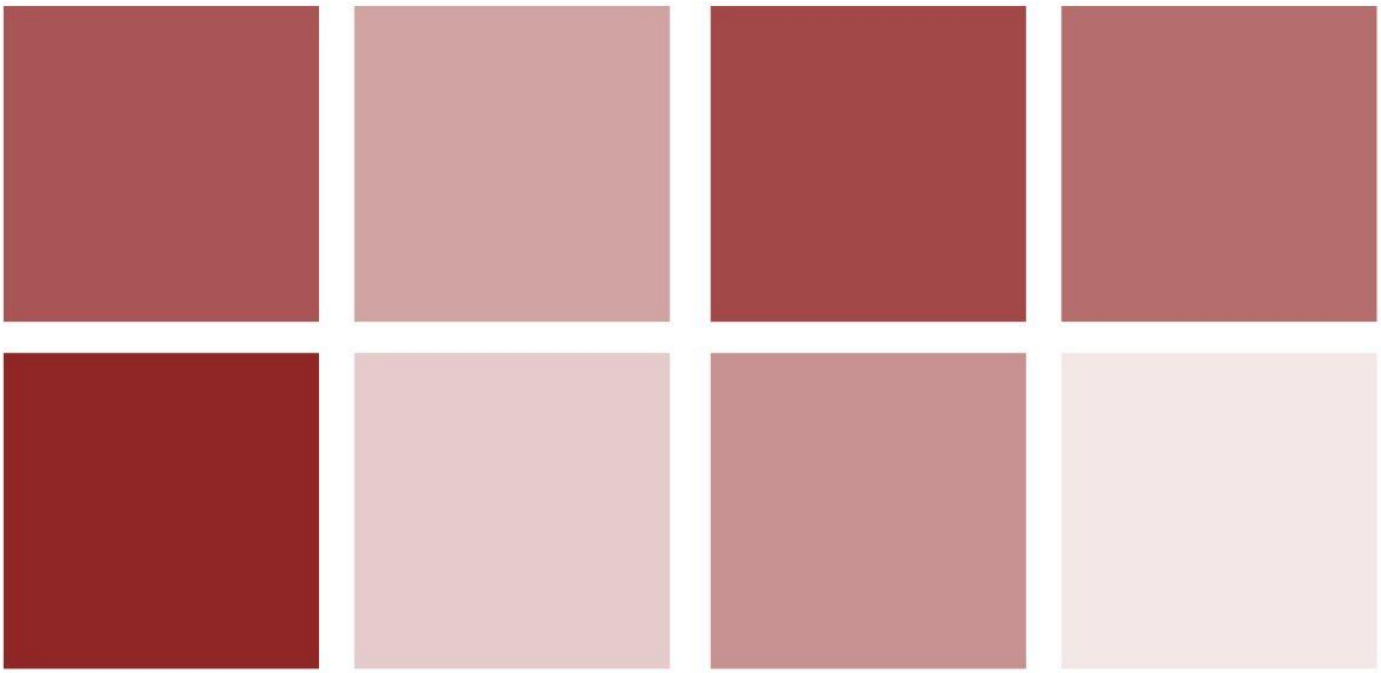
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

XVII edición de los Premios Protección de Datos Personales

Dolores Dozo

Pablo Martínez Quijano

HABEASDAT



Glosario Iberoamericano de Protección de Datos

LA SITUACIÓN ACTUAL EN MATERIA DE PROTECCIÓN DE DATOS DE IBEROAMÉRICA

El cuadro de situación del derecho a la protección de datos personales en Iberoamérica es dispar.

Europa ha puesto a la privacidad en un nivel de excelencia dentro de la comunidad internacional, ostentando España un papel destacado en la actualidad, de consolidación efectiva del respeto a la privacidad de sus ciudadanos.

Al otro lado del atlántico, si bien casi todos los países latinoamericanos han consagrado en sus constituciones el derecho a la protección de datos y el respeto a la intimidad, a la fecha, algunos todavía no han sancionado leyes en materia de protección de datos personales (entre otros Ecuador, El Salvador, Guatemala, República Dominicana).

Luego, hay países que si bien no han dictado normas específicas en materia de protección de datos, sí han regulado algunos institutos, tal como el de Habeas Data (entre ellos Paraguay, Brasil, Honduras, Panamá, Venezuela y Bolivia).

Por último, hay a la fecha ocho países que cuentan con normativa que regula especialmente el derecho a la protección de datos personales, como es el caso de Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú y Uruguay.

Con lo cual, el escenario Iberoamericano presenta grandes mixturas, existiendo brechas entre algunos países de la región, lo que nos reporta un sin número de ciudadanos sin garantía de respeto a su privacidad, y otro tanto de afectados que desconocen los derechos que los asisten.

Todo ello acontece en un contexto donde las nuevas tecnologías desconocen fronteras y avanzan sin miramientos, estando cada día más presente en la vida de los latinoamericanos. So pretexto que la tecnología evoluciona más rápido que el derecho, no puede dejarse a las personas huérfanas de derechos fundamentales.

Dentro de este contexto de vorágine tecnológica, la sociedad latinoamericana se enfrenta al desafío de alcanzar adecuados niveles de cumplimiento de las normas de protección de datos, crear cultura de privacidad, difundir la protección de datos y convertir la privacidad en un derecho efectivo de los ciudadanos.

POR QUÉ UN GLOSARIO

Sin duda la prioridad es difundir, concientizar y hacer extensiva la cultura de protección de datos personales a toda la región. Deviene prioritario impulsar diversas iniciativas dirigidas a difundir la cultura de protección de datos y facilitar el cumplimiento de la Ley.

Para ello, nuestra arma es nuestra lengua. Disponer de un vocabulario que pueda ser interpretado correctamente en cualquier país de la región, sin lugar a vaguedades y ambigüedades, que permita allanar el camino a aquellos países menos maduros en materia de privacidad, a través del intercambio de experiencias, comparación de institutos e información, y la retroalimentación de la experiencia internacional y regional.

El hecho que el Glosario reúna los principales institutos de protección de datos receptados por la Unión Europa, en especial los traspuestos en la Ley Española, cobra especial significancia atendiendo a la raigambre común que el derecho americano comparte con el peninsular, potenciado por el hecho que la mayoría de los legisladores latinoamericanos se han inspirado fuertemente en el sistema español de protección de datos, sin dejar de lado la idiosincrasia y los institutos propios de la región.

El Glosario pone de manifiesto de forma sencilla nuestras diferencias y puntos de unión. Pretende servir de herramienta para intensificar la colaboración mutua; tender redes de aprendizaje; unificar criterios; desarrollar regulación interna a partir de la cooperación mutua y la alineación hacia objetivos comunes; promover el dialogo y la ejecución de iniciativas conjuntas sobre protección de datos; como así también, trabajar en pos de la unificación normativa.

GUÍA DE LECTURA DEL GLOSARIO

Introducción

El presente Glosario recoge los principios, procedimientos e institutos más salientes de la regulación en protección de datos personales en Iberoamérica.

Su contenido ha sido recogido directamente de directivas europeas, leyes, reglamentos, decretos y demás normativa de desarrollo y vigente para los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, España, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal y Uruguay.

Instrucciones

Para la correcta lectura del Glosario se informa que:

- Las definiciones con contenido común a todas las legislaciones, no se indican con ninguna señalización especial.

- Las definiciones con contenido parcialmente común a todas las legislaciones, se identifican con el símbolo de Iberoamérica.

- Las definiciones con contenido específico de cada país, se identifica con la bandera del país y/o los países de que se traten.

Referencias para cada país

Acceso a documentación por usuarios de bases de datos personales: El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. El acceso de personas deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

El término es sinónimo de "acceso a la información" referenciado en la legislación peruana.

Sinónimos: *Acceso a la información por usuarios de bases de datos personales.*

Acceso a la información por usuarios de bases de datos personales: El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad. El término es sinónimo de acceso a la documentación referenciado en la legislación española.

Sinónimos: *Acceso a la documentación por usuarios de bases de datos personales.*

Acceso a los datos por cuenta de terceros: No se considerará comunicación o cesión de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Sinónimos: *Encargado de tratamiento.*

Véase también *Subcontratación de servicios, Cesión de datos, Autorización de la subcontratación.*

Acción de Habeas Data: La acción de protección de los datos personales o de hábeas data es una herramienta judicial, no administrativa, ante la negativa del titular de las bases de datos de responder a su solitud de derechos ARCO, que puede interponer el interesado ante juez competente cuando:

- quiera tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
- en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

 ARG  BRA  URU

Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo.

 CHL

Toda persona estará legitimada para promover acción de Hábeas Data, con miras a garantizar el derecho de acceso a la información previsto en esta Ley, cuando el funcionario público titular o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado, no le haya suministrado lo solicitado o si suministrado lo requerido se haya hecho de manera insuficiente o en forma inexacta.

 PAN

Sinónimos: *Acción de protección de datos personales, Habeas Data.*

Véase también *Juez competente de la acción de habeas data, Legitimados para promover acción de habeas data, procedencia de la acción de habeas data, Procedimiento de la acción de habeas data.*

Acción de protección de datos personales:

(1) La acción procederá:

- Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
- En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

El juez competente será el encargado de conocer y resolver la acción de protección de datos personales mediante denuncia o demanda presentada por el titular en relación al tratamiento de datos personales que lesionen alguno de los derechos contemplados en las Leyes de Protección de Datos Personales.

 ARG  CHL  URU

Sinónimos: *Acción de habeas data, Habeas Data.*

Véase también *Juez competente de la acción de habeas data, Legitimados para promover acción de habeas data, procedencia de la acción de habeas data, Procedimiento de la acción de habeas data.*

(2) El titular de los datos puede interponer la acción de protección de datos personales, en la vía administrativa. La Dirección de Protección de Datos Personales, es el órgano encargado de conocer y resolver la acción de protección de datos personales mediante denuncia presentada por el titular en relación al tratamiento de datos personales que lesionen alguno de los derechos contemplados en la Ley 787. La acción de protección de datos personales, procede:

- Para conocer de los datos personales que han sido objeto de tratamiento en ficheros de datos;
- Cuando se hayan violentado las garantías de confidencialidad, integridad y seguridad en el tratamiento de los datos personales;
- En los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, modificación, inclusión, supresión o cancelación;
- Cuando sean lesionados algunos de los principios que rigen la calidad del tratamiento de datos personales, en el ámbito público y privado;
- Para acceder a información que se encuentre en poder de cualquier entidad pública y privada de la que generen, produzcan, procesen o posean, información personal, en expedientes, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier documento que la administración pública o las entidades privadas tengan en su poder; y

Para exigir la rectificación, actualización, modificación, inclusión, complementación, supresión, bloqueo o cancelación de datos personales tratados en ficheros de datos de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros, ya sea de forma manual, mecánica o informática, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate.

 NIC

Sinónimos: *Ejercicio de derechos ARCO, Procedimiento de Tutela de Derechos, Procedimiento de Protección de derechos.*

Véase también: *Medios de impugnación de decisiones del órgano de control, Recurso contra resolución de protección de datos, Órgano de control.*

Acciones para la seguridad de los datos personales: A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:

- Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- Determinar las funciones y obligaciones de las personas que traten datos personales;
- Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
- Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
- Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
- Llevar a cabo revisiones o auditorías;
- Capacitar al personal que efectúe el tratamiento, y
- Realizar un registro de los medios de almacenamiento de los datos personales.

 MEX

Sinónimos: *Obligaciones del responsable.*

Véase también *Medidas de seguridad de nivel bajo, Medidas de seguridad de nivel medio, Medidas de seguridad de nivel alto, Responsable de seguridad.*

Acta de fiscalización: Las visitas de fiscalización por el Órgano de Control requieren el levantamiento del acta correspondiente, en la que quedará constancia de las actuaciones practicadas durante la visita de verificación. Dicha acta se levantará en presencia de dos testigos propuestos por la persona con quien se entendió la diligencia. Si se hubiera negado a proponerlos o no hubieran participado los propuestos, bastará la firma de la persona con quien se entendió la diligencia o la constancia de su negativa a firmar, de ser el caso.

El acta se elaborará por duplicado y será firmada por el personal fiscalizador y quienes hayan participado en la diligencia. El acta puede incluir la manifestación que los participantes consideren que conviene a su derecho.

Se entregará al fiscalizado uno de los originales del acta de fiscalización, incorporándose el otro a los actuados. PER

El acta de fiscalización tiene su correlato en la legislación mexicana bajo el rotulo "acta de verificación". MEX

Sinónimos: *Acta de verificación, Acta de inspección.*

Véase también *Proceso de Verificación, Visitas de Verificación.*

Acta de inspección: Una vez realizada la inspección, el inspector levantará el acta correspondiente de inspección en el formato diseñado para tal fin y consignando al menos, lo siguiente:

- Indicación del lugar, fecha y hora en que se realiza la inspección;
- Breve referencia de la orden de inspección en caso de denuncia expedida por la autoridad competente y que motiva la realización de esta actividad, haciendo constar que copia de la misma le fue entregada al inspeccionado;
- Datos generales con quien se coordinó la inspección, ya sea el responsable, administrador, gerente, representante legal de la compañía, o similares; y
- El detalle de los hallazgos de la inspección en materia de acciones, u omisiones, que constituyan cumplimiento de las normas y disposiciones regulatorias de la actividad o por el contrario que presuman infracciones y faltas flagrantes o simuladas a las mismas, describiéndolas con el mayor detalle y precisión posible. NIC

El acta de fiscalización tiene su correlato en la legislación mexicana bajo el rotulo "acta de verificación".

Sinónimos: *Acta de verificación, Acta de fiscalización*

Véase también *Constatación de posibles infracciones, Inspección, Procedimiento de inspección.*

Acta de verificación: Las visitas de verificación concluirán con el levantamiento del acta correspondiente, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de verificación. Dicha acta se levantará en presencia de dos testigos propuestos por la persona con quien se hubiera entendido la diligencia o por quien la practique si aquélla se hubiera negado a proponerlos.

El acta que se emita por duplicado será firmada por el personal verificador actuante y por el responsable, encargado o con quien se haya entendido la actuación, quien podrá manifestar lo que a su derecho convenga.

En caso de que el verificado se niegue a firmar el acta, se hará constar expresamente esta circunstancia en la misma. Dicha negativa no afectará la validez de las actuaciones o de la propia acta. La firma del verificado no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al verificado uno de los originales del acta de verificación, incorporándose el otro a las actuaciones.

En las actas de verificación se hará constar:

- Nombre, denominación o razón social del verificado;
- Hora, día, mes y año en que se inicie y concluya la verificación;
- Los datos que identifiquen plenamente el domicilio, tales como calle, número, población o colonia, municipio o delegación, código postal y entidad federativa en que se encuentre ubicado el lugar en que se practique la verificación, así como número telefónico u otra forma de comunicación disponible con el verificado;
- Número y fecha del oficio de comisión que la motivó;
- Nombre y cargo de la persona con quien se entendió la verificación;
- Nombre y domicilio de las personas que fungieron como testigos;
- Datos relativos a la actuación;
- Declaración del verificado, si quisiera hacerla, y
- Nombre y firma de quienes intervinieron en la verificación, incluyendo los de quienes la hubieran llevado a cabo. Si se negara a firmar el verificado, su representante legal o la persona con quien se entendió la verificación, ello no afectará la validez del acta, debiendo el personal verificador asentar la razón relativa.

Los verificados a quienes se haya levantado acta de verificación, podrán formular observaciones en el acto de la verificación y manifestar lo que a su derecho convenga en relación a los hechos contenidos en ella, o bien, por escrito dentro del término de los cinco días siguientes a la fecha en que se hubiere levantado.

