Boletín N° 11. 144 -07

Proyecto de ley, iniciado en mensaje de S. E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

MENSAJE Nº 001-365/

Honorable Senado:

Tengo el honor de someter a vuestra consideración el siguiente proyecto de ley que regula la protección y el tratamiento de los datos personales.

1. ANTECEDENTES GENERALES

2. Desarrollo de la economía digital

En muchos sentidos el Siglo XXI representa el inicio de una nueva era. No sólo porque desde una perspectiva convencional y temporal marca el punto de partida del nuevo milenio, sino también porque en lo que va transcurrido de él se han sucedido cambios y transformaciones sociales, culturales y tecnológicas de extraordinaria envergadura. La mayor de estas transformaciones se puede sintetizar en el proceso de transición desde la sociedad industrial a la sociedad digital.

La sociedad digital ha expandido los espacios de libertad, autonomía y desarrollo de las personas, pero también ha diseñado nuevos y sofisticados sistemas de control y vigilancia que amenazan o limitan esa misma libertad. Parte importante de los desafíos que actualmente enfrentan las sociedades y los gobiernos es crear reglas de conducta que permitan organizar las transformaciones en la sociedad digital. Se trata de diseñar instituciones, marcos normativos e incentivos que permitan generar convergencias entre la información personal y su uso, entre las libertades individuales y el interés público, entre la vida privada y la información pública, entre la interconexión global y las identidades locales, entre la tecnología y la humanidad.

La sociedad del conocimiento y la información han dado paso a una nueva economía: la economía digital. La inserción de los países a esta nueva realidad exige la adaptación de sus regulaciones, prácticas, instituciones y la organización industrial y productiva de las empresas al uso generalizado de las tecnologías de la información.

La expansión de la economía digital tiene evidentes efectos positivos para el bienestar de los ciudadanos. Entre otras cosas, es amigable con el medio ambiente, genera eficiencias en la asignación de recursos, posibilita la creación de nuevos negocios y aumenta la satisfacción de los consumidores.

Las barreras que enfrenta un desarrollo más vigoroso de la economía digital vienen dadas por restricciones en el acceso y uso de las nuevas tecnologías de la información y en la existencia de hábitos y prácticas culturales que enfatizan el uso de sistemas análogos por sobre los sistema digitales. Pero más aún, se alimenta en la desconfianza de los consumidores respecto de la seguridad relativa al cumplimiento de los requisitos de autenticidad, integridad y confidencialidad de las operaciones y sus registros, y en la falta de un marco normativo adecuado y de instituciones eficaces para sancionar las infracciones y resolver las controversias.

Otra restricción importante se encuentra en la configuración de los mercados y en la conducta de los agentes económicos. Muchas empresas mantienen rentas ancladas en prácticas que no son compatibles con sistemas abiertos, competitivos y transparentes propios de una sociedad y de una economía digital. En esta nueva era las empresas exitosas son aquellas que valoran el conocimiento, la información, la innovación y la competencia.

Chile es una economía pequeña y abierta al mundo. Las empresas chilenas se han insertado competitivamente en la economía global y el país es un destino atractivo para las inversiones extranjeras.

Sin embargo, para que Chile mantenga e incremente su trayectoria de desarrollo y crecimiento económico, es necesario, tal como lo ha venido planteando la OCDE en sus recomendaciones, emprender cambios y transformaciones que permitan avanzar hacia una economía más innovadora, basada en el conocimiento e integrada por más empresas que sean capaces de competir a nivel mundial y participar en las cadenas globales de valor, especialmente en el ámbito de los servicios globales.

Una de las mayores deudas en materia regulatoria es la falta de una legislación moderna y flexible que permita cumplir las normas y estándares internacionales en materia de protección y tratamiento de los datos personales.

3. Contexto internacional

Desde el año 2010, Chile es parte de la Organización para la Cooperación y el Desarrollo Económico (OCDE). El ingreso de nuestro país a dicha organización implicó esfuerzos significativos para lograr la adaptación de las políticas públicas y la legislación interna a las recomendaciones que emanan de esa organización, en materia social y económica.

En este sentido, este proyecto de ley recoge las recomendaciones que la propia organización ha puesto a disposición de los países miembros. Entre ellas, destacan las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. Estos instrumentos dan cuenta de los principios y contenidos básicos que deben recoger las normativas internas de los países para asegurar el respeto a la privacidad y la protección de los datos personales.

Las orientaciones de la OCDE relativas al flujo transfronterizo de datos personales es una materia de particular relevancia en este proyecto, dado el acelerado intercambio de información, la expansión del comercio electrónico y el desarrollo de la economía digital. Chile en la actualidad no cuenta con normas en esta materia y su incorporación resulta clave para el desarrollo de mercados emergentes de la economía como la exportación de servicios.

4. DERECHO FUNDAMENTAL A LA VIDA PRIVADA Y SU PROTECCIÓN

La Constitución Política de la República garantiza el derecho fundamental a la vida privada y su protección. A su vez, la Declaración Universal de los Derechos Humanos de las Naciones Unidas prescribe que nadie sufrirá injerencias arbitrarias en su vida privada, su familia, domicilio o correspondencia, ni ataques a su honra o reputación. La Convención Americana sobre Derechos Humanos, denominada "Pacto de San José de Costa Rica", por su parte consagra la protección de la honra y la dignidad de la persona, prohibiendo injerencias arbitrarias en su vida privada.

Consistente con el marco constitucional y los tratados internacionales ratificados por Chile, el año 1999 se dictó la ley N° 19.628, sobre protección de la vida privada, que establece las normas que actualmente regulan la protección y el uso de los datos de carácter personal de las personas naturales, tanto en sus aspectos sustantivos como procedimentales.

Si bien dicha ley constituyó un gran avance al momento de su dictación, es un hecho indiscutido que el acelerado desarrollo tecnológico, la masificación en el uso de las tecnologías de la información, el extendido acceso a internet, la expansión del comercio electrónico, unido a los nuevos desafíos que enfrentan las sociedades y los Estados para reconocer y proteger los derechos de sus ciudadanos, han llevado a que esta normativa haya terminado siendo insuficiente.

La obsolescencia de algunos de sus criterios u orientaciones y la ausencia de una autoridad de control que den eficacia a la ley, son parte de un diagnóstico en el que existe un amplio consenso entre los actores políticos e institucionales, agentes económicos, medios de comunicación social y la ciudadanía en general.

Este diagnóstico compartido se ha expresado en diversas propuestas e iniciativas orientadas a poner de manifiesto la necesidad de impulsar un nuevo marco regulatorio.

En la actualidad existen más de 60 iniciativas legales en tramitación, originadas mayoritariamente en mociones parlamentarias, que se refieren a estas materias, todas las cuales fueron consideradas en la elaboración del presente proyecto de ley. Asimismo, durante el mes de agosto de 2016, la Unidad de Evaluación de la Ley de la Cámara de Diputados presentó un informe en que evaluó los impactos y desafíos de la ley N° 19.628 y formuló un conjunto de conclusiones y recomendaciones, muchas de las cuales fueron recogidas en esta propuesta.

El Poder Judicial también ha sido un actor relevante en este proceso. La Corte Suprema ha contribuido a la reflexión jurídica y al debate doctrinario en torno a la garantía, protección y equilibrio de los diversos derechos fundamentales que entran en juego en este ámbito: vida privada, intimidad, honra, libertad de opinión e información, acceso a la información y transparencia, entre otros.

Por último, también han aportado a este debate el sector privado, las organizaciones empresariales, los académicos, la sociedad civil y la ciudadanía. En particular, es importante destacar las contribuciones técnicas realizadas por el Consejo de la Sociedad Civil de Economía Digital y la Mesa Público Privada de Protección de Datos.

En consecuencia, este proyecto de ley busca balancear y equilibrar las diferentes miradas y opciones técnicas, económicas, jurídicas y políticas que se promueven por los diversos actores, instituciones y grupos de interés que participan de este debate, proponiendo un marco regulatorio que proteja los derechos y libertades de las personas, garantice el tratamiento lícito de los datos personales por parte de terceros, sin entrabar ni entorpecer la libre circulación de la información y, en definitiva, se alcance una legislación moderna y flexible que permita enfrentar los desafíos del país de cara al Siglo XXI.

5. OBJETIVOS DEL PROYECTO DE LEY

1. Objetivo general

Este proyecto de ley tiene como objetivo general actualizar y modernizar el marco normativo e institucional con el propósito de establecer que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular de datos o en los casos que autorice la ley, reforzando la idea de que los datos personales deben estar bajo la esfera de control de su titular, favoreciendo su protección frente a toda intromisión de terceros y estableciendo las condiciones regulatorias bajo las cuales los terceros pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

De esta forma, el principal desafío regulatorio es equilibrar la protección de los derechos de las personas, especialmente el respeto y protección a la vida privada e intimidad, con la libre circulación de la información, asegurando que las reglas de autorización y uso que se establezcan no entraben ni entorpezcan el tratamiento lícito de los datos por parte de las personas, organismos y empresas.

2. Objetivos específicos

En cuanto a los objetivos específicos de este proyecto de ley, se plantean los siguientes:

a. Establecer las condiciones regulatorias que permitan reforzar los derechos de los titulares de datos personales en relación a las operaciones de tratamiento de datos que legítimamente efectúen los agentes privados y públicos.

b. Dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales.

c. Incrementar los estándares legales de Chile en el tratamiento de datos personales para transformarlo en un país con niveles adecuados de protección y seguridad, promoviendo el desarrollo de la economía digital y favoreciendo la expansión del mercado de los servicios globales.

d. Definir estándares regulatorios, condiciones operacionales y un marco institucional que legitime el tratamiento de los datos personales por parte de los órganos públicos, garantizando el cumplimiento de la función pública y los derechos de los ciudadanos.

e. Contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales.

3. CONTENIDO DEL PROYECTO

1. Determinación precisa del ámbito regulatorio

El objeto de la ley es regular el tratamiento de los datos personales, asegurando el respeto y protección de los derechos y libertades fundamentales de los titulares de datos (personas naturales), en particular el derecho a la vida privada.

El ámbito de aplicación de la ley es todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial. Al mismo tiempo, se establece el carácter supletorio de esta normativa para todos aquellos tratamientos de datos regulados en leyes especiales.

Se excluyen expresamente de este régimen regulatorio al tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes especiales dictadas de conformidad al numeral 12 del artículo 19 de la Constitución Política de la República, y el tratamiento que efectúen las personas naturales en relación con sus actividades personales.

Además, cabe señalar que este proyecto de ley no innova respecto de la regulación específica y actualmente vigente, referida al tratamiento de los datos personales

relativos a obligaciones de carácter económico, financiero, bancario o comercial, manteniendo íntegramente las normas contenidas en el Título III de la ley, salvo adecuaciones formales y de referencia.

2. Principios rectores y actualización de definiciones legales

Se incorporan un conjunto de principios rectores en materia de protección y tratamiento de los datos personales que han sido reconocidos en las directrices de la OCDE y en la legislación comparada. Estos principios constituyen el marco teórico y normativo que inspiran toda la regulación del tratamiento de los datos personales y permiten orientar la aplicación e interpretación doctrinaria y jurisprudencial de esta normativa. Estos principios son la licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información.

En el tratamiento de datos personales por parte de los organismos públicos se incorporan además los principios de coordinación, eficiencia, transparencia y publicidad.

Con el objeto de facilitar a los operadores del sistema la aplicación e interpretación de la ley, se actualizan e incorporan nuevas definiciones legales, adaptándolas a las que se usan en las legislaciones más modernas, las recomendaciones técnicas de los organismos internacionales y el estado actual del arte y la técnica.

3. Reforzamiento y ampliación de los derechos de los titulares de datos

Se reconocen al titular de datos personales los derechos de acceso, rectificación, cancelación y oposición, los denominados “derechos ARCO”. Estos derechos son irrenunciables, gratuitos y no puede limitarse su ejercicio en forma convencional.

El derecho de acceso permite solicitar y obtener confirmación acerca de si sus datos personales están siendo tratados por el responsable y acceder a ellos, en su caso. El derecho de rectificación busca que se modifique o completen los datos cuando sean inexactos o incompletos. El derecho de cancelación persigue que se supriman o eliminen los datos del titular por las causales previstas en la ley. El derecho de oposición permite requerir que no se lleve a cabo un tratamiento de datos determinado por la concurrencia de las causales previstas en la ley.

