

VERSIÓN PARA CONSULTA PÚBLICA

RECOMENDACIONES DEL CONSEJO PARA LA TRANSPARENCIA SOBRE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO

I.- Recomendaciones sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado. En ejercicio de la atribución consagrada en el artículo 33 letra m) de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N° 20.285, de 2008, en adelante Ley de Transparencia, consistente en velar por el debido cumplimiento de la Ley N° 19.628, sobre protección de datos de carácter personal, por parte de los órganos de la Administración del Estado, teniendo presente la garantía consagrada en el artículo 19 N° 4 de la Constitución Política de la República, de respeto y protección a la vida privada, y considerando la necesidad de fomentar y promover el cumplimiento de la Ley N°19.628 por parte de estos órganos mediante la especificación de las obligaciones que ésta les impone, el Consejo Directivo acuerda la siguiente recomendación:

1. OBJETO DE LAS RECOMENDACIONES

Las presentes Recomendaciones tienen por objeto establecer los criterios jurídicos aplicables, las obligaciones y limitaciones que deberán observar los órganos de la Administración del Estado en el tratamiento de datos de carácter personal que obren en su poder, con la finalidad de garantizar a las personas el derecho a la protección de los datos de carácter personal que le conciernen y asegurar el debido manejo de los registros o bancos de datos personales necesarios para el ejercicio de sus competencias.

2. ÁMBITO DE APLICACIÓN DE LAS RECOMENDACIONES

Las recomendaciones serán aplicables al tratamiento de datos de carácter personal que efectúen los órganos de la Administración del Estado, entendiendo por tales los comprendidos en el inciso segundo del artículo 1° de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado está contenido en el D.F.L. N°1-19.653, de 2001, del Ministerio Secretaría General de la Presidencia.

Las presentes recomendaciones no serán aplicables a los tratamientos de datos de personas jurídicas, ni al tratamiento de datos de personas fallecidas.

3. DEFINICIONES PREVIAS

Para efectos de la aplicación de éstas recomendaciones deberán considerarse las definiciones contenidas en el artículo 2° de la Ley N° 19.628, de 1999, sobre Protección de la Vida Privada, y, especialmente, se entenderá por:

3.1. **Datos de carácter personal o datos personales**, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

Por tanto, los elementos básicos de la definición son:

- i. Debe tratarse de información relativa a una persona, siendo indiferente la naturaleza del dato, antecedente o hecho de que se trate.
- ii. Debe tratarse de información que permita identificar al titular. Se entiende para estos efectos por identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. No se considerará identificable si es necesario realizar actividades desproporcionadas o en plazos en excesivos.
- iii. El titular sólo puede ser una persona natural.

Quedan comprendidos dentro de esta definición, independiente del soporte en que se encuentren, datos tales como: nombre, edad, sexo, rol único tributario o rol único nacional, estado civil, profesión, domicilio, números telefónicos, dirección postal, etc.

3.2. **Datos sensibles**, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. Estos datos deberán ser especialmente protegidos adoptando especiales medidas de seguridad.

3.3. **Registro o banco de datos**, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos. Por ejemplo, se pueden mencionar: los de personal de una institución, los de datos de clientes, los de datos de beneficiarios de subsidios, las de proveedores, etc.

Por tanto, los registros de datos podrán clasificarse en:

- i. **Registro automatizado**: todo conjunto organizado de datos de carácter personal que para su tratamiento han sido o están sujetos al uso de la informática y que, por ende, requieren de una herramienta tecnológica específica, como por ejemplo un procesador de texto o de cálculo, para su acceso, recuperación o tratamiento.
- ii. **Registro manual**: todo conjunto de datos de carácter personal organizado de forma no automatizada, contenido en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, y estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales. Será en este caso fundamental para su clasificación atender al criterio de estructuración a través del cual se puede acceder al dato, como podría ser el nombre, RUT o RUN, la fecha de nacimiento, etc.

3.4. **Responsable del registro o banco de datos**, el organismo público, de los definidos en el numeral 2 de estas recomendaciones, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. Por tanto, lo que caracteriza al responsable es su capacidad de decisión respecto de la finalidad, contenido y uso del tratamiento de los datos.