El acta de verificación tiene su correlato en la legislación peruana bajo el rotulo "acta de fiscalización".  MEX  PER

Sinónimos: *Acta de inspección, Acta de fiscalización.*

Véase también *Procedimiento de Verificación, Visitas de Verificación, Contenido de las actas de verificación, Fe pública, Plazo del procedimiento de verificación, Resolución del procedimiento de verificación, Verificación.*

Actividades excluidas del ámbito de la protección de datos: Las disposiciones del presente Reglamento no serán aplicables a la información siguiente:

- La relativa a personas morales;
- Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas, y
- La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.  MEX

Asimismo, el régimen de protección de los datos de carácter personal no será de aplicación a los siguientes ficheros y tratamientos:

- A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.
- A los sometidos a la normativa sobre protección de materias clasificadas.
- A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.


ESP

El régimen de protección de datos no será de aplicación a las siguientes bases de datos:

- A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- 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.
- A las bases de datos creadas y reguladas por leyes especiales.


URU

Sinónimos: *Excepciones al ámbito de aplicación el régimen de protección de datos.*

Véase también *Exceptuados al cumplimiento del régimen de protección de datos.*

Acto final: La Agencia resolverá el procedimiento de protección de derechos en el plazo de un mes, a partir de la firmeza de la resolución que resuelva sobre la admisibilidad de la denuncia.


CTR

Sinónimos: *Resolución IFAI, Resolución de derechos arco, Resolución de protección de datos*

Véase también: *Plazo para dictar resolución en el procedimiento de protección de derechos, Procedimiento de protección de derechos.*

Actuaciones previas: Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se

estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.


ESP

Acuerdo de conciliación: El IFAI podrá en cualquier momento del procedimiento de protección de derechos, buscar una conciliación entre el titular de los datos y el responsable. De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.


MEX

Véase también *Conciliación, IFAI, Instituto, Procedimiento de protección de datos.*

Acuerdo de conciliación: Dentro del procedimiento de protección de derechos, el Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.


MEX

Sinónimo: *Conciliación*

Véase también *Instituto.*

Acuerdo de inscripción: Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.


ESP

En el resto de las legislaciones, la inscripción se realiza prescindiendo de este paso, mediante la Resolución de Inscripción.

Véase también *Resolución de Inscripción.*

Acuse de recibo: Tipo de mensaje que se envía para indicar que un correo ha llegado a su destino sin errores. Un acuse de recibo puede también ser negativo, es decir, indicar que un bloque de datos no ha llegado a su destino.

AEPD: Agencia Española de Protección de Datos, autoridad máxima de aplicación en materia de protección de datos personales de España, órgano de control que tiene por objeto velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación conforme lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.


ESP

Véase también *Agencia Española de Protección de Datos, Órgano de control.*

Afectado: Titular de los datos que sean objeto del tratamiento.

Sinónimo: *Interesado, Titular de los datos.*

Agencia de Protección de Datos de los Habitantes (PRODHAB): órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes. Con personalidad jurídica instrumental propia en el desempeño de las funciones, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia gozará de independencia de criterio. CTR

Véase también *Órgano de control*

Agencia Española de Protección de Datos: La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Es la Autoridad de Aplicación en materia de protección de datos personales en el ámbito nacional Español, teniendo por objeto velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación conforme lo dispuesto en el Titulo VI de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

Sinónimo*: AEPD* ESP

Véase también *Órgano de control.*

AGESIC: Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento. Organismo que depende de la Presidencia de la República Oriental del Uruguay, funciona con autonomía técnica y tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las Tecnologías de la Información y las Comunicaciones. URU

Sinónimo: *Agencia para el desarrollo del gobierno de gestión electrónica y la sociedad de la información y del conocimiento.*

Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento: AGESIC. Organismo que depende de la Presidencia de la República Oriental del Uruguay, funciona con autonomía técnica y tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las Tecnologías de la Información y las Comunicaciones. URU

Sinónimo: *AGESIC*.

Almacenamiento de información: dentro de las medidas de seguridad de nivel alto, se exige que los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal se alojen en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad. ESP

Véase también *Medidas de seguridad de nivel alto.*

Ámbito de aplicación: El régimen establecido en las leyes de protección de datos es 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. IBE

Asimismo, el derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda. ARG BRA NIC URU

Véase también *Actividades excluidas del ámbito de la protección de datos,* Exceptuados al cumplimiento del régimen de protección de datos.

Ampliación de los plazos de respuesta de solicitudes ARCO: En caso de que el responsable determine ampliar el plazo de respuesta a una solicitud para el ejercicio de los derechos ARCO o aquél para hacer efectiva la respuesta, éste deberá notificar al solicitante las causas que justificaron dicha ampliación, en cualquiera de los siguientes plazos:

- En caso de ampliar los veinte días para comunicar la determinación adoptada sobre la procedencia de la solicitud, la justificación de la ampliación deberá notificarse dentro del mismo plazo contado a partir del día en que se recibió la solicitud, o
- En caso de ampliar los quince días para hacer efectivo el ejercicio del derecho que corresponda, la justificación de la ampliación deberá notificarse dentro del mismo plazo contado a partir del día en que se notificó la procedencia de la solicitud. MEX

La regulación en protección de datos de Argentina no prevé ampliaciones de plazos al responsable de evacuar la solicitud de derechos ARCO. ARG

La regulación en protección de datos de España no prevé ampliaciones de plazos al responsable de evacuar la solicitud de derechos ARCO. No obstante, está previsto que cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos. ESP

La regulación en protección de datos de Uruguay no prevé ampliaciones de plazos al responsable de evacuar la solicitud de derechos ARCO. URU

Salvo el plazo establecido para el ejercicio del derecho de información, los plazos que correspondan para la respuesta o la atención de los demás derechos, podrán ser ampliados una sola vez, y por un plazo igual, como máximo, siempre y cuando las circunstancias lo justifiquen. La justificación de la ampliación del plazo deberá comunicarse al titular del dato personal dentro del plazo que se pretenda ampliar. PER

Archivo de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Sinónimos: *Registro, Base de datos, Banco de datos, Fichero.*

Auditoría: A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.


ESP

Véase también *Medidas de seguridad de nivel medio.*

Autenticación: Procedimiento de comprobación de la identidad de un usuario. Mediante el mismo se garantiza que el usuario que accede a un sistema de ordenador es quién dice ser. Por lo general, los sistemas de autenticación están basados en el cifrado mediante una clave o contraseña privada y secreta que sólo conoce el auténtico emisor.

Autodeterminación informativa: Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.

Sinónimos: *Principio de autodeterminación informativa.*

Véase también *Derecho a la protección de datos personales.*

Autoridad de Aplicación: Órgano de control en materia de protección de datos, quien realiza todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones estipuladas en las leyes de protección de datos personales.

Sinónimo: *Órgano de Control*

Autoridad Nacional de Protección de Datos Personales: El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones, puede crear oficinas en todo el país. Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley 29733 y de su reglamento. Para tal efecto, goza de potestad sancionadora así como de potestad coactiva.


PER

Sinónimo: *Órgano de Control*

Autorización: El tratamiento de los datos personales sólo puede efectuarse cuando la ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.


CHL

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.

En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este decreto, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el Responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento. COL

Sinónimo: *Consentimiento.*

Véase también *Excepciones a la autorización, Excepciones al consentimiento.*

Autorización de la subcontratación: En las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable de las bases de datos y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización se entenderá como otorgada a través de lo estipulado en éstos. Si la subcontratación no fue prevista en estos instrumentos jurídicos, el encargado deberá obtener la autorización del responsable previo a la subcontratación.

Véase también *Subcontratación de servicios*

Autorización de transferencias internacionales de datos: deberán tramitarse ante el organismo de control. Para que la transferencia internacional de datos sea conforme a derecho, será necesaria la autorización del Director del Organismo de Control del país de que se trate, salvo:

- Que los datos se transfieran a un país que ofrezca un nivel adecuado de protección
- Que se trate de empresas de Estados Unidos que hayan suscrito los principios de Puerto Seguro.
- Que se trate de supuestos legalmente exceptuados de la autorización del Director.
- Que se trate de comunicaciones de datos en el Espacio Económico Europeo (EEE), las que constituyen cesiones de datos a efectos de la aplicación de las leyes europeas de protección de datos. IBE

Para la formalización de las transferencias internacionales en México, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones y condiciones a las que se encuentra sujeto el responsable. Los responsables, en caso de considerarlo necesario, podrán solicitar la opinión del Instituto respecto a si las

transferencias internacionales que realicen cumplen con lo en las leyes de protección de datos personales. MEX

Véase también *Transferencia internacional de datos, Países con nivel adecuado de protección, Puerto seguro.*

Autorregulación Vinculante: Los responsables podrán celebrar códigos deontológicos sectoriales o de buena práctica profesional, de carácter voluntario, vinculantes para quienes se adhieran a los mismos, con reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de aquellas leyes de protección de datos que los recepten. MEX

Sinónimos: *Códigos Tipo, Código de Conducta.*

Aviso de Privacidad:

(1) Documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular, previo al tratamiento de sus datos personales. El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento. Para la difusión de los avisos de privacidad, el responsable podrá valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

El aviso de privacidad deberá contener los elementos a que se refieren los artículos 8, 15, 16, 33, 36 y 43 fracción II de la Ley Federal de Datos Personales.

En términos del artículo 17, fracción II de la Ley, cuando los datos personales sean obtenidos directamente del titular, el responsable deberá proporcionar de manera inmediata al menos la siguiente información:
I. La identidad y domicilio del responsable;
II. Las finalidades del tratamiento, y
III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad.

Cuando los datos personales sean obtenidos de manera indirecta del titular, el responsable deberá observar lo siguiente para la puesta a disposición del aviso de privacidad:
I. Cuando los datos personales sean tratados para una finalidad prevista en una transferencia consentida o se hayan obtenido de una fuente de acceso público, el aviso de privacidad se deberá dar a conocer en el primer contacto que se tenga con el titular, o
II. Cuando el responsable pretenda utilizar los datos para una finalidad distinta a la consentida, es decir, vaya a tener lugar un cambio de finalidad, el aviso de privacidad deberá darse a conocer previo el aprovechamiento de los mismos. MEX

(2) Entre otras cuestiones obliga a poner a disposición de los destinatarios de usuarios de sitios y servicios en internet (salvo aquellos que se limiten exclusivamente al ámbito doméstico o de actividades personales no económicas) de un mínimo de información de forma permanente, fácil, directa y gratuita. Esta información suele incluirse bajo el título "Aviso Legal" o "Aviso de Privacidad" y generalmente incluye los siguientes elementos: una clara identificación delos responsables del sitio que permita establecer una comunicación directa y efectiva; el dominio o dominios utilizados; en el caso de que su actividad estuviese

sujeta a un régimen de autorización administrativa o ejerciera una profesión regulada, los datos relativos a la misma; el número de identificación fiscal que le corresponda; información clara y exacta sobre el precio del producto o servicio si estuviesen publicados en el portal, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío; los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.


IBE

En los casos en los que no sea posible poner a disposición del Titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

Contenido mínimo del Aviso de Privacidad. El aviso de privacidad, como mínimo, deberá contener la siguiente información:

- Nombre o razón social y datos de contacto del responsable del tratamiento.
- El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
- Los derechos que le asisten al titular.
- Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.


COL

Banco de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Sinónimos: *Registro, Archivo, Fichero o Base de datos.*

Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable. Es el conjunto organizado de datos de carácter personal en formato digital o no digital, cualquier que sea la forma o modalidad de su creación, registro, almacenamiento, organización y acceso.

Sinónimos: A*rchivo, Fichero, Registro, Base de datos, Banco de datos.*

Base de datos de titularidad privada: bases de datos cuyo responsable son personas, empresas o entidades de derecho privado. Si se trata de bases de datos de particulares para un uso exclusivamente personal y privado, quedan fuera del ámbito de aplicación de la Ley de Protección de Datos*.*  IBE

La legislación peruana se refiere a las bases de datos privadas como "banco de datos personales de administración privada".  PER

Sinónimos: *Fichero de titularidad privada, Banco de datos personales de administración privada.*

Base de datos de titularidad pública: Bases de datos cuyos responsables son órganos del Estado, organismos de la administración pública, así como las entidades u organismos vinculados o dependientes de las mismas.  IBE

La legislación peruana se refiere a las bases de datos públicas como "banco de datos personales de administración pública".  PER

Sinónimos: *Ficheros de datos de titularidad pública, Banco de datos personales de administración pública.*

Base de datos interna, personal o domestica: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, mantenidos por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean venidas o administradas con fines de distribución, difusión o comercialización.  CTR

Véase también *Exceptuados al cumplimiento del régimen de protección de datos.*

Base de datos manual o no automatizada: todo conjunto de datos de carácter personal organizado de forma manual, no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Sinónimo: *Fichero no automatizado.*

Banco de datos personales de administración privada: Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.  PER

Sinónimos: *Base de datos de titularidad privada, Fichero de titularidad privada*

Banco de datos personales de administración pública: Banco de datos cuya titularidad corresponde a una entidad pública. PER

Sinónimos: *Ficheros de datos de titularidad pública, Base de datos de titularidad pública.*
Bases de datos sensibles: No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Sólo podrán crearse bases de datos que contengan datos personales sensibles cuando:

- Obedezca a un mandato legal;
- Se justifique en términos de protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.
- El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

Véase también *Categoría de datos, Datos especialmente protegidos, Datos sensibles*

Bloqueo: Es la identificación y conservación de los datos de carácter personal con el fin de impedir su tratamiento, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

El bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario.

De resultar procedente la cancelación, el responsable deberá establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación.

Transcurrido el periodo de bloqueo, se llevará a cabo la supresión correspondiente.

Calidad de los datos: Los datos de carácter personal que sean objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; serán exactos y si fuera necesario puestos al día; se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado. ARG COL CTR ESP MEX PER

Sinónimo: *Principio de calidad de los datos.*

Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

Véase también *Derecho de cancelación.*

Canon anual: Todas las bases de datos, públicas o privadas, con fines de distribución, difusión o comercialización, deben inscribirse ante la Agencia, y por ende cancelar ante ésta, la suma de doscientos dólares moneda de curso legal de los Estados Unidos de América (USD $200,00), al tipo de cambio mayor de referencia de venta del Banco Central de Costa Rica del día en que se realice el pago. Dicho monto corresponde al canon anual de regulación y administración de las bases de datos. CTR

Características del consentimiento: La obtención del consentimiento debe ser:

- Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
- Específico: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y
- Informado: que el titular tenga conocimiento previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.
- Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.
- Expreso e Inequívoco/Individualizado: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento. IBE

Véase también *Consentimiento, Requisitos del consentimiento.*

Categoría de datos: Ninguna persona puede ser obligada a proporcionar datos sensibles. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Véase también *Datos sensibles.*

Causales de procedencia de la solicitud de protección de derechos: El procedimiento de protección de derechos procederá cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:

- El titular no haya recibido respuesta por parte del responsable;
- El responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
- El responsable se niegue a efectuar las rectificaciones a los datos personales;
- El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
- El responsable se niegue a cancelar los datos personales;
- El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición, y
- Por otras supuestas violaciones a las Leyes Protección de Datos Personales y/o los Reglamento.

Véase también *Procedimiento de protección de derechos, Procedimiento administrativo de protección de derechos, Procedimiento de tutela de derechos, Procedimiento trilateral de tutela de derechos.*

Censo promocional: Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes que correspondan, una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.  ESP

Certificación en protección de datos personales: Los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales. En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley Federal de Datos Personales.  MEX

Cesión de datos: Toda revelación o tratamiento de datos realizada a una persona distinta del interesado.