Con el objeto de asegurar un ejercicio eficaz de los derechos ARCO, se establece un procedimiento directo y eficaz para que cualquier titular de datos pueda recurrir directamente ante el responsable de datos ejerciendo el correspondiente derecho ARCO, permitiéndose bloquear transitoriamente los datos en cuestión. Si el responsable no acoge la solicitud o no responde dentro del plazo que le fija la ley, el titular puede presentar un reclamo ante la autoridad de control. La resolución de la autoridad de control es reclamable ante la Corte de Apelaciones respectiva.

Siguiendo las tendencias regulatorias más modernas se introduce el derecho a la portabilidad de los datos personales, en virtud del cual el titular de datos puede solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos.

Por otro lado y haciéndose cargo de un debate actual, complejo y que exige armonizar diversos bienes sociales, esta propuesta legislativa incorpora y refuerza la regulación del denominado "derecho al olvido" en relación a los datos relativos a infracciones penales, civiles, administrativas y disciplinarias. Se busca contar con una regla que equilibre adecuadamente el derecho de las personas a reducir el acceso a información desfavorable y que afecta su reputación social, con el derecho a la información y el interés público que hay envuelto en el acceso a ella.

4. Consentimiento del titular como la principal fuente de legitimidad del tratamiento de datos

Concordante con el principio que los datos personales deben estar bajo la esfera de control de su titular, se establece el consentimiento como la fuente principal de legitimidad del tratamiento de los datos personales.

El consentimiento del titular debe ser libre, informado, inequívoco, otorgado en forma previa al tratamiento y específico en cuanto a su finalidad o finalidades.

Se consideran excepciones a las regla del consentimiento, tales como cuando la información ha sido recolectada de una fuente de acceso público; cuando sean datos relativos a obligaciones de carácter económico, financiero, bancario o comercial; o cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular.

5. Régimen de responsabilidades de los responsables de datos

Con el objeto de reforzar la legitimidad del tratamiento de datos, se crean una serie de obligaciones y deberes para los responsables de datos, tales como acreditar la licitud del tratamiento que realizan; deberes de información; deberes de reserva y confidencialidad, de información y transparencia, y el deber de adoptar medidas de seguridad y reportar las vulneraciones dichas medidas.

Por otro lado, haciéndose cargo del propósito deliberado de no imponer trabas excesivas a la circulación de información, se establecen estándares diferenciados de cumplimiento de los deberes de información y de seguridad para personas naturales y jurídicas, el tamaño de la empresa y el volumen y las finalidades de los datos que trata.

Se regulan también la cesión o transferencia de las bases de datos personales que disponga o administre el responsable de datos, así como el régimen del tratamiento que efectúa un tercero o mandatario en representación o por encargo del responsable.

Una de las principales innovaciones de esta nueva normativa es la regulación del tratamiento automatizado de grandes volúmenes de datos, o “Big Data”, protegiendo la facultad de control del titular sobre su propia información, pero reconociendo también la licitud del acceso y uso de la información por parte de terceros y particularmente, de las empresas.

6. Nuevos estándares para el tratamiento de datos sensibles y categorías especiales de datos personales

Se eleva el estándar para el tratamiento de los datos sensibles, estableciendo que sólo puede realizarse cuando el titular consienta libre e informadamente, en forma expresa.

Manteniendo la coherencia con el actual modelo normativo, se reconocen excepciones que legitiman el tratamiento de los datos personales sensibles, como cuando el titular ha hecho manifiestamente públicos su dato sensible o cuando exista una situación de emergencia médica o de salud, por ejemplo.

Adicionalmente, se introducen normas especiales para el tratamiento de los datos personales relativos a la salud, los datos biométricos y los datos relativos al perfil biológico humano; para el tratamiento de datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público; y para el tratamiento de los datos personales de geolocalización o de movilidad del titular.

7. Tratamiento de datos personales de niños, niñas y adolescentes

Se establece como regla basal que el tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.

Siguiendo las mejores prácticas de la legislación comparada y las recomendaciones internacionales, se regula en forma diferencia las autorizaciones de tratamiento para los niños y niñas y para los adolescentes. En el caso de los niños y niñas, el tratamiento de datos requiere el consentimiento previo, específico y expreso de quien tiene a su cargo el cuidado personal. Respecto de los adolescentes, se establece que sus datos personales sensibles sólo pueden ser tratados con el consentimiento de quien tiene a su cargo el cuidado personal del adolescente. Para los demás datos personales, rigen las normas generales de autorización.

Consistente con la orientación protectora de los datos personales de los niños, niñas y adolescentes, se establece una obligación especial para los establecimientos educacionales y para las personas o entidades públicas o privadas que traten o administren este tipo de datos, incluyendo a quienes ejercen su cuidado personal, de velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

8. Regulación del flujo transfronterizo de datos personales

El proyecto de ley incorpora una regulación específica para la transferencia internacional de datos personales, ajustándola a los estándares y recomendaciones de la OCDE.

Se distingue entre países que disponen de un marco normativo que proporciona niveles adecuados de protección de datos y aquellos que no, entendiendo que un país posee niveles adecuados de protección de datos cuando cumple con estándares similares o superiores a los fijados en la ley chilena en materia de protección y tratamiento de datos personales. La autoridad de control, siguiendo parámetros técnicos y los estándares de la OCDE, determinará los países que poseen una legislación adecuada.

En el caso de los países adecuados se reconoce amplia autonomía a los intervinientes para transferir datos, sujeto al cumplimiento de las reglas generales. En el caso de países no adecuados, se permite la transferencia de datos sólo en un conjunto de circunstancias que autorizan el envío de la información, bajo la responsabilidad legal de quien efectúa la transferencia de datos y con aviso previo a la autoridad de control.

9. Modernización de estándares para el tratamiento de datos personales por organismos públicos

Siendo la ley una de las fuentes de legitimidad del tratamiento de datos personales, el tratamiento de los datos personales que efectúan los órganos públicos será lícito cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas legales correspondientes. Cumpliéndose esas condiciones, no se requiere el consentimiento del titular.

Con el objeto de evitar flujos innecesarios de los datos personales, pero al mismo tiempo promover la interconectividad y la eficiencia en la gestión pública, se regula la facultad de los órganos públicos para comunicar o ceder datos personales a otros órganos públicos, siempre que la comunicación o cesión de los datos sea necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. Se establece también que pueden comunicar o ceder datos personales cuando se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites o reiteración de requerimientos de información o documentos para los titulares. También se regula la comunicación y cesión de datos a personas o entidades privadas.

Del mismo modo, se consagran y regulan los principios que rigen el tratamiento de los datos personales por parte de los órganos públicos, los derechos que se reconocen a los titulares, la forma de ejercer estos derechos y se define un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos.

Se define un régimen especial de responsabilidades y sanciones para que el tratamiento de datos se realice conforme a los principios y obligaciones establecidos en la ley.

Se regula también un régimen de excepción para el tratamiento de datos protegidos por normas de secreto o confidencialidad; cuando se refiere al tratamiento de datos vinculados a la investigación de infracciones penales, civiles y administrativas; cuando correspondan a actividades relacionadas con la seguridad de la nación, el orden público o la seguridad pública, y cuando en los casos que se hayan declarado estado de catástrofe o estado de emergencia.

Por último, se regulan las actividades de tratamiento de los datos personales que efectúan 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. Se contempla un modelo regulatorio, de fiscalización y cumplimiento compatible con la autonomía de estas instituciones.

10. Creación de una autoridad de control

Para efectos de velar por la protección de los derechos y libertades de las personas titulares de datos y por el adecuado cumplimiento de las normas relativas al tratamiento de los datos, se requiere contar con una autoridad de control dotada de facultades para regular, supervisar, fiscalizar y en última instancia, sancionar los incumplimientos. Sin una autoridad de control con potestades normativas y fiscalizadoras suficientes, la ley tiene escasa eficacia.

Con tal propósito, se crea una institución especializada y de carácter técnico, denominada “Agencia de Protección de Datos Personales, encargada de velar y fiscalizar el cumplimiento de esta normativa, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda y se encuentra afecto al Sistema de Alta Dirección Pública.

Con el objeto de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia, se consagra un modelo de coordinación regulatoria entre ambas instituciones.

11. Modelo general de cumplimiento de la ley

Se contempla un catálogo específico de infracciones a los principios y obligaciones establecidos en la ley, que se califican en leves, graves y gravísimas, estableciendo sanciones correlativas a la gravedad de la infracción que van desde la amonestación escrita a multas que oscilan entre 1 y 5.000 UTM. En casos excepcionales se contempla el cierre o clausura de las operaciones de tratamiento de datos.
La determinación de las infracciones y la aplicación de la sanción respectiva corresponden a la Agencia de Protección de Datos Personales. En el caso de los

órganos públicos y de los agentes de la Administración del Estado, las investigaciones las realiza la Agencia y las sanciones las aplica la Contraloría General de la República.

Se incorpora, asimismo, un procedimiento de reclamación judicial de ilegalidad para cualquier persona natural o jurídica que se vea afectada por una resolución de la Agencia de Protección de Datos Personales, ante la Corte de Apelaciones correspondiente. Para el conocimiento y resolución de estas controversias se establece un procedimiento judicial concentrado y de rápida resolución.

Finalmente, como una forma de incentivar y promover el cumplimiento de la ley, y siguiendo las recomendaciones de la OCDE, se regula la adopción por parte del sector privado y del sector público de modelos de prevención de infracciones, fijando para ellos los estándares y requisitos mínimos con los que deberán cumplir.

La certificación y supervisión de estos programas estará a cargo de la Agencia de Protección de Datos Personales.

12. Disposiciones transitorias

Por último, el proyecto contempla disposiciones transitorias que la ley entrará en vigencia el día primero del mes décimo tercero posterior a su publicación en el Diario Oficial.

Los reglamentos señalados en la ley deberán dictarse dentro de los seis meses posteriores la publicación.

Se establece el plazo de nueve meses para que, mediante uno o más decretos con fuerza de ley, el Presidente de la República regule al personal de la Agencia de Protección de Datos Personales. Dentro de los 60 días siguientes a la publicación de la ley deberá convocarse al concurso público para nombrar al primer director o directora de la Agencia de Protección de Datos Personales.

En mérito de lo expuesto, tengo el honor de someter a vuestra consideración el siguiente

PROYECTO DE LEY:

“Artículo primero.- Introdúcense las siguientes modificaciones a la ley Nº 19.628, sobre protección de la vida privada:

1) Reemplázase el artículo 1 por el siguiente:

“Artículo 1.- Objeto y ámbito de aplicación. La presente ley tiene por objeto regular el tratamiento 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 quienes son titulares de estos datos, en particular, el derecho a la vida privada.

Todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial quedará sujeto a las disposiciones de esta ley. Con todo, en los asuntos no regulados en las leyes especiales se aplicarán supletoriamente las normas de esta ley.

El régimen de tratamiento y protección de los datos personales establecidos en esta ley no se aplicará al tratamiento de datos que realicen los medios de comunicación social en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República, ni al que efectúen las personas naturales en relación con sus actividades personales.”.

2) Modifícase el artículo 2 del siguiente modo:

a) Intercálase el siguiente epígrafe: “Definiciones.”.

b) Reemplázanse las letras c), f), g) e i) por las siguientes:

“c) Comunicación o transmisión de datos personales: dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos. Las comunicaciones que realice el responsable de datos deben contener información exacta, completa y veraz.

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

g) Datos personales sensibles: aquellos datos personales que conciernen o se refieren a las características físicas o morales de una persona, tales como el origen racial, ideología, afiliación política, creencias o convicciones religiosas o filosóficas, estado de salud físico o psíquico, orientación sexual, identidad de género e identidad genética y biomédica.

i) Fuentes de acceso público: todas aquellas bases de datos personales, públicas o privadas, cuyo acceso o consulta puede ser efectuado en forma lícita por cualquier persona, sin existir restricciones o impedimentos legales para su acceso o utilización.

