DISPOSICION 7/2008
DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES (D.N.P.D.P.)

Hábeas data. Aprobación del documento "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público". Se aprueban el Texto modelo de "Convenio de Confidencialidad" y el diseño del isologotipo, denominado "Sello Argentino de Privacidad".
del 22/08/2008; Boletín Oficial 27/08/2008

VISTO el Expediente MJSyDH Nº166.118/08 y las competencias atribuidas a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES por la Ley Nº25.326 y su Decreto Reglamentario Nº1558 del 29 de noviembre de 2001, y
CONSIDERANDO:
Que en virtud de lo dispuesto en el Anexo III del Decreto Nº163 de fecha 2 de marzo de 2005, entre las funciones asignadas a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES se especifica, en el punto 15, la de "Coordinar las actividades de la Administración Pública Nacional referidas a la protección de datos personales".
Que, asimismo, entre las funciones de la citada Dirección Nacional se encuentra la de mantener un registro permanente de los archivos, registros, bases o bancos de datos alcanzados por la Ley Nº25.326.
Que mediante la Disposición DNPDP Nº02 del 20 de noviembre de 2003 se dispuso la habilitación del REGISTRO NACIONAL DE BASES DATOS y se aprobaron sus bases técnico-jurídicas.
Que por Disposición Nº02 del 1º de febrero de 2006 se implementó, a partir del 3 de abril de 2006, el RELEVAMIENTO INTEGRAL DE BASES DE DATOS PERSONALES DEL ESTADO NACIONAL, previéndose la posibilidad de que la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES dispusiera la inscripción en el REGISTRO NACIONAL DE BASES DE DATOS de aquellas bases que considerara se encontraban en condiciones de adecuación a la normativa vigente.
Que la inscripción en el ámbito público ha operado en su totalidad.
Que por ello, se estima pertinente aprobar una "GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO", como un documento de adopción voluntaria que establezca pautas de conducta con relación a la protección de los datos personales y en particular a la aplicación de pautas de confidencialidad.
Que con referencia a este último tema, también se ha considerado adecuado aprobar un texto modelo de "Convenio de Confidencialidad", a ser utilizado por los organismos públicos con el objetivo de optimizar la protección legal del titular de los datos personales y a fin de que los empleados públicos tomen conciencia de esta obligación.
Que en dicho documento, los funcionarios públicos se comprometen a mantener reserva de los datos personales a que pudieran acceder en ejercicio de sus funciones, así como también que conozcan que esa reserva se extiende aún concluida la relación laboral.
Que a fin de que los administrados conozcan qué organismos públicos han adoptado la Guía que se aprueba por la presente, quienes adhieran a sus términos y principios y se

hallen inscriptos en el REGISTRO NACIONAL DE BASES DE DATOS podrán solicitar a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la identificación correspondiente, consistente en un isologotipo que podrán utilizar en la página web propia, denominado "Sello Argentino de Privacidad".
Que con el objeto de garantizar la veracidad de la inclusión del isologotipo en la página web de cada uno de los requirentes, éstos deberán establecer sobre el mismo un enlace a la página web de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES en la que se publica el listado de los adherentes a la citada Guía.
Que con el objetivo de contar con un ámbito de participación, intercambio de experiencias y discusión de temas relacionados con la protección de los datos personales en el ámbito estatal, se propicia la creación del FORO DE PROTECCION DE DATOS PERSONALES.
Que el artículo 22 de la Ley Nº25.326 dispone que en el acto de creación de una base de datos pública se deben indicar, entre otros puntos, las oficinas ante las que se pudieren efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación, actualización, supresión o sometimiento a confidencialidad de datos personales.
Que a fin de facilitar la tarea de las dependencias que deban cumplir con esa misión, se ponen a disposición de las mismas instrucciones y modelos de escritos que éstas podrán proporcionar a los titulares de los datos interesados en el ejercicio de alguno de los citados derechos.
Que sin perjuicio de las funciones de asistencia y asesoramiento relativas a los alcances de la Ley Nº25.326 que tiene la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES respecto de todos las personas que lo requieran, lo que incluye también a los organismos públicos en general, se dispone crear una Mesa de Ayuda habilitada particularmente para atender las necesidades de los organismos que adhieran a la Guía que se aprueba por este acto.
Que la presente medida se dicta en uso de las facultades conferidas por el artículo 29, inciso 1, apartado b), de la Ley Nº25.326, el artículo 29, inciso 5, apartado e) del Anexo I del Decreto Nº1558 del 29 de noviembre de 2001 y el punto 15 del Anexo III del Decreto Nº163 del 2 de marzo de 2005.
Por ello,
EL DIRECTOR NACIONAL
DE PROTECCION DE DATOS PERSONALES
DISPONE:

Artículo 1º - Apruébese el documento "GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO", que como Anexo I forma parte del presente, como un instrumento orientativo en materia de reglas de privacidad y confidencialidad en el tratamiento de datos personales.
Art. 2º - Apruébese el texto modelo de "Convenio de Confidencialidad" que podrá ser adoptado por los distintos organismos públicos, que como Anexo II forma parte del presente.
Art. 3º - Apruébese el diseño del isologotipo que identificará a los organismos públicos que adhieran a los términos y principios contenidos en la "GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO", denominado "Sello Argentino de Privacidad", el que como Anexo III forman parte de la presente medida.
Art. 4º - Los organismos públicos que apliquen la Guía que se aprueba por el artículo 1º, podrán hacer uso del isologotipo aprobado por el artículo 2º en la página web propia. Para ello deberán solicitar mediante nota escrita la autorización de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la que proveerá el archivo gráfico correspondiente si se reúnen las condiciones indicadas.
Art. 5º - Aquellos organismos públicos que hagan uso de la opción dispuesta por la presente Disposición deberán establecer sobre el isologotipo un enlace a la página web de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES en la que se

publica el listado de los adherentes a la "GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO".
Art. 6º - Créase el FORO DE PROTECCION DE DATOS PERSONALES que será dirigido por el CENTRO DE JURISPRUDENCIA, INVESTIGACION Y PROMOCION DE LA PROTECCION DE LOS DATOS PERSONALES creado por Disposición DNPDP Nº03 del 11 de abril de 2008.
Art. 7º - Los organismos públicos adherentes a la Guía que se aprueba por este acto tendrán a su disposición las instrucciones y modelos de escritos que como Anexo IV se agregan a la presente, a fin de proporcionarlos a las personas que deseen efectuar trámites relacionados con la protección de sus datos personales relativos al ejercicio de los derechos de acceso, rectificación, actualización supresión y sometimiento a normas de confidencialidad de sus datos personales.
Art. 8º - Los organismos públicos adherentes a la Guía que se aprueba por la presente podrán utilizar la Mesa de Ayuda que se habilitará al efecto, para que puedan mantener actualizada su inscripción ante el REGISTRO NACIONAL DE BASES DE DATOS, así como para la resolución de cualquier inconveniente relacionado con la materia de protección de datos personales.
Art. 9º - Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.
Juan A. Travieso.

ANEXO I
GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD
PARA LAS BASES DE DATOS DEL AMBITO PUBLICO
I.- INTRODUCCION
II.- EL DERECHO A LA PROTECCION DE LOS DATOS PERSONALES EN LA LEY Nº25.326
• OBJETO
• DEFINICIONES
Datos personales
Datos sensibles
Archivo, registro, base o banco de datos
Tratamiento de datos
Responsable de archivo, registro, base o banco de datos
Datos informatizados
Titular de los datos
Usuario de datos
Disociación de datos
• PRINCIPIOS DE TRATAMIENTO DE DATOS PERSONALES
Calidad
No automaticidad
Datos sensibles
Consentimiento
Publicidad
Casos de no aplicabilidad de la ley de protección de datos personales
• TRATAMIENTOS BASICOS REGULADOS
Información a proporcionar al titular de los datos
Cesión de Datos Personales
Transferencia Internacional
• OBLIGACIONES DEL RESPONSABLE DEL BANCO DE DATOS
Inscripción
Seguridad de los datos
Secreto

Deber de respuesta
• DERECHOS DE LAS PERSONAS
Derecho de acceso
Derechos de rectificación, actualización, confidencialidad y supresión
Derecho de consulta al REGISTRO NACIONAL DE BASES DE DATOS
III.- TEMAS ESPECIALMENTE RELACIONADOS CON EL ESTADO NACIONAL
Decreto Nº1172/03 - Anexo VII - Acceso a la Información Pública
Supuestos especiales - artículo 23 de la Ley Nº25.326
IV.- SANCIONES
Sanciones disciplinarias
Sanciones administrativas
Sanciones penales

I.- INTRODUCCION

Todo tratamiento de datos personales genera un potencial riesgo para el derecho a la privacidad.

Para enfrentar esas amenazas se ha establecido el derecho humano a la autodeterminación informativa, esto es el derecho que tiene toda persona de controlar los alcances de su información personal.