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.

El consentimiento para la cesión es revocable. Existen excepciones donde no se requiere recabar el consentimiento del interesado para el tratamiento y cesión de sus 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.

Cesionario: Persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos, distinto del responsable, del encargado del tratamiento y del titular de los mismos.

Véase también *Responsable, Encargado del tratamiento.*

Cesión masiva de datos: 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 de datos. 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.

 ARG  COL  MEX

Cifrado: Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.

Clickstream: Rastro que un usuario va dejando de su paso por las distintas páginas Web que visita. El nombre deriva de que esta navegación se basa en saltar de una página a otra mediante un "click" del ratón.

Códigos de conducta: Los responsables podrán celebrar códigos deontológicos sectoriales o de buena práctica profesional, de carácter voluntario, vinculantes para quienes se adhieran a los mismos, con reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de aquellas leyes de protección de datos que los recepten.

 IBE

Sinónimos*: Códigos tipo, Autorregulación Vinculante.*

Véase también *Inscripción de códigos tipo y de conducta.*

Códigos tipo: Los responsables podrán celebrar códigos deontológicos sectoriales o de buena práctica profesional, de carácter voluntario, vinculantes para quienes se adhieran a los mismos, con reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de aquellas leyes de protección de datos que los recepten.

 ESP  MEX

Sinónimos*: Código de Conducta y Autorregulación vinculante.*

Véase también *Inscripción de códigos tipo y de conducta.*

Comisión Nacional para la Protección de Datos Personales: Autoridad administrativa independiente, con poderes de autoridad, que funciona adscripta a la Asamblea de la República. Ejerce sus competencias en todo el territorio nacional como autoridad de control de protección de datos personales.

 POR

Véase también *Órgano de control.*

Cómputo de plazos de respuesta a solicitudes ARCO:

El responsable o usuario debe responder a la solicitud de acceso proporcionando la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. La respuesta a la solicitud de rectificación, supresión o actualización de los datos personales del afectado, debe efectivizarse en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. ARG

El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. La respuesta a la petición sobre derechos ARCO debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. URU

El responsable deberá contestar la solicitud de derechos ARCO en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros. El responsable resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud y tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. ESP

El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso. MEX

El plazo máximo para la respuesta ante el ejercicio del derecho de acceso será de veinte días contados desde el día siguiente de la presentación de la solicitud por el titular de datos personales. Si la solicitud fuera estimada y el responsable no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez (10) días siguientes a dicha respuesta. PER

El responsable, deberá evacuar la consulta de información dentro del plazo de cinco días hábiles a partir de la recepción de la solicitud. CTR

El titular contará con diez (10) días hábiles para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente. En caso de que la información proporcionada en la solicitud sea insuficiente o errónea para atenderla, el responsable de ficheros de datos podrá requerir al titular, por una vez y dentro de los cinco (5) días hábiles siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma. NIC

El término máximo para atender la petición o reclamo será de quince días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.

En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince días hábiles contados a partir del día siguiente a la fecha de

presentación de la reclamación, prorrogables por ocho días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga "reclamo en trámite" y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos días hábiles siguientes a haber recibido la información de la fuente.  COL

Sinónimos*: Plazo para responder derechos ARCO.*

Véase también *Derechos ARCO.*

Comunicación de datos: Toda revelación o tratamiento de datos realizada a una persona distinta del interesado. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado, salvo excepciones previstas en la legislación aplicable.

Véase también *Cesión de datos, Excepciones al consentimiento, Principio de finalidad.*

Conciliación: Dentro del procedimiento de protección de derechos, el Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.  MEX

Sinónimos*: Acuerdo de conciliación.*

Véase también *Instituto, Procedimiento de protección de derechos.*

Condiciones generales para ejercer ARCO: El ejercicio de los derechos se lleva a cabo mediante solicitud dirigida al titular del banco de datos personales o responsable del tratamiento, la misma que contendrá:

- Nombres y apellidos del titular del derecho y acreditación de los mismos, y en su caso de su representante conforme al artículo precedente.
- Petición concreta que da lugar a la solicitud.
- Domicilio, o dirección que puede ser electrónica, a efectos de las notificaciones que correspondan.
- Fecha y firma del solicitante.
- Documentos que sustenten la petición, de ser el caso.

La legislación peruana contempla, además de las mencionadas, el posible pago de una contraprestación para ejercer derechos ARCO.  PER

Sinónimos*: Solicitud de derechos ARCO*

Véase también *Procedimiento de derechos ARCO, Requisitos de solicitud de acceso*

Confidencialidad: Característica o atributo de la información por el que la misma sólo puede ser revelada a los usuarios autorizados en tiempo y forma determinados.

Consejo Consultivo: El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales de Uruguay, funciona asistido por un Consejo Consultivo. URU

El Director de la Agencia Española de Protección de Datos estará asesorado por un Consejo Consultivo. ESP

La Dirección Nacional de Protección de Datos Personales de Argentina contará con un Consejo Consultivo, que se desempeñará "ad honorem", encargado de asesorar al Director Nacional en los asuntos de importancia. ARG

Consentimiento: Manifestación de voluntad del titular de los datos, mediante la cual se avala el tratamiento de los mismos. Para que el tratamiento de datos sea licito, la manifestación de voluntad debe ser libre, inequívoca, específica e informada. De lo contrario, el consentimiento será nulo.

El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos.

Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.

Sinónimos*: Autorización*

Véase también *Características del consentimiento, Consentimiento expreso, Consentimiento informado.*

Consentimiento escrito: Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externalice mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento.

Consentimiento expreso: Manifestación de inequívoca, específica e informada mediante el cual el titular de los datos consiente el tratamiento de sus datos personales ya sea de forma verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. El consentimiento expreso también debe ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

Véase también *Consentimiento, Consentimiento informado.*

Consentimiento informado: Consentimiento precedido de una explicación al titular de los datos, en forma expresa y clara sobre la finalidad para la que serán tratados sus datos personales, quiénes pueden ser sus destinatarios; la existencia del fichero o base de datos, y los datos de Responsable; el carácter obligatorio o facultativo de la recogida de datos personales; las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; la vía de ejercicio de los derechos ARCO.

Véase También *Consentimiento, Derechos ARCO, Responsable.*

Consentimiento para el tratamiento de datos de menores de edad: Tratándose de menores de catorce años se requiere el consentimiento de los padres o tutores. A partir de los 14 años, para procederse al tratamiento de los datos se requiere el consentimiento del

menor, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

En ningún caso podrán recabarse del menor, datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madreo tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos.

Corresponderá al Responsable articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Consentimiento tácito: se considera que la persona titular acepta el tratamiento de sus datos personales, cuando quien posee su información, le hubiese informado y dicha persona no se oponga a ello.

Consentimiento verbal: Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo externalice oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

Constatación de posibles infracciones: La Agencia podrá realizar inspecciones administrativas de oficio, con el fin de constatar si existen posibles infracciones a la Ley o al Reglamento. En dicho caso el funcionario asignado deberá dejar constancia de la inspección mediante el levantamiento de un acta.


CTR

Sinónimos: *Inspecciones, Fiscalización, Verificación*

Consultas: Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco días hábiles siguientes al vencimiento del primer término.


COL

Sinónimos: *Derecho de acceso.*

Contenido de la respuesta a derechos ARCO: La respuesta de una solicitud de derechos ARCO, debe contener información clara, exenta de codificaciones y en su caso acompañado

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.

Contrato de transmisión de datos: El contrato que suscriba el Responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el responsable.

Mediante dicho contrato el encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:

- Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
- Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales.


COL

En el resto de Iberoamérica la relación entre el encargado y el responsable también debe documentarse pero el nombre que se le dará a ese acuerdo o contrato queda bajo la libre autonomía de voluntad de las partes.


IBE

Contrato global: Acuerdo de voluntades mediante el cual las partes manifiestan o expresan su consentimiento, sea de manera física o electrónica, y que tiene por objeto el servicio de un conjunto de consultas realizadas por un mismo solicitante a una base de datos que contenga datos personales, mediante el pacto de una remuneración pecuniaria en atención al volumen.


CTR

Control de acceso: Los usuarios de datos personales tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Exclusivamente el personal autorizado podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero. En caso de que exista personal ajeno al responsable que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Contrato celebrado por vía electrónica o contrato electrónico: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

Control de acceso: Exclusivamente el personal autorizado podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Cookies: Conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha hecho, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un fichero en el ordenador del usuario para ser utilizada en una próxima visita a dicho servidor. Además, existen servidores que restringen la utilización de determinadas funcionalidades de sus servicios o, incluso, deniegan el uso de los mismos si el usuario decide no aceptarla la grabación o colocación de la cookie en su ordenador.

Copias de respaldo: Dentro de las medidas de nivel básico, deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, , de forma que sea posible su recuperación. ESP

La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. PER

Véase también *Medidas de seguridad de nivel medio.*

Cortafuegos: Sistema de seguridad que permite controlar las comunicaciones entre redes informáticas. Instalado entre Internet y una red local permite evitar en esta última, accesos no autorizados, protegiendo con ello su información interna.

Criterio de archivo: El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Criterio de minimización: El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

Véase también *Principio de finalidad.*

Cumplimiento de la solicitud ARCO por el responsable: La obligación de responder la solicitud ARCO se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio por el que se informe, rectifique, cancele y/o conceda la oposición a los datos personales del titular. En caso que el Responsable no posea datos personales relativos al solicitante, deberá igualmente contestar la solitud ARCO por la negativa. La entrega de los datos personales será gratuita, previa acreditación de la identidad, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.

La solicitud de derechos ARCO en Perú puede estar asociada al pago de una contraprestación 

Sinónimos: *Otorgamiento del acceso.*

Véase también *Condiciones generales para ejercer ARCO, Derechos ARCO.*

Datos académicos: Curriculum vitae, trayectoria educativa, títulos, matriculas habilitantes, certificados, condición de alumno, calificaciones, etc.

Dato caduco: el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.  CHL

Dato de acceso irrestricto: Los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.  CTR

Sinónimos: *Fuentes de acceso público, Bases de datos de titularidad pública, Bancos de datos personales de titularidad pública, Ficheros de titularidad pública.*

Dato de acceso restringido: Los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.  CTR

Sinónimos: *Bases de datos de titularidad privada, Banco de datos personales de administración privada, Fichero de titularidad privada.*

Dato de carácter personal: Es sinónimo de dato de carácter personal. Dependiendo del país de que se trate, tiene distintas acepciones.

Cualquier información concerniente a una persona física identificada o identificable. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables.  IBE

Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.  ARG  BRA  NIC  URU

Sinónimos*: Datos personales.*

Datos de características personales y físicas: Tipo de sangre, ADN, huella digital, altura, peso, discapacidades, color de piel, iris y cabellos, señales particulares, etc.

Datos de carácter personal relacionados con la salud: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Sinónimos*: Datos de salud.*

Datos de identificación: Nombre, apellido, domicilio, teléfono, pin, correo electrónico, firma, Documento nacional de identidad, fecha de nacimiento, edad, nacionalidad, estado civil, sexo, imagen, dirección de IP, etc.

Dato de interconexión: Forma de tratamiento que consiste en la posibilidad de correlacionar los datos de un fichero con ficheros de otro responsable, o ficheros del mismo responsable pero para distintos fines.  POR

Dato disociado: Aquél que no permite la identificación de un afectado o interesado.

Sinónimos*: Disociación de datos, Desasociación de datos.*

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

Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. COL

Sinónimo*: Fuentes accesibles al publico*

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Datos especialmente protegidos: Sinónimo del término "datos sensibles". Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Podrán ser objeto de tratamiento los datos de carácter personal referidos a la salud y a la vida sexual, ideología , afiliación sindical y creencias, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Sinónimos: Datos sensibles.

Datos ideológicos: creencias religiosas, afiliación política, sindical, pertenencia a organizaciones de la sociedad civil, asociaciones religiosas, etc.

Datos de salud: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico, psiquiátrico, régimen de licencias, etc.

Sinónimo: *Datos de carácter personal relacionados con la salud.*

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

Datos laborales: puesto, empleador, domicilio, correo electrónico institucional, teléfono del trabajo, legajo, nómina, sanciones, licencias, seguridad social, aportes, historial en la empresa, etc.

Datos patrimoniales: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, información de consumos, situación de solvencia, etc.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables.  IBE

Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.  ARG  URU

Sinónimo: *Dato de carácter personal.*

Datos relativos a bases de datos con fines de publicidad: En la recopilación de domicilios o direcciones, reparto de documentos, publicidad, prospección comercial, venta directa o a distancia, 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.

Cuando los datos sean facilitados por los propios interesados u obtenidos con su consentimiento, debe previamente informarse las finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

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.  ARG  ESP  URU

Sinónimo: *Datos con fines de publicidad y prospección comercial.*

Datos relativos a encuestas, fines históricos, estadísticas: Las normas de la protección de datos no se aplicarán a las encuestas de opinión, mediciones, estadísticas, 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.  ARG  ESP

Datos relativos a la actividad comercial o 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, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

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 y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.  ARG  ESP  URU

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. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho. 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.  ARG

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. 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.  URU

Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y al momento de constituirse en mora, que en caso de no producirse el pago en el término previsto para ello, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.  ESP

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. 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. En tal sentido, no podrán realizar un tratamiento de los citados datos personales para finalidades distintas a las autorizadas por su titular, salvo orden judicial o mandato legal expreso. PER URU

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley. COL

Datos sensibles: Datos personales que afectan la esfera más íntima de su titular. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, información referente a la salud presente y futura, información genética, creencias o convicciones religiosas, filosóficas o morales, afiliación sindical, opiniones políticas, e información referida a la preferencia y vida sexual.

Serán considerados sensibles aquellos datos de carácter personal:

- Que afecten a la esfera más íntima del interesado; o
- Cuya utilización indebida pueda:
  - Dar origen a una discriminación ilegal o arbitraria, o
  - Conllevar un riesgo grave para el interesado.

La legislación debe establecer las garantías necesarias para preservar los derechos de los interesados y fijar condiciones adicionales para el tratamiento de datos de carácter personal considerados sensibles.

Sinónimos*: Datos personales sensibles, Datos especialmente protegidos.*

Deber de acreditar puesta a disposición: Los Responsables deberán conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999. COL

Deber de confidencialidad: La persona responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado o, en su caso, con la persona responsable.

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Véase también *Principio de confidencialidad.*

Deber de informar: 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 y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
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.

Sinónimos*: Obligación de informar.*

Deber de secreto: El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Decisión individual automatizada: Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

Una persona puede verse sometida a una decisión automatizada cuando dicha decisión:

- se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o
- esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Sinónimos*: Derecho a la impugnación de valoraciones personales, Derecho al tratamiento objetivo de datos personales, Impugnación de valoraciones.*

Declarante: Persona física que cumplimenta la solicitud de inscripción ante el Registro de Bases de Datos. No debe necesariamente coincidir con el titular/responsable.

Declaración de ficheros: Todo fichero/base de datos que contenga datos de carácter personal, debe inscribirse en el Registro que al efecto habilite el organismo de control, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos.

Están obligados a notificar la creación, modificación o supresión de ficheros al Registro que corresponda, aquellas personas físicas o jurídicas, de naturaleza pública o privada, titulares de ficheros que contengan datos de carácter personal.

La inscripción de un fichero deberá mantenerse actualizada. Cualquier modificación que afecte al contenido de la inscripción deberá ser previamente notificada al Registro, a fin de proceder a su inscripción. Asimismo, cuando el responsable de una base de datos decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el Registro.