3.5. **Tratamiento de datos**, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma. Estas operaciones pueden ser realizadas directamente por el responsable del registro o, también, por el encargado del tratamiento.

A modo ejemplar se entienden incorporadas dentro del concepto de tratamiento las siguientes acciones:

- i. *Almacenar*, que consiste en la conservación o custodia de datos en un registro o banco de datos;
- ii. *Disociar*, referido a todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable;
- iii. *Comunicar, transmitir o ceder*, es decir, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas. Sin perjuicio de ello, el acceso a los datos por un encargado del tratamiento no se considerará cesión;
- iv. *Bloquear*, que consiste la suspensión temporal de cualquier operación de tratamiento de los datos almacenados;
- v. *Modificar*, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.
- vi. *Eliminar o cancelar*, esto es, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello, lo que conlleva el cese del tratamiento en forma definitiva.

3.6. **Encargado del tratamiento o mandatario**, aquella persona natural o jurídica que realiza un tratamiento de datos por encargo o mandato del responsable de la base de datos, al que le serán aplicables las reglas generales en la materia. El encargo o mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos, y el encargado estará obligado a respetar esas estipulaciones en el cumplimiento de su encargo.

3.7. **Fuentes accesibles al público**, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes. Es decir, su consulta debe poder ser realizada por cualquier persona, como por ejemplo, los contenidos en diarios y boletines oficiales o en medios de comunicación social.

3.8. **Dato caduco**, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si

no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

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

4. PRINCIPIOS ORIENTADORES DE LA PROTECCIÓN DE DATOS

Los organismos de la Administración del Estado que traten datos personales deberán observar los principios orientadores de la protección de datos: licitud, calidad, información, seguridad, confidencialidad y cesión o comunicación.

4.1. **Principio de licitud.** De conformidad con el artículo 4° de la Ley N° 19.628, sólo es posible tratar datos de carácter personal cuando :

- a. Exista autorización legal, ya sea de la propia Ley N° 19.628 o de otras normas de igual rango, o
- b. En su defecto, concurra autorización o consentimiento expreso del titular de los datos, lo que exige que la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y de su posible comunicación al público, en consecuencia, se trata de un consentimiento informado, que debe prestarse de manera expresa y por escrito, y previamente al almacenamiento del dato.

No obstante lo anterior, cuando los órganos de la Administración del Estado efectúen el tratamiento no será necesario el consentimiento del titular de los datos, respecto de las materias de su competencia y con sujeción a las reglas que la ley establece, siendo, por tanto, igualmente obligatorio informar a la persona el propósito del almacenamiento y su posible comunicación al público.

4.2. **Principio de calidad de los datos.** Este principio consiste en que los datos tratados deben ser exactos, adecuados, pertinentes y no excesivos, y deberá ser observado durante la recogida y posterior tratamiento de los datos. Concurren, por tanto, tres principios rectores:

- a. **Principio de veracidad.** De conformidad con el inciso segundo del artículo 9° de la Ley N° 19.628, los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular. Por consiguiente, el organismo o servicio público responsable de la base de datos deberá, sin necesidad de requerimiento del titular de los mismos: eliminar los datos caducos y aquellos que estén fuera de su competencia; bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuáles no corresponda su cancelación; y modificar los datos inexactos, equívocos o incompletos.
- b. **Principio de finalidad.** Según lo dispone el inciso primero del artículo 9° de la Ley N° 19.628, los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. La referida finalidad en el caso de órganos de la Administración del Estado debe estar determinada expresamente y corresponder a materias propias de su competencia.
- c. **Principio de proporcionalidad.** Este principio implica que sólo pueden recabarse

aquellos datos que sean necesarios para conseguir los fines que motivan su recolección, es decir, aquellos que sean adecuados a la finalidad que lo motiva, pertinentes para conseguir la referida finalidad y no excesivos en relación a la finalidad para la cual se han obtenido. En aplicación de este principio, los órganos o servicios públicos deberán optar, de entre los diversos tratamientos que le permitan conseguir los fines pretendidos dentro del ámbito de sus competencias, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos.