En nuestro país, ello ha sido contemplado conforme lo establecido en el tercer párrafo del artículo 43 de la CONSTITUCION NACIONAL, cuando garantiza que toda persona podrá interponer acción de hábeas data para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos, no pudiendo afectarse el secreto de las fuentes de información periodística.

Posteriormente, la LEY Nº25.326, de Protección de Datos Personales, reglamentó esta garantía constitucional a fin de hacer efectiva la protección de los derechos de las personas.

La citada ley es una norma de orden público que exige que las bases de datos se ajusten a sus disposiciones, reglamentando la actividad de las bases de datos que procesan información personal, sea por medios informáticos o manuales y sometiéndolas a la supervisión y control de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Organo de Control a nivel nacional, que actúa en esfera del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS.

Más allá de los eventuales riesgos a la intimidad a que se ha aludido, así como de las previsiones legales para prevenirlos, no debe olvidarse que la evolución de la tecnología ha permitido, entre otras cosas, el desarrollo de una Administración Pública informatizada que acumula datos personales de los individuos, los que deben ser tratados por empleados públicos formados adecuadamente en políticas de privacidad y confidencialidad.

La presente GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO tiene por objeto lograr la optimización de los procesos de tratamiento de datos personales por parte de las bases de datos públicas, para lo cual es necesario impulsar un conjunto de acciones tendientes a modificar hábitos con el objetivo de encaminarlos hacia prácticas acordes con la protección de datos personales.

Al mismo tiempo, es un documento que procura instaurar entre los funcionarios públicos la cultura de la protección de datos personales como un elemento de singular importancia en el ejercicio de sus funciones.

Por ello, es importante que los agentes públicos suscriban convenios de confidencialidad a través de los cuales tomen conciencia de las implicancias de revelar información personal obtenida en el marco de sus tareas.

II.- EL DERECHO A LA PROTECCION DE LOS DATOS PERSONALES EN LA LEY Nº25.326

• OBJETO

La LEY Nº25.326 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, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional (artículo 1º).

• DEFINICIONES

A los fines de la ley 25.326 se entiende por:

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: 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: datos personales sometidos a 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.

• PRINCIPIOS DE TRATAMIENTO DE DATOS PERSONALES

Calidad: este principio requiere que los datos recabados sean: adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para la que fueron recogidos; que la recolección no pueda hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley; que no puedan utilizarse los datos para finalidades distintas o incompatibles con las que motivaron su obtención; que los datos sean exactos y puedan actualizarse; que se almacenen de modo que el titular pueda ejercer el derecho de acceso; que sean destruidos cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados.

No automaticidad: el poder público tiene prohibido adoptar decisiones judiciales o actos administrativos que tengan como "único" fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

Datos sensibles: estos datos sólo pueden tratarse cuando medien razones de interés general autorizadas por ley o con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Esto implica también que ninguna persona pueda ser obligada a proporcionar datos que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual y que esté prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, excepto que, como se dijo precedentemente existan razones de interés general autorizadas por ley (v.g.: la Ley Nº23.551 establece en el artículo 38 que los empleadores son agentes de retención de los importes que en concepto de cuotas de afiliación u otros aportes deban tributar los trabajadores a las asociaciones sindicales con personería gremial).

