**Legislación**

**Trabajo Práctico Ley de Habeas Data**

**LEY DE HABEAS DATA**

Ley 25.326 - DECRETO Nº 995

Objeto

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas,

Definiciones

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- Archivo, registro, base o banco 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.

- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Licitud

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos

Calidad de los datos

Los datos personales que se recojan deben ser ciertos, adecuados, pertinentes y no excesivos.

La recolección de datos no puede hacerse por medios desleales,

Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

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

Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Consentimiento

El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá se fehaciente

No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

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 a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes

Información

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados.

b) La existencia del archivo, registro, banco de datos.

c) El carácter obligatorio o facultativo de las respuestas al cuestionario.

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Categoría de datos

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes.

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.

Seguridad de los datos

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Deber de confidencialidad

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial.

Cesión

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley.

c) Se realice entre dependencias de los órganos del Estado.

d) Se trate de datos personales relativos a la salud.

e) Se hubiera aplicado un procedimiento de disociación de la información.

4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas.

Transferencia internacional

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional.

b) Intercambio de datos de carácter médico.

c) Transferencias bancarias o bursátiles.

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales.

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Derechos de los titulares de datos

Derecho de Información

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

Derecho de acceso

El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales.

El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses.

Contenido de la información

La información debe ser suministrada en forma clara.

La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular.

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

Derecho de rectificación, actualización o supresión

Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado.

El incumplimiento de esta obligación habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data.

Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables.

Excepciones

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

Gratuidad

La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

Registro de archivos de datos. Inscripción

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) 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.

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

Archivos, registros o bancos de datos públicos

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Organos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Supuestos especiales

1. 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 los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquéllos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública sin consentimiento de los afectados, 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.

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

Prestación de servicios informatizados de datos personales

1. 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.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos

Prestación de servicios de información crediticia

En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito.

A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses

Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años

La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Archivos, registros o bancos de datos con fines de publicidad

En la recopilación de domicilios, reparto de documentos, se podrán tratar datos que sean aptos para establecer perfiles determinados 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.

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

Archivos, registros o bancos de datos relativos a encuestas

Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

Órgano de Control

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 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 archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

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) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Vetado pór el Poder Ejecutivo

3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones. Vetado por el Poder Ejecutivo

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.

Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control

Sanciones

el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

Sanciones penales

1°. Será reprimido con la pena de prisión de un mes a dos años el que insertará o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionará a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

"Será reprimido con la pena de prisión de un mes a dos años el que:

1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.

2°. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

**Reglamentación**

**PROTECCION DE LOS DATOS PERSONALES**

Decreto 1558/2001

**CAPITULO II**

**PRINCIPIOS GENERALES RELATIVOS A LA PROTECCION DE DATOS**

**ARTICULO 4º.**-

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES efectuará controles de oficio sobre el cumplimiento de este principio legal, y aplicará las sanciones pertinentes al responsable o usuario en los casos que correspondiere.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES procederá, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar el cumplimiento de las disposiciones legales y reglamentarias en orden a cada una de las siguientes etapas del uso y aprovechamiento de datos personales:

a) legalidad de la recolección o toma de información personal;

b) legalidad en el intercambio de datos y en la transmisión a terceros o en la interrelación entre ellos;

c) legalidad en la cesión propiamente dicha;

d) legalidad de los mecanismos de control interno y externo del archivo, registro, base o banco de datos.

**ARTICULO 5º.**- El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley Nº 25.326.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración.

El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo.

No es necesario el consentimiento para la información que se describe en los incisos a), b), c) y d) del artículo 39 de la Ley Nº 21.526.

En ningún caso se afectará el secreto bancario, quedando prohibida la divulgación de datos relativos a operaciones pasivas que realicen las entidades financieras con sus clientes, de conformidad con lo dispuesto en los artículos 39 y 40 de la Ley Nº 21.526.

**ARTICULO 9º.**- La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES promoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización.

**ARTICULO 11.**- Al consentimiento para la cesión de los datos le son aplicables las disposiciones previstas en el artículo 5º de la Ley Nº 25.326 y el artículo 5º de esta reglamentación.

En el caso de archivos o bases de datos públicas dependientes de un organismo oficial que por razón de sus funciones específicas estén destinadas a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto.

