



Ley N° 18.331

PROTECCIÓN DE DATOS PERSONALES Y ACCIÓN DE "HABEAS DATA"

(República Oriental del Uruguay. Publicada D.O. 18 de agosto de 2008 - N° 27549)

El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General,

DECRETAN:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1º. Derecho humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.

Artículo 2º. Ámbito subjetivo.- El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda.

Artículo 3º. Ámbito objetivo.- El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

No será de aplicación a las siguientes bases de datos:

A) A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

B) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

C) A las bases de datos creadas y reguladas por leyes especiales.

Artículo 4º. Definiciones.- A los efectos de la presente ley se entiende por:

A) Base de datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.



B) Comunicación de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.

C) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.

D) Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

E) Dato sensible: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

F) Destinatario: persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero.

G) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.

H) Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

I) Fuentes accesibles al público: aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

J) Tercero: la persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

K) Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

L) Titular de los datos: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente ley.

M) Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

N) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

CAPÍTULO II



PRINCIPIOS GENERALES

Artículo 5º. Valor y fuerza.- La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales:

- A) Legalidad.
- B) Veracidad.
- C) Finalidad.
- D) Previo consentimiento informado.
- E) Seguridad de los datos.
- F) Reserva.
- G) Responsabilidad.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Artículo 6º. Principio de legalidad.- La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia.

Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

Artículo 7º. Principio de veracidad.- Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley.

Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley.

Artículo 8º. Principio de finalidad.- Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.



La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia.

Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular.

Artículo 9º. Principio del previo consentimiento informado.- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley.

No será necesario el previo consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.

Artículo 10. Principio de seguridad de los datos.- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.



Artículo 11. Principio de reserva.- Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.

Artículo 12. Principio de responsabilidad.- El responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley.

CAPÍTULO III

DERECHOS DE LOS TITULARES DE LOS DATOS

Artículo 13. Derecho de información frente a la recolección de datos.- Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

- A) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.
- B) La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
- C) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
- D) Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.
- E) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

Artículo 14. Derecho de acceso.- Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.



Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos.

La información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data.

La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Artículo 15. Derecho de rectificación, actualización, inclusión o supresión.- Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.

El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley.

No procede la eliminación o supresión de datos personales salvo en aquellos casos de:

- A) Perjuicios a los derechos e intereses legítimos de terceros.
- B) Notorio error o falsedad.
- C) Contravención a lo establecido por una obligación legal.

Durante el proceso de verificación, rectificación o inclusión de datos personales, el responsable de la base de datos o tratamiento, ante el requerimiento de terceros por acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión.

En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos o del tratamiento debe notificar la rectificación, inclusión o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato.



La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular.

Artículo 16. Derecho a la impugnación de valoraciones personales.- Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.

La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 17. Derechos referentes a la comunicación de datos.- Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando:

- A) Así lo disponga una ley de interés general.
- B) En los supuestos del artículo 9º de la presente ley.
- C) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.
- D) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.



DATOS ESPECIALMENTE PROTEGIDOS

Artículo 18. Datos sensibles.- Ninguna persona puede ser obligada a proporcionar datos sensibles. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular.

Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.

Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato.

Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente.

Artículo 19. Datos relativos a la salud.- Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley.

Artículo 20. Datos relativos a las telecomunicaciones.- Los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la presente ley.

Asimismo, deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional.



Artículo 21. Datos relativos a bases de datos con fines de publicidad.- En la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

El titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo.

Artículo 22. Datos relativos a la actividad comercial o crediticia.- Queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley, se permite el tratamiento de toda información autorizada por la normativa vigente.

Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.

Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma.

Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, el acreedor deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

Artículo 23. Datos transferidos internacionalmente.- Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia.

La prohibición no regirá cuando se trate de:



- 1) Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso.
- 2) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.
- 3) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.
- 4) Acuerdos en el marco de tratados internacionales en los cuales la República Oriental del Uruguay sea parte.
- 5) Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

También será posible realizar la transferencia internacional de datos en los siguientes supuestos:

- A) Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.
- B) Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado.
- C) Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.
- D) Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
- E) Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.
- F) Que la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta.

Sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos.

Dichas garantías podrán derivarse de cláusulas contractuales apropiadas.



BASES DE DATOS DE TITULARIDAD PÚBLICA

Artículo 24. Creación, modificación o supresión.- La creación, modificación o supresión de bases de datos pertenecientes a organismos públicos deberán registrarse conforme lo previsto en el capítulo siguiente.

Artículo 25. Base de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia.- Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Artículo 26. Excepciones a los derechos de acceso, rectificación y cancelación.- Los responsables de las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas.

El titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 27. Excepciones al derecho a la información.- Lo dispuesto en la presente ley no será aplicable a la recolección de datos, cuando la información del titular afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.