Las dudas o controversias que se susciten sobre si una determinada base de datos es considerada fuente de acceso público serán resueltas por la Agencia de Protección de Datos Personales, quien podrá identificar categorías genéricas, clases o tipos de registros o bases de datos que posean esta condición.”.

c) Elimínase la letra j), pasando la actual letra k) a ser j) y así sucesivamente.

d) Sustitúyense las actuales letras l), m), n), ñ) y o), que pasaron a ser k), l), m), n)

y ñ), respectivamente, por las siguientes:

“k) Proceso de anonimización o disociación: procedimiento en virtud del cual los datos personales no pueden asociarse al titular ni permitir su identificación, por haberse destruido el nexo con toda información que lo identifica o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gasto o trabajo desproporcionados. Un dato anonimizado deja de ser un dato personal.

l) 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 o responsable: persona natural o jurídica, pública o privada, a quien compete decidir acerca del tratamiento de datos personales, con independencia de si los datos son tratados directamente por él o a través de un tercero o mandatario, y de su localización.

n) Titular de datos o titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

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 de cualquier forma los datos personales.”.

e) Agréganse los siguientes literales o), p), q), r), s), t) y u), nuevos:

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

p) Derecho de acceso: derecho del titular de datos a solicitar y obtener del responsable confirmación acerca de si sus datos personales están siendo tratados por él, acceder a ellos en su caso, y a la información prevista en esta ley.

q) Derecho de rectificación: derecho del titular de datos a solicitar y obtener del responsable que modifique o complete sus datos personales, cuando están siendo tratados por él y sean inexactos o incompletos.

r) Derecho de cancelación: derecho del titular de datos a solicitar y obtener del responsable que suprima o elimine sus datos personales, de acuerdo a las causales previstas en la ley.

s) Derecho de oposición: derecho del titular de datos que se ejerce ante el responsable con el objeto de requerir que no se lleve a cabo un tratamiento de datos determinado, de conformidad a las causales previstas en la ley.

t) Derecho a la portabilidad de los datos personales: derecho del titular de datos a solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos.

u) Registro Nacional de Cumplimiento y Sanciones: registro nacional de carácter público administrado por la Agencia de Protección de Datos Personales, que consigna las sanciones impuestas a los responsables de datos por infracción a la ley, los modelos de prevención de infracciones que implementes los responsables y los programas de cumplimiento debidamente certificados.”.

3) Reemplázase el artículo 3 por el siguiente:

“Artículo 3.- Principios. El tratamiento de los datos personales se rige por los siguientes principios:

a) Principio de licitud del tratamiento. Los datos personales sólo pueden tratarse con el consentimiento de su titular o por disposición de la ley.

b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el titular otorgue nuevamente su consentimiento, los datos provengan de fuentes de acceso público o así lo disponga la ley.

c) Principio de proporcionalidad. Los datos personales que se traten deben limitarse a aquellos que resulten necesarios en relación con los fines del tratamiento.

Los datos personales deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser cancelados o anonimizados. Un período de tiempo mayor requiere autorización legal o consentimiento del titular.

d) Principio de calidad. Los datos personales deben ser exactos y, si fuera necesario, completos y actuales, en relación con los fines del tratamiento.

e) Principio de responsabilidad. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a esta ley.

f) Principio de seguridad. En el tratamiento de los datos personales se deben garantizar niveles adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado, pérdida, filtración, destrucción o daño accidental y aplicando medidas técnicas u organizativas apropiadas.

g) Principio de información. Las prácticas y políticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.”.

4) Reemplázase el título I por el siguiente:

“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 de acceso, rectificación, cancelación, oposición y portabilidad 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.

En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos.

Artículo 5.- Derecho de acceso. El titular de datos tiene derecho a solicitar y obtener del responsable confirmación acerca de si los datos personales que le conciernen están siendo tratados por él y, en tal caso, acceder a dichos datos y a la siguiente información:

a) Los datos tratados y su origen.

b) La finalidad o finalidades del tratamiento.

c) Las categorías, clases o tipos de destinatarios a los que se han comunicado o cedido los datos o se prevé comunicar o ceder, según corresponda.

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

El responsable no estará obligado a entregar al titular la información establecida en las letras anteriores cuando el titular ya disponga de esta información por haber ejercido este derecho con anterioridad; cuando su comunicación resulte imposible o requiera de un esfuerzo no razonable; cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana; cuando los datos estén protegidos por una norma de secreto o una obligación de confidencialidad que impida su comunicación, o cuando lo disponga expresamente la ley.

Artículo 6.- Derecho de rectificación. El titular de datos tiene derecho a solicitar y obtener del responsable la rectificación de los datos personales que le conciernen y que están siendo tratados por él, cuando sean inexactos, desactualizados o incompletos.

La rectificación y su contenido serán públicas y deberán difundirse cuando así lo requiera el titular y sea necesario para los fines del tratamiento realizado.

Artículo 7.- Derecho de cancelación. El titular de datos tiene derecho a solicitar y obtener del responsable la cancelación o supresión de los datos personales que le conciernen cuando éstos no resulten necesarios en relación con los fines del tratamiento; cuando haya retirado su consentimiento para el tratamiento y éste no tenga otro fundamento legal; cuando se trate de datos caducos; cuando los datos hayan sido obtenidos o tratados ilícitamente por el responsable o cuando la cancelación deba realizarse para el cumplimiento de una obligación legal.

Sin perjuicio de lo anterior, no procede la cancelación o supresión de los datos en los siguientes casos:

a) Cuando el tratamiento sea necesario para ejercer el derecho a las libertades de emitir opinión y de informar regulado por las leyes a que se refiere el artículo 19 N° 12 de la Constitución Política de la República.

b) Cuando se requiera el tratamiento de los datos para el cumplimiento de una obligación legal o la ejecución de un contrato del que el titular es parte.

c) Cuando existan razones de interés público en el ámbito de la salud pública.

d) Cuando el tratamiento se realice con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, en la medida que la cancelación de los datos imposibilite u obstaculice gravemente el propósito de este tratamiento.

e) Cuando se requieran para la formulación, ejercicio o defensa de una reclamación formulada en el marco de esta ley.

Artículo 8.- Derecho de oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:

a) Cuando el tratamiento de datos afecte sus derechos y libertades fundamentales.

b) Cuando el tratamiento de datos sea utilizado exclusivamente con fines de marketing directo de bienes o servicios, así como cualquier otro propósito comercial o fines publicitarios, salvo que exista un contrato entre las partes que expresamente contemple dicho uso de su información.

c) 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, salvo las excepciones previstas en el artículo 15 ter de esta ley.

d) Cuando el titular de los datos hubiere fallecido. En este caso, la oposición deberá ser formulada por los herederos. Con todo, no procederá la oposición cuando el tratamiento de los datos se realice exclusivamente con fines históricos, estadísticos o científicos o para estudios o investigaciones que atiendan fines de interés público.

Artículo 9.- Derecho a la portabilidad de los datos personales. El titular de datos tiene derecho a solicitar y recibir del responsable una copia de los datos personales que le conciernen de manera estructurada, en un formato genérico y de uso común que permita ser operado por distintos sistemas, y a comunicarlos o transferirlos a otro responsable de datos, cuando concurran las siguientes circunstancias o requisitos:

a) El titular haya entregado sus datos personales directamente al responsable.

b) Se trate de un volumen relevante de datos y sean tratados en forma automatizada.

c) Exista consentimiento del titular para el tratamiento o se requiera para la ejecución o cumplimiento de un contrato.

El responsable debe utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho.

El responsable también debe comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.

Artículo 10.- Forma y medios de ejercer los derechos del titular de datos. Los derechos reconocidos en esta ley se ejercen por el titular, en forma personal o debidamente representado, ante el responsable de datos. Si los datos personales del titular se encuentran en una base de datos que es administrada o tratada por diversos responsables, el titular puede ejercer sus derechos ante cualquiera de ellos.

Los responsables de datos deben implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz. Los medios dispuestos por el responsable deben ser sencillos en su operación.

El ejercicio de los derechos de rectificación, cancelación y oposición siempre serán gratuitos para el titular. El derecho de acceso también se ejercerá en forma gratuita, al menos, trimestralmente.

El responsable de datos sólo puede exigir el pago de los costos directos en que incurra cuando el titular ejerza su derecho de acceso más de una vez en el trimestre o cuando ejerza el derecho a la portabilidad.

La Agencia de Protección de Datos Personales deberá velar por el efectivo ejercicio y cumplimiento de los derechos que esta ley reconoce al titular.

Artículo 11.- Procedimiento ante el responsable de datos. Para ejercer los derechos que le reconoce esta ley, el titular debe presentar una solicitud o requerimiento escrito ante el responsable dirigido a la dirección de correo electrónico establecida para este fin o a través de un formulario de contacto o de un medio electrónico equivalente. La solicitud o el medio de contacto deben contener, a lo menos, las siguientes menciones:

a) Individualización del titular y de su representante legal o mandatario, según corresponda, y autenticación de su identidad de acuerdo a los procedimientos, formas y modalidades que establezca el reglamento.

b) Indicación de una dirección de correo electrónico o de otro medio electrónico equivalente para comunicar la respuesta.

c) Identificación de los datos personales o del tratamiento determinado, según corresponda, respecto de los cuales se ejerce el derecho correspondiente.

d) En las solicitudes de rectificación el titular debe indicar las modificaciones o actualizaciones precisas a realizar y acompañar, en su caso, los antecedentes que las sustenten. Cuando se trate de solicitudes de cancelación u oposición al tratamiento de datos, el titular debe indicar la causal o fundamento invocado para ello y acompañar también los antecedentes que las sustenten, si correspondiere. En el caso del derecho de acceso, basta con la individualización del titular.

e) Cualquier otro antecedente que facilite la localización de los datos personales.

Recibida la solicitud, el responsable debe pronunciarse sobre ella inmediatamente o a más tardar dentro de los 10 días hábiles siguientes a la fecha de ingreso.

El responsable debe responder por escrito al titular a la dirección de correo electrónico fijada por éste. Cuando la respuesta se entregue por otro medio electrónico, el responsable debe almacenar los respaldos que le permitan demostrar la transmisión y recepción de la respuesta, su fecha y el contenido íntegro de ella.
En caso de denegación total o parcial de la solicitud, el responsable debe fundar su decisión indicando la causa invocada y los antecedentes que la justifican. En esta misma oportunidad, el responsable debe señalar al titular que dispone de un plazo de 10 días hábiles para formular una reclamación ante la Agencia de Protección de Datos Personales, de acuerdo al procedimiento establecido en el artículo 45.

Transcurridos los 10 días hábiles a que hace referencia el inciso segundo sin que haya respuesta del responsable, el titular puede formular directamente una reclamación ante la Agencia de Protección de Datos Personales, en los mismos términos del inciso anterior.

Cuando se formule una solicitud de rectificación o cancelación, el titular tiene derecho a solicitar y obtener del responsable el bloqueo temporal de los datos. La solicitud de bloqueo temporal debe ser fundada y el responsable deberá responder a este requerimiento dentro de los 2 días hábiles siguientes a su recepción. En caso de negativa, el responsable deberá invocar una causa justificada y fundar su respuesta.

La rectificación o cancelación de los datos se aplicarán sólo respecto de los responsables a quienes se les haya formulado la solicitud.”.

5) Reemplázase el título II por el siguiente:

“Título II
Del tratamiento de los datos personales y de las categorías especiales de datos

Párrafo Primero
Del consentimiento del titular, de las obligaciones y deberes del responsable y del tratamiento de datos en general

Artículo 12.- Regla general del tratamiento de datos. Es lícito el tratamiento de los datos personales que le conciernen al titular cuando otorgue su consentimiento para ello o lo autorice la ley.

El consentimiento del titular debe ser libre e informado, otorgarse en forma previa al tratamiento y debe ser específico en cuanto a su finalidad o finalidades. Debe manifestarse de manera inequívoca, mediante una declaración verbal, escrita o realizada a través de un medio electrónico equivalente o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular.
Cuando el consentimiento lo otorgue un mandatario, éste deberá encontrase expresamente premunido de esta facultad.

El titular puede 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 tiene efectos retroactivos.

Los medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular.