La cesión masiva de datos personales de registros públicos a registros privados sólo puede ser autorizada por ley o por decisión del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto a los principios de protección establecidos en la Ley Nº 25.326. No es necesario acto administrativo alguno en los casos en que la ley disponga el acceso a la base de datos pública en forma irrestricta. Se entiende por cesión masiva de datos personales la que comprende a un grupo colectivo de personas.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES fijará los estándares de seguridad aplicables a los mecanismos de disociación de datos.

El cesionario a que se refiere el artículo 11, inciso 4, de la Ley Nº 25.326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.

**ARTICULO 12.**- La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.

**DERECHOS DE LOS TITULARES DE DATOS**

**ARTICULO 14.**-

El derecho de acceso permitirá:

a) conocer si el titular de los datos se encuentra o no en el archivo, registro, base o banco de datos;

b) conocer todos los datos relativos a su persona que constan en el archivo;

c) solicitar información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos;

d) solicitar las finalidades para las que se recabaron;

e) conocer el destino previsto para los datos personales;

f) saber si el archivo está registrado conforme a las exigencias de la Ley Nº 25.326.

**ARTICULO 15**

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES elaborará un formulario modelo que facilite el derecho de acceso de los interesados.

Podrán ofrecerse como medios alternativos para responder el requerimiento, los siguientes:

a) visualización en pantalla;

b) informe escrito entregado en el domicilio del requerido;

c) informe escrito remitido al domicilio denunciado por el requirente;

d) transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información;

e) cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario del mismo.

**CAPITULO IV**

**USUARIOS Y RESPONSABLES DE ARCHIVOS, REGISTROS Y BANCOS DE DATOS**

**ARTICULO 21.**- El registro e inscripción de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se habilitará una vez publicada esta reglamentación en el Boletín Oficial.

Deben inscribirse los archivos, registros, bases o bancos de datos públicos y los privados a que se refiere el artículo 1º de esta reglamentación.

A los fines de la inscripción de los archivos, registros, bases y bancos de datos con fines de publicidad, los responsables deben proceder de acuerdo con lo establecido en el artículo 27, cuarto párrafo, de esta reglamentación.

**ARTICULO 25.**- Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento y que disponga, en particular:

a) que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

b) que las obligaciones del artículo 9º de la Ley Nº 25.326 incumben también al encargado del tratamiento.

**ARTICULO 26.**- A los efectos del artículo 26, inciso 2, de la Ley Nº 25.326, se consideran datos relativos al cumplimiento o incumplimiento de obligaciones los referentes a los contratos de mutuo, cuenta corriente, tarjetas de crédito, fideicomiso, leasing, de créditos en general y toda otra obligación de contenido patrimonial, así como aquellos que permitan conocer el nivel de cumplimiento y la calificación a fin de precisar, de manera indubitable, el contenido de la información emitida.

En el caso de archivos o bases de datos públicos dependientes de un organismo oficial destinadas a la difusión al público en general, se tendrán por cumplidas las obligaciones que surgen del artículo 26, inciso 3, de la Ley Nº 25.326 en tanto el responsable de la base de datos le comunique al titular de los datos las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido difundidas durante los últimos SEIS (6) meses.

Para apreciar la solvencia económico-financiera de una persona, conforme lo establecido en el artículo 26, inciso 4, de la Ley Nº 25.326, se tendrá en cuenta toda la información disponible desde el nacimiento de cada obligación hasta su extinción. En el cómputo de CINCO (5) años, éstos se contarán a partir de la fecha de la última información adversa archivada que revele que dicha deuda era exigible. Si el deudor acredita que la última información disponible coincide con la extinción de la deuda, el plazo se reducirá a DOS (2) años. Para los datos de cumplimiento sin mora no operará plazo alguno para la eliminación.

A los efectos del cálculo del plazo de DOS (2) años para conservación de los datos cuando el deudor hubiere cancelado o extinguido la obligación, se tendrá en cuenta la fecha precisa en que se extingue la deuda.

A los efectos de dar cumplimiento a lo dispuesto por el artículo 26, inciso 5, de la Ley Nº 25.326, el BANCO CENTRAL DE LA REPUBLICA ARGENTINA deberá restringir el acceso a sus bases de datos disponibles en Internet, para el caso de información sobre personas físicas, exigiendo el ingreso del número de documento nacional de identidad o código único de identificación tributaria o laboral del titular de los datos, obtenidos por el cesionario a través de una relación contractual o comercial previa.