CAPÍTULO VI

BASES DE DATOS DE TITULARIDAD PRIVADA

Artículo 28. Creación, modificación o supresión.- Las personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos de carácter personal, que no sean para un uso exclusivamente individual o doméstico, deberán registrarse conforme lo previsto en el artículo siguiente.

Artículo 29. Inscripción registral.- Toda base de datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control, de acuerdo a los criterios reglamentarios que se establezcan.

Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deberá contener la inscripción, entre los cuales figurarán necesariamente los siguientes:

- A) Identificación de la base de datos y el responsable de la misma.
- B) Naturaleza de los datos personales que contiene.
- C) Procedimientos de obtención y tratamiento de los datos.
- D) Medidas de seguridad y descripción técnica de la base de datos.
- E) Protección de datos personales y ejercicio de derechos.
- F) Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos.
- G) Tiempo de conservación de los datos.
- H) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
- I) Cantidad de acreedores personas físicas que hayan cumplido los 5 años previstos en el artículo 22 de la presente ley.
- J) Cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera, de acuerdo a lo previsto en el artículo 22 de la presente ley.

Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la presente ley.

Respecto a las bases de datos de carácter comercial ya inscriptos en el Órgano Regulador, se estará a lo previsto en la presente ley respecto del plazo de adecuación.



Artículo 30. Prestación de servicios informatizados de datos personales.- Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presume la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

CAPÍTULO VII

ÓRGANO DE CONTROL

Artículo 31. Órgano de Control.- Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso.

Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico.

Artículo 32. Consejo Consultivo.- El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales funcionará asistido por un Consejo Consultivo, que estará integrado por cinco miembros:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser un Legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica.
- Un representante del sector privado, que se elegirá en la forma establecida reglamentariamente.



Sesionará presidido por el Presidente de la Unidad Reguladora y de Control de protección de Datos Personales.

Sus integrantes durarán cuatro años en sus cargos y sesionarán a convocatoria del Presidente de la Unidad Reguladora y de Control de Datos Personales o de la mayoría de sus miembros.

Podrá ser consultado por el Consejo Ejecutivo sobre cualquier aspecto de su competencia y deberá ser consultado por éste cuando ejerza potestades de reglamentación.

Artículo 33. Recursos.- La Unidad Reguladora y de Control de Datos Personales formulará su propuesta de presupuesto de acuerdo a lo previsto en el artículo 214 de la Constitución de la República.

Artículo 34. Cometidos.- El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

A) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.

C) Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.

D) Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.

E) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.

F) Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.

G) Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.

H) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.



Artículo 35. Potestades sancionatorias.- El órgano de control podrá aplicar las siguientes medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso que se violen las normas de la presente ley:

- 1) Apercibimiento.
- 2) Multa de hasta quinientas mil unidades indexadas.
- 3) Suspensión de la base de datos respectiva. A tal efecto se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la suspensión de las bases de datos, hasta por un lapso de seis días hábiles, respecto de los cuales se comprobare que infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales y la suspensión deberá decretarse dentro de los tres días siguientes a aquel en que la hubiere solicitado la AGESIC, la cual quedará habilitada a disponer por sí la suspensión si el Juez no se pronunciare dentro de dicho término.

En este último caso, si el Juez denegare posteriormente la suspensión, ésta deberá levantarse de inmediato por la AGESIC.

Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la suspensión, no tendrán efecto suspensivo.

Para hacer cumplir dicha resolución, la AGESIC podrá requerir el auxilio de la fuerza pública.

La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura, Nº 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Artículo 36. Códigos de conducta.- Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

CAPÍTULO VIII

ACCIÓN DE PROTECCIÓN DE DATOS PERSONALES

Artículo 37. Habeas data.- Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder.



Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

Artículo 38. Procedencia y competencia.- El titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.

B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Serán competentes para conocer en las acciones de protección de datos personales o habeas data:

1) En la capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos.

2) Los Juzgados Letrados de Primera Instancia del Interior a quienes se haya asignado competencia en dichas materias.

Artículo 39. Legitimación.- La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado.

En el caso de personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos.

Artículo 40. Procedimiento.- Las acciones que se promuevan por violación a los derechos contemplados en la presente ley se registrarán por las normas contenidas en los artículos que siguen al presente. Serán aplicables en lo pertinente los artículos 14 y 15 del Código General del Proceso.

Artículo 41. Trámite de primera instancia.- Salvo que la acción fuera manifiestamente improcedente, en cuyo caso el tribunal la rechazará sin sustanciarla y dispondrá el archivo de las actuaciones, se convocará a las partes a una audiencia pública dentro del plazo de tres días de la fecha de la presentación de la demanda.