Corresponde al responsable probar que el tratamiento de datos realizado contó con el consentimiento del titular o fue efectuado por disposición de la ley.

Artículo 13.- Excepciones al consentimiento. No se requiere el consentimiento del titular en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales que han sido recolectados de una fuente de acceso público.

b) Cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del título III de esta ley.

c) Cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular.

Artículo 14.- Obligaciones del responsable de datos. El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley, tiene las siguientes obligaciones:

a) Informar y poner a disposición del titular, de manera expedita y cuando le sean requeridos, los antecedentes que acrediten la licitud del tratamiento de datos que realiza.

b) Asegurar que los datos personales se recojan con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.

c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y veraz.
d) Cumplir con los demás principios que rigen el tratamiento de los datos personales previstos en esta ley.

Artículo 14 bis.- Deber de secreto o confidencialidad. El responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo aquellos que provengan de fuentes de acceso público o el titular los ha hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular.

El deber de secreto o confidencialidad no obsta a las comunicaciones o cesiones de datos que deba realizar el responsable en conformidad a la ley, y al cumplimiento de la obligación de dar acceso al titular e informar el origen de los datos, cuando esta información le sea requerida por el titular o por un órgano público dentro del ámbito de sus competencias legales.

El responsable debe adoptar las medidas necesarias con el objeto que sus dependientes o las personas naturales o jurídicas que ejecuten operaciones de tratamiento de datos bajo su responsabilidad, cumplan el deber de secreto o confidencialidad establecidos en este artículo.

Quedan sujetas a la obligación de secreto o confidencialidad las personas e instituciones y sus dependientes que, en cumplimiento de una obligación legal, han

remitido información a un organismo público sujeto al régimen de excepciones establecido en el artículo 24, en cuanto al requerimiento y al hecho de haber remitido dicha información.

Artículo 14 ter.- Deber de información y transparencia. El responsable de datos debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos, la siguiente información:

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

b) La individualización del responsable de datos, su representante legal, y la identificación del encargado de prevención si existiere.

c) La dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente a través del cual se le notifican las solicitudes que realicen los titulares.

d) Las categorías, clases o tipos de bases de datos que administra; la descripción genérica del universo de personas que comprenden las bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos; y las finalidades del tratamiento que realiza.

e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra.

Artículo 14 quáter.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica 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 el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

Si las bases de datos que opera el responsable tienen distintos niveles de criticidad deberá adoptar las medidas de seguridad que correspondan al nivel más alto.

Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de criticidad y a la tecnología disponible.

Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos debe reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración,

pérdida o alteración accidental o ilícita de los datos personales que trate, o la comunicación o acceso no autorizados a dichos datos.

El responsable de datos deberá 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.

Cuando dichas vulneraciones se refieran a datos personales sensibles o a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación debe realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se debe realizar 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.

Artículo 14 sexies.- Diferenciación de estándares de cumplimiento. Los estándares o condiciones mínimas que se impongan al responsable de datos para el cumplimiento de los deberes de información y de seguridad establecidos en los artículos 14 ter y 14 quáter, respectivamente, serán determinados considerando si el responsable es una persona natural o jurídica; el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, y el volumen y las finalidades de los datos personales que trata.

Los estándares de cumplimiento y las medidas diferenciadas serán especificados en un reglamento dictado por el Ministerio de Hacienda y suscrito por el Ministro o Ministra de Economía, Fomento y Turismo.

Artículo 15.- Cesión o transferencia de bases de datos personales. Se podrán ceder todo o parte de las bases de datos personales que disponga o administre el responsable de datos cuando la cesión sea necesaria para cumplir con los fines del tratamiento o las funciones del cedente o del cesionario, de conformidad con las disposiciones de esta ley.

La cesión de datos personales requiere el consentimiento previo del titular a quien conciernen los datos, salvo las excepciones legales.

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

Con el objeto que el titular preste su consentimiento a la cesión, el responsable debe entregar la información necesaria que le permita conocer la finalidad a la cual se destinarán los datos y el tipo de actividades que realiza el cesionario.
La cesión de datos debe constar por escrito o a través de cualquier medio electrónico idóneo. En ella se deberá individualizar a las partes, las bases de datos que son objeto de la cesión, las finalidades previstas para el tratamiento y los demás antecedentes o estipulaciones que acuerden el cedente y el cesionario.

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

Una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales, respecto de las bases de datos que fueron objeto de la cesión. El cedente, por su parte, también mantiene la calidad de responsable de datos, respecto de las operaciones de tratamiento que continúe realizando.

Si se verifica una cesión de datos sin contar con el consentimiento del titular, siendo éste necesario, o sin informarle acerca de la finalidad a la cual serán destinados los datos 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 datos recibidos, sin perjuicio de las responsabilidades legales que correspondan.

A las cesiones de datos anonimizados no le son aplicables las reglas señaladas en este artículo.

Artículo 15 bis.- Tratamiento de datos por parte de un tercero o mandatario. El responsable puede efectuar el tratamiento de datos en forma directa o a través de un tercero mandatado para este efecto. En este último caso, el tercero o mandatario realiza el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable, quedándole prohibido su tratamiento, cesión o entrega para un objeto distinto del convenido con el responsable.

Si el tercero trata, cede o entrega los datos o la base de datos con un objeto distinto del encargo convenido o a una persona distinta del responsable, se le considerará 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 que obran en su poder deben ser cancelados o devueltos al responsable de datos, según corresponda.
Artículo 15 ter.- Tratamiento automatizado de grandes volúmenes de datos.- El responsable de datos puede establecer procedimientos automatizados de tratamiento y de transferencia de grandes volúmenes de datos, siempre que éstos cautelen los derechos del titular y el tratamiento guarde relación con las finalidades de las personas o entidades participantes.

El titular de datos tiene derecho a solicitar al responsable que ninguna decisión que le afecte de manera significativa se adopte exclusivamente basada en el tratamiento automatizado de sus datos, salvo que sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, exista consentimiento previo y explícito del titular o lo disponga la ley.

Párrafo Segundo
Del tratamiento de los datos personales sensibles

Artículo 16.- Regla general para el tratamiento de datos personales sensibles. El tratamiento de los datos personales sensibles sólo puede realizarse cuando el titular a quien conciernen estos datos preste su consentimiento libre e informado, otorgado previamente, para un tratamiento específico y lo manifieste en forma expresa a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

No obstante lo anterior, no se requiere el consentimiento del titular en los siguientes casos:

a) Cuando el tratamiento se refiere a datos personales sensibles que el titular ha hecho manifiestamente públicos.

b) Cuando el tratamiento es realizado por una fundación, una asociación o cualquier otra entidad que no persiga fines de lucro, cuya finalidad sea política, filosófica, religiosa, cultural, deportiva, sindical o gremial, siempre que el tratamiento que realicen se refiera exclusivamente a sus miembros o afiliados, tenga por objeto cumplir sus finalidades específicas, la entidad otorgue las garantías necesarias para evitar un uso o tratamiento no autorizado, y los datos no se comuniquen o cedan a terceros. Cumpliéndose todas estas condiciones, las entidades señaladas no requerirán el consentimiento de los titulares para tratar sus datos personales, incluidos sus datos sensibles. En caso de duda o controversia administrativa o judicial, el responsable de datos deberá acreditar que el tratamiento realizado cumple con los requisitos anteriores.

c) Cuando el tratamiento de los datos personales, incluidos los datos relativos a la salud del titular, 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 de otorgar su consentimiento. Una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

d) Cuando el tratamiento de datos personales sensibles lo autoriza o mandata expresamente la ley.

Artículo 16 bis.- Datos personales relativos a la salud. Los datos personales relativos a la salud del titular sólo pueden ser objeto de tratamiento cuando sean necesarios

para el diagnóstico de una enfermedad o para la determinación de un tratamiento médico, siempre que el diagnóstico o el tratamiento, según corresponda, 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, establecido en la ley o en un contrato.

También es lícito el tratamiento de los datos personales relativos a la salud del titular, en los siguientes casos:

a) Cuando exista una urgencia médica o sanitaria declarada por la autoridad.

b) Cuando se deba calificar el grado de dependencia o discapacidad de una persona.

c) Cuando resulte indispensable para la ejecución o cumplimiento de un contrato cuyo objeto o finalidad exija tratar datos relativos a la salud del titular.

d) Cuando sean utilizados con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana o para el desarrollo de productos o insumos médicos que no podrían desarrollarse de otra manera.

Artículo 16 ter.- Datos personales biométricos. El responsable que trate datos personales biométricos, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz, deberá proporcionar al titular la siguiente información específica:

a) La identificación del sistema biométrico usado.

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

c) El período durante el cual los datos biométricos serán utilizados.

d) La forma en que el titular puede ejercer sus derechos.

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

Con todo, no se podrán crear o mantener bancos de huellas digitales o de otros datos biométricos, salvo expresa autorización legal.

Artículo 16 quáter.- Datos personales relativos al perfil biológico humano. El responsable de datos sólo puede realizar tratamiento de datos personales relativos al perfil biológico del titular, tales como los datos genéticos, proteómicos o metabólicos, para los siguientes fines:

a) Realizar diagnósticos médicos.

b) Prestar asistencia médica o sanitaria en caso de urgencia.

c) Realizar estudios o investigaciones científicas, médicas, epidemiológicas, antropológicas, arqueológicas o de medicina forense, que vayan en beneficio de la salud humana.

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

Queda prohibido el tratamiento y la cesión de los datos relativos al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido recolectados en el ámbito laboral, educativo, deportivo, social o de seguros, salvo que la ley expresamente autorice su tratamiento en casos calificados.

Los prestadores institucionales de salud, sean públicos o privados, que requieren tratar datos personales relativos al perfil biológico humano dentro del marco de las funciones que les señala el Código Sanitario o la ley Nº 20.120 y su normativa complementaria, deben adoptar y mantener los más altos estándares de control, seguridad y resguardo de esta información y de las muestras biológicas recolectadas.
El resultado de los estudios e investigaciones científicas que utilicen datos personales relativos al perfil biológico humano pueden ser publicados o difundidos libremente, debiendo previamente anonimizarse los datos que se publiquen.

Párrafo Tercero
Del tratamiento de categorías especiales de datos personales

Artículo 16 quinquies.- Datos personales relativos a los niños, niñas y adolescentes. El tratamiento de los datos personales que conciernen a los niños, niñas y adolescentes sólo puede realizarse atendiendo al interés superior de éstos y al respeto de su autonomía progresiva.

Cumpliéndose la exigencia establecida en el inciso anterior, para tratar los datos personales de los niños y niñas se requiere el consentimiento otorgado en forma específica, expresa y previa por quien tiene a su cargo el cuidado personal, salvo que expresamente lo autorice o mandate la ley.

Los datos personales de los adolescentes, salvo los datos personales sensibles, se pueden tratar de acuerdo a las normas de autorización previstas en esta ley para los adultos. Los datos personales sensibles de los adolescentes sólo se podrán tratar con el consentimiento otorgado en forma específica, expresa y previa por quien tiene a su cargo el cuidado personal, salvo que expresamente lo autorice o mandate la ley.

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

Es una obligación especial de los establecimientos educacionales y de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes, incluido quienes ejercen su cuidado personal, velar por el uso lícito y la protección de la información personal que concierne a los niños, niñas y adolescentes.

Artículo 16 sexies.- Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones. Las personas naturales o jurídicas, de derecho público o privado, podrán tratar datos personales con fines históricos, estadísticos, científicos y para estudios o investigaciones que atiendan fines de interés público, cuando el titular haya prestado su consentimiento en forma inequívoca, específica, previa e informada.
El responsable de datos debe acreditar, cuando le sea requerido, que ha adoptado todas las medidas de calidad y seguridad necesarias con el objeto de resguardar que los datos se utilicen exclusivamente para tales fines. Cumplidas estas condiciones, el responsable puede almacenar y utilizar los datos por un período indeterminado de tiempo.

Los registros o bases de datos que se traten con estos fines se pueden ceder a otras personas naturales o jurídicas, previo consentimiento del titular y siempre que los cesionarios los utilicen para los mismos fines. El cedente debe asegurarse que el cesionario adopte medidas de calidad y seguridad iguales o superiores a las adoptadas por él.