4.3. **Principio de información.** De acuerdo a lo dispuesto en los artículos 4° y 20 de la Ley N°19.628, aunque los organismos públicos estén facultados para efectuar tratamientos de datos de carácter personal sin consentimiento del titular de los mismos respecto de materias de su competencia, igualmente éstos deberán, previamente a la recolección de los datos, informar a su titular acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con el tratamiento de la información, de la posible comunicación a terceros y de los derechos que pueden ser ejercidos por ellos.

4.4. **Principio de seguridad.** Conforme a lo establecido en el artículo 11 de la Ley N°19.628, el responsable de los registros o bases donde se almacenen datos personales, con posterioridad a su recolección, deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Por tanto, los órganos de la Administración del Estado deberán aplicar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

4.5. **Principio de confidencialidad o secreto.** Según lo prescribe el artículo 7° de la Ley N°19.628, las personas que trabajan en el tratamiento de datos personales o tengan acceso a estos de otra forma (como aquellos funcionarios públicos autorizados para el acceso a bancos de datos de los organismos respectivos), están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

4.6. **Principio de cesión o comunicación.** En virtud de este principio los datos personales contenidos en un registro o banco de datos pueden darse a conocer de cualquier forma a personas distintas del titular. El órgano o servicio público responsable del registro sólo podrá establecer un procedimiento de transmisión para fines que digan directa relación con sus competencias legales y las de los organismos participantes y, en tal caso, deberá cautelar los derechos de los titulares. Por su parte, el receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión, salvo que se trate de datos personales accesibles al público en general o se trasmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en tratados y convenios vigentes. El procedimiento de transmisión se encuentra regulado en el numeral 6.5. de esta recomendación.

5. DERECHOS DE LOS TITULARES DE DATOS PERSONALES.

Los titulares de datos personales, conforme a lo establecido en el artículo 12 de la Ley N°19.628, pueden ejercer respecto de los órganos de la Administración del Estado, los

derechos que se describen en este numeral, teniendo presente las características de independencia, gratuidad y sencillez y las presentes recomendaciones que en cada caso se señalan.

- 5.1. **Derecho a acceder a sus propios datos.** Toda persona tiene derecho a exigir del órgano o servicio que sea responsable de un banco información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

En este caso la información será entregada en forma absolutamente gratuita, no siendo posible ni siquiera cobrar los costos directos de reproducción de esa información.

Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular podrá requerir información a cualquiera de ellos.

El acceso podrá también solicitarse mediante el ejercicio del derecho de acceso a la información contemplado en la Ley de Transparencia, cuando la persona solicite información sobre datos relativos a su persona, es decir, sea el titular del dato personal requerido e invoque expresamente ésta ley. En este caso se entenderá que el alcance, gratuidad y requerimiento de acceso se regirán por lo dispuesto en los párrafos precedentes y, en todo lo demás, de acuerdo a lo prescrito en dicha ley.

- 5.2. **Derecho de rectificación o modificación.** Toda persona tiene derecho a exigir que los datos que sean erróneos, inexactos, equívocos o incompletos, se modifiquen, siempre que se acredite debidamente cualquiera de dichas circunstancias y se indique con claridad la corrección solicitada. Lo anterior, es sin perjuicio de la rectificación o modificación de oficio por parte del órgano o servicio público, en aplicación directa del principio de calidad de los datos.

- 5.3. **Derecho de cancelación o eliminación.** Toda persona tiene derecho a exigir que se eliminen aquellos datos cuyo almacenamiento carece de fundamento legal o se encuentran caducos, salvo que concurra alguna excepción legal.

En el caso de los numerales 5.2. y 5.3., la rectificación y cancelación serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular copia del registro alterado en la parte pertinente. No estarán autorizados a cobrar los órganos o servicios públicos los costos directos de reproducción por la entrega de dicha información. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya concurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente por el titular del dato o debidamente representado.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el órgano responsable del banco deberá avisarles a la brevedad posible la operación efectuada. Si no fuere posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos. De todo ello, deberá informar oportunamente y por escrito al titular del dato.