En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El tribunal, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad, e interrogará a los testigos y a las partes, sin perjuicio de que aquéllos sean, a su vez, repreguntados por los abogados. Gozará de los más amplios poderes de policía y de dirección de la audiencia.

En cualquier momento podrá ordenar diligencias para mejor proveer.

La sentencia se dictará en la audiencia o a más tardar, dentro de las veinticuatro horas de su celebración. Sólo en casos excepcionales podrá prorrogarse la audiencia por hasta tres días.

Las notificaciones podrán realizarse por intermedio de la autoridad policial. A los efectos del cómputo de los plazos de cumplimiento de lo ordenado por la sentencia, se dejará constancia de la hora en que se efectuó la notificación.

Artículo 42. Medidas provisionales.- Si de la demanda o en cualquier otro momento del proceso resultare, a juicio del tribunal, la necesidad de su inmediata actuación, éste dispondrá, con carácter provisional, las medidas que correspondieren en amparo del derecho o libertad presuntamente violados.

Artículo 43. Contenido de la sentencia.- La sentencia que haga lugar al habeas data deberá contener:

A) La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.

B) La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo.

C) El plazo para el cumplimiento de lo dispuesto, que será fijado por el tribunal conforme las circunstancias de cada caso, y no será mayor de quince días corridos e ininterrumpidos, computados a partir de la notificación.

Artículo 44. Recurso de apelación y segunda instancia.- En el proceso de habeas data sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente.

El recurso de apelación deberá interponerse en escrito fundado, dentro del plazo perentorio de tres días. El tribunal elevará sin más trámite los autos al superior cuando hubiere desestimado la acción por improcedencia manifiesta, y lo sustanciará con un traslado a la contraparte, por tres días perentorios, cuando la sentencia apelada fuese la definitiva.

El tribunal de alzada resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos. La interposición del recurso no suspenderá las medidas de amparo decretadas, las cuales serán cumplidas inmediatamente después de notificada la sentencia, sin necesidad de tener que esperar el transcurso del plazo para su impugnación.



Artículo 45. Sumariedad. Otros aspectos.- En los procesos de habeas data no podrán deducirse cuestiones previas, reconvencciones ni incidentes. El tribunal, a petición de parte o de oficio, subsanará los vicios de procedimiento, asegurando, dentro de la naturaleza sumaria del proceso, la vigencia del principio de contradictorio.

Cuando se plantee la inconstitucionalidad por vía de excepción o de oficio (artículos 509 numeral 2 y 510 numeral 2 del Código General del Proceso) se procederá a la suspensión del procedimiento sólo después que el Magistrado actuante haya dispuesto la adopción de las medidas provisorias referidas en la presente ley o, en su caso, dejando constancia circunstanciada de las razones de considerarlas innecesarias.

CAPÍTULO IX

DISPOSICIONES TRANSITORIAS

Artículo 46. Adecuación de las bases de datos.- Las bases de datos deberán adecuarse a la presente ley dentro del plazo de un año de su entrada en vigor.

Artículo 47. Traslado del órgano de control referente a datos comerciales.- Se establece el plazo de ciento veinte días corridos para que el actual órgano de control en materia de protección de datos comerciales, a cargo del Ministerio de Economía y Finanzas, realice el traslado de la información y documentación a la AGESIC.

Artículo 48. Derogación.- Se deroga la Ley Nº 17.838, de 24 de setiembre de 2004.

Artículo 49. Reglamentación.- El Poder Ejecutivo deberá reglamentar la presente ley dentro de los ciento ochenta días de su promulgación.

Sala de Sesiones de la Asamblea General, en Montevideo, a 6 de agosto de 2008.

RODOLFO NIN NOVOA,

Presidente.

Hugo Rodríguez Filippini,

Secretario.

Marti Dalgarrondo Añón,



Secretario.

MINISTERIO DEL INTERIOR

MINISTERIO DE RELACIONES EXTERIORES

MINISTERIO DE ECONOMÍA Y FINANZAS

MINISTERIO DE DEFENSA NACIONAL

MINISTERIO DE EDUCACIÓN Y CULTURA

MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS

MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA

MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

MINISTERIO DE SALUD PÚBLICA

MINISTERIO DE GANADERÍA, AGRICULTURA Y PESCA

MINISTERIO DE TURISMO Y DEPORTE

MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL Y MEDIO AMBIENTE

MINISTERIO DE DESARROLLO SOCIAL

Montevideo, 11 de agosto de 2008.

De acuerdo a lo dispuesto por el artículo 145 de la Constitución de la República, cúmplase, acúcese recibo, comuníquese, publíquese e insértese en el Registro Nacional de Leyes y Decretos, la Ley por la que se establecen normas de protección de datos personales.

TABARÉ VÁZQUEZ.

DAISY TOURNÉ.

GONZALO FERNÁNDEZ.