La falta de declaración de las bases de datos personales al Registro correspondiente, puede dejar al responsable incurso en falta leve o grave a la Ley de Protección de Datos.

Sinónimos: *Registración de bases de datos, Declaración de ficheros, Inscripción de bases de datos, Inscripción de ficheros.*

Demanda de Habeas Data: La demanda o reclamación deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. Si se tratase de ficheros públicos, se procurará establecer el organismo estatal del cual dependen.

El accionante deberá alegar las razones por las cuales entiende que obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos ARCO. 

Véase también *Acción de habeas data, Procedimiento de habeas data, Sentencia de habeas data.*

Denegación de solicitud ARCO: El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

- Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
- Cuando en su base de datos, no se encuentren los datos personales del solicitante;
- Cuando se lesionen los derechos de un tercero;
- Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
- Cuando la rectificación, cancelación u oposición haya sido previamente realizada. La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular.

En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

Sinónimos*: Negativa por parte del responsable*

Véase también*: Negativa parcial por parte del responsable*

Denuncia de protección de datos ante el órgano de control: Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante el Órgano de control, que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa establecidas en esta ley. 

En España este procedimiento responde a la voz "Procedimiento de Tutela de Derechos" y, en México y Costa Rica a "Procedimiento de Protección de Derechos".

Sinónimos: *Procedimiento de tutela de derechos, Procedimiento de protección de derechos, Procedimiento administrativo de protección de datos.*

Véase también *Órgano de control, Sanciones*.

Departamento de datos personales: Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley de Datos Personales de México. Asimismo fomentará la protección de datos personales al interior de la organización. MEX

Depuración de datos personales: Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Derecho a impedir el suministro: El titular de datos personales tiene derecho a impedir que estos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de estos. PER

Sinónimos*: Derecho de oposición.*

Derecho al olvido: La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo diez años, desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular. CTR

Costa Rica es el único país que tiene regulado por ley el derecho al olvido. En el resto de Iberoamérica, el derecho al olvido es una construcción doctrinaria y jurisprudencial que combina los derechos de cancelación y oposición y no se encuentra expresamente recogida en los textos legales. IBE

Véase también *Derecho de Cancelación, Derecho de Oposición.*

Derecho al olvido digital: El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros.

En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales una vez terminada la relación contractual, el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien. NIC

Nicaragua es el único país que tiene regulado por ley el derecho al olvido digital.

Véase también *Derecho al olvido, Derecho de Cancelación, Derecho de Oposición.*

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 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. ARG URU

Sinónimos: *Tratamiento de datos en decisiones sin intervención humana valorativa, Impugnación de valoraciones, Derecho al tratamiento objetivo de datos personales.*

Derecho a la protección de datos personales: Derecho humano a la autodeterminación informativa, que tiene toda persona de controlar los alcances de su información personal. El derecho a la protección de datos personales se traduce como la facultad de una persona de controlar y administrar a su voluntad, la información personal que otros tienen de él o de los menores a su cargo.

Las leyes en protección de datos atribuyen a los ciudadanos la titularidad, el control, el poder de disposición y autodeterminación sobre sus datos personales supeditando el tratamiento de los mismos al consentimiento e información previa.

Sinónimos*: Derecho a la autodeterminación informativa.*

Derecho al tratamiento objetivo de datos personales: El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés. PER

Sinónimos*: Derecho a la impugnación de valoraciones personales, Impugnación de valoraciones, Decisión individual automatizada.*

Derecho constitucional a la protección de datos: Algunos países de Latinoamérica y todos los países miembros de la Unión Europea incluyen dentro de sus cartas magnas el derecho fundamental a la protección de datos personales.

La Constitución Argentina, garantiza el derecho de habeas data en su artículo 43: *"Toda persona puede interponer acción expedita y rápida de amparo (…) toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos"."*

La Constitución de Brasil, en su artículo 5, apartados LXXII LXXVII, reconoce el derecho de Habeas Data *"(…) a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo (…)son gratuitas las acciones de "habeas*

corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía".

La Constitución de Chile, dentro de sus preceptos ordena en su artículo 19 *"La constitución asegura a todas las personas*:(…) 4º El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia".

La Constitución de Colombia, reconoce el derecho a la protección de datos personales en su artículo 15*: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*

La Constitución de Costa Rica, reconoce el derecho a la protección de datos en sus artículos 23 y 24 bis, los que respectivamente ordenan: *"Artículo 23. El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley". "Artículo 24 bis. Toda persona tiene derecho a tener o no tener personalidad virtual, donde su presencia, contenido y proyección se encuentre regulada por cada una de ellas. No podrá ser utilizada con fines discriminatorios en perjuicio de su titular. El Estado garantizará que la información contenida en la personalidad virtual goce de la adecuada seguridad informática y jurídica, con exclusión de terceros no autorizados que pretendan obtenerla. El Estado podrá hacer uso del contenido de la personalidad virtual de las personas, previa autorización de éstas, siempre que se realice en beneficio y provecho de las mismas."*

La Constitución de la República del Ecuador reconoce el derecho a la protección de datos mediante lo dispuesto en su artículo 23 inciso 8vo.: *"Art. 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: (…)8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona".* Asimismo, garantiza su cumplimiento mediante lo ordenado en el artículo 94 de su Carta Magna: *"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito".*

La Constitución de El Salvador en su artículo 2 establece: *"(…) Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."*

La Constitución Española garantiza el derecho a la protección de datos personales en su artículo 18, inciso 4to. *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

La Constitución de Guatemala garantiza en su artículo 24 la *"inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna".* Asimismo, el artículo 31 ordena el *"acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".*

La Constitución de la República de Honduras en su artículo 76 dispone que *"Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen".*

La Constitución de los Estados Unidos Mexicanos recogen el derecho a la protección de datos personales en los Artículo 6 y 16, los que establecen, respectivamente *"La información sobre la vida privada y los datos personales en los archivos gubernamentales serán protegidos conforme a las leyes secundarias"* y "(…) Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas".

La Constitución de Nicaragua reconoce el derecho a la protección de datos en su artículo 26 cuando establece *"Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo;(…). A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".*

La Constitución de Panamá en su artículo 29 dispone: *"La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales. (…) se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. Igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas (…)".*

La Constitución de la República del Perú en su artículo 2 establece que *"Toda persona tiene derecho a: (…) 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal (…). Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".* Asimismo el artículo 200 recepta la Acción de Hábeas Data, que procede contra el hecho u omisión, parte de cualquier autoridad funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2, inciso 5) y 6) de la Constitución de la República del Perú.

La Constitución de la República Dominicana reconoce el derecho a la protección de datos en su artículo 44 inciso 2do que establece *"toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.* Asimismo el artículo 70 de la Carta Magna recepta el instituto de hábeas data:" *Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística".*

La Constitución de la República Oriental del Uruguay no hace mención expresa al derecho a la protección de datos personales.

La Constitución de la República de Venezuela establece en su artículo 28 que "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados (…) conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas (…). Asimismo, el artículo 60 dispone "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática (…)". Como corolario, el artículo 281 recepta la acción de habeas data.

Derecho de acceso: El titular de los datos tiene derecho a solicitar al responsable, tendrá derecho a recabar de la persona responsable, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.

Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo.

La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo.

Sinónimos*: Consultas.*

Derecho de actualización: Toda persona tiene derecho a que sean rectificados y/o actualizados los datos personales de los que sea titular incluidos en un banco de datos. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o actualización de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

Véase también *Derecho de rectificación.*

Derecho de cancelación: El interesado tendrá derecho a solicitar a la persona responsable la cancelación o supresión de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

La cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión.

La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado.

Cuando proceda, la persona responsable cancelará o suprimirá los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la

legislación nacional aplicable o, por las relaciones contractuales entre la persona responsable y el interesado, o para no dañar derechos de terceros.

Véase también *Derecho de supresión.*

Derecho de consulta al Registro de Bases de Datos: Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro que habilite al efecto el órgano de control, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro será de consulta pública y gratuita.

Sinónimos: *Derecho de información.*

Véase también *Registro de Bases de Datos Personales*, *Registro General de Protección de Datos, Registro Nacional de Bases de Datos, Registro Nacional de Protección de datos personales.*

Derecho de 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.

Sinónimos*: Impugnación de valoraciones personales, Derecho al tratamiento objetivo de datos personales, Decisión individual automatizada.*

Derecho de inclusión: Derecho que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando acredite un interés fundado. Toda persona física o jurídica tendrá derecho a solicitar la inclusión 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 inclusión, 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.

Derecho de información: (1) Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

- La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.
- 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.
- El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
- Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.
- La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

El derecho de información está reconocido en toda Iberoamérica, aunque ciertas legislaciones se refieren a este derecho directamente mediante el "deber de informar".

En argentina, el "derecho de información" es el llamado derecho de consulta en otras legislaciones.  IBE

Sinónimos*: Deber de informar*

(2) Cualquier persona podrá conocer, solicitando la información al Registro habilitado al efecto, la existencia de tratamiento de datos, sus finalidades y la identidad del responsable respecto a sus datos de carácter personal. El Registro será de consulta pública y gratuita.  ARG

Sinónimos*: Derecho de consulta al Registro de bases de datos*

Derecho de niños, niñas y adolescentes: En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.  COL

Derecho de oposición: El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable. De resultar procedente, el responsable no podrá tratar los datos relativos al titular. El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.

Derecho de rectificación: Toda persona tiene derecho a que sean rectificados y/o actualizados los datos personales de los que sea titular incluidos en un banco de datos. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o actualización

de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

Véase también *Derecho de actualización.*

Derecho de supresión: El interesado tendrá derecho a solicitar a la persona responsable la cancelación o supresión de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

Cuando proceda, la persona responsable cancelará o suprimirá los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable o, por las relaciones contractuales entre la persona responsable y el interesado, o para no dañar derechos de terceros.

Véase también *Derecho de cancelación, Bloqueo, Derecho al olvido digital, Derecho al olvido.*

Derecho humano a la protección de datos: El derecho a la protección de datos personales es inherente a la persona humana.

Véase también *Derecho constitucional a la protección de datos.*

Derechos ARCO: La legislación en protección de datos reconoce una serie de derechos a los ciudadanos, el derecho de acceso, rectificación, cancelación y oposición de sus datos personales (ARCO). Así, el titular de los datos puede solicitar información sobre qué datos tienen y cómo los han obtenido (derecho de acceso), la rectificación de los mismos, la cancelación de los datos en sus ficheros (derecho de cancelación) o la oposición a que traten sus datos para un uso o fin determinado (derecho de oposición).

El ejercicio de cada uno de estos derechos es independiente entre sí, no es necesario agotar uno para ejercer alguno de los otros tres.

Véase también *Derecho de acceso, Derecho de cancelación, Derecho de rectificación, Derecho de oposición.*

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.

No se considera comunicación o cesión de datos el acceso por parte de un encargado del 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.

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.

Véase también *Consentimiento*, *Principio de finalidad*.

Destinatario: Persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Véase también *Cesionario*.

Días: Días hábiles. Salvo que expresamente se indique que se computarán días corridos.

Dirección de Protección de Datos Personales: Dirección de Protección de Datos Personales adscrita al Ministerio de Hacienda y Crédito Público, que cuenta con un Director designado por la máxima autoridad administrativa de dicho ministerio y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.


NIC

Dirección General de Protección de Datos Personales: Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones.


PER

Dirección Nacional de Protección de Datos: La Dirección Nacional de Protección de Datos Personales -DNPD- es el órgano de control argentino creado en el ámbito nacional, para la efectiva protección de los datos personales. Goza de autonomía funcional y actúa como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Tiene a su cargo el Registro de las Bases de Datos, y las atribuciones de inspección, sanción y supervisión del cumplimiento de la Ley de Habeas Data, entre otras.


ARG

Véase también *DNPD.*

Directorios de correo: Conjunto de direcciones de correo electrónico, estructurado para la realización de búsquedas. Es un concepto similar al de "guía telefónica", aplicado a las direcciones de correo electrónico.

Disociación de datos: El procedimiento mediante el cual los datos personales no pueden asociarse a su titular ni permitir, por su estructura, contenido grado de desagregación, la identificación a una persona determinada o determinable.

Sinónimos: *Desasociación de datos.*

Documento de seguridad: Instrumento que contiene los procedimientos y medidas de seguridad física, administrativa y técnica para garantizar la confidencialidad, integridad y disponibilidad de los datos contenidos en los sistemas de datos personales.

Sinónimos: *Protocolo mínimo de actuación, Políticas de tratamiento.*

Domicilio del titular de datos: En las solicitudes de derechos ARCO, se deberá indicar el domicilio o cualquier otro medio para que sea notificada la respuesta. En caso de no cumplir

con este requisito, el responsable tendrá por no presentada la solicitud, dejando constancia de ello.

Véase también *Derechos ARCO, Solicitud ARCO*.

DNPD: Dirección Nacional de Protección de Datos, autoridad máxima Argentina de aplicación en materia de protección de datos personales, órgano de control que tiene por objeto realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la Ley de Habeas Data 25.326. ARG

Sinónimos: *Dirección Nacional de Protección de Datos.*

Ejercicio de derechos ARCO: El ejercicio de cualquiera de los derechos ARCO no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos.

La entrega de los datos personales será gratuita, previa acreditación de su identidad, debiendo cubrir el titular únicamente los gastos justificados de envío o el costo de reproducción en copias u otros formatos.

Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.  IBE

La legislación peruana contempla la posibilidad de exigir una contraprestación para el ejercicio de los derechos ARCO.  PER

Sinónimos*: Petición de habeas data.*

Véase también *Derechos ARCO, Gratuidad ARCO, Procedimiento de derechos ARCO, Intervalos para solicitar derechos ARCO.*

Encargado: Persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable.

Sinónimos: *Encargado del tratamiento, Subcontratista.*

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Sinónimos: *Encargado, Subcontratista*

Véase también *Acceso a los datos por cuenta de terceros, Subcontratación de servicios, Cesión de datos, Autorización de la subcontratación.*

Entorno digital: Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos.

Excepciones al ámbito de aplicación del régimen de protección de datos: Las disposiciones del presente Reglamento no serán aplicables a la información siguiente:

- La relativa a personas morales;

- Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas, y
- La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista. MEX

Asimismo, el régimen de protección de los datos de carácter personal no será de aplicación a los siguientes ficheros y tratamientos:

- A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.
- A los sometidos a la normativa sobre protección de materias clasificadas.
- A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos. ESP

El régimen de protección de datos no será de aplicación a las siguientes bases de datos:

- A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- 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.
- A las bases de datos creadas y reguladas por leyes especiales. URU

Sinónimos: *Actividades excluidas del ámbito de la protección de datos.*

Véase también *Exceptuados al cumplimiento del régimen de protección de datos.*

Excepciones al consentimiento: No será necesario el consentimiento cuando:

- Esté previsto en una Ley o se recaben para el ejercicio de funciones propias del Estado;
- Los datos figuren en fuentes de acceso público;
- Los datos personales se sometan a un procedimiento previo de disociación;
- Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

- Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o
- Se dicte resolución de autoridad competente. IBE
- Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes. ARG PER
- Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27.332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
- Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos. PER

Véase también *Consentimiento.*

Excepciones a los derechos ARCO: Los responsables de los ficheros 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 los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación. ESP

Sinónimos: *Denegación de solicitud ARCO, Negativa a responder derechos ARCO, Negativa parcial a responder derechos ARCO.*

Excepción a la autorización: No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios. Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos. CHL

Sinónimos: *Excepción al consentimiento*.