- 5.4. **Derecho al bloqueo de datos.** Es el derecho a exigir la suspensión temporal de cualquier operación de tratamiento de los datos almacenados (letra b) del artículo 2° de la ley). Procede cuando el titular ha proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones informativas y no desee continuar figurando en el registro respectivo de modo temporal o definitivo, o cuando los datos personales por tanto, el bloqueo de datos implica una reserva de los mismos.
- 5.5. **Procedimiento y formulario para el ejercicio de los derechos.** Los órganos o servicios públicos deberán establecer procedimientos y disponer de formularios simplificados que faciliten el ejercicio de los derechos señalados en los numerales precedentes. Los formularios estarán disponibles en cada una de las Oficinas de Información, como también en sus respectivas páginas web. En los referidos formularios deberá exigirse:
- a) El nombre y apellidos del titular de los datos. Lo anterior se acreditará mediante fotocopia de la cédula de identidad o pasaporte. Además, regirá la misma exigencia en caso de actuar mediante apoderado a su respecto.
 - b) La dirección del solicitante a efectos de notificación.
 - c) El derecho que se ejerce y una descripción simple de los hechos en que se funda.
 - d) La fecha y la firma del solicitante, estampada por cualquier medio habilitado.
 - e) Los documentos acreditativos de la solicitud, en caso de ser precedente.
- 5.6. **Ejercicio independiente.** Cada uno de los derechos señalados en los numerales 5.1. a 5.4. podrá ser ejercido en forma independiente, es decir, no puede exigirse el ejercicio de ninguno de ellos como condición o requisito previo para el ejercicio del otro. A modo ejemplar, no podrá exigirse ejercer el derecho de acceso en forma previa ni concurrente al ejercicio del derecho de rectificación.
- 5.7. **Ejercicio a través de apoderado.** Los derechos señalados en los numerales 5.1. a 5.4. podrán ser ejercidos personalmente o mediante apoderado. En este último caso, el apoderado tendrá las mismas facultades que el titular del dato, salvo manifestación expresa en contrario.
- El poder deberá constar en escritura pública o documento privado suscrito ante notario y el apoderado deberá acreditar al ejercer el derecho, mediante la correspondiente documentación, la identidad del titular del dato y la calidad de apoderado.
- 5.8. **Ejercicio de los derechos ante el encargado del tratamiento.** En caso de que el organismo de la Administración del Estado hubiese encargado el tratamiento de los datos a un tercero, los titulares de éstos podrán ejercer sus derechos directamente ante él o ante el órgano o servicio, a su elección. En el contrato respectivo deberá establecerse la forma en que se dará respuesta en estos casos, buscando en todo momento responder en forma oportuna y adecuada al titular del dato.
- 5.9. **Prohibición de limitación.** Los derechos señalados en los numerales 5.1. a 5.4. no podrán ser limitados por medio de ningún acto o convención.
- 5.10. **Límites al ejercicio de los derechos.** No obstante lo dispuesto en los numerales precedentes, no podrá solicitarse información, modificación, cancelación o bloqueo

de datos personales cuando:

- i. Ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo de la administración del Estado requerido,
 - ii. Afecte la reserva o secreto establecidos en disposiciones legales de rango de ley de quórum calificado, es especial, las establecidas en la Ley de transparencia de la función pública y de acceso a la información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285,
 - iii. La seguridad de la nación,
 - iv. El interés nacional o
 - v. Hubiesen sido almacenados por mandato legal. En este caso el mandato legal deberá ser expreso y autorizar al órgano o servicio para hacer tratamiento de datos respecto de un determinado banco de datos, como por ejemplo, los registros de datos de nacimiento que tiene en su poder el Servicio de Registro Civil e Identificación. La procedencia de la modificación, cancelación o bloqueo de los datos en esos casos estará sometida y tendrá el alcance que establezca la ley respectiva.
- 5.11. **Obligación de evacuar respuesta.** El órgano o servicio público estará obligado a evacuar respuesta a la solicitud efectuada por el titular de los datos, en el plazo señalado en el 5.12., aunque no disponga de los datos de carácter personal de la persona que ejerció el derecho.
- 5.12. **Plazo de respuesta y efectos de la falta de pronunciamiento en tiempo o de la denegación.** Si el órgano o servicio responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, solicitando amparo a los derechos consagrados en este numeral, de acuerdo al procedimiento establecido en el inciso segundo del artículo 16 de la Ley 19.628.