DANILO ASTORI.

JOSÉ BAYARDI.

MARÍA SIMON.

VÍCTOR ROSSI.

DANIEL MARTÍNEZ.



EDUARDO BONOMI.

MARÍA JULIA MUÑOZ.

ERNESTO AGAZZI.

HÉCTOR LESCANO.

CARLOS COLACCE.

MARINA ARISMENDI.

DECRETO Nº 414/2009

PROTECCIÓN DE DATOS PERSONALES – ACCIÓN DE “HABEAS DATA” – REGLAMENTACIÓN.

(República Oriental del Uruguay. Publicada D.O. 15 de septiembre de 2008)

Montevideo, 31 de Agosto de 2009

Visto: que con fecha 11 de agosto de 2008 se promulgó la Ley Nº 18.331 de Protección de Datos Personales y Acción de "Habeas Data".

Resultando: I) que razones de juridicidad y conveniencia imponen estatuir aquellos aspectos básicos y primarios de la reglamentación, que ordenen y favorezcan su puesta en práctica de acuerdo con el postulado constitucional de que el derecho a la protección de datos personales es inherente a la personalidad humana y por lo tanto está comprendido en el art. 72 de la Constitución (art. 1 de la Ley).

II) que las facultades legales del Órgano de Control creado por los artículos 31 y siguientes de la Ley, incluyen la potestad regulatoria cuyo ejercicio permitirá continuar ordenando y favoreciendo la puesta en práctica de las actividades correspondientes;

Considerando: I) que la consagración del nuevo régimen legal para la protección de datos personales y acción de "habeas data", articula un conjunto de derechos y obligaciones vinculados a la recolección y tratamiento, automatizados o manuales, de los datos de las personas físicas y jurídicas; II) que es conveniente la adecuación del ordenamiento jurídico nacional en la materia al régimen de derecho comparado de mayor recibo,



fundamentalmente el consagrado por los países europeos a través de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos.

III) que asimismo corresponde reglamentar el funcionamiento de la Unidad Reguladora y de Control de Datos Personales creada por la preindicada Ley, la que tendrá a su cargo los cometidos que por ella se le asignan.

Atento: a lo precedentemente expuesto y a lo preceptuado en las disposiciones citadas y en el artículo 168 ordinal 4º de la Constitución.

El Presidente de la República, actuando en Consejo de Ministros

D E C R E T A:

TÍTULO I. DISPOSICIONES GENERALES

Capítulo I. Ámbito de Aplicación

Artículo 1º.- Ámbito subjetivo. El derecho a la protección de los datos personales se aplica a las personas físicas, directa o indirectamente, a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas.

Por extensión se aplica a las personas jurídicas, las que gozarán del régimen tuitivo en cuanto corresponda.

Artículo. 2º.- Ámbito objetivo. El régimen jurídico de la protección de datos personales se aplica a su recolección, registro y todo tipo de tratamiento, automatizado o no, bajo cualquier soporte y modalidad de uso, tanto sea en el ámbito público como privado.

Este régimen no será aplicable a las siguientes bases de datos:

- A) Las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, entendiéndose por éstas las que se desarrollan en un ámbito estrictamente privado, entre otros, los archivos de correspondencia y agendas personales.
- B) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
- C) Las creadas y reguladas por leyes especiales.

Artículo. 3º.- Ámbito territorial. Los tratamientos de datos personales están sometidos a la Ley que se reglamenta cuando:

- A) Sean efectuados por un responsable de base de datos o tratamiento establecido en territorio uruguayo, siendo éste el lugar donde ejerza su actividad, cualquiera sea su forma jurídica.



B) El responsable de la base de datos o tratamiento no esté establecido en territorio uruguayo pero utilice en el tratamiento de datos medios situados en el país.

Exceptúanse de la regla precedente, los casos en que los citados medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable de la base de datos o tratamiento designe un representante, con domicilio y residencia permanente en territorio nacional, ante el Órgano de Control, a los efectos de cumplir con las obligaciones previstas por la Ley que se reglamenta y en esta reglamentación. Tal designación no impedirá las acciones legales que puedan ser promovidas contra el responsable de la base de datos o tratamiento, ni disminuirá su responsabilidad en cuanto al cumplimiento de las obligaciones impuestas legal o reglamentariamente.

Capítulo II. Definiciones

Artículo 4º.- Definiciones. A los efectos del presente reglamento, y sin perjuicio de las definiciones contenidas en la Ley que se reglamenta, se entiende por:

A) Bloqueo de datos: procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento.

B) Cancelación o Supresión de datos: procedimiento mediante el cual el responsable cesa en el uso de los datos. La supresión o cancelación implicará el bloqueo de dichos datos durante el plazo establecido en la normativa vigente; vencido éste se deberá proceder a su eliminación definitiva.