Consentimiento: por principio general el tratamiento de datos personales por parte de las entidades públicas no requerirá el consentimiento del titular de los datos, en la medida en que el organismo actúe dentro de su respectiva competencia.
Se requerirá el consentimiento sólo cuando el tratamiento de datos pretendido exceda las atribuciones específicas del órgano administrativo. En tal caso, el consentimiento deberá ser libre, expreso e informado y deberá realizarse por escrito o por otro medio que se le equipare. Dicho consentimiento puede ser revocado en cualquier momento, sin efectos retroactivos. Si el interesado revoca el consentimiento, el tratamiento de sus datos personales que se haga de allí en más será ilícito, por lo tanto la validez de la revocación debe considerarse al momento en que el organismo toma conocimiento de la misma y, si bien la Ley Nº25.326 consagra expresamente la gratuidad para el ejercicio de los derechos de rectificación, actualización y supresión, la revocación del consentimiento no podría de ninguna manera estar prohibida, en tanto la facultad del consentimiento forma parte del ejercicio de un derecho humano fundamental de orden público, eje sobre el que se desarrolla la licitud del tratamiento de datos personales. En caso de que los datos personales correspondientes a la persona que revoca el consentimiento hubiesen sido cedidos a un tercero, deberá notificarse tal circunstancia al cesionario, atento que tanto éste como el cedente responden solidaria y conjuntamente por la observancia de las normas de protección de datos personales ante el Organo de Control y el titular de los datos.
Publicidad: 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 sus datos personales incluidos en la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó dicha información.
Casos de no aplicabilidad de la ley de protección de datos personales: la LEY Nº25.326 no se aplica 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.
• TRATAMIENTOS BASICOS REGULADOS
Información a proporcionar al titular de los datos: el ciudadano tiene derecho a estar informado por completo acerca de los usos que se darán a sus datos personales, razón por la cual el responsable o usuario de la base de datos deberá informarle en forma expresa y clara acerca de la existencia del archivo, nombre del responsable y su domicilio; la finalidad de la base de datos y sus destinatarios; el carácter obligatorio u optativo de responder al cuestionario que se le proponga; las consecuencias de brindar datos, su negativa a darlos o la inexactitud de los mismos; la posibilidad de ejercer los derechos de acceso, rectificación o supresión y, en caso de preverse cesiones de los datos, a quién y con qué fin se cederán los mismos.
Cesión de Datos Personales: las distintas dependencias de la Administración Pública podrán ceder entre sí sus datos, en forma directa y sin consentimiento del titular de los datos, en la medida que sea necesario para el cumplimiento de sus respectivas competencias.
Los Organismos Públicos podrán ceder de manera no masiva al sector privado los datos personales no sensibles en su poder, cuando dicha cesión se realice con motivo del ejercicio de las funciones propias del organismo o en virtud de obligación legal y se justifique con el cumplimiento del requisito del interés legítimo, previa identificación del cesionario, verificando el fiel cumplimiento de los principios de protección de datos que resulten aplicables al caso y que con dicha cesión no se ocasionan perjuicios al titular del dato.
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 Nº25.326 y que con dicha cesión no se ocasionan perjuicios a los titulares del dato. 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.
No se podrán ceder datos sensibles, salvo para aquellos casos en los cuales existan razones de interés general fundadas en ley.
En todos los casos de cesión de datos personales, 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 ante el organismo de control y el titular de los datos de que se trate, aunque podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.
Transferencia Internacional: únicamente se realizará una transferencia internacional de datos personales cuando se garanticen niveles de protección adecuados, salvo que el titular preste su consentimiento expreso o se trate de colaboración judicial internacional, intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica previa disociación de los datos que no permita la identificación de sus titulares, transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable, cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte, 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.
No será necesario el consentimiento del titular del dato en caso de transferencia internacional de datos desde un registro público que esté legalmente constituido para facilitar información al público y que 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 legales y reglamentarias para la consulta.
Además del cumplimiento de los requisitos para la transferencia internacional, deberá cumplirse con los requisitos del art. 11 de la ley 25.326 en caso de que la misma consista en una cesión de datos.
La DIRECCION NACIONAL DE PROTECCION DE DATOS está facultada para evaluar de oficio o a petición de parte el adecuado nivel de protección de terceros países u organismos internacionales.
• OBLIGACIONES DEL RESPONSABLE DEL BANCO DE DATOS
Inscripción: para que el tratamiento de datos personales sea lícito, el titular del archivo de datos que contenga este tipo de datos deberá estar inscripto en el REGISTRO NACIONAL DE BASES DE DATOS que ha habilitado la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES del MINSTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS y respetar en su operación los principios que establece la Ley Nº25.326 y las reglamentaciones que se dicten en su consecuencia.
Seguridad de los datos: el responsable de la base de datos debe adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado, estando prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad.
Secreto: el deber de secreto respecto de los datos personales tratados, es una obligación que corresponde al responsable de la base de datos y a toda persona que efectúe tratamiento de datos personales, obligación que se mantiene aún finalizada la relación que permitió el acceso al banco de datos.
El obligado por el secreto profesional o normas de confidencialidad sólo puede ser relevado