Véase también *Autorización.*

Excepción de la prohibición de transferir a países no adecuados: La prohibición no regirá en los siguientes supuestos:

- Cuando sea para solicitar o proveer auxilio o colaboración judicial internacional;
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias, bancarias o bursátiles, conforme a su regulación específica;
- Cuando la transferencia se hubiera acordado en el marco de tratados internacionales o convenios en los cuales el país de origen de los datos 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.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Véase también *transferencia internacional de datos.*

Exceptuados al cumplimiento del régimen de protección de datos: El régimen de protección de los datos de carácter personal no será aplicable:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.
- A los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

El régimen de protección de los datos de carácter personal no será aplicable: a los ficheros de uso exclusivamente personal o doméstico.

El régimen de protección de los datos de carácter personal no será de aplicación a las siguientes bases de datos:

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

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

URU

Las previsiones legales en protección de datos personales no serán aplicables a la información siguiente:

- La relativa a personas morales;
- Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas,
- La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.

MEX

Las previsiones legales en protección de datos personales no serán de aplicación a:

- El tratamiento de datos personales realizado por personas naturales para fines exclusivamente domésticos, personales o relacionados con su vida privada o familiar.
- Los contenidos o destinados a ser contenidos en bancos de datos personales de la administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de competencias asignadas por ley a las respectivas entidades públicas siempre que tengan por objeto:
    - La defensa nacional.
    - La seguridad pública y,
    - El desarrollo de actividades en materia penal para la investigación y represión del delito.

PER

Los principios, los derechos y las garantías establecidos en la normativa de protección de datos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando se persigan los siguientes fines:

- La seguridad del Estado.
- La seguridad y el ejercicio de la autoridad pública.
- La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.
- El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.
- La adecuada prestación de servicios públicos.
- La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

CTR

- El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

- A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
- A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
- A las bases de datos y archivos de información periodística y otros contenidos editoriales;
- A las bases de datos y archivos regulados por la Ley 1266 de 2008;
- A las bases de datos y archivos regulados por la Ley 79 de 1993.


COL

Véase también *Ámbito de aplicación, Actividades excluidas al ámbito de protección de datos.*

Expectativa razonable de privacidad: Confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes y en cumplimiento de la normativa vigente.


MEX

Exportador de datos personales: responsable de los datos de carácter personal que son objeto de transferencia internacional a un país tercero.

Faltas: Salvo en Costa Rica, en el resto de Iberoamérica se utiliza la voz "infracciones".

Sinónimos: *Infracciones.*

Fe Pública: En el ejercicio de las funciones de verificación, el personal del Instituto estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

Fecha de la inscripción: Se computará como fecha de inscripción definitiva de las bases de datos la correspondiente a la Resolución o Notificación del órgano de control.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Sinónimos: *Archivo, Registro, Base de datos, Banco de datos*.

Fichero de exclusión del envío de comunicaciones comerciales: Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Fichero no automatizado: Todo conjunto de datos de carácter personal organizado de forma manual, no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Sinónimos: *Bases de datos no automatizadas.*

Ficheros comunes de envío de comunicaciones comerciales: Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad. A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Véase también *Datos relativos a bases de datos con fines de publicidad.*

Ficheros de información sobre solvencia patrimonial y crédito: En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter

patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre él mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.  ARG  ESP  URU

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. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho. 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.  ARG

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. 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.  URU

Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y al momento de constituirse en mora, que en caso de no producirse el pago en el término previsto para ello, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.  ESP

Véase también *Datos relativos a la actividad comercial o crediticia, Ficheros de información sobre solvencia patrimonial y créditos.*

Ficheros de datos de titularidad privada: ficheros cuyo responsable son personas, empresas o entidades de derecho privado. Si se trata de bases de datos de particulares para un uso exclusivamente personal y privado, quedan fuera del ámbito de aplicación de la Ley de Protección de Datos.

Sinónimos: B*ases de datos de titularidad privada, Banco de datos personales de administración privada.*

Ficheros de datos de titularidad pública: Ficheros de los que sean responsables los órganos del Estado y las instituciones de la administración pública, así como las entidades u organismos vinculados o dependientes de las mismas.

Sinónimos: B*ases de datos de titularidad pública, Banco de datos personales de administración pública.*

Ficheros de las Fuerzas y Cuerpos de Seguridad: Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de protección de datos personales.

La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto.

Ficheros temporales: Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Firma electrónica: Conjunto de datos electrónicos añadidos a un mensaje que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Para su generación se suelen utilizar técnicas criptográficas.

Flujo transfronterizo de datos personales: Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

El titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley. En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente Ley.

Sinónimos: *Transferencia internacional de datos.*

Véase también *Excepción a la prohibición de transferir a países no adecuados*

Forma de recabar el consentimiento: El responsable del tratamiento podrá solicitar el consentimiento del interesado a través de los siguientes modos, salvo cuando la Ley exija la obtención del consentimiento expreso para el tratamiento de los datos.

El responsable podrá dirigirse al afectado, informándole y concediéndole un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. Cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a

cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos.

Cuando se solicite el consentimiento del interesado a través de este procedimiento, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.  ESP

Sinónimos: *Modo de obtener autorización.*

Fuentes accesibles al público: Bases de datos que contienen datos personales que pueden ser utilizados y tratados sin consentimiento de la persona afectada, sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los directorios telefónicos en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo; los Diarios y Boletines oficiales y los medios de comunicación.

La inclusión de datos adicionales requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

Garantía de confidencialidad: Obligación de toda persona física o jurídica, pública o privada, que tenga participación en el tratamiento o almacenamiento de datos personales, de cumplir con el deber de confidencialidad que exige la Ley. CTR

Sinónimos: *Secreto profesional, Principio de confidencialidad*.

Garantías efectivas: toda persona interesada tiene derecho a un procedimiento administrativo sencillo y rápido ante la PRODHAB, con el fin de ser protegido contra actos que violen sus derechos fundamentales a la protección de datos personales.

Sinónimos*: Procedimiento administrativo de protección de datos, Procedimiento trilateral de tutela de derechos, Procedimiento de tutela de derechos, Procedimiento de protección de datos.* CTR

Gestión de soportes: dentro de las medidas de nivel medio, Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Dentro de las medidas de nivel alto, la identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos. ESP

Véase también *Medidas de seguridad de nivel medio.*

Graduación de sanciones: Cuando ocurra una vulneración a la seguridad de los datos personales, atendiendo al carácter intencional o no del infractor, el tipo de infracción y la voluntad de cumplimiento del infractor, el órgano de control podrá atenuar la sanción que corresponda.

Véase también *Sanciones*

Gratuidad ARCO: La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.


IBE

Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.


MEX

La legislación peruana contempla la posibilidad de exigir una contraprestación para el ejercicio de los derechos ARCO.


PER

Si la misma persona reitera su solicitud ARCO en un período menor a doce meses, podrá solicitársele el pago de una contraprestación, a menos que existan modificaciones sustanciales en las políticas de privacidad o aviso de privacidad que motiven nuevas consultas.


COL

CTR

MEX

Véase también *Derechos ARCO, Ejercicio de los derechos ARCO.*

Grupos sin personalidad jurídica: Las personas integrantes de un grupo que actúe sin personalidad jurídica y que trate datos personales para finalidades específicas o propias del grupo se considerarán también responsables o encargados, según sea el caso.

Habeas Data: Es el derecho, en ejercicio de una acción constitucional o legal, que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección o eliminación de esa información si le causara algún perjuicio. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido relevancia para seguir siendo informada.

Este derecho se fue expandiendo y comenzó a ser reglamentado tanto por leyes de habeas data como por normas de protección de datos personales (que suelen tener un capítulo procesal donde se describe el objeto de la acción de habeas data, la legitimación pasiva y activa, y la prueba y la sentencia).

Véase también *Acción de habeas data*.

Identificación del afectado: Cualquier procedimiento de reconocimiento del afectado y/o elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social del titular de los datos.

Identificación del personal verificador: Al iniciar la visita, el personal verificador deberá exhibir credencial vigente con fotografía, expedida por el Instituto que lo acredite para desempeñar dicha función, así como la orden escrita fundada y motivada a la que se refiere el artículo anterior, de la que deberá dejar copia con quien se entendió la visita.  MEX

Al iniciar la visita, el personal fiscalizador deberá exhibir credencial vigente con fotografía, expedida por la Dirección General de Protección de Datos Personales que lo acredite como tal.  PER

Véase también *IFAI, Instituto, Dirección general de protección de datos personales, Visitas de verificación, Visitas de fiscalización.*

IFAI: El Instituto Federal de Acceso a la Información y Protección de Datos es la Autoridad de Aplicación en materia de protección de datos de los Estados Unidos Mexicanos, conforme lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.  MEX

Véase también *Instituto.*

Importador de datos personales: La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Improcedencia de la solicitud de protección de derechos: La solicitud de protección de datos será desechada por improcedente cuando:

- El Instituto no sea competente;
- El Instituto haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente;
- Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo;
- Se trate de una solicitud de protección de datos ofensiva o irracional, o
- Sea extemporánea.  MEX

Impugnación de valoraciones: Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 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 de carácter personal que ofrezca una definición de sus características o personalidad.

En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

Sinónimos: *Derecho a la impugnación de valoraciones personales, Tratamiento de datos en decisiones sin intervención humana valorativa, Derecho al tratamiento objetivo de datos personales*

Incidencia de seguridad: Se entiende por incidencia o vulneración de seguridad cualquier anomalía que afecte o pueda afectar a la seguridad e integridad de los datos de carácter personal (estén automatizados o no).

Sinónimos: *Vulneración de seguridad.*

Infracciones: Constituyen infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

- No responder a la solicitud de derechos ARCO, sin razón fundada;
- Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de derechos ARCO;
- Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;
- Dar tratamiento a los datos personales en contravención a los principios establecidos en la Ley;
- Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la ley federal de protección de datos personales en posesión de particulares;
- Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;
- No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64 federal de protección de datos personales en posesión de particulares;
- Incumplir el deber de confidencialidad;
- Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12 de la ley federal de protección de datos personales en posesión de particulares;
- Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;
- Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
- Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
- Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;
- Obstruir los actos de verificación de la autoridad;
- Recabar datos en forma engañosa y fraudulenta;
- Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;
- Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO;
- Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de la Ley federal de protección de datos personales en posesión de particulares, y

- Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la Ley federal de protección de datos personales en posesión de particulares. MEX

Constituyen infracciones a la Ley Orgánica de Protección de Datos (LOPD) las siguientes:

Son infracciones leves: No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en la LOPD; no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos; el incumplimiento del deber de información al afectado; la transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en la LOPD.

Son infracciones graves: Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente; tratar datos de carácter personal sin recabar el consentimiento, cuando éste sea necesario; tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD, salvo cuando sea constitutivo de infracción muy grave; la vulneración del deber de guardar secreto; el impedimento o la obstaculización del ejercicio de los derechos ARCO; el incumplimiento del deber de información cuando los datos no hayan sido recabados del propio interesado; el incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la LOPD; mantener los datos de carácter personal sin las debidas condiciones de seguridad; No atender los requerimientos o apercibimientos de la AEPD o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma; obstruir al ejercicio de la función inspectora de la AEPD; la comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello, salvo que la misma sea constitutiva de infracción muy grave.

Son infracciones muy graves: La recogida de datos en forma engañosa o fraudulenta; tratar o ceder los datos de carácter personal de modo contrario a lo dispuesto en la LOPD; no cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un requerimiento de la AEPD para ello; transferir internacionalmente de datos de carácter personal con destino a países que no proporcionen un nivel de protección adecuado o sin autorización del Director de la AEPD salvo en los supuestos en los que conforme a la LOPD dicha autorización no resulta necesaria. ESP

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 Ley 18.331:

Apercibimiento.

Multa de hasta quinientas mil unidades indexadas.

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 ley 18.331. URU

Constituye infracción sancionable toda acción u omisión que contravenga o incumpla alguna de las disposiciones contenidas en la Ley 29.733 o en su reglamento. Las infracciones se califican como leves, graves y muy graves.

Son infracciones leves:

- Dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario conforme a lo dispuesto en la Ley.
- No atender, impedir u obstaculizar el ejercicio de los derechos ARCO del titular.
- Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.

Son infracciones graves:

- Dar tratamiento a los datos personales contraviniendo los principios establecidos en la Ley 29.733 o incumpliendo sus demás disposiciones o las de su Reglamento.
- Incumplir la obligación de confidencialidad.
- No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos ARCO del titular.
- Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.

Son infracciones muy graves:

- Dar tratamiento a los datos personales contraviniendo los principios establecidos en la Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la Ley o su reglamento.
- Suministrar documentos o información falsa o incompleta a la Autoridad Nacional de Protección de Datos Personales.
- No cesar en el tratamiento ilícito de datos personales, cuando existiese un previo requerimiento de la Autoridad Nacional de Protección de Datos Personales para ello.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales, no obstante haber sido requerido para ello por la Autoridad Nacional de Protección de Datos Personales.


PER

La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 6 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.


CHL

Serán consideradas faltas leves, para los efectos de la Ley Nº 8968:

- Recolectar datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada.
- Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

Serán consideradas faltas graves, para los efectos de esta ley:

- Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos.
- Transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en la ley.
- Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
- Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a la ley.
- Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

Serán consideradas faltas gravísimas:

- Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles.
- Obtener, de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.
- Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la ley.
- Proporcionar a un tercero información falsa o distinta contenida en un archivo de datos, con conocimiento de ello.
- Realizar tratamiento de datos personales sin encontrarse debidamente inscrito ante la Prodhab, en el caso de los responsables de bases de datos cubiertos por el artículo 21 de la ley.
- Transferir, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares.

Son infracciones leves a esta ley, las siguientes:

- Tratar datos personales sin el consentimiento expreso ya sea por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos de su titular, cuanto la ley así lo exija;
- Omitir la inclusión, complementación, rectificación, actualización, supresión o bloqueo, cancelación, de oficio o a petición del titular, de los datos personales que se encuentran en ficheros de datos públicos y privados;
- Incumplir las instrucciones dictadas por la Dirección de Protección de Datos Personales;

- Obtener datos personales a través de formularios u otros impresos, sin que figure en los mismos, en forma claramente legible, las advertencias que se utilizarán para crear ficheros; y
- Remitir publicidad a través de medios electrónicos, a titulares que han manifestado expresamente su negativa a recibirla.

Son infracciones graves, las siguientes:

- El tratamiento de datos personales por medios fraudulentos o que infrinjan las disposiciones contempladas en la Ley N◦787;
- Impedir u obstaculizar el ejercicio del derecho a la autodeterminación informativa al titular de los datos personales, así como negar injustificadamente la información solicitada;
- Violentar el secreto profesional;
- Reincidir en las infracciones leves;
- Mantener ficheros de datos, inmuebles, equipos o herramientas sin las condiciones mínimas de seguridad, integridad y confidencialidad requeridas por las disposiciones aplicables; y
- Obstruir las inspecciones que realice la Dirección de Protección de Datos Personales.


NIC

Las entidades que por negligencia no cumplieron con la obligación de notificar a la DPA tratamiento de los datos personales mencionados en los apartados 1 y 5 del artículo 27 de la Ley 67/98, o proporcionar información falsa para cumplir con el requisito de notificación de las infracciones los términos previstos en el artículo 29 de la misma, o cuando, después de notificado por DPA, mantengan el acceso a las redes abiertas de transmisión de datos de carácter personal a responsables que no cumpla con las disposiciones de esta Ley, podrán aplicarse las siguientes multas:

- En el caso de una persona física, un mínimo de 50 mil y un máximo de 500.000 euros;
- En el caso de una persona jurídica o entidad no incorporada, un mínimo de 300.000 y un máximo de 3.000.000 euros.