C) Cesión de datos: comunicación de acuerdo con lo establecido en el artículo 4º literal B) de la Ley que se reglamenta.

D) Dato personal relacionado con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética.

E) Exportador de datos personales: la persona física o jurídica, pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a otro país.

F) Importador de datos personales: persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de éstos, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

G) Interesado: titular del dato de acuerdo con lo establecido en el artículo 4º literal L) de la Ley que se reglamenta.

H) Transferencia internacional de datos: tratamiento de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo



por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.

Capítulo III. Consentimiento

Artículo 5º.- Consentimiento informado para recolección y tratamiento de datos. Cuando se solicite el consentimiento del titular para la recolección y tratamiento de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos, y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario, el consentimiento será nulo.

Artículo 6º.- Formas de recabar el consentimiento. Deberá facilitarse al titular un medio sencillo, claro y gratuito para que manifieste su consentimiento o su negativa al tratamiento de sus datos.

Se entenderá cumplido tal deber cuando se permita al titular la elección entre dos opciones claramente identificadas, que no se encuentren premarcadas a favor o en contra.

Corresponderá al responsable de la base de datos o el tratamiento recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, por parte del titular, a través de cualquier medio conforme a derecho.

El responsable de la base de datos o el tratamiento podrá solicitar el consentimiento del titular a través del procedimiento establecido en este artículo, sin perjuicio de otras formas o modalidades que le ofrezcan similares o superiores garantías.

Vencido el plazo de diez días hábiles desde que el titular de los datos reciba la solicitud de consentimiento sin que se manifieste, su silencio equivaldrá a una negativa.

Capítulo IV. Seguridad

Artículo 7º.- Medidas de seguridad. Tanto el responsable como el encargado de la base de datos o tratamiento deberán proteger los datos personales que sometan a tratamiento, mediante aquellas medidas técnicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad.

Artículo 8º.- Vulneración de seguridad. Cuando el responsable o encargado de la base de datos o tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos de los interesados, deberán informarles de este extremo.

TÍTULO II. Derechos de los Titulares de Datos

Capítulo I. Derecho de acceso



Artículo 9º.- Derechos de los titulares de los datos. Los derechos de los titulares de los datos previstos en la Ley que se reglamenta se ejercerán:

A) Por el titular o su representante, acreditando la identidad de ambos en su caso; se aplicará por extensión a las personas jurídicas en cuanto corresponda.

B) En forma conjunta o independiente.

C) Exento de formalidades y en forma gratuita.

D) Mediante comunicación dirigida al responsable de la base de datos o tratamiento, que contendrá:

a. Identificación del titular.

b. Motivo de la solicitud.

c. Domicilio real y domicilio constituido a efecto de las notificaciones.

d. Fecha y firma del solicitante.

e. Documentos acreditantes de la solicitud.

El responsable deberá contestar la solicitud en el plazo de cinco días hábiles desde su presentación.

La información que se proporcione, cualquiera sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos.

Artículo. 10º.- Derecho de rectificación. El derecho de rectificación es el que tiene el titular a que se modifiquen los datos que resulten ser inexactos o incompletos.

Artículo. 11º.- Derecho de actualización. El derecho de actualización es el que tiene el titular a que se modifiquen los datos que resulten inexactos a la fecha de ejercicio del derecho.

Artículo. 12º.- Derecho de inclusión. El derecho de inclusión es el que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando acredite un interés fundado.

Artículo. 13º.- Derecho de supresión. El derecho de supresión es el que tiene el titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados o excesivos.

La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas y de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular, que justificaren el tratamiento de los datos.

El responsable deberá documentar ante el titular haber cumplido con lo solicitado indicando las cesiones o transferencias de los datos suprimidos e identificando al cesionario.



Artículo. 14º.- Derechos referentes a la comunicación o la cesión de datos. La comunicación o la cesión de datos a terceros, solamente procede para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario de ésta, previo consentimiento del titular de los datos a quien se le debe informar inequívocamente la finalidad de dicha comunicación, identificando al destinatario y el tipo de actividad que desarrolla.

No se considera comunicación o cesión de datos el acceso por parte de un encargado de tratamiento, que resulte necesario para la prestación de un servicio al responsable, salvo que este acceso implique la existencia de un nuevo vínculo entre el encargado del tratamiento y el titular.

TÍTULO III. RÉGIMEN REGISTRAL

Capítulo I. Inscripción en el Registro de Bases de Datos

Personales

Artículo 15º.- Actos y documentos inscribibles. En el Registro de Bases de Datos Personales de la URCDP, creado por el artículo 1º del Decreto Nº 664/008, de 22 de diciembre de 2008, deberán inscribirse:

A) Las personas físicas que creen, modifiquen o supriman bases de datos de carácter personal, que no sean para uso exclusivamente personal o doméstico.