Los responsables que hayan tratado datos personales exclusivamente con estas finalidades pueden efectuar publicaciones con los resultados y análisis obtenidos, debiendo previamente adoptar las medidas necesarias para anonimizar los datos que se publiquen.

Artículo 16 septies.- Datos de geolocalización. El tratamiento de los datos personales de geolocalización o de movilidad del titular se puede efectuar cuando el titular haya prestado su consentimiento en forma inequívoca.

El titular de datos deberá ser informado de manera clara, suficiente y oportuna, antes de obtener su consentimiento, del tipo de datos de geolocalización o movilidad que serán tratados, de la finalidad y duración del tratamiento y si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido.

En cualquier momento el titular podrá revocar el consentimiento otorgado.

Los datos de geolocalización se podrán tratar sin limitaciones cuando previamente hayan sido anonimizados.”.

6) Reemplázase en el artículo 17 la frase “banco de datos” por la expresión “base de datos”, todas las veces que aparece en el texto.

7) Modifícase el artículo 19 de la siguiente forma:

a) Reemplázase en el inciso primero el guarismo “12” por el guarismo “4”.

b) Reemplázase la frase “bancos de datos” por la expresión “bases de datos” todas las veces que aparece en el texto.

c) Sustitúyese en el inciso final la frase “de acuerdo a lo previsto en el artículo 16” por la frase “de conformidad a lo dispuesto en el título VII de esta ley”.

8) Reemplázase el título IV por el siguiente:

“Título IV
Del tratamiento de datos personales por los órganos públicos

Artículo 20.- Regla general del tratamiento de datos por órganos públicos. Es lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias, de conformidad a las normas establecidas en sus leyes especiales y a las disposiciones previstas en este título. En esas condiciones, los órganos públicos actúan como responsables de datos y no requieren el consentimiento del titular para tratar sus datos personales.

Los órganos públicos tampoco requieren el consentimiento del titular cuando, cumpliendo las exigencias establecidas en el inciso anterior, realizan tratamiento de datos personales exclusivamente con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

Artículo 21.- Principios y normas aplicables al tratamiento de datos de los órganos públicos. El tratamiento de los datos personales que realicen los órganos públicos se rige por los principios establecidos en el artículo 3 de esta ley y 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. Conforme al principio de eficiencia, se debe evitar la duplicación de procedimientos y trámites entre los organismos del Estado, entre los organismos públicos y los particulares, y en 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 de Trasparencia de la función pública y de acceso a la información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285.

Sin perjuicio de las demás normas establecidas en el presente título, son aplicables al tratamiento de datos que efectúen los órganos públicos las disposiciones establecidas

en los artículos 14, 14 bis, 14 ter, 14 quáter y 14 quinquies, los artículos de los párrafos segundo y tercero del título II, los artículos del título V y los artículos del párrafo cuarto del título VII de esta ley.

Artículo 22.- Comunicación o cesión de datos por un órgano público. Los órganos públicos están facultados para comunicar o ceder datos personales específicos o todo o parte de sus bases de datos a otros órganos públicos, siempre que la comunicación o cesión de los datos resulte necesaria para el cumplimiento de funciones legales y ambos órganos actúen dentro del ámbito de sus competencias. La comunicación o cesión de los datos se debe realizar para un tratamiento específico y el órgano público receptor no los podrá utilizar para otros fines.

Asimismo, se podrán comunicar o ceder datos o bases de datos personales entre organismos públicos, cuando ellos se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites para los ciudadanos o reiteración de requerimientos de información o documentos para los mismos titulares.

El órgano público receptor de los datos sólo puede conservarlos por el tiempo necesario para efectuar el tratamiento específico para el cual fueron requeridos, luego de lo cual deberán ser cancelados o anonimizados. Estos datos se podrán almacenar por un tiempo mayor cuando el órgano público requiera atender reclamaciones o impugnaciones, realizar actividades de control o seguimiento, o sirvan para dar garantía de las decisiones adoptadas.

Para los efectos de poder comunicar o ceder datos personales a personas o entidades privadas, los organismos públicos deberán contar con el consentimiento inequívoco del titular, obtenido al momento de la recolección de los datos o con posterioridad a ella. 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 Ley de Trasparencia de la función pública y de acceso a la información de la Administración del Estado, contenida en el artículo primero 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.
Respecto de la comunicación de los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, se aplicará lo dispuesto en el artículo 25 de esta ley.

Las cesiones de todo o parte de sus bases de datos personales realizadas por un órgano público deberán constar por escrito a través de un convenio suscrito por el cedente y el órgano o persona cesionaria de la información. En el convenio se establecerán las finalidades específicas de los tratamientos para los cuales se utilizarán los datos.

Artículo 23.- Ejercicio de los derechos del titular y reclamo de ilegalidad. El titular de datos puede ejercer ante el órgano público los derechos de acceso y rectificación que les reconoce esta ley. El titular no podrá cancelar ni oponerse al tratamiento de datos

efectuado por un órgano público salvo que el tratamiento realizado sea contrario a las disposiciones de este título.

El ejercicio de los derechos del titular se deberá realizar de acuerdo al procedimiento establecido en el artículo 11 de esta ley, dirigiéndose al jefe superior del servicio. En todo lo no regulado se aplicarán supletoriamente las normas de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de la Administración del Estado.

Las personas que se vean afectadas por la resolución de un órgano público, sea que les deniegue el ejercicio de un derecho reconocido en esta ley o adopte una decisión o dicte una acto que infrinja los principios y obligaciones establecidos en ella, causándole perjuicio, podrá 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 47 de esta ley. El informe a que alude la letra d) del artículo 47 será evacuado por el órgano público reclamado.

Sin perjuicio de lo anterior, la Corte de Apelaciones respectiva podrá requerir informe a la Agencia de Protección de Datos Personales 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 y obligaciones establecidos en esta ley.

Artículo 24.- Régimen de excepciones. Las disposiciones de la presente ley no se aplican a los órganos públicos que, actuando en cumplimiento de sus funciones legales y dentro del ámbito de sus competencias, realizan tratamiento de datos personales en los siguientes casos:

a) Cuando efectúen tratamiento de datos que se encuentran protegidos por normas de secreto o confidencialidad establecidas en sus respectivas leyes. Cuando en cumplimiento de una obligación legal un órgano público comunica o cede a otro órgano público datos protegidos por normas de secreto o confidencialidad, el organismo público receptor deberá tratarlos manteniendo la misma obligación de secreto o confidencialidad.

b) Cuando realicen tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas.

c) Cuando efectúen operaciones de tratamiento de datos personales en actividades relacionadas con la seguridad de la nación, la defensa nacional o la mantención del orden público o la seguridad pública.

d) Cuando se haya declarado estado de catástrofe o estado de emergencia, de conformidad a la ley y mientras permanezca vigente la respectiva declaración.

Sin perjuicio de lo señalado en el inciso anterior, los tratamientos de datos personales que realicen los organismos públicos deberán cumplir siempre con los principios de licitud del tratamiento, calidad, seguridad y responsabilidad establecidos en esta ley.

Artículo 25.- Datos relativos a infracciones penales, civiles, administrativas y disciplinarias. Los datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas o disciplinarias sólo pueden ser tratados por los organismos públicos para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y en los casos expresamente previstos en la ley.

En las comunicaciones o difusión de información que realicen los organismos públicos con ocasión del tratamiento de estos datos personales, deberán velar en todo momento porque la información comunicada o hecha pública sea exacta, suficiente, actual y completa.

No podrán comunicarse o hacerse públicos los datos personales relativos a la comisión y condena de infracciones penales, civiles, administrativas o disciplinarias una vez prescrita la acción penal, civil, administrativa o disciplinaria respectiva o una vez que se haya cumplido o prescrito la pena o la sanción impuesta, lo que deberá ser declarado o constatado por la autoridad pública competente. Lo anterior es sin perjuicio de la incorporación, mantenimiento y consulta de esta información en los registros que llevan los órganos públicos por expresa disposición de la ley, en la forma y por el tiempo previsto en la ley que establece la obligación específica correspondiente. Las personas que se desempeñen en los órganos públicos están obligadas a guardar secreto respecto de esta información, la que deberá ser mantenida como información reservada.

Cuando la ley disponga que la información relativa a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias deba hacerse pública a través de su incorporación en un registro de sanciones o su publicación en el sitio web de un órgano público o en cualquier otro medio de comunicación o difusión, sin fijar un período de tiempo durante el cual deba permanecer disponible esta información, se seguirán las siguientes reglas:

a) Respecto de las infracciones penales se aplicarán los mismos plazos establecidos para la eliminación de las anotaciones prontuariales señaladas en el decreto ley N° 409, de 1932 y el decreto N° 64, de 1960, ambos del Ministerio de Justicia.

b) Respecto de las infracciones civiles, administrativas y disciplinarias permanecerán accesibles al público por el período de cinco años.

Exceptúanse de la prohibición de comunicación los casos en que la información sea solicitada por los Tribunales de Justicia u otro organismo público para el cumplimiento de sus funciones legales y dentro del ámbito de su competencia, quienes deben guardar secreto respecto de ella y mantener la debida reserva.

Artículo 26.- Reglamento. Las condiciones para la comunicación o cesión de datos personales entre organismos públicos y con personas u organismos privados, se regularán a través de un reglamento dictado por el Ministerio Secretaría General de la Presidencia, suscrito por el Ministro o Ministra de Hacienda. En este mismo reglamento se regularán los procedimientos de anonimización de los datos personales, especialmente los datos personales sensibles.”.

9) Reemplázase el título V por el siguiente:

“Título V
De la transferencia internacional de datos personales

Artículo 27.- Reglas aplicables a países con niveles adecuados de protección de datos. Se podrán realizar operaciones y actividades de transferencia internacional de datos personales a personas, entidades u organizaciones sujetas al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos.

Se entiende que el ordenamiento jurídico de un país posee niveles adecuados de protección de datos, cuando cumple con estándares similares o superiores a los fijados en esta ley. La Agencia de Protección de Datos Personales determinará los países que poseen niveles adecuados de protección de datos, considerando, a los menos, lo siguiente:

a) El establecimiento de principios para el tratamiento de los datos personales.

b) La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos.

c) La imposición de obligaciones de información y seguridad a los responsables del tratamiento de los datos.
d) La determinación de responsa-bilidades en caso de infracciones.

La transferencia internacional de datos considera las operaciones de comunicación, transmisión o cesión de datos personales, según la necesidad y finalidades del tratamiento.

Artículos 28.- Reglas aplicables a países que no poseen niveles adecuados de protección de datos. Excepcionalmente, se podrán realizar operaciones específicas de transferencia internacional de datos a personas, entidades u organizaciones sujetas al ordenamiento jurídico de países cuyas legislaciones no cumplan con niveles adecuados de protección de datos, en los siguientes casos:

a) Cuando exista consentimiento expreso del titular de datos para realizar una transferencia o transmisión específica y determinada de datos.

b) Cuando se refiera a transferencias internacionales bancarias, financieras o bursátiles específicas y se realicen conforme a la legislación especial que corresponda.

c) Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador de acuerdo a las normas de la ley N° 18.045, de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas internas en materia de tratamiento de datos personales.

d) Cuando se deban transferir los datos para dar cumplimiento a obligaciones adquiridas en tratados o convenios internacionales que hayan sido ratificados por el Estado chileno y se encuentren vigentes.

e) Cuando la transferencia resulte necesaria por la aplicación de convenios de cooperación, intercambio de información o supervisión que hayan sido suscritos por los órganos del Estado para el cumplimiento de sus funciones y en el ejercicio de sus competencias.

f) Cuando la transferencia o el intercambio de datos haya sido autorizado expresamente por la ley a un organismo público para el cumplimiento de sus funciones legales.

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

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

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

Los responsables deberán informar previamente y en forma electrónica a la Agencia de Protección de Datos Personales la transferencia o transmisión internacional de datos.
En todos aquellos casos en que sea posible, las operaciones de transferencia o transmisión internacional de datos deberán quedar amparadas por cláusulas contractuales que establezcan los derechos y garantías de los titulares y las obligaciones de los responsables.