de esa obligación por resolución judicial y cuando medien razones de seguridad y salud públicas, y de defensa nacional.
El funcionario público se encuentra particularmente sujeto a este deber en virtud de lo dispuesto en la legislación específica que regula su relación de empleo.
Teniendo en consideración que los funcionarios públicos toman conocimiento, en el desempeño de sus funciones, de información que puede contener datos personales, con el objetivo de optimizar la protección legal del titular de los datos personales y a fin de que se tome conciencia de esta obligación por parte de quienes tienen que cumplirla, resulta propicia la suscripción de convenios de confidencialidad, en los que los funcionarios se comprometan expresamente a mantener reserva de los datos personales a que accedan en ejercicio de sus funciones, así como también que conozcan que esa reserva se extiende aún concluida la relación laboral.
Deber de respuesta: el responsable o usuario del archivo, registro, base o banco de datos deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado, debiendo para ello valerse de cualquiera de los medios autorizados (por escrito, medios electrónicos, telefónicos, de imagen u otro medio idóneo a tal fin), a opción del titular de los datos, o las preferencias que el interesado hubiere expresamente manifestado al interponer el derecho de acceso.
La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES elaboró a tal fin un formulario modelo que facilita el derecho de acceso de los interesados.
• DERECHOS DE LAS PERSONAS
Derecho de acceso: el titular de los datos tiene derecho a conocer la totalidad de los datos referidos a su persona que pudieran existir en una base de datos.
Para ello, puede hacer uso del derecho de acceso, a fin de conocer si su información se encuentra registrada en ese archivo, registro, base o banco de datos y, en caso afirmativo, cuáles son los datos, las fuentes y los medios a través de los cuales se obtuvieron sus datos, como asimismo conocer las finalidades para las que se recabaron dichos datos y conocer el destino previsto para los mismos y, finalmente, saber si el archivo está registrado conforme a las exigencias de la LEY Nº25.326.
El reclamo se debe formular directamente ante el responsable del archivo o base de datos, quien deberá proporcionar la información dentro de los DIEZ (10) días corridos de recibida la solicitud. El incumplimiento de esta obligación habilitará al interesado a promover la acción judicial de Hábeas Data, así como también podrá denunciar el hecho ante la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.
Si se tratara de archivos o bancos de datos públicos dependientes de un organismo oficial destinados a la difusión al público en general, las condiciones para el ejercicio del derecho de acceso podrán ser propuestas por el organismo y aprobadas por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la cual deberá asegurar que los procedimientos sugeridos no vulneren ni restrinjan en modo alguno las garantías propias de ese derecho.
El derecho de acceso puede ser denegado 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, así como también cuando pudiera 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.
Derechos de rectificación, actualización y supresión: a solicitud del titular del dato, o advertido el error o falsedad, el responsable o usuario del banco de datos procederá, siempre de manera gratuita, a la rectificación, supresión o actualización de los datos personales del afectado dentro del plazo de CINCO (5) días hábiles de requerido. El incumplimiento de esta obligación habilitará al interesado a promover la acción judicial de Hábeas Data.
La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
Derecho de consulta al REGISTRO NACIONAL DE BASES DE DATOS: las personas