En caso que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. El procedimiento ante la Corte Suprema se someterá a las normas establecidas en los incisos tercero y siguientes del artículo 16 de la Ley N°19.628.

Sin perjuicio de lo anterior, el titular de los datos también podrá ejercer el derecho de acceso a la información regulado por la Ley de Transparencia, para acceder a los datos relativos a su persona que obren en poder de la Administración, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente, caso en el cual y ante la negativa del órgano respectivo de entregar la información o vencido el plazo legal contemplado para ello, podrá recurrir ante este Consejo solicitando amparo a su derecho.

6. OBLIGACIONES ESPECÍFICAS DE LOS ORGANISMOS DE LA ADMINISTRACIÓN DEL ESTADO

6.1. Condiciones de licitud en el tratamiento de los datos.

Los organismos de la Administración del Estado pueden realizar tratamiento de datos personales, sólo y exclusivamente respecto de las materias de su competencia y con sujeción a las reglas que la ley establece, no requiriendo en dicho caso el consentimiento del titular. Asimismo, deberán tener en consideración las presentes recomendaciones que velan por el adecuado cumplimiento de la Ley N° 19.628 cuando el tratamiento lo realice un órgano de esta naturaleza.

6.2. Requerimientos para el tratamiento de datos.

Los órganos o servicios públicos deben sujetarse en el tratamiento de los datos, según el artículo 20, a las reglas establecidas en la Ley N° 19.628, con la sola excepción de la exigencia relativa al consentimiento del titular. En consecuencia:

- a) Los órganos de la Administración del Estado tienen el deber de informar al titular de los datos, según lo dispone el artículo 4° de la Ley N° 19.628, el propósito del almacenamiento de sus datos personales, es decir, la finalidad perseguida con el tratamiento de la información, y la posible comunicación a terceros. Además, deberá informarse la denominación del órgano o servicio responsable del tratamiento de la base de datos y los derechos que le asisten al titular para la protección de sus datos personales.

Se recomienda especialmente a los órganos o servicios públicos que dispongan de una política proactiva de difusión de información en esta materia a fin de dar cabal cumplimiento al deber de informar antes señalado. Por ejemplo, podrán contemplar estos antecedentes en la Política de Privacidad poniéndola a disposición permanente del público en los respectivos sitios web institucionales, mediante afiches o la mención a tal política en los formularios en que se soliciten datos personales (formulario de registro), señalando dónde se encuentra ésta, entre otras.

- b) Los órganos o servicios públicos deberán necesariamente, de conformidad al artículo 9° de la Ley N° 19.628, efectuar el tratamiento de los datos personales cumpliendo con la finalidad tenida en vista, declarada e informada al momento de su recolección o recogida, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Asimismo, esta finalidad debe estar explicitada, a modo ejemplar, en la política de privacidad, formulario de registro, formulario papel u otro, para de esta manera informar adecuadamente a su titular.
- c) En virtud del principio de calidad de los datos y de los artículos 6° y 9°, inciso segundo, de la Ley N° 19.628, los órganos o servicios públicos deberán de oficio y sin necesidad de requerimiento del titular de los datos: eliminar los datos caducos y aquéllos que se encuentren fuera de su competencia por carecer de fundamento legal; bloquear los datos cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; y modificar

los datos inexactos, equívocos o incompletos.

- d) En virtud del principio de seguridad y del artículo 11 de la Ley N°19.628, los órganos o servicios públicos deberán, desde el momento de la recolección, adoptar todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar su alteración, pérdida, transmisión y acceso no autorizado, haciéndose responsable de los daños causados. En este sentido, los organismos públicos deberán aplicar diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de aquellos datos definidos como sensibles deberán adoptarse niveles de seguridad más altos que aquellos que no poseen dicha calidad.
- e) Los órganos o servicios públicos deberán exigir a sus funcionarios cumplir con la obligación de secreto o confidencialidad en relación a los datos que provengan o hayan sido recolectados de fuentes no accesibles al público, contemplada en el artículo 7° de la Ley N°19.628, en especial respecto de los que trabajen en el tratamiento de datos personales o tengan acceso a éstos de cualquier otra forma, como aquellos funcionarios autorizados para el acceso a bases de datos en los organismos respectivos. Se extenderá este deber a los demás datos y antecedentes relacionados con el banco de datos. Asimismo, la referida obligación del funcionario público no cesará por haber terminado sus obligaciones en ese campo, es decir, por dejar de desempeñarse en el tratamiento o acceso a dichos registros.