Cuando no se verifique ninguna de las circunstancias señaladas en las letras anteriores, la Agencia de Protección de Datos Personales podrá autorizar la transferencia o transmisión internacional de datos, siempre que el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos. La Agencia de Protección de Datos Personales podrá imponer condiciones previas para que se verifique la transferencia.

Artículos 29.- Exclusiones, comunicaciones y fiscalización.- No se considera transferencia internacional de datos personales cuando un responsable efectúa operaciones de tratamiento a través de un tercero sujeto a la legislación de otro país, siempre que ese tercero efectúe las operaciones de tratamiento por encargo y bajo las instrucciones del responsable de datos de acuerdo a lo establecido en el artículo 15 bis de esta ley.

El mandato o encargo señalado en el inciso anterior deberá constar a través de un contrato escrito. La realización de estas operaciones deberá ser comunicada previamente y en forma electrónica a la Agencia de Protección de Datos Personales.

La Agencia de Protección de Datos Personales fiscalizará las operaciones de transferencia o transmisión internacional de datos, pudiendo formular recomendaciones, adoptar medidas conservativas y en casos calificados, suspender temporalmente el envío de los datos.”.

10) Intercálanse los siguientes títulos VI, VII y VIII, nuevos:

“Título VI
De la Agencia de Protección de Datos Personales

Artículo 30.- Agencia de Protección de Datos Personales. Créase la Agencia de Protección de Datos Personales, organismo público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, encargado de velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales y su protección, sometido a la supervigilancia del Presidente de la República a través del Ministerio de Hacienda y afecto al Sistema de Alta Dirección Pública establecido en la ley N° 19.882.

El domicilio de la Agencia de Protección de Datos Personales será la ciudad de Santiago.

Artículo 31.- Funciones y atribuciones. La Agencia de Protección de Datos Personales tendrá las siguientes funciones y atribuciones:

a) Dictar instrucciones y normas generales y obligatorias con el objeto de regular las operaciones de tratamiento de datos personales conforme a los principios establecidos en esta ley, salvo aquellos tratamientos de datos regidos por leyes especiales y sujetos a la potestad normativa de otro órgano público. Las instrucciones y normas generales que dicte la Agencia de Protección de Datos Personales deberán ser emitidas previa consulta pública efectuada a través de la página web institucional.

b) Prestar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral

y los demás tribunales especiales creados por ley, en la dictación y ejecución de las políticas y normas internas de estos organismos, con el objeto que sus operaciones y actividades de tratamiento de datos personales se realicen conforme a los principios y obligaciones establecidos en esta ley.

c) Fiscalizar el cumplimiento de las disposiciones de esta ley respecto de las operaciones y actividades de tratamiento de datos personales.

d) Requerir a quienes realicen tratamiento de datos personales la información que fuere necesaria para el cumplimiento de sus funciones normativas y fiscalizadoras.

e) Resolver los reclamos que formulen los titulares de datos en contra de los responsables de datos por infracción a esta ley, sus reglamentos o las instrucciones y normas generales dictadas por la Agencia de Protección de Datos Personales.

f) Ejercer la potestad sancionadora sobre las personas naturales o jurídicas, salvo los órganos públicos, que traten datos personales con infracción a esta ley e imponer las sanciones establecidas en ella.

g) Determinar las infracciones e incumplimientos en que incurran los órganos públicos en sus operaciones de tratamiento de datos, respecto de los principios y obligaciones establecidos en esta ley.

h) Requerir a la Contraloría General de la República que instruya los procedimientos administrativos competentes con el objeto de establecer las responsabilidades administrativas y aplicar las sanciones respectiva, al jefe superior del órgano público y a sus funcionarios, según corresponda, por infracción a los principios y obligaciones establecidos en esta ley.

i) Desarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación al respeto y protección del derecho a la vida privada y a la protección de sus datos personales.

j) Colaborar con los órganos públicos en el diseño e implementación de políticas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento.

k) Celebrar convenios de cooperación y prestación de servicios con órganos públicos y desarrollar programas de asistencia técnica.

l) Participar, recibir cooperación y colaborar con organismos públicos internacionales en materias propias de su competencia.

m) Solicitar la representación judicial de sus intereses al Consejo de Defensa del Estado de conformidad a la ley.

n) Certificar, registrar y supervisar los modelos de prevención de infracciones y los programas de cumplimiento y administrar el Registro Nacional de Cumplimiento y Sanciones.

o) Ejercer las demás funciones y atribuciones que la ley le encomiende.

Artículo 32.- Coordinación regulatoria. Cuando la Agencia de Protección de Datos Personales deba dictar una instrucción o norma de carácter general y obligatoria que pueda tener efectos en los ámbitos de competencia del Consejo para la Transparencia, de acuerdo a las funciones y atribuciones señaladas en la ley N° 20.285, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas y asegurar la coordinación, cooperación y colaboración entre ambos órganos.

El Consejo para la Transparencia deberá evacuar el informe solicitado dentro del plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento a que se refiere el inciso precedente.

La Agencia de Protección de Datos Personales considerará el contenido de la opinión del Consejo para la Transparencia expresándolo en la motivación de la instrucción o norma que dicte, de conformidad a lo dispuesto en el artículo 41 de la ley N° 19.880. Transcurrido el plazo sin que se hubiere recibido el informe, se procederá conforme al inciso segundo del artículo 38 de dicha ley.

A su vez, cuando el Consejo para la Transparencia deba dictar una instrucción general que tenga claros efectos en los ámbitos de competencia de la Agencia de Protección de Datos Personales, de acuerdo a las funciones y atribuciones señaladas en esta ley, el Consejo remitirá los antecedentes y requerirá informe a la Agencia de Protección de Datos Personales, quien deberá evacuarlo en el plazo de treinta días corridos, contado desde la fecha en que hubiere recibido el requerimiento. El Consejo considerará el contenido de la opinión de la Agencia de Protección de Datos Personales expresándolo en la motivación de la instrucción general que dicte al efecto.

Artículo 33.- Del Director o Directora de la Agencia de Protección de Datos Personales. La dirección y administración superior de la Agencia de Protección de Datos Personales estará a cargo de un Director o Directora, quien será el jefe superior del Servicio, 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, afecto al primer nivel jerárquico.

Son funciones y atribuciones del Director o Directora las siguientes:

a) Velar por el respeto, defensa y protección de los derechos y libertades de las personas que son titulares de datos, en particular el derecho a la vida privada, promoviendo una cultura de información, educación y participación ciudadana de acuerdo a los principios y derechos establecidos en esta ley.

b) Fiscalizar y supervigilar el tratamiento de los datos personales que realicen las personas naturales y jurídicas con el objeto que cumplan los principios y obligaciones establecidos en esta ley.

c) Asesorar al Ministro o Ministra de Hacienda en el estudio y proposición de las reformas legales aplicables al tratamiento de los datos personales y su protección.

d) Interpretar administrativamente las disposiciones legales en materia de protección y tratamiento de datos personales, dictar normas generales e impartir instrucciones para su aplicación y fiscalización.

e) Absolver las consultas sobre la aplicación e interpretación de las normas relativas a la protección de datos y su tratamiento que formulen las personas naturales y jurídicas.

f) Planificar las labores de fiscalización de la Agencia de Protección de Datos Personales y desarrollar políticas y programas que promuevan la prevención y la autorregulación.

g) Dirigir, organizar, planificar y coordinar el funcionamiento de la Agencia de Protección de Datos Personales; dictar las órdenes necesarias para una marcha expedita de ésta y supervigilar el cumplimiento de las instrucciones que imparta.

h) Representar a la Agencia de Protección de Datos Personales en todos los asuntos que le competan, incluidos recursos judiciales y los recursos extraordinarios que se interpongan en contra de la Dirección con motivo de actuaciones administrativas o jurisdiccionales.

i) Presentar al Ministerio de Hacienda, antes del 31 de marzo de cada año, una memoria anual sobre la marcha de la Agencia de Protección de Datos Personales.

j) Proponer al Presidente de la República, por intermedio del Ministerio de Hacienda, las medidas que, a su juicio, convenga adoptar para la mejor marcha de la Agencia de Protección de Datos Personales y desarrollar todas las iniciativas tendientes a tal fin.

Artículo 34.- Incompatibilidades e Inhabilidades. El desempeño del cargo de Director o Directora exige dedicación exclusiva y es incompatible con el desempeño de todo otro cargo o servicio, sea o no remunerado, que se preste en el sector privado. Asimismo, este cargo es 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 públicas, 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 es incompatible con cualquier otro servicio o empleo remunerado o gratuito en otros poderes del Estado.

El cargo de Director o Directora es compatible con el desempeño de cargos docentes en instituciones públicas o privadas reconocidas por el Estado, hasta un máximo de doce horas semanales. Del mismo modo, el Director o Directora puede 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.

El o la cónyuge o conviviente civil del Director o Directora y sus parientes hasta el segundo grado de consanguinidad inclusive, no podrán ser director o directora ni tener participación en la propiedad de una empresa cuyo objeto o giro comercial verse sobre recolección, tratamiento o comunicación de datos personales.

En todo lo no expresamente regulado en este artículo, regirán las normas del párrafo 2 del título III de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 1-19653, de 2000, del Ministerio Secretaría General de la Presidencia.

Artículo 35.- Del personal. El personal de la Agencia de Protección de Datos Personales 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, de 2004, y en materia de remuneraciones, a las normas del decreto ley N° 249, de 1974, que fija Escala Única de Sueldos, y su legislación complementaria.

En caso de ejercerse acciones judiciales por actos formales, acciones u omisiones producidos en el ejercicio de su cargo, en contra del personal de la Agencia de Protección de Datos Personales, incluido su Director o Directora, la Agencia de Protección de Datos Personales deberá proporcionarles defensa jurídica. Esta defensa se extenderá a todas aquellas acciones que se inicien en su contra por los motivos señalados, incluso después de haber cesado en el cargo.

Artículo 36.- Del patrimonio. El patrimonio de la Agencia de Protección de Datos Personales estará formado por:

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

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

c) Las donaciones que la Agencia de Protección de Datos Personales acepte. Las donaciones no requerirán del trámite de insinuación judicial a que se refiere el artículo 1401 del Código Civil.

d) Las herencias y legados que la Agencia de Protección de Datos Personales acepte, lo que deberá hacer siempre con beneficio de inventario. Dichas asignaciones estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten.

e) Los aportes de la cooperación internacional.

Título VII
De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades de los responsables de datos

Artículo 37.- Régimen general de responsabilidad. El responsable de datos, sea una persona natural o jurídica, de derecho público o privado, que en sus operaciones de tratamiento de datos personales infrinja los principios y obligaciones establecidos en esta ley, será sancionado de conformidad con las normas del presente título.

Párrafo Primero
De la responsabilidad por infracciones a la presente ley

Artículo 38.- Infracciones leves, graves y gravísimas. Las infracciones a los principios y obligaciones establecidos en esta ley cometidas por los responsables de datos se califican, atendida su gravedad, en leves, graves y gravísimas.

Se consideran infracciones leves las siguientes:

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

b) 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.

c) No responder o responder fuera de plazo las solicitudes formuladas por el titular de datos en conformidad a esta ley.

d) No informar o no remitir a la Agencia de Protección de Datos Personales las comunicaciones previstas en esta ley o en sus reglamentos.

e) No dar cumplimiento a las instrucciones impartidas por la Agencia de Protección de Datos Personales que no estén sancionadas específicamente como infracción grave o gravísima.

f) No efectuar el bloqueo temporal de los datos personales del titular cuando éste lo haya solicitado fundadamente o denegar la solicitud sin causa justificada.

g) Impedir el ejercicio legítimo del derecho a la portabilidad de los datos personales del titular.

h) Cometer cualquier otra infracción a los principios, deberes y obligaciones establecidas en esta ley que no sea calificada como una infracción grave o gravísima.

Se consideran infracciones graves las siguientes:

a) Tratar los 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 aquélla para la cual fueron recolectados.

b) Comunicar 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 proporcionalidad, 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) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las fundaciones, asociaciones o cualquier otra entidad que no persiga fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, deportiva, sindical o gremial, respecto de los datos de sus asociados.

f) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis.

g) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, cancelación u oposición del titular.

h) 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 de la Agencia de Protección de Datos Personales.

i) 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 quinquies.

j) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley.

k) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público.

l) Entregar información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones.

m) Recolectar maliciosamente a través de niños, niñas o adolescentes datos personales de integrantes de su grupo familiar.

n) No dar cumplimiento a las instrucciones específicas y directas que le haya impartido la Agencia de Protección de Datos Personales.