La multa se incrementa al doble sus límites cuando se trata de datos sujetos a investigación de antecedentes.

Practican un delito punible con multa mínima de 100.000 euros y un máximo de euros 1.000.000 entidades que no cumplan alguna de las siguientes disposiciones de esta Ley: designar un representante; el incumplimiento de las obligaciones establecidas en los artículos 5, 10, 11, 12, 13, 15, 16 y 31 inc. 3.

La pena se elevará al doble sus límites cuando se haya cumplido con las obligaciones establecidas en los artículos 6, 7, 8, 9, 19 y 20.


POR

Inmovilización de ficheros: En el supuesto previsto como infracción muy grave en la LOPD, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los

responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Inscripción de códigos tipo y códigos de conducta: Determinadas regulaciones exigen la inscripción u notificación de los códigos tipo por ante su autoridad de aplicación. El procedimiento para la inscripción de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

Véase también *Código tipo, Código de conducta.*

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.

Inspección: Las autoridades de control, con el objeto de comprobar el cumplimiento por los Responsables de la Ley de Protección de Datos, podrán realizar inspecciones, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

La inspección puede iniciarse de oficio o a petición de parte. Cualquier persona podrá denunciar ante la autoridad de aplicación las presuntas violaciones a la protección de datos personales, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos.

Para llevar a cabo la inspección, la autoridad de aplicación tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive.

Los funcionarios que ejerzan la inspección están obligados a guardar confidencialidad sobre la información que conozca derivada de la inspección correspondiente.

Sinónimos: *Verificación, Constatación de posibles infracciones, Fiscalización.*

Véase también *Procedimiento de Inspección*

Instituto: Instituto Federal de Acceso a la Información y Protección de Datos. Autoridad de Aplicación en materia de protección de datos de los Estados Unidos Mexicanos.

Sinónimos: *IFAI.*

Integridad: Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

Interesado: Titular de los datos que sean objeto del tratamiento.

Sinónimos: A*fectado, Titular de datos.*

Intervalos para solicitar derechos ARCO: Solo podrá ser ejercitado a intervalos no inferiores a 12 meses. ESP

El derecho de acceso solo podrá ser ejercitado a intervalos no inferiores a 6 meses, salvo que se acredite un interés legítimo al efecto. ARG URU

Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas. MEX

Si la misma persona reitera su solicitud ARCO en un período menor a doce meses, podrá solicitársele el pago de una contraprestación, a menos que existan modificaciones sustanciales en las políticas de privacidad o aviso de privacidad que motiven nuevas consultas. COL CTR MEX

Véase también Ejercicio de derechos ARCO.

Juicio de nulidad: Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa. MEX

Véase también *IFAI, Recurso contra Resoluciones Protección de Datos Personales.*

Legitimados para ejercer derechos ARCO: Los derechos ARCO se ejercerán por el titular, previa acreditación de su identidad; o través de su representante, previa acreditación de la identidad del titular y del representante, y la existencia de la representación.

Los derechos de los Titulares establecidos en la Ley, podrán ejercerse por las siguientes personas:

- Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Véase también *Derechos ARCO.*

Legitimados para promover acción de habeas data: La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

Ley de Orden Público: Las normas de orden púbico son irrenunciables e imperativas, en el sentido de que deben cumplirse cualquiera que sea la voluntad de las partes. Son normas que hacen a los principios generales del derecho y al conjunto de principios superiores del ordenamiento jurídico que no puede quedar relegado en manera alguna al arbitrio de los individuos. Si una ley es de orden público, las partes no pueden dejarla sin efecto en sus contratos.

En Argentina, la Ley 25.326 de Protección de los Datos Personales es de orden público.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, es de orden público y de observancia general en toda la República.

En Perú, la Ley 29733 de Protección de Datos Personales es de orden público.

En Brasil, la Ley 9507/97 posee aplicabilidad inmediata.

Ley de Protección de Datos de carácter Personal: Ley portuguesa que regula la protección de datos personales, publicada bajo el número 67 de 1998.

Ley de Protección de Datos Personales: Ley Peruana que regula la protección de datos personales, publicada bajo el número 29.733. Tiene el objeto de garantizar el derecho fundamental a la protección de datos personales, prevista en el Artículo 2 numeral 6to de la Constitución del Perú.

Ley de Protección de Datos Personales: Ley 787/2012 de Nicaragua, que regula la protección de los datos personales. Tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efectos de garantizar el derecho a la privacidad personal y familiar, y el derecho a la autodeterminación informativa. NIC

Ley de Protección de Datos Personales y Acción de "Habeas Data": Ley Uruguaya de protección de datos, registrada bajo Ley Nº 18.331. Define su objeto y ámbito de aplicación 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 en los tres primeros artículos de su plexo normativo, siendo: "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 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". URU

Ley de Protección de la persona frente al tratamiento de sus datos personales:: La Ley No. 8969 del 5 de septiembre de 2011, regula el tratamiento de los datos personales en Costa Rica.

Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. CTR

Ley de Protección de los Datos Personales: Ley Argentina que regula la protección de datos personales, publicada bajo el número 25.326, también conocida como Ley de Habeas Data. La citada 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, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43 Ver Texto, párr. 3 de la Constitución Nacional. Como particularidad, la Ley Argentina protege, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En relación al escueto ámbito de aplicación definido en el Art. 1 de la Ley, el mismo queda salvado por lo dispuesto en su Decreto Reglamentario 1558/2001, que establece: "ARTICULO 1º.- A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito". ARG

Ley Estatutaria 1266 de 2008: Ley Colombiana de 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas

con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política de Colombia, así como el derecho a la información establecido en el artículo 20 de la Constitución Política de Colombia, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. COL

Ley Federal de Protección de Datos Personales en Posesión de los Particulares: Ley Mexicana de protección de datos, también conocida como LFPDPPP. Se trata de una Ley de orden público y de observancia general en toda la República, que tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. MEX

Ley Orgánica: En España la Ley de Protección de Datos de carácter personal 15/1999, de 13 de diciembre es una Ley Orgánica. En el territorio español, las leyes orgánicas se relacionan con las ordinarias de una forma no jerárquica, opuesto a la situación que se da entre leyes y reglamentos; se trata de una organización basada en las características de cada asunto a regular, de modo que se limite el alcance de cada tipo de ley. Esto garantiza el análisis de cada caso en concreto y la aplicación de las leyes que correspondan a su naturaleza, y no de aquéllas que pesen más. A continuación se enumeran las materias que en España deben ser medidas a través de las leyes orgánicas:

- La concepción de los derechos de carácter fundamental y de la libertad de la comunidad;
- La acción de aprobar o modificar los Estatutos de Autonomía;
- Cualquier procedimiento relacionado con el régimen general de elecciones.

En Chile, las leyes orgánicas pertenecen a un apartado especial de leyes dentro del ordenamiento jurídico, y se refieren a materias taxativamente detallados. Las leyes orgánicas necesitan de una mayoría equivalente a cuatro de cada siete votos por parte de los senadores y diputados, ya sea para su aprobación, modificación o derogación.
En República Dominicana, una ley orgánica se concibe para regular un derecho fundamental, tal como lo son: la forma y la administración de los poderes públicos; el ejercicio de las funciones públicas; el régimen de elecciones; las cuestiones relacionadas con la economía y las finanzas a nivel nacional; las decisiones que requieren de la confección de un presupuesto, de planificación o de inversión de carácter público; la organización del territorio; las acciones de tipo constitucional; la defensa y la seguridad nacional.

En Colombia ciertos temas deben ser regulados mediante las leyes orgánicas, y giran en torno a: las actividades de tipo legislativo; normas pensadas para preparar, aprobar y ejecutar el presupuesto de renta; cualquier acción que afecte las leyes de aprobaciones, del plan nacional de desarrollo y aquéllas que se conciben para asignar competencias de carácter normativo a los organismos nacionales. Las leyes orgánicas deben necesariamente pasar por el Pleno de las Cámaras: exclusión de la delegación de su aprobación en las Comisiones legislativas permanentes (art. 75.3 CE).

Ley Orgánica de Protección de Datos: Ley Española 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. ESP

Ley que dicta normas para la transparencia en la gestión pública, establece la acción de Habeas Data y otras disposiciones: Ley Panameña No.6 de 22 de enero de

2002, que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones.

Ley que Reglamenta la Información de Carácter Privado: Ley Paraguaya publicada bajo el Nº 1682/2001 que reglamenta la información de carácter privado, modificada por la Ley Nº 1969 que modifica, amplía y deroga varios artículos de la Ley n° 1682 que reglamenta la información de carácter privado. La Ley 1969 tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares.

Ley que regula el servicio de información sobre el historial de crédito de los consumidores o clientes: Ley Panameña No. 24/2002, que regula sectorialmente aspectos relativos a la protección de datos personales de consumidores y clientes, que tiene por objeto proteger y garantizar la confiabilidad, veracidad, actualización, y el buen manejo de los datos personales de consumidores y clientes, relativos a su historial de crédito, incorporados o susceptibles de ser incorporados a un registro de datos.

Ley sobre Protección de la vida privada: Ley Nº 19.628 que ordena el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

Límites al derecho a la protección de datos: Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Listado de exclusión: Base de datos que tiene por objeto registrar de manera gratuita la negativa del titular al tratamiento de sus datos personales. Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas.

Sinónimos*: Depuración de datos personales.*

Mandato: En el caso de que el tratamiento de datos personales se efectúe por mandato, deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos. El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo. CHL

Sinónimos*: Subcontratación de servicios, Acceso a datos por cuenta de terceros.*

Véase también*: Encargado del Tratamiento, Encargado.*

Medidas compensatorias: Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares o a la antigüedad de los datos, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios generales expedidos por el Instituto, mismos que serán publicados en el Diario Oficial de la Federación.

Los casos que no actualicen los criterios generales emitidos por el Instituto requerirán la autorización expresa de éste, previo a la instrumentación de la medida compensatoria. MEX

Véase también *Instituto, IFAI.*

Medidas de seguridad: Control o grupo de controles de seguridad para proteger los datos personales. Las medidas de seguridad serán adecuadas conforme al tipo de datos de que se trate. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con independencia del sistema de tratamiento.

Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad de nivel básico: Funciones y obligaciones del personal. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento. **Registro de incidencias.** Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. **Control de acceso.** Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con

derechos distintos de los autorizados. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio. **Gestión de soportes y documentos.** Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. **Identificación y autenticación.** El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible. **Copias de respaldo y recuperación.** Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad. ESP

Medidas de seguridad de nivel medio: Responsable de seguridad. En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de

coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento. **Auditoría.** A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de la autoridad de aplicación que corresponda. **Gestión de soportes y documentos.** Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. **Identificación y autenticación.** El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. **Control de acceso físico.** Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información. **Registro de incidencias.** En el registro de incidencias deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Medidas de seguridad de nivel alto: Gestión y distribución de soportes. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el

documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos. **Copias de respaldo y recuperación.** Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación. **Registro de accesos.** De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. El período mínimo de conservación de los datos registrados será de dos años. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: Que el responsable del fichero o del tratamiento sea una persona física; Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales; La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad. **Telecomunicaciones.** Cuando deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

- Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
- Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
- Garantizar la eliminación de datos de forma segura.

Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

- El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
- El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y
- Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Medios de difusión: Para la difusión el responsable podrá valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

Medios de impugnación de decisiones del órgano de control: Contra las resoluciones que resuelven cuestiones relativas a las violaciones a los preceptos de las leyes de protección de datos o a los procedimientos de acceso, rectificación, cancelación y oposición, emitidas por los órganos de control, se agota la vía administrativa, quedando abierta la vía recursiva judicial.

Sinónimos: *Recurso contra resolución de protección de datos.*

Véase también *Juicio de nulidad, Órgano de control, Acción de habeas data, Acción de protección de datos personales.*

Medios para el cumplimiento del derecho de acceso: La obligación de acceso se dará por cumplida cuando el responsable ponga a disposición del titular los datos personales, de forma gratuita, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular.

Sinónimos: *Obligación de acceso a la información, Medios para el cumplimiento de derechos ARCO*

Medios para el cumplimiento de derechos ARCO: El titular, para el ejercicio de los derechos ARCO, podrá presentar, por sí mismo o a través de su representante, la solicitud ante el responsable junto con la acreditación de su identidad.

El responsable deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado.

La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, remotos, telefónicos, de imagen, visualización en pantalla, informe escrito, correo electrónico, u otro idóneo a tal fin.

El responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.  IBE

Cuando las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, se estará a lo dispuesto en aquéllas que ofrezcan mayores garantías al titular, y no contravengan las disposiciones previstas en la Ley.  MEX

Sinónimos: *Obligación de acceso a la información, Medios para el cumplimiento de derechos de acceso, Respuesta del responsable.*

Véase también *Servicios de atención al público.*

Medidas para el cumplimiento del principio de responsabilidad: El responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad. Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:

- Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;
- Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;

- Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;
- Destinar recursos para la instrumentación de los programas y políticas de privacidad;
- Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;
- Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;
- Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;
- Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento,
- Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastreara los datos personales durante su tratamiento.


MEX

Sinónimos*: Obligaciones del responsable.*

Véase también *Medidas de seguridad, Políticas de Tratamiento, Protocolo mínimo de actuación.*

Modo de obtener la autorización: los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (I) por escrito, (II) de forma oral o (III) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.


CHL

COL

Sinónimos*: Forma de obtener el consentimiento.*

Movimiento internacional de datos: No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal con destino a países que no proporcionen un nivel de protección adecuado, salvo que, además de haberse observado lo dispuesto en las leyes de protección de datos del país de origen de los datos, se obtenga autorización previa de la autoridad de aplicación.

Sinónimos: *Transferencia internacional de datos*

Negación a pedidos de derechos ARCO: El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

- Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
- Cuando en su base de datos, no se encuentren los datos personales del solicitante;
- Cuando se lesionen los derechos de un tercero;
- Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
- Cuando la rectificación, cancelación u oposición haya sido previamente realizada. La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular.

En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

Sinónimos: *Denegación de solicitud ARCO.*

Negativa parcial por parte del responsable: El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

- Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
- Cuando en su base de datos, no se encuentren los datos personales del solicitante;
- Cuando se lesionen los derechos de un tercero;
- Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
- Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. MEX

Negativa por parte del responsable: El responsable que niegue el ejercicio de cualquiera de los derechos ARCO deberá justificar su respuesta, así como informar al titular el derecho que le asiste para solicitar el inicio del procedimiento de protección de derechos ante la autoridad de aplicación que corresponda.

Sinónimos: *Negación a pedidos de derechos ARCO, procedimiento de protección de derechos, acción de protección de datos, procedimiento de tutela de derechos.*

Nivel adecuado de protección de datos: El carácter adecuado del nivel de protección que ofrece el país de destino de una transferencia de datos se evaluará por la autoridad de aplicación, atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la declaración de país adecuado efectuada por la Unión Europea; la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos; el país de origen y el país de destino final; las normas de derecho, generales o sectoriales, vigentes en el país tercero de

que se trate; el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Véase también *Países con nivel adecuado de protección de datos.*

Nivel de seguridad: Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.
- Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquéllos que contengan datos derivados de actos de violencia de género.


ESP

Nivel suficiente de protección de datos: Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.


PER

Normas PEM (Privacy Enhanced Mail): Correo con Privacidad Mejorada. Norma aplicable al protocolo de correo electrónico utilizado en Internet, que permite cifrar de manera automática los mensajes de correo electrónico antes de enviarlos. No es necesario invocar procedimientos separados para cifrar el mensaje de correo.