**ARTICULO 27.**- Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.

Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los NOVENTA (90) días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros.

En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.

A los fines de garantizar el derecho de información del artículo 13 de la Ley Nº 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse, las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio.

Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la Ley Nº 25.326.

Los datos vinculados a la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley Nº 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6º y 11, inciso 1, de la Ley Nº 25.326 y la mención de su derecho a solicitar el retiro de la base de datos.

**ARTICULO 28.**- Los archivos, registros, bases o bancos de datos mencionados en el artículo 28 de la Ley Nº 25.326 son responsables y pasibles de las multas previstas en el artículo 31 de la ley citada cuando infrinjan sus disposiciones.

**CAPITULO V**

**CONTROL**

**ARTICULO 29.**

1. Créase la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la Ley Nº 25.326.

PUNTOS CLAVES DE LA LEY

Los puntos clave de la Ley de Protección de Datos Personales de Argentina:

1. Consentimiento: Las organizaciones deben obtener el consentimiento informado y expreso de las personas antes de recopilar y procesar sus datos personales.

2. Derechos de los titulares de datos: Los titulares de datos tienen derechos, como el acceso a sus datos personales, la rectificación de información incorrecta, la eliminación de datos innecesarios o desactualizados, y la oposición al tratamiento de sus datos en ciertas circunstancias.

3. Seguridad de datos: Las organizaciones deben implementar medidas de seguridad adecuadas para proteger los datos personales de accesos no autorizados o divulgación.

4. Transferencias internacionales: La ley establece restricciones y requisitos para la transferencia de datos personales fuera de Argentina, asegurando que se mantenga un nivel adecuado de protección de datos.

5. Registro de bases de datos: Las organizaciones que procesan datos personales deben registrar sus bases de datos en el Registro Nacional de Bases de Datos, y estas bases de datos deben cumplir con los principios y requisitos establecidos por la ley.

6. Responsable de datos: Las organizaciones deben designar a una persona responsable de la protección de datos personales (llamado "Encargado" o "Responsable" en la ley) que se encargue de cumplir con las obligaciones establecidas por la ley.

Otras normas consultadas

* Ley 25.326 de Protección de Datos Personales
* Ley 27.409 de Infraestructura Crítica
* Reglamento General de Protección de Datos (RGPD)
* Ley 25.506 de Firma Digital
* Ley 26.951 de Ciberseguridad

Resultados de su lectura e interpretación:

A través del análisis de las regulaciones pertinentes, se han identificado las siguientes normativas que deben ser implementadas con el propósito de cumplir con los requisitos establecidos por la Ley de Habeas Data:

1. Clasificación de la información: Esta normativa adquiere un papel fundamental en la identificación precisa de los datos personales que requieren salvaguardia y protección.
2. Consentimiento informado: Esta normativa estipula de manera inequívoca que la recopilación de datos personales solo puede llevarse a cabo previa obtención del consentimiento expreso por parte del titular de dichos datos.
3. Seguridad de la información: Esta regulación establece de manera categórica la obligación de salvaguardar los datos personales contra cualquier forma de acceso no autorizado, uso indebido, divulgación, alteración o destrucción.

Recomendaciones y Normativas Relacionadas

Recomendaciones:

En aras de fortalecer la salvaguardia de los datos personales, se sugiere la adopción de las siguientes medidas adicionales:

1. Implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI): La instauración de un SGSI auxilia a las organizaciones en la identificación, evaluación y mitigación de los riesgos inherentes a la seguridad de la información.

2. Formación de los empleados en materia de protección de datos personales: Resulta imperativo instruir a los empleados acerca de la trascendencia de la protección de datos personales y de las medidas que deben adoptar para preservar dicha información.

3. Realización de auditorías periódicas: Las auditorías regulares constituyen una herramienta fundamental para verificar la eficacia de las medidas de seguridad de la información.