Se consideran infracciones gravísimas las siguientes:

a) Efectuar tratamiento de datos personales de manera manifiestamente fraudulenta.

b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento.

c) Comunicar, transmitir o ceder a terceros, a sabiendas, información no veraz, incompleta, inexacta o desactualizada del titular de datos.

d) Vulnerar, a sabiendas, el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias.

e) Comunicar 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.

f) Tratar datos personales sensibles con manifiesta falta de diligencia o cuidado.

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 confidencialidad, disponibilidad o integridad de los datos personales.

h) Actuar con falta de diligencia o cuidado en la protección de los datos personales que conciernen a los niños, niñas y adolescentes, especialmente respecto de quienes pesa la obligación especial de cuidado de esta información y que con ocasión de ello, se han efectuado tratamientos de datos de niños, niñas y adolescentes con infracción a las normas de esta ley.

Artículo 39.- Sanciones. Las sanciones a las infracciones en que incurran los responsables de datos serán las siguientes:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 50 unidades tributarias mensuales.

b) Las infracciones graves serán sancionadas con multa de 51 a 500 unidades tributarias mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de 501 a 5.000 unidades tributarias mensuales.

Artículo 40.- Determinación del monto de las multas. La cuantía de la multa, dentro del rango asignado para cada tipo de infracción, será determinada por la Agencia de Protección de Datos Personales teniendo en cuenta los siguientes criterios:

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

b) Si la conducta fue realizada por el responsable de datos con falta de diligencia o cuidado, a sabiendas o maliciosamente.

c) Si el infractor es una persona natural o jurídica.

d) Si se trata de una fundación, asociación o cualquier otra entidad que no persiga fines de lucro y cuya finalidad sea política, filosófica, religiosa, sindical o gremial.

e) En el caso de las empresas se debe tener en cuenta el monto de las ventas de la empresa infractora conforme a lo dispuesto en el artículo 16 de la ley Nº 20.416.

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

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

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

i) La existencia de circunstancias atenuantes de responsabilidad o de atenuantes calificadas.

Cuando concurran circunstancias atenuantes, la Agencia de Protección de Datos Personales estará autorizada para rebajar la sanción que corresponda a la infracción cometida dentro del rango respectivo o aplicar la sanción prevista para una infracción de menor gravedad. Cuando concurran atenuantes calificadas de responsabilidad, la Agencia de Protección de Datos Personales podrá, además, exonerar la conducta del infractor.

En caso que exista reiteración o reincidencia, la Agencia de Protección de Datos Personales puede aplicar una multa de hasta tres veces el monto señalado en el artículo anterior, según corresponda al tipo de infracción cometida.

Se entenderá que hay reiteración o reincidencia, cuando existan dos o más sanciones ejecutoriadas impuestas en virtud de la presente ley, en un período de 24 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.

Artículo 41.- Atenuantes de responsabilidad. Se consideran circunstancias atenuantes de responsabilidad las acciones unilaterales de reparación que realice el responsable de datos y los acuerdos reparatorios convenidos con los titulares de datos afectados.

Constituyen también atenuantes de responsabilidad la conducta anterior del responsable de datos y la colaboración que preste en la investigación administrativa que practique la Agencia de Protección de Datos Personales.

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

También constituye una atenuante calificada de responsabilidad que el responsable acredite haber cumplido diligentemente sus deberes de dirección y supervisión para la protección de los datos personales sujetos a tratamiento, lo que se verificará con el certificado expedido de acuerdo a lo dispuesto en el artículo 53 de esta ley.

Artículo 42.- Sanciones accesorias. En caso que se impongan multas por infracciones graves o gravísimas reiteradas y existan circunstancias debidamente justificadas, la Agencia de Protección de Datos Personales podrá disponer la suspensión de las operaciones de 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 a las exigencias establecidas en la presente ley, de acuerdo a lo dispuesto en la resolución de la Agencia de Protección de Datos Personales que ordenó la suspensión.

Si el responsable 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 tratamiento de datos personales.

Cuando la suspensión afecte a una entidad sujeta a supervisión por parte de un organismo público de carácter fiscalizador, la Agencia de Protección de Datos Personales deberá previamente poner los antecedentes en conocimiento de la autoridad regulatoria correspondiente y coordinar con ella la aplicación de la sanción con el objeto de no afectar a los usuarios del servicio que será suspendido.

Artículo 43.- Registro Nacional de Cumplimiento y Sanciones. Créase el Registro Nacional de Cumplimiento y Sanciones administrado por la Agencia de Protección de Datos Personales. El registro será público y su acceso gratuito. Se consultará y llevará en forma electrónica.

En este registro se deberán consignar a los responsables de datos que hayan sido sancionados por infringir los principios y obligaciones establecidos de esta ley, señalar la conducta infraccionada, las circunstancias atenuantes y agravantes de responsabilidad y la sanción impuesta.

Las anotaciones en el registro serán de acceso público por el período de 5 años a contar de la fecha en que se practicó la anotación.

Artículo 44.- Prescripción. Las infracciones previstas en esta ley prescriben en el plazo de tres años, contado desde la ocurrencia del hecho que originó la infracción.

En caso de infracciones continuadas, el plazo de prescripción se contará desde el día en que la infracción haya cesado.

Se interrumpe la prescripción con la notificación del inicio del procedimiento administrativo correspondiente.

Las sanciones que se impongan por una infracción a la presente ley prescriben en el plazo de dos años, contados desde la fecha en que la resolución que impone la sanción quede ejecutoriada.
Las acciones establecidas en esta ley prescribirán en el plazo de tres años.

Las acciones civiles que deriven de una infracción a la presente ley prescribirán en el plazo de tres años, contado 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 45.- Procedimiento administrativo de tutela de derechos. El titular de datos podrá reclamar ante la Agencia de Protección de Datos Personales cuando el responsable le haya denegado, en forma expresa o tácita, una solicitud en que ejerce cualquiera de los derechos que le reconoce esta ley.

La reclamación presentada se tramitará conforme a las siguientes reglas:

a) Deberá ser presentada por escrito, 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. La reclamación deberá señalar la decisión impugnada, acompañar todos los antecedentes

en que se funda e indicar una dirección de correo electrónico donde se practicarán las notificaciones.

b) Recibido el reclamo, la Agencia de Protección de Datos Personales, dentro de los 3 días siguientes, deberá determinar si éste cumple con los requisitos establecidos en la letra anterior para ser acogido a tramitación. La resolución de la Agencia de Protección de Datos Personales que no acoja a trámite la reclamación deberá ser fundada y se notificará al titular.

c) Acogido el reclamo a tramitación, la Agencia de Protección de Datos Personales 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 a que alude la letra c) del artículo 14 ter.

d) 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 pueden hacer valer todos los medios de prueba que estimen convenientes.

e) 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 Agencia de Protección de Datos Personales procederá al archivo de los antecedentes, previa aplicación de la sanción, cuando correspondiere.

f) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución. Puede, asimismo, instar a las partes a alcanzar un acuerdo. Logrado un acuerdo, se archivarán los antecedentes.

g) La resolución del reclamo debe dictarse por la Agencia de Protección de Datos Personales 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 período probatorio, según corresponda. La resolución que resuelva el reclamo deberá ser fundada.

h) En contra de esta resolución sólo procede el recurso de reposición, el que deberá ser interpuesto dentro del plazo de 5 días contado desde su notificación. La resolución que resuelva el recurso de reposición debe 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 47.

i) La interposición del reclamo administrativo suspende las operaciones de tratamiento o cesión de los datos personales que son objeto de la reclamación.

En todo lo no previsto en este artículo se aplicarán supletoriamente y en lo que corresponda las normas de la ley Nº 19.880.

Artículo 46.- Procedimiento administrativo por infracción de ley. El procedimiento sancionatorio por las infracciones que cometan los responsables de datos por incumplimiento o vulneración de los principios y obligaciones establecidas en esta ley será instruido por la Agencia de Protección de Datos Personales conforme a las siguientes reglas:

a) La Agencia de Protección de Datos Personales podrá iniciar un procedimiento sancionatorio de oficio, a petición de parte, 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 45 de esta ley.

b) La Agencia de Protección de Datos Personales deberá presentar una formulación de cargos en contra del responsable de datos en que describa los hechos que configuran la infracción, los principios y obligaciones incumplidos o vulnerados por el responsable, las normas legales infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

c) La formulación de cargos debe notificarse al responsable de datos a la dirección de correo electrónico señalada en la letra c) del artículo 14 ter.

d) El responsable de datos tiene un plazo de 10 días para presentar sus descargos. En esa oportunidad el responsable de datos puede acompañar todos los antecedentes que estime pertinente para desacreditar los hechos imputados. Junto con los descargos, el responsable podrá fijar una dirección de correo electrónico distinta a la señalada en la letra c) del artículo 14 para la realización de las demás comunicaciones y notificaciones.

e) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia de Protección de Datos Personales podrá abrir un término probatorio de 7 días, en el caso que existan hechos sustanciales, pertinentes y controvertidos.

f) La Agencia de Protección de Datos Personales 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.

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

h) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

i) La resolución que ponga fin al procedimiento sancionatorio debe ser fundada y resolver 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 y obligaciones establecidos en la ley por el responsable o su absolución, según corresponda. En caso que la Agencia de Protección de Datos Personales considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida. Esta resolución debe dictarse dentro de los 20 días siguientes de 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.

j) La resolución que establezca el incumplimiento o vulneración a los principios y obligaciones de esta ley y aplique la sanción correspondiente debe ser fundada. Esta resolución debe indicar también los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y el plazo para su interposición.

k) En contra de esta resolución sólo procede el recurso de reposición que debe ser interpuesto dentro del plazo de 5 días, contado desde la notificación respectiva. La resolución que resuelva el recurso de reposición debe dictarse en el plazo de 10 días y será reclamable judicialmente conforme al artículo siguiente.

En todo lo no previsto en este artículo se aplicarán supletoriamente y en lo que corresponda, las normas de la ley Nº 19.880.

Párrafo Tercero
Del procedimiento de reclamación judicial

Artículo 47.- Reclamación judicial. Las personas naturales o jurídicas que se vean afectadas por una resolución final o de término de la Agencia de Protección de Datos Personales 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, cuando procediere, las razones por las cuales el acto le perjudica. Si la reclamación no cumple con estos requisitos, la Corte podrá declararla inadmisible.

b) El titular de datos o el responsable de los mismos, según corresponda, podrá 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 produzca un daño irreparable al recurrente.

d) Recibida la reclamación, la Corte requerirá de informe a la Agencia de Protección de Datos Personales, 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 o revocar la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable.

i) En todo aquello no 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 de los órganos públicos, de la autoridad o jefe superior del órgano y de sus funcionarios

Artículo 48.- Responsabilidad administrativa de la autoridad o jefe superior del órgano público. La autoridad o jefe superior de un órgano público debe velar para que el órgano respectivo realice el tratamiento de los datos personales con arreglo a los principios y obligaciones establecidos en el título IV de esta ley.

Las infracciones a los principios y obligaciones establecidos en esta ley por parte del órgano público serán sancionadas con multa de 20% a 50% de la remuneración mensual de la autoridad o jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza de los datos tratados y el número de titulares afectados.

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

Tratándose de datos personales sensibles, la multa será del 50% de la remuneración mensual de la autoridad o jefe superior del órgano público y procederá la suspensión en el cargo de hasta treinta días.

Las infracciones en que incurra un órgano público en el tratamiento de los datos personales serán determinadas por la Agencia de Protección de Datos Personales, en virtud de una fiscalización de oficio o como resultado de un reclamo o denuncia presentada por un particular.

Las sanciones administrativas señaladas en este artículo serán aplicadas por la Contraloría General de la República, previa instrucción de una investigación sumaria, 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 Agencia de Protección de Datos Personales. En la investigación administrativa la Contraloría General de la República deberá tomar en consideración el informe emanado de la Agencia de Protección de Datos Personales.