B) Las personas jurídicas públicas, estatales o no, y las privadas, que creen, modifiquen o supriman bases de datos de carácter personal, salvo las excepciones previstas en la Ley que se reglamenta.

De acuerdo con lo establecido en el art. 3 de la mencionada Ley no es de aplicación la excepción del ámbito personal o doméstico para las personas jurídicas.

C) Los códigos de conducta de práctica profesional que establezcan normas para el tratamiento de datos personales.

D) Las autorizaciones de transferencias internacionales de datos personales.

Esta inscripción se llevará a cabo bajo los criterios reglamentarios contenidos en la Ley, en el presente Decreto, en el Decreto Nº 664/008, de 22 de diciembre de 2008, u otras disposiciones que dicte la URCDP, de conformidad a las facultades legales conferidas.

Artículo. 16º.- Contenido y forma de inscripción. Los responsables de todas las bases de datos o tratamientos deberán inscribirlas en el Registro de la URCDP de acuerdo con el artículo 5º del Decreto Nº 664/008, de 22 de diciembre de 2008, proporcionando la siguiente información:

A) Identificación de la base de datos y el responsable de la misma.

B) Procedimientos de obtención y tratamiento de los datos.

C) Medidas de seguridad y descripción técnica de la base de datos.



- D) Protección de datos personales y ejercicio de derechos.
 - E) Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos.
 - F) Tiempo de conservación de los datos.
 - G) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
 - H) Datos sometidos a tratamiento en dicha base de datos.
 - I) Certificación de firma del responsable de cada base de datos.
 - J) Domicilio constituido y correo electrónico a efectos de las notificaciones.
- Sin perjuicio de éstos, la URCDP quedará facultada para agregar los elementos que considere necesarios.

Artículo. 17º.- Plazo de inscripción. Las bases de datos de carácter personal existentes, dispondrán de un plazo máximo de 90 días contados a partir de la publicación del presente Decreto en el Diario Oficial, para adecuarse a los requisitos y las condiciones de inscripción establecidos en la presente reglamentación y proceder a su registro. Las bases de datos que se crearen con posterioridad a la fecha de la aprobación del decreto, deberán ser inscriptas dentro de un plazo máximo de 90 días a partir del inicio de sus actividades.

Artículo. 18º.- Inscripción provisoria. En todas las inscripciones previstas por la Ley que se reglamenta, vencido el término de diez días hábiles previsto en el artículo 5º literal B) del Decreto N° 664/008, de 22 de diciembre de 2008, sin que se regularice la inscripción provisoria, ésta caducará de pleno derecho.

Artículo. 19º.- Fecha de la inscripción. Se computará como fecha de inscripción definitiva la correspondiente a la Resolución de la URCPD.

Los responsables de bases de datos de carácter personal deberán exhibir en un lugar visible accesible a los usuarios el número y fecha de la citada resolución.

Artículo. 20º.- Actualización al Registro. Los responsables de las bases de datos deberán mantener actualizados los datos inscriptos en el Registro de Base de Datos Personales, comunicando trimestralmente las actualizaciones.

TÍTULO IV. ÓRGANO DE CONTROL

Capítulo I. Presidencia

Artículo 21º.- Presidencia de la URCDP. La dirección técnica y administrativa de la URCDP será ejercida por un Consejo Ejecutivo de tres miembros, de acuerdo con lo establecido en el artículo 31 de la Ley que se reglamenta.



La Presidencia de la URCDP será rotativa anualmente entre los integrantes del Consejo Ejecutivo, a excepción del Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). En ausencia temporal del Presidente de la URCDP, la Presidencia será ejercida en forma interina por el restante miembro nombrado por el Poder Ejecutivo.

Artículo. 22º.- Cometidos del Presidente. Al Presidente del Consejo Ejecutivo o a quien lo sustituya corresponde:

- A) La representación de la URCDP en sus relaciones externas por sí o por medio de apoderado en forma.
- B) Cumplir y hacer cumplir las normas constitucionales, legales y reglamentarias y ejecutar y hacer ejecutar las decisiones del Consejo Ejecutivo.
- C) Presidir las sesiones del Consejo Ejecutivo y dirigir sus deliberaciones.
- D) Adoptar las medidas que creyere conveniente en caso de urgencia, dando cuenta en la primera sesión del Consejo Ejecutivo y estando a lo que se resuelva.
- E) Estructurar el orden del día.
- F) Convocar las sesiones ordinarias y extraordinarias.
- G) Someter a la aprobación del Consejo Ejecutivo la planificación de la Unidad y el proyecto de memoria anual.
- H) Firmar las actas, las resoluciones del Consejo Ejecutivo y la correspondencia oficial.
- I) Firmar los contratos y documentos de cualquier naturaleza, debidamente autorizados por el Consejo Ejecutivo.
- J) Fiscalizar la administración ejecutiva y el desempeño de los funcionarios y demás personas que presten servicios en la URCDP, dando cuenta al Consejo Ejecutivo.