Objeto de la Ley de Protección de datos: La LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. ESP

La ley 25.3236 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. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas. ARG

La Ley Federal de Protección de Datos en Posesión de Particulares es de orden público y de observancia general en toda la República de México y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. MEX

La Ley de Protección de Datos Personales tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. PER

La Ley Estatutaria 1581 de 2012 tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. COL

La ley ordena el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. CHL

La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. CTR

Obligación de acceso a la información: La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio.

En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo, bastará con que así se le indique al titular, para tener por cumplida la solicitud. MEX

Sinónimos: *Medios para el cumplimiento del derecho de acceso, Medios para el cumplimiento de derechos ARCO*, *Respuesta del responsable*

Obligación de informar: Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:

- De la existencia de una base de datos de carácter personal.
- De los fines que se persiguen con la recolección de estos datos.
- De los destinatarios de la información, así como de quiénes podrán consultarla.
- Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.
- Del tratamiento que se dará a los datos solicitados.
- De las consecuencias de la negativa a suministrar los datos.
- De la posibilidad de ejercer los derechos que le asisten.
- De la identidad y dirección del responsable de la base de datos.

Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible**.** CTR

Sinónimos: *Deber de informar.*

Obligaciones del responsable: 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, de modo 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. IBE

A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:

- Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- Determinar las funciones y obligaciones de las personas que traten datos personales;
- Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
- Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
- Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
- Llevar a cabo revisiones o auditorías;
- Capacitar al personal que efectúe el tratamiento, y
- Realizar un registro de los medios de almacenamiento de los datos personales.

El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores. MEX

El titular y el encargado del banco de datos personales, según sea el caso, tienen las siguientes obligaciones:

- Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la presente Ley.
- No recopilar datos personales por medios fraudulentos, desleales o ilícitos.
- Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.
- No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.
- Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.
- Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.
- Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.
- Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones, en el marco de un procedimiento administrativo en curso solicitado por la parte afectada.

Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
- Informar a solicitud del Titular sobre el uso dado a sus datos;
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.


COL

Sinónimos: *Acciones para la seguridad de los datos personales.*

Véase también R*esponsable de seguridad, Medidas de seguridad de nivel medio, Medidas de seguridad de nivel alto, Documento de seguridad, Políticas de tratamiento, Protocolo mínimo de actuación, Principio de seguridad de los datos.*

Obtención del consentimiento: El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.


IBE

La voz "obtención del consentimiento" es utilizada por igual en todo Iberoamérica. Sin embargo, legislaciones como la de Costa Rica utilizan "otorgamiento del consentimiento" para referirse a idénticas cuestiones.


CTR

Sinónimos: *Otorgamiento del consentimiento.*

Oficial de Datos Personales: Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley Federal de Datos Personales. Asimismo fomentará la protección de datos personales al interior de la organización.


MEX

Véase también *Departamento de datos personales.*

Oposición al tratamiento de finalidades distintas: El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.

Órgano de control: 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. URU

La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. ESP

El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones, puede crear oficinas en todo el país. PER

La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos la normativa que regula su ejercicio. COL

La Dirección Nacional de Protección de Datos, es la autoridad máxima Argentina de aplicación en materia de protección de datos personales, órgano de control que tiene por objeto realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la Ley de Habeas Data 25.326. ARG

La Agencia de Protección de Datos de los Habitantes es el órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes. Con personalidad jurídica instrumental propia en el desempeño de las funciones, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia gozará de independencia de criterio. CTR

El Instituto Federal de Acceso a la Información y Protección de Datos es la Autoridad de Aplicación en materia de protección de datos de los Estados Unidos Mexicanos, conforme lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento. MEX

La Dirección de Protección de Datos Personales adscrita al Ministerio de Hacienda y Crédito Público, cuenta con un Director designado por la máxima autoridad administrativa de dicho ministerio y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.

NIC

Otorgamiento del acceso: El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

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

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.  ESP

Sinónimos: *Cumplimiento de la solicitud ARCO por el responsable*

Otorgamiento del consentimiento: Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

No será necesario el consentimiento expreso cuando:

- Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.
- Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.
- Los datos deban ser entregados por disposición constitucional o legal.

Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.  CTR

Sinónimos: *Obtención del consentimiento.*

Países con nivel adecuado de protección: Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes: Suiza Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000; Canadá: Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; Argentina: Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003; Guernsey: Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003; Isla de Man: Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004; Jersey: Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008; Islas Feroe: Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010; Andorra: Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010; Israel: Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011; Uruguay: Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012; Nueva Zelanda: Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

Véase también *Nivel adecuado de protección de datos.*

Persona identificable: Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas.


IBE

El concepto de persona identificable se aplicará por extensión a las personas jurídicas en cuanto corresponda.


ARG

BRA

NIC

URU

Petición de Habeas Data: Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros, la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.

La petición de Habeas Data se resolverá en el plazo máximo de cinco días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente, adicionalmente tendrá un plazo de quince días hábiles para proporcionar la información solicitada.

La petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional establecido en el Artículo 23 de la Constitución Política del Estado. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa.


BOL

Esta es la única referencia específica a derechos a la protección de datos e intimidad referidos en el Decreto Supremo 28168 de la República de Bolivia.

Sinónimos: *Derechos ARCO.*

Plazos de conservación de los datos personales: Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo

contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.

Plazo del procedimiento de verificación: El procedimiento de verificación tendrá una duración máxima de ciento ochenta días, este plazo comenzará a contar a partir de la fecha en que el IFAI hubiera dictado el acuerdo de inicio y concluirá con la determinación del mismo, el cual no excederá de ciento ochenta días. El Instituto podrá ampliar por una vez y hasta por un periodo igual este plazo. MEX

Véase también *Procedimiento de verificación, IFAI, Instituto.*

Plazo para dictar resolución en el procedimiento de protección de derechos: El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo. MEX

Los recursos interpuestos deberán ser resueltos, el de Reconsideración por la Agencia dentro de los ocho días hábiles posteriores a su presentación y en caso de haberse interpuesto Recurso de Apelación deberá remitir el mismo y el respectivo expediente al Ministro (a) de Justicia y Paz dentro de los siguientes tres días hábiles, a partir de la notificación de la Resolución del Recurso de Reconsideración. El Ministro de Justicia y Paz, deberá resolver el Recurso de apelación dentro del plazo de ocho días hábiles posteriores al recibo del expediente. CTR

Véase también *Procedimiento de protección de derechos, Acto final.*

Plazo para responder solicitud de derecho de acceso: El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. El derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. ARG

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

El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso. MEX

El plazo máximo para la respuesta ante el ejercicio del derecho de acceso será de veinte días contados desde el día siguiente de la presentación de la solicitud por el titular de datos personales. Si la solicitud fuera estimada y el responsable no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez días siguientes a dicha respuesta. PER

El responsable, deberá evacuar la consulta de información dentro del plazo de cinco días hábiles a partir de la recepción de la solicitud. CTR

Plazo para responder solicitud de derecho ARCO: El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

MEX

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

URU

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

CHL

El responsable, deberá dar trámite a toda solicitud para el ejercicio de los derechos personales del titular. El plazo para que se atienda la solicitud será de cinco días hábiles, contados a partir del día siguiente en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular, la correspondiente fecha de recepción.

El responsable o usuario debe responder a la solicitud de acceso proporcionando la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. La respuesta a la solicitud de rectificación, supresión o actualización de los datos personales del afectado, debe efectivizarse en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

ARG

El responsable deberá contestar la solicitud de derechos ARCO en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros. El responsable resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud y tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

ESP

El plazo máximo para la respuesta ante el ejercicio del derecho de acceso será de veinte días contados desde el día siguiente de la presentación de la solicitud por el titular de datos personales. Si la solicitud fuera estimada y el responsable no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez días siguientes a dicha respuesta.

PER

El responsable, deberá evacuar la consulta de información dentro del plazo de cinco días hábiles a partir de la recepción de la solicitud.

CTR

El titular contará con diez días hábiles para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente. En caso de que la información proporcionada en la solicitud sea insuficiente o errónea para atenderla, el responsable de ficheros de datos podrá requerir al titular, por una vez y dentro de los cinco días hábiles siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma.

NIC

El término máximo para atender la petición o reclamo será de quince días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y

señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.

En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince días hábiles contados a partir del día siguiente a la fecha de presentación de la reclamación, prorrogables por ocho días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga "reclamo en trámite" y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos días hábiles siguientes a haber recibido la información de la fuente. COL

Sinónimos*: Cómputo de plazos para responder derechos ARCO.*

Plazo para responder solicitud de rectificación, actualización o supresión El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data. ARG

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

El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso. MEX

Tratándose del ejercicio de los derechos de rectificación, cancelación u oposición, el plazo máximo de respuesta del titular del banco de datos personales o responsable del tratamiento será de diez (10) días contados desde el día siguiente de la presentación de la solicitud correspondiente. PER

Véase también *Ampliación de plazos.*

Plazo para responder derecho de información: El plazo máximo de respuesta ante el ejercicio del derecho de información será de ocho días contados desde el día siguiente de la presentación de la solicitud correspondiente. PER

Véase también *Derecho de información.*

Políticas de tratamiento de la información: Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
- Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.
- Derechos que le asisten como Titular.
- Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
- Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 5° del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.

Sinónimos: *Documento de seguridad, Protocolo mínimo de actuación.*

Prestador de servicios de tratamiento: persona física o jurídica, distinta de la persona responsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable.

La persona responsable podrá realizar tratamientos de datos de carácter personal a través de uno o varios prestadores de servicios de tratamiento, debiendo para ello: velar porque cada prestador de servicios de tratamiento garantice un nivel de protección adecuado; y articular la relación jurídica a través de un contrato u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido, y que establezca el compromiso del prestador de servicios de tratamiento de cumplir con estas garantías y de asegurar que los datos de carácter personal sean tratados siguiendo las instrucciones de la persona responsable.

Cuando, por cuenta de terceros, se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación.

Una vez ejecutada la prestación materia del contrato o del convenio, según el caso, los datos personales tratados deben ser suprimidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se pueden conservar con las debidas condiciones de seguridad, plazos y garantías legales.

Sinónimos: *Encargado, Encargado del tratamiento.*

Prestación de servicios de tratamiento sin acceso a datos: El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Véase también: *Encargado, Encargado del tratamiento*

Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley. COL

Principio de autodeterminación informativa: Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias. CTR

Véase también A*utodeterminación informativa, Derecho a la protección de datos personales.*

Principio de calidad de los datos: El tratamiento de datos personales será el que resulte necesario, cierto, adecuado, relevante, pertinente y no excesivo en relación con las finalidades previstas y el ámbito para los que se hubieren obtenido.

La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las normas.

Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

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. El responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.

En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable. ARG COL CTR ESP MEX PER

Sinónimos: *Principio de veracidad.*

Principio de confidencialidad: 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 aun después de finalizada su relación con el titular del archivo de datos. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

El principio de reserva y el principio de confidencialidad son sinónimos e instruyen sobre los mismos aspectos. Las legislaciones solo difieren en su denominación. La normativa uruguaya responde al "principio de reserva" cuando el resto de Iberoamérica lo hace al "principio de confidencialidad".

Sinónimos: P*rincipio de reserva*

Véase también *Secreto profesional.*

Principio de consentimiento: El responsable deberá obtener el consentimiento para el tratamiento de los datos personales, a menos que no se trate de excepciones al consentimiento.

Véase también *Consentimiento, Excepciones al consentimiento, Responsable*.

Principio de disposición de recurso: Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Principio de finalidad: El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del responsable. El responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

Principio de información: El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales. El responsable deberá habilitar procedimientos sencillos, ágiles y eficaces que permitan a los interesados revocar su consentimiento en cualquier momento, y que no impliquen demoras o costes indebidos, ni ingreso alguno para la persona responsable.

Principio de lealtad: El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por las leyes de protección de datos.

No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales.

Principio de legalidad: (1) Es sinónimo del principio de licitud. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas. Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por las leyes de protección de datos y demás normativa aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos

personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por las leyes de protección de datos.  IBE

Sinónimos: *Principio de licitud.*

(2) La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.  URU

Principio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.  COL

Principio de licitud: El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación de protección de datos y el derecho internacional.  MEX

Sinónimos: *Legalidad.*

Principio de nivel de protección adecuado: Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley de Protección de Datos o por los estándares internacionales en la materia.  PER

Si bien este principio no se encuentra expresamente recogido como tal en otras legislaciones como si lo está en la regulación peruana en la materia, todas las normas de protección de datos personales de Iberoamérica lo receptan, permitiendo la transferencia internacional de datos a aquellos países que cuenten con nivel adecuado.  IBE

Véase también *Flujo transfronterizo de datos personales, Transferencia internacional de datos, Nivel adecuado de protección de datos.*

Principio de proporcionalidad: El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas para su recogida. En particular, el responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.  MEX  PER

Sinónimos: *Principio de calidad.*

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, cuando hayan sido recogidos de fuentes no accesibles al público. Esta obligación subsistirá aún después de finalizada la relación con el responsable de la base de datos.  URU

El principio de reserva y el principio de confidencialidad son sinónimos e instruyen sobre los mismos aspectos. Las legislaciones solo difieren en su denominación. La normativa uruguaya

responde a la voz "principio de reserva" y el resto de legislación iberoamericana a la voz "principio de confidencialidad".  IBE

Sinónimos: *Principio de confidencialidad*

Véase también *Secreto profesional.*

Principio de responsabilidad: El responsable deberá adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en la legislación nacional aplicable, y dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias. El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado.

Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación, códigos tipo, o cualquier otro mecanismo que determine adecuado para tales fines.  MEX  URU

Sinónimos: Principio de seguridad de los datos, Seguridad de los datos.

Véase también *Esquemas de autorregulación, Códigos tipo, Responsable.*

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.

 ARG  COL  ESP  PER  URU

Sinónimos: *Principio de responsabilidad, Seguridad de los datos.*

Principio de Transparencia: El responsable debe contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere. Debe facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos ARCO, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

Principio de veracidad: es sinónimo del principio de calidad de los datos. El tratamiento de datos personales será el que resulte necesario, cierto, adecuado, relevante, pertinente y no excesivo en relación con las finalidades previstas y el ámbito para los que se hubieren obtenido.

La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las normas.

Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

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.

En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.  COL  URU

Sinónimos: *Principio de calidad de los datos.*

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 consentimiento deberá figurar en forma expresa y destacada, previa notificación al requerido de datos de las condiciones a las que quedará sujeto el tratamiento de sus datos personales. No será necesario el previo consentimiento cuando:

- Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
- 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.
- Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.
- Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

 URU

Principio general de legitimación: Como regla general, los datos de carácter personal sólo podrán ser tratados cuando concurra alguno de los siguientes supuestos:

- Previa obtención del consentimiento libre, inequívoco e informado del interesado.
- Cuando un interés legítimo de la persona responsable justifique el tratamiento, siempre y cuando no prevalezcan los intereses legítimos, derechos o libertades de los interesados;
- Cuando el tratamiento sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el interesado;
- Cuando el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable, o sea llevado a cabo por una Administración Pública que así lo precise para el legítimo ejercicio de sus competencias;
- Cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona**.**

Procedimiento Administrativo de Protección de Derechos: Se trata de un procedimiento ante el Órgano de Control, de carácter administrativo, para que los titulares de datos puedan reclamar frente a lo que consideran un incumplimiento de alguno de sus derechos ARCO o de lo previsto en las leyes de protección de datos personales, por parte del responsable de las bases de datos. De resolverse favorablemente la petición del titular, el Órgano de Control podrá aplicar diversas sanciones

En España este procedimiento responde a la voz "Procedimiento de Tutela de Derechos" y, en México y Costa Rica a "Procedimiento de Protección de Derechos". En Perú se denomina "Procedimiento trilateral de tutela". En Costa Rica se lo conoce con la voz "Garantías Efectivas".