tienen el derecho de consultar al Organo de Control en forma gratuita sobre la existencia de archivos, registros o bases de datos, sus finalidades y la identidad de sus responsables.
El ejercicio de este derecho, que no debe confundirse con el antes mencionado derecho de acceso, facilita sin embargo el ejercicio de éste, por cuanto informa al titular de los datos aquellos antecedentes que necesita para formular su reclamo.
III.- TEMAS ESPECIALMENTE RELACIONADOS CON EL ESTADO NACIONAL
Decreto Nº1172/03 - Anexo VII - Acceso a la Información Pública
Por esta normativa se aprueba el Reglamento General de Acceso a la Información Pública para el Poder Ejecutivo Nacional con el objeto de constituir una instancia de participación ciudadana por la cual una persona pueda ejercitar su derecho a requerir, consultar y recibir información de los organismos, entidades, empresas, sociedades, dependencias y todo otro ente que actúe en jurisdicción de dicho poder.
Según lo establecido en el artículo 6º de dicha norma, el solicitante no necesita acreditar un interés legítimo a fin de requerir, consultar y recibir información de los organismos, entidades, empresas, sociedades, dependencias y todo otro ente que actúe en jurisdicción del Poder Ejecutivo Nacional, bastando la sola petición del solicitante para acceder a la información requerida. Sin embargo, en la Ley Nº25.326, es requisito para ceder información la existencia de interés legítimo tanto en cedente como en cesionario.
Por su parte, el artículo 16 del citado Decreto Nº1172/03 señala que los obligados a informar pueden exceptuarse de proveer la información requerida cuando una ley o decreto así lo establezca o, entre otros casos, cuando se trate de "información referida a datos personales de carácter sensible -en los términos de la Ley Nº25.326- cuya publicidad constituya una vulneración del derecho a la intimidad y al honor, salvo que se cuente con el consentimiento expreso de la persona a que se refiere la información solicitada".
Esta remisión a la Ley Nº25.326, limitada solamente a los datos sensibles que hace el Decreto Nº1172/03 no implica desconocer que toda otra información de carácter personal quede fuera del amparo de los principios constitucionales que la citada norma legal.
Por su parte, la Ley Nº25.326 de Protección de Datos Personales, es una ley de orden público, que establece condiciones a la cesión de información personal a terceros, las que son ineludibles para evaluar la licitud del acto administrativo que resuelva sobre la entrega de información de las personas en poder del Estado.
En este punto cabe señalar que en cuanto a la obligación impuesta por el Decreto Nº1172/03 como fundamento permisivo de la cesión de la información personal pretendida hemos de considerar la supremacía que el ordenamiento legal positivo le reconoce a una ley, además específica (Ley Nº25.326) por sobre un Decreto (el Nº1172/03), más aún cuando este último contempla -como ya se ha señalado- que los sujetos obligados a proporcionar la información podrán exceptuarse cuando una ley así lo establezca.
Sin embargo, lo señalado no significa que dicha ley niegue el derecho de acceso a la información, sino que lo supedita, en cuanto a datos personales se refiera, a ciertos requisitos que no obstan ni son restricciones al acceso de la información pública, sino garantías para afirmar el derecho a la privacidad.
Por tales motivos, se entiende que la libre cesión de información del Poder Ejecutivo Nacional a terceros dispuesta por el Decreto 1172/03, en lo que respecta a la información de las personas, se encuentra condicionada por las disposiciones de la Ley Nº25.326.
Por ello, se sugiere que, cuando las solicitudes de acceso a la información pública que reciban los organismos públicos impliquen brindar datos personales, se efectúe la pertinente consulta a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a fin de que ésta aconseje la forma de efectuar la cesión de tales datos con pleno cumplimiento de las normas de protección de datos personales.
Supuestos especiales - artículo 23 de la Ley Nº25.326
La Ley Nº25.326 establece que quedan sujetos al régimen por ella establecido, aquellos 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 aquellos sobre antecedentes personales que proporcionen dichos bancos 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, fuerzas de seguridad, organismos policiales o inteligencia, 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. Los archivos, en tales casos, deberán ser específicos y establecidos 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.
IV.- SANCIONES
Ya se ha hecho referencia, entre las obligaciones del titular del banco de datos, al principio de secreto, por el cual debe mantener en reserva la información relativa a los datos personales que opere en el tratamiento de datos personales.
También se dijo que, en el ámbito público, los funcionarios están obligados a ello por las normas que rigen la prestación de sus servicios.
Infringir este deber de secreto puede dar lugar a las siguientes sanciones disciplinarias, administrativas y/o penales, previéndose en este último caso un agravante si el que delinque es funcionario público.
Sanciones disciplinarias: la Ley Nº22.140, que regula el Régimen Jurídico Básico de la Función Pública, exige con carácter general y sin perjuicio de lo que establezcan normas particulares que los funcionarios públicos deben guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tengan conocimiento en el ejercicio o con motivo del ejercicio de sus funciones, independientemente de lo que establezcan las disposiciones vigentes en materia de secreto o reserva administrativa, excepto cuando sea liberado de esa obligación por la autoridad que la reglamentación determine.
El no cumplimiento de esta exigencia traerá como consecuencia la imposición de las sanciones disciplinarias correspondientes.
Sanciones administrativas: por su parte, la Disposición DNPDP Nº07 de fecha 8 de noviembre de 2005 aprueba la Clasificación de Infracciones y la Graduación de Sanciones por incumplimiento a las normas de la Ley Nº25.326, de Protección de Datos Personales.
En lo concerniente al deber de secreto que corresponde al responsable de la base de datos, a su encargado o a cualquier persona que, en definitiva, efectúe tratamiento de datos personales, dicha Disposición estima como infracción "leve" la vulneración del deber de secreto por parte del responsable y personas que intervengan en cualquier etapa de un tratamiento de datos personales; como "grave" cuando ello ocurre respecto de datos personales que se encuentren asentados en archivos, registros, bases o bancos de datos y como "muy grave" cuando se trate de datos sensibles o datos recabados o tratados para fines penales y contravencionales.
Sanciones penales: la Ley 25.326 estableció la incorporación al Código Penal de las siguientes sanciones penales:
1. artículo 117 bis: "1º. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2º. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. 3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4º. 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".
2. artículo 157 bis: "Será reprimido con la pena de prisión de un mes a dos años el que: 1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2º. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley; 3º.

Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años". (con las modificaciones introducidas por el artículo 8º de la Ley Nº26.388 de Delitos Informáticos).

ANEXO II

CONVENIO DE CONFIDENCIALIDAD

En virtud de los servicios prestados en .....(organismo público)....., ...(nombre del empleado)....., tendré acceso a los bancos de datos, archivos e información que mi empleador autorice, y tomo conocimiento que en caso de consistir dicha información en datos personales, la misma es confidencial y se encuentra protegida por la Ley Nº25.326, cuyo artículo 10 dispone: "El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos...".

En consecuencia, me comprometo a guardar la máxima reserva y secreto sobre la información personal a que acceda en virtud de las funciones encomendadas; a utilizar los datos de carácter personal a los que tenga acceso, única y exclusivamente para cumplir con mis obligaciones; a observar y adoptar cuantas medidas de seguridad sean necesarias para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso; a no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni siquiera a efectos de su conservación, salvo autorización legal o instrucción expresa y por escrito de la autoridad a cargo del Organismo Público Responsable del Banco de Datos.

De igual modo, me comprometo, tras la extinción del presente contrato, a no conservar en mi poder copia alguna de los datos personales a los que hubiere accedido en función de mis tareas.

En razón de ello, adoptaré en el tratamiento de la información personal todas aquellas precauciones que sean necesarias para evitar que personas físicas o jurídicas no autorizadas tomen conocimiento total o parcial de aquélla, y cumpliré escrupulosamente con las instrucciones que puedan ser dictadas en cada momento por mi superior para la protección de dicha información.

En ....., a los ..... días del mes de ..... de 200.....

ANEXO III

DISEÑO DEL ISOLOGITOPO DENOMINADO "SELLO ARGENTINO DE PRIVACIDAD"

El isologotipo se compone de:

Circulo color:

R: 0

G: 150

194

Imagen Huella color:

R: 0

G: 150

B: 194

Fuentes tipográficas:

Myriad Pro Italic: "www.jus.gov.ar/datospersonales"

Color Negro:

R: 26

G: 23
B: 27
Myriad Pro Italic: "Dirección Nacional de Protección de Datos Personales"
Color Negro:
R: 26
G: 23
B: 27
Arial: "BASES DE DATOS PUBLICAS"
Color Blanco:
R: 255
G: 255
B: 255
Arial Black: "SELLO ARGENTINO DE PRIVACIDAD"
Color Blanco:
R: 255
G: 255
B: 255
NOTA: Este isologotipo acredita solamente la adhesión a la "GUIA DE BUENAS PRACTICAS EN POLITICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL AMBITO PUBLICO".

ANEXO IV

INSTRUCCIONES Y MODELOS DE ESCRITOS PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACION Y SUPRESION DE DATOS PERSONALES

DERECHO DE ACCESO

• La solicitud del derecho de acceso sólo podrá ser efectuada en formal personal. Se debe acompañar fotocopia del D.N.I. Si se trata de personas fallecidas, este derecho podrán ejercerlo sus sucesores universales acreditando dicha circunstancia con copia certificada, por el juzgado a cargo, de la declaratoria judicial de herederos.

• El derecho de acceso podrá solicitarse en forma gratuita con intervalos no inferiores a seis (6) meses, salvo causa justificada.

• Si usted desconoce la direccion del responsable del banco de datos puede consultar la información de contacto de los responsables inscriptos en el Registro Nacional de Bases de Datos de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS en www.jus.gov.ar/datospersonales/. La mencionada Dirección Nacional no dispone de los datos contenidos en ningún banco de datos.

• La solicitud debe dirigirse directamente ante el organismo público del que se presume o tiene la certeza que posee sus datos.

CARTA MODELO PARA EL EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL BANCO DE DATOS O DEL TRATAMIENTO DE DATOS

Nombre: ..... Dirección: ..... Nº..... Piso .... Depto .....

Localidad: ..... Código Postal: .....

Provincia: .....

DATOS DEL SOLICITANTE

....(nombre)....., con domicilio en ..... nº....., piso ....., depto ..... de la .....(localidad)....., Provincia de ....., Código Postal ....., teléfono ....., con D.N.I ....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 14 de la Ley Nº25.326, y los artículos 14 y 15 de la Reglamentación de la Ley Nº25.326 aprobada por Decreto Nº1558/01.