Normativas Específicas:

A continuación, se detallan las normativas específicas que deben ser implementadas para cumplir con la Ley de Habeas Data:

1. Clasificación de la información (Normativa 203):

Conforme a la Ley de Habeas Data, se establece la obligación de categorizar los datos personales según su nivel de sensibilidad. Estos datos se pueden dividir en dos categorías principales:

a. Datos sensibles: Incluyen información que revela aspectos como la raza, origen étnico, opiniones políticas, convicciones religiosas, estado de salud o vida sexual de una persona.

b. Datos no sensibles: Agrupan aquellos datos personales que no contienen información de la naturaleza mencionada previamente.

La clasificación de la información es esencial para garantizar la implementación de medidas de protección más rigurosas sobre los datos personales sensibles.

2. Consentimiento informado (Artículo 5 de la Ley 25.326):

De acuerdo con la Ley de Habeas Data, la recolección de datos personales solo es admisible previa obtención del consentimiento explícito del titular de dichos datos. Este consentimiento debe cumplir con los siguientes criterios:

a. Debe ser otorgado de manera libre, sin coacción ni presión alguna.

b. Debe ser expreso, indicando claramente la voluntad del titular de conceder el consentimiento.

c. Debe ser informado, lo que significa que el titular debe estar debidamente instruido acerca del propósito de la recopilación de datos y de sus derechos en relación a dicha información.

d. El consentimiento puede ser otorgado por escrito, verbalmente o mediante medios electrónicos.

Es importante destacar que existen excepciones en las cuales no se requiere el consentimiento del titular, como cuando el tratamiento es necesario para cumplir con obligaciones legales, ejecutar un contrato, proteger intereses vitales o realizar investigaciones científicas o históricas sin fines lucrativos.

3. Seguridad de la información (Normativas 205 seguridad física – Normativas 208 plan de contingencias – Normativa 221 acceso a los datos):

Conforme a la Ley de Habeas Data, se estipula que los datos personales deben estar protegidos contra el acceso no autorizado, uso indebido, divulgación, alteración o destrucción. Para lograr esta protección, las organizaciones deben implementar medidas de seguridad de la información, tales como:

a. Control de acceso: Limitar el acceso a datos personales únicamente a las personas autorizadas por sus responsabilidades.

b. Encriptación: Aplicar técnicas de encriptación para resguardar los datos personales contra divulgaciones no autorizadas.

c. Respaldo de datos: Realizar copias de seguridad de los datos personales con el propósito de prevenir pérdidas o destrucción accidental.

Implementación:

La implementación de estas normativas y recomendaciones demanda un esfuerzo sustancial por parte de las organizaciones, aunque resulta esencial para cumplir con las disposiciones de la Ley de Habeas Data y asegurar la integridad de los datos personales de los ciudadanos.

Normativas Adicionales Consideradas Aplicables a la Ley de Habeas Data:

- Normativa 203: Clasificación de Datos

Esta normativa cobra relevancia debido a la necesidad de:

a. Obtener el consentimiento expreso del titular de los datos para el tratamiento de datos sensibles.

b. Establecer una finalidad específica y legítima para el tratamiento de datos sensibles.

c. Garantizar que el tratamiento de datos sensibles sea proporcional a la finalidad establecida.

El incumplimiento de estos requisitos conlleva posibles sanciones administrativas para los responsables del tratamiento de datos personales.

- Normativa 206: Proyectos de Sistemas de Información

Esta normativa resulta crucial al definir los actores responsables en proyectos de sistemas de información, incluyendo el Comité de Información Pública, líderes de proyectos, responsables de áreas de desarrollo de sistemas, desarrolladores, programadores e implementadores. Asimismo, establece la importancia de la auditoría de sistemas de información para evaluar el cumplimiento de la norma.

La normativa 206 se enfoca en los requisitos que deben cumplir los proyectos de sistemas de información que manejan datos personales, garantizando la protección de dichos datos durante todo su ciclo de vida.

- Normativa 220: Gestión de Datos

Esta normativa subraya la necesidad de establecer niveles de autorización de acceso adecuados para garantizar la correcta definición de quiénes pueden acceder a los datos. Esto es esencial para evitar conflictos y filtraciones innecesarias, además de facilitar la identificación de responsables.

La gestión de datos, según la normativa 220, asegura un control adecuado sobre el acceso a la información, lo que contribuye a la seguridad y privacidad de los datos personales.

Es importante destacar que el cumplimiento de estas normativas es fundamental para garantizar la protección de datos personales en consonancia con la Ley de Habeas Data de Argentina.