6.3. Tratamiento de datos personales relativos a delitos, infracciones administrativas o faltas disciplinarias.

Los órganos de la Administración del Estado, conforme a lo dispuesto en el artículo 21 de la Ley N°19.628, que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. En este caso, en virtud del principio de calidad y veracidad del dato, deberá el órgano o servicio proceder de oficio al bloqueo o cancelación, según corresponda conforme a la normativa que rija el referido registro.

Por consiguiente, los órganos deberán abstenerse de publicar en virtud del artículo 7°, letra g) de la Ley de Transparencia, referido a los actos y resoluciones que tengan efectos sobre terceros, los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena y aplicarán, de ser procedente, el principio de divisibilidad respecto de los actos o resoluciones que los contengan.

Con todo, cuando el Consejo conozca de un reclamo por incumplimiento de los deberes de transparencia activa o de un amparo por denegación de acceso a la información, podrá autorizar la comunicación de este tipo de datos cuando así lo exija el interés público, en aplicación de la Ley de Transparencia.

Se exceptuarán de la prohibición de comunicación, los casos en que esa información

les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ello la debida reserva o secreto y, en todo caso, les serán aplicables los siguientes artículos de la Ley N°19.628:

- a) El artículo 5° que regula el procedimiento automatizado de transmisión de datos,
- b) El artículo 7° que consagra el principio de secreto exigible a los funcionarios públicos,
- c) El artículo 11 que establece el principio de seguridad y
- d) El artículo 18 referido a la prohibición de comunicación de datos personales relativos a obligaciones de carácter económico, financiero bancario o comercial cuando han transcurrido cinco años desde que la obligación se hizo exigible, después de haber sido pagada o haberse extinguido la obligación por otro modo legal, sin perjuicio de la comunicación a los tribunales de Justicia de la información que requieran con motivo de juicios pendientes.

6.4. Inscripción de las bases de datos en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos

Los órganos de la Administración del Estado deberán inscribir todos los bancos de datos personales que obren en su poder en el registro de los bancos de datos personales a cargo de organismos públicos que lleva el Servicio de Registro Civil e Identificación, de acuerdo a lo establecido en el artículo 22 de la Ley N° 19.628 y en el Decreto Supremo N°779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos.

- a) Características del registro. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende.
- b) Requisitos de la inscripción. Conforme a la normativa aludida, el organismo público responsable del banco de datos para efectos de la inscripción, debe proporcionar, a lo menos:
 - i. El nombre del banco de datos personales, es decir, la denominación que el propio organismo le dé al banco de datos que inscriba y que sirva para su identificación;
 - ii. El organismo público responsable del banco de datos personales respectivo;
 - iii. El RUT correspondiente al organismo público;
 - iv. El fundamento jurídico de la existencia del banco de datos personales, es decir, se deben indicar las normas legales que sancionan en forma específica la existencia de un registro en particular, o las normas de carácter general, sectorial u orgánica que habiliten al organismo público para tratar los datos personales y almacenarlos en bancos de datos;
 - v. La finalidad del banco de datos;