SOLICITA:

1.- Que me facilite gratuitamente el acceso a los datos existentes sobre mi persona en sus

bases o registros en el plazo máximo de diez (10) días a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin contestación expresa, la misma ha sido denegada. En este caso se podrá formular la denuncia ante la Dirección Nacional de Protección de Datos Personales y quedará expedita la vía para ejercer la acción de protección de los datos personales, en virtud de lo dispuesto por el artículo 14 de la Ley Nº25.326 y el artículo 14 de su Decreto Reglamentario Nº1558/01.

2.- Que si la solicitud del derecho de acceso fuese estimada, se ponga a mi disposición en la mesa de entradas o se remita por correo la información a la dirección arriba indicada dentro del plazo de diez días corridos de efectuada la solicitud de acceso.

3.- Que esta información comprenda de modo legible y claro los datos que sobre mi persona obren en sus registros y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En ..... a los ..... días del mes de ..... de 20.....

DERECHOS DE RECTIFICACION, ACTUALIZACION, SUPRESION O SOMETIMIENTO A CONFIDENCIALIDAD DE DATOS PERSONALES

• Casos en que procede la solicitud

1. Datos erróneos
2. Datos falsos
3. Datos incompletos
4. Datos desactualizados

• El pedido de rectificación, actualización, supresión o sometimiento a confidencialidad debe ejercerse ante el responsable del archivo, registro, base o banco de datos público.

• Si usted desconoce el domicilio del responsable del banco de datos puede consultar la información de contacto de los responsables inscriptos en el Registro Nacional de Bases de Datos de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS en www.jus.gov.ar/datospersonales/. La mencionada Dirección Nacional no dispone de los datos contenidos en ningún banco de datos.

• El plazo que tiene el responsable del archivo, registro, base o banco de datos público para realizar la rectificación, actualización o supresión es de CINCO (5) días hábiles y se computa a partir de que se recepciona el reclamo del titular de los datos.

• El trámite es personal. Es necesario acompañar la fotocopia del D.N.I. para que el responsable de la base de datos pueda comprobar la identidad del titular de los datos.

• Además de identificar los datos que deban actualizarse, rectificarse y/o suprimirse, el solicitante deberá justificar legalmente las razones de su petición y verificar que ésta sea la vía idónea para encauzar su pedido.

• El afectado o titular de los datos personales debe dirigirse directamente ante el organismo público que posee sus datos.

CARTA MODELO PARA EL EJERCICIO DE LOS DERECHOS DE RECTIFICACION, ACTUALIZACION, SUPRESION O SOMETIMIENTO A CONFIDENCIALIDAD DE DATOS PERSONALES

DATOS DEL RESPONSABLE DEL BANCO DE DATOS

Nombre: .....

Domicilio: .....

C.P..... Localidad:.....

Provincia: .....

DATOS DEL SOLICITANTE (TITULAR DE LOS DATOS PERSONALES)

.....(nombre)....., con domicilio en ..... Nº...., piso ....., depto. ...., Localidad ....., Código Postal ....., Provincia ....., teléfono ....., con D.N.I ....., del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer el derecho de rectificación / actualización / supresión / sometimiento a confidencialidad, de conformidad con el artículo 16 de la Ley Nº25.326, y el artículo 16 de su Decreto Reglamentario Nº1558/01.

SOLICITO:

1. Que en el plazo de cinco (5) días hábiles desde la recepción de esta solicitud se proceda gratuitamente a la rectificación / actualización / supresión / sometimiento a confidencialidad, de los siguientes datos relativos a mi persona que se encuentren en su base de datos: .....
2. Que los precitados datos deben ser rectificados / actualizados / suprimidos o sometidos a confidencialidad en virtud de .....
3. Que la rectificación / actualización / supresión / sometimiento a confidencialidad de los datos una vez realizada se me comunique por escrito, sea poniendo dicha información a mi disposición en la mesa de entradas o se la remita por correo a la dirección arriba indicada dentro del plazo de CINCO (5) días hábiles.
4. Que para el caso que el responsable del banco de datos considere que la rectificación / actualización / supresión o sometimiento a confidencialidad no procede, lo comunique en forma motivada, por escrito y dentro del plazo de cinco (5) días.
Se deja constancia que si transcurre el plazo sin que en forma expresa se conteste la petición efectuada, ésta se entenderá denegada, en cuyo caso se podrá interponer el reclamo ante la Dirección Nacional de Protección de Datos Personales y quedará expedita la vía para ejercer la acción de protección de los datos personales, en virtud de lo dispuesto por el artículo 16 inciso 3 de la Ley Nº25.326.
En..... a los ..... días del mes de..... de 20.....