas por la Dirección Nacional de Protección de Datos.

Las sanciones señaladas en los incisos anteriores serán aplicadas por la Contraloría General de la República, previa instrucción de una investigación sumaria o de un sumario administrativo, de acuerdo a las normas de su ley orgánica. El procedimiento administrativo correspondiente podrá ser iniciado directamente por la Contraloría General de la República o a requerimiento de la Dirección Nacional de Protección de Datos

Asimismo, las sanciones previstas en este artículo deberán ser publicadas en el sitio Web de la Dirección Nacional de Protección de Datos y del respectivo órgano o servicio, dentro del plazo de cinco días hábiles, contados desde que la respectiva resolución quede a firme.

**Artículo 52.- Responsabilidad del funcionario infractor.**

Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento de investigación sumaria o en el sumario administrativo respectivo, se determinan eventuales responsabilidades individuales de uno o más funcionarios del órgano público, la misma Contraloría General de la República iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios.

En caso que se determine que cualquiera de estos funcionarios es responsable de alguna de las infracciones graves o gravísimas señaladas en el artículo 41, ellas se considerarán una falta grave a la probidad administrativa. Asimismo, se podrá multar a estos funcionarios por hasta el doble del beneficio pecuniario obtenido mediante su infracción. En el evento de que no sea posible determinar el beneficio económico obtenido por los infractores, se podrán aplicar multas hasta por una suma equivalente al 50% de la remuneración mensual.

**Artículo 53.- Deber de los funcionarios de reserva y confidencialidad**

Los funcionarios de los órganos públicos que traten datos personales y especialmente, cuando se refiera a datos personales sensibles, deberán guardar reserva y secreto de la información de que tomen conocimiento y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones y competencias del órgano respectivo o utilizarla en beneficio propio o de terceros. Para efectos de lo dispuesto en el inciso segundo del artículo 125 de la ley N° 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2005, del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.

**Párrafo Quinto: de la Responsabilidad Civil**

**Artículo 54.- Norma general**

El responsable de datos deberá indemnizar el daño patrimonial y moral que cause al o los titulares, cuando en sus operaciones de tratamiento de datos infrinja los principios, deberes u obligaciones establecidos en esta ley y les cause perjuicio, sin perjuicio de los demás derechos que concede esta ley al o los titulares.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Dirección Nacional de Protección de Datos o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo judicial y se tramitará de conformidad a las normas generales del Código de Procedimiento Civil.

**Párrafo sexto: Modelo de prevención de infracciones**

**Artículo 55.- Modelo de prevención de infracciones.**

El responsable de datos podrá adoptar un modelo de prevención de infracciones que deberá contener, a lo menos, los siguientes elementos:

1. Designación de un encargado de prevención.

2. Definición de medios y facultades del encargado de prevención. El responsable de datos deberá disponer que el encargado de prevención disponga de los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

3. Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

a) La identificación del tipo de información que la entidad recolecta o trata, el ámbito jurisdiccional en que opera, el tipo de datos que almacena y el o los lugares donde residen los titulares cuya información se recolecta o trata.

b) La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en el artículo 41.

c) El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones.

d) Mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley.

e) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

4. Supervisión y certificación del modelo de prevención de infracciones.

La regulación interna a que dé lugar la implementación del modelo y del programa, en su caso, deberán 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 personales o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de la misma, o bien, como una obligación del reglamento interno del que trata el artículo 153 y siguientes del Código del Trabajo. En este último caso, se deberán realizar las medidas de publicidad establecidas en el artículo 156 de ese mismo cuerpo legal

**Artículo 56.- Certificación, registro, supervisión del modelo de prevención de infracciones y reglamento.**

La Dirección Nacional de Protección de Datos será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúne los requisitos y elementos establecidos en la ley y su reglamento, y supervisarlos.

La Dirección Nacional creará un registro público en que consten las entidades que posean una certificación y aquellas cuya certificación sea revocada.

Un reglamento dictado por el Ministerio de Hacienda y suscrito por el Ministro Secretario General de la Presidencia y de Economía, Fomento y Turismo, establecerá los requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión de los modelos de prevención de infracciones y los programas de cumplimiento.

**Artículo 57.- Atenuante especial por prevención de infracciones.**

Los responsables de datos que incurran en alguna de las infracciones previstas en el artículo 41, podrán atenuar su responsabilidad si acreditan haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales bajo su responsabilidad o tratamiento.

Se considerará que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, los responsables o encargados del tratamiento de datos personales hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir la infracción cometida, lo que deberá constar en un certificado emitido por la Dirección Nacional de Protección de Datos.

**Artículo 58.- Vigencia de los certificados.**

Los certificados expedidos por la Dirección Nacional de Protección de Datos tendrán una vigencia de dos años. Sin perjuicio de lo anterior, quedarán sin efecto en los siguientes casos:

a) Por revocación efectuada por la Dirección Nacional de Protección de Datos

b) Por fallecimiento del responsable de datos en caso de tratarse de una persona natural o por disolución de la persona jurídica

c) Por resolución judicial ejecutoriada

d) Por cese voluntario de la actividad del responsable de datos o de quien realice el tratamiento de los mismos

El término de vigencia de un certificado por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro

**Artículo 59.- Revocación de la certificación**

La Dirección Nacional de Protección de Datos podrá revocar la certificación o indicada en los artículos precedentes, si el responsable no da cumplimiento a lo establecido en este Párrafo. Con este objeto, la Dirección Nacional podrá requerir toda aquella información que fuere necesaria para el ejercicio de sus funciones.

Los responsables podrán exceptuarse de entregar la información solicitada cuando la misma esté amparada por una obligación de secreto o reserva, debiendo acreditar dicha circunstancia.

Para el caso de incumplimiento de la entrega de información requerida, así como la entrega de información falsa, incompleta o manifiestamente errónea, será sancionado en conformidad con esta ley.

Con todo, para el caso que el certificado haya sido revocado por la Dirección Nacional, para volver a solicitarlo se deberá acreditar fehacientemente que la causal que dio origen a su revocación ha sido subsanada

**Título Final**

**Artículo 60.- Reglamentos.**

Sin perjuicio de los reglamentos específicos que se señalan en el texto de esta ley, a través de uno o más reglamentos del Ministerio de Hacienda y suscritos por el Ministro Secretario General de la Presidencia, se establecerán las normas de ejecución de la presente ley, en todas aquellas materias necesarias para su aplicación. Asimismo, a través de uno o más reglamentos emanados de las mismas autoridades, se regularán, especialmente, la forma, requisitos y procedimientos para la implementación de los sistemas biométricos; los plazos, forma, operación e inscripción en el Registro Nacional de Responsable de Datos y los mecanismos de actualización del registro; y, las modalidades y procedimientos para determinar los registros y las bases de datos que tienen una finalidad doméstica.

ARTÍCULOS TRANSITORIOS

Artículo primero transitorio.

La presente ley entrará en vigencia el día primero del mes diecinueve posterior a su publicación en el Diario Oficial, sin perjuicio de las excepciones que se establecen en las normas siguientes

Artículo segundo transitorio.

Las normas relativas a la obligación de registro de los responsables de datos entrarán en vigencia el día primero del mes trece posterior a la instalación de la Dirección Nacional de Protección de Datos

Artículo tercero transitorio.

Dentro de los nueve meses siguientes a la fecha de publicación de la presente ley, deberán dictarse los reglamentos referidos en sus artículos…