- vi. El o los tipos de datos almacenados en dicho banco, pudiendo corresponder, a modo ejemplar, a cualquiera de las siguientes categorías de datos: biométricos (como ADN, firma, fotografía, impresiones dactilares, etc), civiles (como datos de los padres, domicilio, fecha de nacimiento, lugar de nacimiento, nombres, apellidos, datos del cónyuge, estado civil, fecha de matrimonio, sexo, fecha de defunción, lugar de defunción, nacionalidad, RUN, etc), económicos y financieros (como cuentas bancarias, ingresos, tarjetas de crédito, deudas, RUT, etc), generales (calidad de conductor de vehículos motorizados, habilidades, membresía a organizaciones, etc), judiciales o legales (como condenas, infracciones de tránsito, consumo y tráfico de estupefacientes, violencia intrafamiliar, etc.), de salud (como enfermedades, discapacidad, intervenciones, alergias, etc.), sociales (nivel educacional, religión, profesión, ocupación u oficio, etnia, etc.) y otros datos referidos a cualquier otra información concerniente a personas naturales, identificadas o identificables, almacenada en la base de datos del organismo respectivo; y
 - vii. Una descripción del universo de personas que comprende.
- c) Procedimiento de inscripción. El procedimiento de inscripción de los bancos de datos personales a cargo de los órganos de la Administración del Estado se encuentra regulado en el Decreto Supremo N°779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos y en las resoluciones que el Director Nacional estime pertinente dictar al efecto, en especial, la Resolución (E) N°1540, de 2010, que establece el procedimiento de inscripción de registros y/o bancos de datos personales a cargo de los organismos públicos o la que la reemplace.
 - d) Oportunidad de la inscripción. Los órganos o servicios públicos deberán inscribir la base de datos cuando se inicien las actividades del banco y en todo caso, antes de que se proceda al tratamiento de los datos contenidos en él.
 - e) Correcciones de la inscripción. Cualquier corrección relativa a errores u omisiones de una inscripción deberá ser requerida por el propio organismo responsable de dicha inscripción en el Registro de Bancos de Datos Personales, siguiendo el mismo procedimiento establecido para la inscripción.
 - f) Modificaciones de la inscripción. Cualquier modificación de una inscripción deberá ser requerida por el propio organismo responsable de la inscripción en el Registro de Bancos de Datos Personales, en el plazo de 15 días contados desde que se produzca cualquier cambio en la información proporcionada, de acuerdo a lo establecido en la letra b) del presente numeral.

6.5. Comunicación o transmisión de datos personales

Los organismos de la Administración del Estado sólo podrán establecer procedimientos de comunicación, transmisión o cesión de datos de carácter personal para fines que digan directa relación con sus competencias legales y las de los organismos participantes y, en tal caso, deberá cautelar los derechos de los titulares. Dicho procedimiento deberá contemplar, a lo menos, las siguientes etapas: requerimiento expreso, admisibilidad del mismo y firma de un convenio de transmisión, de acuerdo a las exigencias que se señalan a continuación.

El requerimiento de datos personales efectuado a un órgano o servicio público deberá contener las siguientes especificaciones:

- a) La individualización del requirente, el que puede ser un organismo público o privado;
- b) El motivo y el propósito del requerimiento, con indicación expresa del tratamiento de datos que se busque efectuar y la finalidad del mismo,
- c) El tipo de datos que se desea transmitir,
- d) La forma en que la transmisión guarda relación con sus tareas y finalidades, y
- e) Las medidas de seguridad de los datos que adoptará.

La admisibilidad del requerimiento deberá ser evaluada por el órgano o servicio responsable del banco de datos que lo recibe, el que deberá verificar que la comunicación guarde relación con sus tareas o finalidades, es decir, que se encuentra dentro del ámbito de sus competencias, y establecerá los requisitos específicos para la protección de los derechos de protección de datos en el convenio respectivo. En esta etapa, los órganos públicos deberá garantizar la igualdad de trato en el acceso a esta información por parte de todas las entidades que efectúen el requerimiento correspondiente y cumplan con los requisitos establecidos.

De la transmisión, la fecha, el motivo y propósito de la misma, los requisitos específicos para la protección de los datos personales transmitidos y la obligación del solicitante de utilizar los datos personales sólo para los fines que motivaron la transmisión deberá dejarse constancia en un convenio de comunicación o transmisión suscrito por ambas partes, el que se entenderá aprobado una vez que se encuentre totalmente tramitado el o los correspondientes actos administrativos de aprobación, según se trate de uno o más órganos públicos. Por tanto, a lo menos deberá contener:

- i. Identificación del órgano público que transmite los datos y del destinatario de los mismos,
- ii. Identificación del banco de datos, según la denominación dada en la inscripción efectuada en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos,
- iii. Las medidas de seguridad que deberán adoptar tanto el que transmite los datos como el destinatario de los mismos durante todo el procedimiento de transmisión y posterior tratamiento de los datos por éste último,
- iv. La indicación de que el receptor de los datos tendrá la calidad de responsable del tratamiento, estando sometido a las mismas obligaciones, multas y responsabilidad de indemnizar en caso de tratamiento indebido de los datos, que el órgano público que efectuó la transmisión,
- v. El plazo que el destinatario conservará los datos transmitidos, y
- vi. Los cursos de acción que deberá seguir el destinatario una vez que haya efectuado el tratamiento que motivó la transmisión, ya sea que se acuerde la destrucción o devolución del banco de datos al transmisor y de cualquier otro soporte donde consten los datos objetos de la comunicación.