Capítulo II. Consejo Ejecutivo

Artículo 23º.- Atribuciones del Consejo Ejecutivo. El Consejo Ejecutivo tendrá los siguientes cometidos:

- A) Difundir los derechos que con este régimen se garantizan y propiciar su conocimiento.
- B) Concertar convenios con organismos internacionales, previa autorización del Poder Ejecutivo.
- C) Asegurar la regularidad y eficiencia de las actividades propias de la Unidad, ejerciendo las potestades que le asigna la Ley que se reglamenta y las de administración correspondientes a la Unidad.
- D) Designar al funcionario o funcionarios que representarán a la Unidad en todas aquellas gestiones en que no fuere posible la intervención del Consejo Ejecutivo o de alguno de sus miembros.



- E) Dictar las normas y reglamentaciones que se deben cumplir en el desarrollo de las actividades comprendidas por la Ley que se reglamenta; incluyendo las medidas de seguridad en el tratamiento y conservación de los datos personales, que deberán observar los responsables, encargados y usuarios de bases de datos públicas y privadas.
- F) Resolver dentro de su competencia, todos los asuntos que propongan sus miembros.
- G) Realizar todas aquellas actividades necesarias para el cumplimiento de sus cometidos.
- H) Asesorar al Poder Ejecutivo sobre la normativa y proyectos de ley, en sus diferentes etapas, que refieran total o parcialmente a la protección de datos personales.
- I) Solicitar informes circunstanciados a entidades públicas y privadas, garantizando la seguridad y confidencialidad de los datos y elementos recibidos.
- J) Aplicar sanciones de acuerdo con lo establecido en el artículo 35 de la Ley que se reglamenta.
- K) Mantener actualizado y disponible para la consulta el Registro de Bases de Datos Personales.
- L) Expedir las autorizaciones previstas en la Ley que se reglamenta.
- M) Expedir certificados de inscripción y habilitación en caso de corresponder.

Artículo 24º.- Funcionamiento del Consejo Ejecutivo. El Consejo Ejecutivo dictará su reglamento interno, con las siguientes bases:

- A) Las resoluciones se tomarán por mayoría. Si se produjera empate el asunto será tratado en la próxima sesión y si éste subsistiera, el voto del Presidente se computará doble.
- B) Cuando el Consejo Ejecutivo lo resuelva podrá formar Comisiones Especiales, ya sea con carácter permanente o extraordinario, con el objeto de asesorar o realizar trabajos, estudios o investigaciones que se dispongan.

Artículo 25º.- Publicidad. La URCDP hará públicas las resoluciones que adopte, mediante la publicación en su sitio web, en forma posterior a la notificación. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan.

En el caso de dictarse actos de carácter general se publicarán en el sitio web antes indicado y en el Diario Oficial.

Capítulo III. Consejo Consultivo

Artículo 26º.- Funcionamiento del Consejo Consultivo. El Consejo Consultivo será convocado por el Consejo Ejecutivo, con una antelación mínima de cinco días y sesionará con una mayoría simple de sus integrantes.

Habiendo quórum para sesionar, el Presidente declarará abierta la sesión, disponiendo leer el acta o actas anteriores correlativas si las hubiera.



De todo lo actuado por el Consejo Consultivo se dejará constancia en acta, la cual una vez aprobada será firmada por todos los asistentes.

Artículo 27º.- Votación. Las decisiones se tomarán por mayoría de sus miembros. El Presidente tiene voz pero no voto.

Artículo 28º.- Elección de representantes del Consejo Consultivo. El representante del área académica en el Consejo Consultivo será designado por la Facultad de Derecho de la Universidad de la República a propuesta del Instituto de Derecho Informático.

El representante del sector privado en el Consejo Consultivo será designado por la Cámara Nacional de Comercio y de Servicios.

TÍTULO V. NORMAS DE ACTUACIÓN

Artículo 29º.- Principios aplicables. La actuación administrativa de la URCDP se desarrollará con arreglo a los principios de imparcialidad, celeridad, eficacia, verdad material, informalismo, debido proceso, impulsión de oficio, buena fe, motivación de las decisiones y simplicidad, los que servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la tramitación de cualquier asunto.

Artículo 30º.- Tramitación. Iniciado un asunto, de naturaleza interna o externa, promovido por un interesado o de oficio, su instrucción deberá completarse en el mínimo tiempo posible.

En todo lo no previsto expresamente en este Decreto, se aplicarán las normas contenidas en el Decreto Nº 500/991, de 27 de setiembre de 1991 y sus modificativos.