En la determinación de la responsabilidad administrativa de la autoridad o jefe superior del órgano público se deben considerar las circunstancias que atenúan su responsabilidad, especialmente la establecida en el inciso final del artículo 41.

Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia de Protección de Datos Personales y del respectivo órgano o servicio, conforme al artículo 7 de la ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285, dentro del plazo de cinco días hábiles, contados desde que la respectiva resolución quede firme.

Artículo 49.- Responsabilidad del funcionario infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el informe elaborado por la Agencia de Protección de Datos Personales o en el procedimiento de investigación sumaria o en el sumario administrativo que instruye la Contraloría General de la República, se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en la ley N° 18.834.

En caso que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios involucrados es responsable de alguna de las infracciones graves o gravísimas señaladas en el artículo 38 de esta ley, esta conducta se considerará una falta grave a la probidad administrativa. En tales circunstancias, se podrá multar a estos funcionarios por hasta el doble del beneficio pecuniario obtenido mediante la infracción. En el evento de que no sea posible determinar el beneficio económico obtenido por los infractores, se podrá aplicar una multa de hasta el 50% de la remuneración mensual del funcionario.

Artículo 50.- Deberes de reserva y confidencialidad. Los funcionarios de los órganos públicos que traten datos personales, y especialmente cuando se refieran a datos personales sensibles o datos relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias, deben guardar secreto o confidencialidad

respecto de la información que tomen conocimiento en el ejercicio de sus cargos y abstenerse de usar dicha información con una finalidad distinta de la que corresponda a las funciones legales del órgano público 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, se estimará que los hechos que configuran 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 51.- 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 y obligaciones establecidos en esta ley y les cause daño, sin perjuicio de los demás derechos que concede esta ley al o los titulares de datos.

La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia de Protección de Datos Personales 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
Del modelo de prevención de infracciones

Artículo 52.- Modelo de prevención de infracciones. Los responsables de datos, sean personas naturales o entidades o personas jurídicas, públicas o privadas, podrán adoptar modelos de prevención de infracciones que deben contener, a lo menos, los siguientes elementos:

a) Designación de un encargado de prevención o delegado de protección de datos personales.

b) Definición de medios y facultades del encargado de prevención.

El responsable de datos debe disponer que el encargado de prevención cuente con 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.

c) Establecimiento de un programa de cumplimiento que deberá contemplar, a lo menos, lo siguiente:

i) La identificación del tipo de información que trata, el ámbito jurisdiccional en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos.

ii) 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 38.

iii) 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.

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

v) 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.

d) Supervisión y certificación del modelo de prevención de infracciones.

La regulación interna a que dé lugar la implementación del modelo y el programa, en su caso, deberán ser incorporados expresamente como una obligación en los contratos de trabajo o de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de las entidades que actúen como responsables de datos o los terceros que efectúen el tratamiento, incluidos los máximos ejecutivos de 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 deben realizar las medidas de publicidad establecidas en el artículo 156 del mismo Código.

Artículo 53.- Certificación, registro, supervisión del modelo de prevención de infracciones y reglamento. La Agencia de Protección de Datos Personales será la entidad encargada de certificar que el modelo de prevención de infracciones y el programa de cumplimiento reúna los requisitos y elementos establecidos en la ley y su reglamento, y supervisarlos.

La Agencia de Protección de Datos Personales 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 o Ministra Secretario General de la Presidencia y por el Ministro o Ministra 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 54.- Atenuante especial por prevención de infracciones. Los responsables de datos que incurran en alguna de las infracciones previstas en el artículo 38 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 considera que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, los responsables de datos hubieren adoptado e implementado un modelo de organización, administración y supervisión para prevenir infracciones, lo que deberá constar en un certificado emitido por la Agencia de Protección de Datos Personales.

Artículo 55.- Vigencia de los certificados. Los certificados expedidos por la Agencia de Protección de Datos Personales tendrán una vigencia de tres años. Sin perjuicio de lo anterior, quedarán sin efecto en los siguientes casos:

a) Por revocación efectuada por la Agencia de Protección de Datos Personales.

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.

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 56.- Revocación de la certificación. La Agencia de Protección de Datos Personales puede revocar la certificación indicada en los artículos precedentes si el responsable no da cumplimiento a lo establecido en este párrafo. Con este objeto la Agencia de Protección de Datos Personales podrá requerir toda aquella información que fuere necesaria para el ejercicio de sus funciones.

Los responsables pueden exceptuarse de entregar la información solicitada cuando ésta esté amparada por una obligación de secreto o confidencialidad, debiendo acreditar dicha circunstancia.

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

Cuando un certificado haya sido revocado por la Agencia de Protección de Datos Personales para volver a solicitarlo el responsable de datos debe acreditar fehacientemente que la causal que dio origen a su revocación ha sido subsanada.

Título VIII
Del tratamiento de datos personales por el Congreso Nacional, el Poder Judicial y organismos públicos dotados de autonomía constitucional

Artículo 57.- Regla general del tratamiento de datos personales. Es lícito el tratamiento de los datos personales que efectúan 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, cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas especiales que se establecen en sus respectivas leyes orgánicas y a las disposiciones del título IV de esta ley aplicables a los órganos públicos, con excepción de lo dispuesto en el artículo 14 quinquies. En esas condiciones, estas instituciones y organismos detentan la calidad de responsables de datos y no requieren el consentimiento del titular para efectuar el tratamiento de sus datos personales.

Corresponde a los órganos internos de las instituciones y organismos señalados en el inciso anterior ejercer las funciones y adoptar las decisiones que esta ley encomienda a la Agencia de Protección de Datos Personales.

Las autoridades superiores de los órganos internos de estas instituciones deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, especialmente aquéllas que permitan el ejercicio de los derechos que se reconocen a los titulares de datos y las que fijan los estándares o condiciones mínimas de control, seguridad y resguardo que se deben observar en el tratamiento de los datos personales, pudiendo requerir para ello la asistencia técnica de la Agencia de Protección de Datos Personales. Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación a las infracciones que se produzcan en el tratamiento de los datos personales.

Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia de Protección de Datos Personales.

Artículo 58.- Ejercicio de los derechos y reclamaciones. Los titulares de datos ejercerán los derechos que le reconoce esta ley ante 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, de acuerdo a los procedimientos que dispongan estas instituciones y organismos para estos efectos, de conformidad a lo señalado en el artículo anterior.

En caso que el Congreso Nacional, la Contraloría General de la República, el Ministerio Público, el Banco Central o el Servicio Electoral denieguen injustificada o arbitrariamente el ejercicio de un derecho reconocido por esta ley a un titular de

datos, o bien infrinjan algún principio, deber u obligación establecida en ella, causándole perjuicio, el titular que se vea agraviado o afectado por la decisión del organismo, podrá reclamar ante la Corte de Apelaciones, de acuerdo al procedimiento dispuesto en el artículo 47 de esta ley.

Las autoridades superiores del Poder Judicial, del Tribunal Constitucional, de la Justicia Electoral y de los demás tribunales especiales creados por ley, deberán asegurarse que en el tratamiento de los datos personales que realizan estas instituciones se cumplen estrictamente con los principios y deberes, y se respeten los derechos de los titulares establecidos en esta ley, adoptando las medidas de fiscalización y control interno que resulten necesarias y adecuadas para esta finalidad.”.

11) Intercálase en el título final, antes del actual artículo 24, que pasó a ser 59, el siguiente artículo 59, nuevo, pasando el actual artículo 24 a ser artículo 60:

“Artículo 59.- 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 o Ministra Secretario General de la Presidencia, se establecerán las demás normas necesarias para la ejecución de la presente ley.”.

Artículo segundo.- Reemplázase el literal m) del artículo 33 de la ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, contenida en el artículo primero de la ley N° 20.285, por el siguiente:

“m) Velar por la protección de los datos de carácter personal con sujeción a lo dispuesto en la ley N° 19.628, en los ámbitos de la transparencia de la función pública y el acceso a la información.”.

ARTÍCULOS TRANSITORIOS

Artículo primero transitorio.- Las modificaciones a las leyes N° 19.628, sobre protección de la vida privada, y Nº 20.285, sobre acceso a la información pública, contenidas en el artículo primero y segundo, respectivamente, de la presente ley, entrarán en vigencia el día primero del mes décimo tercero posterior a la publicación de la presente ley en el Diario Oficial.

Artículo segundo transitorio.- Las bases de datos constituidas con anterioridad a la entrada en vigencia de la presente ley deberán adecuarse a los términos previstos en ella dentro del plazo de cuarenta y ocho meses, contado desde su entrada en vigencia. Con todo, los titulares de datos podrán ejercer los derechos que les confiere esta ley ante el responsable de datos, a partir de la entrada en vigencia de la ley.

Artículo tercero transitorio.- Los reglamentos referidos en la presente ley deberán dictarse dentro de los seis meses siguientes a la fecha de su publicación en el Diario Oficial.

Artículo cuarto transitorio.- Dentro de los sesenta días anteriores a la entrada en vigencia de las modificaciones a la ley N° 19.628, sobre protección de la vida privada, contenida en el artículo primero de la presente ley, el Servicio de Registro Civil e Identificación deberá eliminar el registro de bases de datos personales contemplado en el actual artículo 22 de la ley N° 19.628.

Artículo quinto transitorio.- Facúltase al Presidente de la República para que, dentro del plazo de nueve meses contado de la fecha de publicación de esta ley, establezca mediante uno o más decretos con fuerza de ley, expedidos a través del Ministerio de Hacienda, las normas necesarias para regular las siguientes materias:

1) Fijar la planta de personal de la Agencia de Protección de Datos Personales y dictar todas las normas necesarias para la adecuada estructuración y operación de ésta. En especial, podrá determinar los grados y niveles de la Escala Única de Sueldos que se asignen a dichas plantas; el número de cargos para cada grado y planta; los requisitos específicos para el ingreso y promoción de dichos cargos; sus denominaciones y los niveles jerárquicos, para efectos de la aplicación de lo dispuesto en el título VI de la ley N° 19.882 y en el artículo 8 de la ley Nº 18.834, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Asimismo, determinará las normas necesarias para la aplicación de la asignación de modernización de la ley N° 19.553 en su aplicación transitoria.

2) Determinar la dotación máxima del personal de la Agencia de Protección de Datos Personales, a cuyo respecto no regirá la limitación establecida en el inciso segundo del artículo 10 del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda.

3) Determinar la fecha para la entrada en vigencia de las plantas que fije y la iniciación de actividades de la Agencia de Protección de Datos Personales.

Artículo sexto transitorio.- El Presidente de la República, por decreto expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia de Protección de Datos Personales, y transferirá a ella los fondos necesarios para que se cumplan sus funciones, pudiendo al efecto crear, suprimir o modificar los capítulos, asignaciones, ítem y glosas presupuestarias que sean pertinentes.

Artículo séptimo transitorio.- Dentro de los sesenta días siguientes a la publicación de la presente ley, se deberá convocar al concurso público para el nombramiento del primer director o directora de la Agencia de Protección de Datos Personales, conforme al Sistema de Alta Dirección Pública regulado en la ley N° 19.882. El Presidente de la República podrá nombrar al Director o Directora de la Agencia de Protección de Datos Personales antes de la fecha en que ésta inicie sus actividades,

para efectos de la instalación de la misma. En tanto no inicie sus actividades dicha Agencia, la remuneración del Director, grado 1C, de la Escala Única de Sueldos, se financiará con cargo a la Partida del Presupuesto del Ministerio de Hacienda, Capítulo 01, Programa 01.

Artículo octavo transitorio.- Los órganos públicos que establezcan un encargado de prevención o delegado de protección de datos personales deberán designar a un funcionario de la dotación vigente del respectivo organismo.

Artículo noveno transitorio.- El mayor gasto que irrogue la aplicación de esta ley en el transcurso del primer año presupuestario de vigencia será financiado con reasignaciones del presupuesto del Ministerio de Hacienda, y en lo que faltare con cargo a recursos del Tesoro Público. Para los años siguientes se estará a lo que indique la Ley de Presupuestos respectiva.”.

Dios guarde a V.E.,