Por ejemplo, si el organismo utiliza un servicio Web que permite la consulta directa entre

los sistemas de información de las diversas entidades participantes o si dos organismos públicos suscriben convenios de intercambio de datos personales deberán cumplir con lo dispuesto en el artículo 5° de la Ley N° 19.628 y las precedentes recomendaciones.

No serán aplicables las recomendaciones contenidas en este numeral a los convenios o contratos celebrados entre órganos o servicios públicos y particulares cuando este último tenga la calidad de encargado del tratamiento, esto es, actúa bajo las instrucciones del organismo responsable de la base de datos, quien tiene las facultades para decidir acerca de la base de datos misma. En ese caso, deberá estarse a las exigencias contempladas en el numeral 6.6. siguiente.

6.6. Tratamiento de datos a través de un encargado o mandatario

Los órganos o servicios públicos, en conformidad a lo dispuesto en el artículo 8° de la Ley N°19.628, podrán encargar el tratamiento de los datos a un tercero, que tendrá la calidad de encargado del tratamiento o mandatario.

El contrato de prestación de servicios de tratamiento que encargue el tratamiento de datos personales deberá ser otorgado por escrito, dejando especial constancia de: que el tratamiento se efectúa a cuenta y riesgo del organismo responsable del tratamiento, de las condiciones de utilización de los datos, de las medidas de seguridad que se deban adoptar y de las exigencias de confidencialidad de las personas que trabajen en el tratamiento y, en general, de la necesidad de dar cumplimiento a las obligaciones establecidas en la Ley N°19.628 y las presentes recomendaciones.

En estos casos no se entenderá que existe transmisión, comunicación o cesión de datos entre el responsable del tratamiento y el encargado del mismo.

6.7. Medidas de Seguridad de los bancos o registros de datos.

En virtud del principio de seguridad y del artículo 11 de la Ley N°19.628, los organismos de la Administración del Estado deberán adoptar todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos.

Para ello, los organismos públicos deberán aplicar diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de los datos sensibles deberán adoptarse niveles de seguridad más altos que en relación a aquellos que no poseen dicha calidad.

Los organismos públicos deberán adoptar todas las medidas de seguridad de sistemas para el resguardo de los bancos de datos personales que sean pertinentes a la naturaleza de los datos tratados, por lo que se recomienda, especialmente, adoptar las medidas de seguridad establecidas en el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprobó la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos.

Se recomienda, en aplicación del artículo 11 y siguientes del Decreto Supremo señalado, que cada organismo de la Administración del Estado establezca una política que fije las directrices generales que orienten la materia de seguridad en relación a las bases de datos que se encuentran en su poder, que defina un encargado de seguridad al interior

del servicio, mediante el correspondiente acto administrativo, y que a cada banco de datos se le asigne un responsable.

6.8. Obligaciones en caso tratamiento de datos para encuestas, estudios de mercado y sondeos de opinión.

De acuerdo a lo establecido en el artículo 3° de la Ley N°19.628, cuando los órganos o servicios públicos recolecten datos personales a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que la ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas, debiendo sólo comunicarse los datos que tengan la calidad de estadísticos, es decir, los que en su origen, o como consecuencia de un tratamiento, no pueden ser asociados a un titular identificado o identificable, por haber sido aplicado a su respecto un procedimiento de disociación de datos.

Asimismo, el titular del dato puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Para ello el órgano o servicio deberá informar, conjuntamente con los aspectos señalados y al momento de realizarse la recopilación, que le asiste el derecho a oponerse, en cualquier tiempo, a la utilización de los datos con los fines indicados.

6.9. Responsabilidad por las infracciones y derecho a indemnización.

De conformidad al artículo 23 de la Ley N° 19.628, el órgano de la Administración del Estado responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

Santiago, XX de xxxxxxxx de 2011.