Artículo 31º.- Procedimiento relativo al ejercicio de la potestad sancionatoria. Ante una posible infracción de la Ley Nº 18.331 y su reglamentación, la URCDP podrá:

A) Realizar las inspecciones que el Consejo Ejecutivo entienda pertinente, las que serán dispuestas por resolución fundada.

B) Solicitar ante la justicia competente las medidas pertinentes, cuando exista riesgo de pérdida de la prueba. La solicitud de dichas medidas necesitará resolución fundada del Consejo Ejecutivo.

C) Comunicar las actuaciones al responsable de la base de datos o tratamiento a efectos de otorgarle vista, confiriéndole un plazo de diez días, contados a partir del siguiente al de su notificación para evacuarla. Transcurrido el plazo establecido, se elevarán las actuaciones para resolución del Consejo Ejecutivo, el que tendrá un plazo de treinta días para expedirse. La resolución que recaiga será impugnabile de acuerdo con las normas vigentes en la materia.



Artículo 32º.- Multas. El monto de las multas previstas en el numeral 2) del artículo 35 de la Ley que se reglamenta, será recaudado por AGESIC y la totalidad de lo producido por su cobro se verterá a Rentas Generales.

Artículo 33º.- Suspensión. La AGESIC promoverá la suspensión de la base de datos de acuerdo con lo previsto en el art. 35 numeral 3º de la Ley 18.331, previo pronunciamiento del Consejo Ejecutivo de la URCDP, en los casos que se comprobare que se han infringido o transgredido la Ley y/o su reglamentación.

Artículo 34º.- Procedimiento de autorización de transferencias internacionales de datos. El procedimiento para la autorización de transferencia internacional de datos a terceros países, de conformidad con lo expresado en el artículo 23 de la Ley que se reglamenta, se iniciará siempre a solicitud del exportador que pretenda llevarla a cabo.

Artículo 35º.- Contenido de la solicitud de transferencia internacional de datos. Dicha solicitud, además de los requisitos legalmente exigidos, deberá contener:

A) La identificación de la base de datos y su código de inscripción en el Registro de Bases de Datos Personales.

B) La descripción de la transferencia, respecto de la que se solicita la autorización, con indicación de la finalidad que la justifica, adjuntando la documentación acreditante.

Cuando la autorización se fundamente en la existencia de un contrato entre el importador y el exportador de los datos, deberá aportarse copia del mismo acreditándose la concurrencia de poder suficiente de sus otorgantes.

Podrán realizarse transferencias internacionales de datos en empresas multinacionales, únicamente entre la matriz y sus filiales y/ o sucursales y entre éstas, cuando posean códigos de conducta debidamente inscriptos ante la URCDP. Esto será de aplicación a los organismos internacionales.

Artículo 36º.- Procedimiento de inscripción de códigos de conducta. El procedimiento para inscripción en el Registro de Bases de Datos Personales de los códigos de conducta se iniciará siempre a solicitud del responsable de la base de datos.

La solicitud deberá acompañarse de los siguientes documentos:

A) Identificación de la institución.

B) Identificación del código de conducta y su responsable.

C) Contenido del código de conducta.

La inscripción de los códigos de conducta se registrará por el mismo procedimiento establecido para las bases de datos.



Artículo 37º.- Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos. El procedimiento para la autorización de conservación de datos personales con fines históricos, estadísticos o científicos se iniciará siempre a petición del responsable que pretenda obtener la declaración.

En el escrito de solicitud el responsable deberá:

- A) Identificar el tratamiento de datos al que pretende aplicarse la excepción.
- B) Establecer las causas que justificarían la declaración.
- C) Presentar las medidas que el responsable de la base de datos se propone implantar para garantizar el derecho a los ciudadanos.
- D) Acompañar los documentos necesarios para justificar su solicitud.

Previo a adoptar resolución, la URCDP podrá solicitar la opinión de instituciones u organismos, públicos o privados, que tengan competencia o mérito para ser consultados en relación al caso.

Artículo 38º.- Tratamiento con fines históricos, estadísticos o científicos. La URCDP podrá, previa solicitud del responsable del tratamiento conforme al procedimiento establecido en el artículo precedente, autorizar el mantenimiento íntegro o parcial de los datos, atendiendo a la finalidad de sus valores históricos, estadísticos o científicos.

Artículo 39º.- Suspensión de la eliminación de la base de datos. La presentación de la solicitud suspende la obligación de eliminar la base de datos, hasta tanto se decida sobre la misma.

Artículo 40º.- Derogación. Deróganse el literal d) del artículo 5º y el artículo 6 del Decreto 664/2008 de 22 de diciembre de 2008.

Artículo. 41º.- Comuníquese, publíquese, etc. 