Sinónimos: *Procedimiento de tutela de derechos, Procedimiento de protección de derechos, denuncia de protección de datos ante el órgano de control, Procedimiento trilateral de tutela, Garantías efectivas.*

Véase también Órgano de control, Sanciones.

Procedimiento ante negativa en el cese de tratamiento: En caso de negativa por parte del responsable al cese en el tratamiento ante la revocación del consentimiento, el titular podrá presentar denuncia ante el Órgano de control correspondiente.

Procedimiento de autorización de transferencia internacional: El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros con nivel de protección no adecuado, se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

- La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción.
- La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
- La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

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

Cuando el Director de la Autoridad de Aplicación resuelva autorizar la transferencia internacional de datos, se dará traslado a quien corresponda a fin de proceder a su inscripción.

El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en el Órgano de Control de la solicitud. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Procedimiento de derechos ARCO: Salvo cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones por servicios prestados o productos y por este medio permita al afectado ejercer sus derechos ARCO, el ejercicio de estos derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá: Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente; Petición en que se concreta la solicitud; Dirección a efectos de notificaciones, fecha y firma del solicitante; Documentos acreditativos de la petición que formula, en su caso.

El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta, debiendo conservar la acreditación del cumplimiento del mencionado deber.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

Procedimiento de desasociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

Sinónimos: *Disosiación de datos*

Véase también *Dato disociado.*

Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

Sinónimos: *Disosiación de datos, Desasociación de datos.*

Véase también *Dato disociado.*

Procedimiento de fiscalización: Tiene por objeto determinar si concurren las circunstancias que justifiquen la iniciación del procedimiento sancionador, con identificación del titular del banco de datos personales o del responsable del tratamiento y la presunta comisión de actos contrarios a la normativa en protección de datos.

El procedimiento de fiscalización se inicia siempre de oficio como consecuencia de:

- Iniciativa directa de la Dirección de Supervisión y Control o del Director General de Protección de Datos Personales.
- Por denuncia de cualquier entidad pública, persona natural o jurídica.

En ambos casos, se requerirá al responsable información relativa al tratamiento de datos personales o la documentación necesaria. Para ello, podrán hacerse visitas de fiscalización.

Sinónimos: *Procedimiento de inspección, Procedimiento de verificación.*

Procedimiento de Habeas Data:

Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y cuando los archivos de datos se encuentren interconectados en redes inter jurisdiccionales, nacionales o internacionales.

Admitida la acción el juez requerirá al responsable la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

El responsable no podrá alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

Cuando se oponga a la remisión del informe invocando haber respondido el pedido de derechos ARCO, deberá acreditarlo.

Al contestar el informe, el responsable deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado. Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda y ofrecer la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días, pasado lo cual, se dictará sentencia.

El procedimiento se sujetará a las reglas siguientes:

La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere el párrafo anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.  CHL

Las acciones que se promuevan por violación a los derechos contemplados en la Ley 18.331 se regirán por las siguientes estipulaciones:

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.

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. Efectuado todo ello, se dictará sentencia.

En el proceso de habeas data sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente.

En los procesos de habeas data no podrán deducirse cuestiones previas, reconvenciones 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.  URU

La acción de Hábeas Data será de competencia de los Tribunales Superiores que conocen de la acción de Amparo de Garantías Constitucionales, cuando el funcionario titular o responsable de registro, archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial. Cuando el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias o en toda la República, será de competencia del Pleno de la Corte Suprema de Justicia.

La acción de Hábeas Data se tramitará mediante procedimiento sumario sin formalidades, sin necesidad de abogado, y en lo que respecta a la sustanciación, impedimentos, notificaciones y apelaciones, se aplicarán las normas que para estas materias se regulan en el ejercicio de la acción de Amparo de Garantías Constitucionales.  PAN

Véase también*: Sentencia de habeas data, Legitimados en la acción de habeas data.*

Procedimiento de Inspección: La DNPD, con el objeto de comprobar el cumplimiento por los Responsables de la Ley de Protección de Datos, podrá realizar inspecciones, requiriendo

al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas. La inspección puede iniciarse de oficio o a petición de parte. Cualquier persona podrá denunciar ante la DNPD las presuntas violaciones a las disposiciones previstas en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos.

Para llevar a cabo la inspección, la DNPD tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive. La DNPD está obligada guardar confidencialidad sobre la información que conozca derivada de la inspección correspondiente.


ARG

Sinónimos: *Procedimiento de fiscalización, Procedimiento de verificación.*

Véase también *DNPD, Dirección Nacional de Protección de Datos, Inspección*.

Procedimiento de protección de derechos: procederá cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:

- El titular no haya recibido respuesta por parte del responsable;
- El responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
- El responsable se niegue a efectuar las rectificaciones a los datos personales;
- El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
- El responsable se niegue a cancelar los datos personales;
- El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición, y
- Por otras causas que a juicio del órgano de control sean procedentes conforme a la Ley de Protección de Datos o a su Reglamento.


CTR

MEX

El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable. En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.

La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de la misma al responsable, para que, en el plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del responsable las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación. Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.

El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.

Las resoluciones del Instituto podrán: Sobreseer o desechar la solicitud de protección de datos por improcedente, o Confirmar, revocar o modificar la respuesta del responsable.

El Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante la Prodhab, que una base de datos pública o privada actúa en contravención de los principios básicos para la protección de los datos y la autodeterminación informativa.

Recibida la denuncia, se conferirá al responsable de la base de datos un plazo de tres días hábiles para que se pronuncie acerca de la veracidad de tales cargos. La persona denunciada deberá remitir los medios de prueba que respalden sus afirmaciones junto con un informe, q ue se considerará dado bajo juramento. La omisión de rendir el informe en el plazo estipulad o hará que se tengan por ciertos los hechos acusados.

A más tardar un mes después de la presentación de la denuncia, la Prodhab deberá dictar el acto final. Contra su decisión cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

Sinónimos: *Procedimiento de tutela de derechos, Procedimiento trilateral de tutela, Procedimiento administrativo de protección de derechos.*

Véase también *Derechos ARCO, IFAI, Instituto, Acuerdo de conciliación, conciliación, medios de impugnación de resoluciones administrativas, Juicio de nulidad, PRODHAB, Acto final, Garantías efectivas.*

Procedimiento de tutela de derechos: Procedimiento administrativo, iniciado a instancia del afectado o afectados y con posterioridad a la solicitud de derechos ARCO de que se trate, donde expresa con claridad el contenido de su reclamación y los preceptos de la LOPD que consideran vulnerados.

Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo. ESP

Sinónimos: *Procedimiento de protección de derechos, Procedimiento trilateral de tutela, Procedimiento administrativo de protección de derechos.*

Procedimiento de tutela directa: El ejercicio de los derechos ARCO se inicia con la solicitud que el titular de los datos personales debe dirigir directamente al titular del banco de datos personales o responsable del tratamiento. La denegatoria o la respuesta insatisfactoria habilitan al solicitante a iniciar el procedimiento administrativo ante la Dirección General de Protección de Datos Per PER

sonales.

Sinónimos: *Ejercicio de derechos ARCO.*

Procedimiento de Verificación: El IFAI, con el objeto de comprobar el cumplimiento por los Responsables de la Ley de Protección de Datos, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas. El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del Instituto. Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el IFAI, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.

En el procedimiento de verificación el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive. El IFAI está obligado a guardar confidencialidad sobre la información que conozca derivada de la verificación correspondiente. MEX

La Agencia podrá verificar, en cualquier momento, que la base de datos esté cumpliendo con los términos establecidos en el protocolo mínimo de actuación. CTR

Véase también *Instituto, IFAI*.

Procedimientos para conservación, bloqueo y supresión de los datos personales: El responsable establecerá y documentará procedimientos para la conservación y, en su caso,

bloqueo y supresión de los datos personales, que incluyan los periodos de conservación de los mismos.

Procedimiento sancionador: Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

- Identificación de la persona o personas presuntamente responsables.
- Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
- Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.
- Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.
- Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.
- Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.
- Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.  ESP

El procedimiento de imposición de sanciones dará comienzo con la notificación al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento y le otorgará un término de quince días para que rinda pruebas y manifieste por escrito lo que a su derecho convenga. En caso de no rendirlas, el Instituto resolverá conforme a los elementos de convicción de que disponga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del presunto infractor las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación.

El Instituto, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, resolverá en definitiva dentro de los cincuenta días siguientes a la fecha en que inició el procedimiento sancionador. Dicha resolución deberá ser notificada a las partes. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.  MEX

El procedimiento sancionador será promovido siempre de oficio, en atención a un informe de la Dirección de Supervisión y Control que puede obedecer a una denuncia de parte o a decisión motivada del Director General de Protección de Datos Personales.

La Dirección de Sanciones puede, mediante resolución expresa y motivada, decidir el archivamiento de los casos que no ameriten el inicio del procedimiento sancionador, no obstante el informe de la Dirección de Supervisión y Control. Contra esta decisión puede recurrir el denunciante.

Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento. La Dirección de Sanciones notificará a las partes la resolución de inicio del procedimiento, que entre otros, contendrá el plazo para presentar los descargos y pruebas. El administrado en un plazo máximo de quince días, contado a partir del día siguiente de la notificación citada, presentará su descargo, argumentos por medio de los cuales desvirtúe la infracción que se presuma y las pruebas correspondientes. En caso se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que versarán y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos requisitos dichas pruebas se tendrán por no ofrecidas.

Vencido el plazo para la presentación del descargo, se realizarán de oficio todas las actuaciones necesarias para el examen de los hechos y podrá disponer una visita de fiscalización, si no se hubiere hecho antes.

Concluidas las actuaciones instructivas, la Dirección de Sanciones emitirá resolución cerrando la etapa instructiva dentro de los cincuenta días contados desde el inicio del procedimiento. Dentro de los veinte días posteriores a la notificación de cierre de instrucción deberá resolverse en primera instancia. Cuando haya causa justificada, la Dirección de Sanciones podrá ampliar por una vez y hasta por un período igual, el plazo de cincuenta días.

La resolución que resuelve el procedimiento sancionador será notificada a todas las partes intervinientes en el procedimiento.  PER

De oficio a instancia de parte, la Prodhab podrá iniciar un procedimiento tendiente a demostrar si una base de datos regulada por esta ley está siendo empleada de conformidad con sus principios; para ello, deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido  CTR

El procedimiento se ajustará a las siguientes disposiciones:

La DNPD iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Nº 25.326 y sus normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios.

Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de cinco días hábiles, presente por escrito su descargo y ofrezca las pruebas que hacen a su derecho.

Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Concluidas las diligencias sumariales, se dictará la resolución definitiva dentro del término de veinte días hábiles.  ARG

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: Apercibimiento, Multa de hasta quinientas mil unidades indexadas, Suspensión de la base de datos respectiva.

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.

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. URU

La Dirección de Protección de Datos Personales iniciará el procedimiento de imposición de sanciones cuando determine presuntas infracciones a la Ley y a las regulaciones que de ella se deriven, susceptibles de ser pasibles de la aplicación de sanciones.

El procedimiento iniciará con la notificación que se haga al presunto infractor. La notificación irá acompañada de un informe que describa los hechos constitutivos de la presunta infracción, emplazando al presunto infractor para que en un término de quince días hábiles, contados a partir de la notificación, manifieste lo que tenga a bien y rinda las pruebas que estime convenientes.

Una vez presentadas las pruebas por el presunto infractor, el órgano de control deberá resolver si las admite o rechaza, y se procederá a su evacuación. Evacuadas, en su caso, las pruebas, se notificará al presunto infractor que cuenta con cinco días hábiles para presentar alegatos, contados a partir del día siguiente de que surta efectos la notificación. Al término de dicho plazo se cerrará la instrucción y la resolución deberá emitirse en un plazo no mayor de cincuenta días hábiles, siguientes a los que inició el procedimiento. Cuando haya causa justificada, la Dirección podrá ampliar por una vez y hasta por un período igual el plazo de cincuenta días al que refiere el párrafo anterior. NIC

La Superintendencia de Industria y Comercio y la Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones:

Multas de carácter personal e institucional hasta por el equivalente a mil quinientos (1.500) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, por violación a la presente ley, normas que la reglamenten, así como por la inobservancia de las órdenes e instrucciones impartidas por dicha Superintendencia. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Suspensión de las actividades del banco de datos, hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de las condiciones y requisitos previstos en la presente ley, así como por la inobservancia de las órdenes e instrucciones impartidas por las Superintendencias mencionadas para corregir tales violaciones.

Cierre o clausura de operaciones del banco de datos cuando, una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión. Cierre inmediato y definitivo de la operación de bancos de datos que administren datos prohibidos. COL

Procedimiento trilateral de tutela: El procedimiento administrativo de tutela de Derecho se sujeta a lo dispuesto por los artículos 219 al 228 de la Ley Nº 27444, Ley del Procedimiento Administrativo General en lo que le sea aplicable, y será resuelto mediante resolución del Director General de Protección de Datos Personales. Contra esta resolución solo procede recurso de reconsideración, el que, una vez resuelto, agota la vía administrativa.

Para iniciar el procedimiento, sin perjuicio de los requisitos generales, el titular de los datos personales deberá presentar con su solicitud de tutela:

1. El cargo de la solicitud que previamente envió al titular del banco de datos personales o responsable del tratamiento para obtener de él, directamente, la tutela de sus derechos.

2. El documento que contenga la respuesta del titular del banco de datos personales o responsable del tratamiento que, a su vez, contenga la denegatoria de su pedido o la respuesta que considere no satisfactoria, de haberla recibido.

El plazo máximo en que debe resolverse la solicitud de tutela de derechos será treinta (30) días, contado desde el día siguiente de recibida la contestación del reclamado o desde el vencimiento del plazo para formularla y podrá ampliarse hasta por un máximo de treinta (30) días adicionales, atendiendo a la complejidad del caso.  PER

Sinónimos: *Procedimiento de protección de derechos, Procedimiento de tutela de derechos*.

PRODHAB: Agencia de Protección de Datos de los Habitantes, órgano de control de protección de datos personales de Costa Rica.  CTR

Sinónimos: *Agencia de Protección de Datos de los Habitantes.*

Protocolo de actuación: Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.

Para que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.

La manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, "iuris tantum", el cumplimiento de las disposiciones contenidas en esta ley, para los efectos de autorizar la cesión de los datos contenidos en una base.  CTR

Sinónimos: *Registro, Inscripción registral*.

Protocolo mínimo de actuación: El responsable establecerá y documentará procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de los datos personales, en el sitio o en la nube, con base en los protocolos mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales. Además deberá el responsable de la base de datos velar por la aplicación del principio de calidad de la información. Los responsables deberán confeccionar un protocolo mínimo de actuación, el cual deberá ser transmitido al encargado para su fiel cumplimiento y donde al menos, se deberá especificar lo siguiente:

- Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable;
- Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;
- Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad;
- Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento.
- Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento.
- Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos.

Sinónimos: *Documento de seguridad, Políticas de tratamiento.*

Prueba de la autorización: Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

Sinónimos: *Prueba del consentimiento*.

Prueba de la obtención del consentimiento: Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.

Sinónimos: *Prueba de la autorización.*

Prueba del aviso de privacidad: Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.

Publicidad de las resoluciones del Órgano de control: Todas las resoluciones serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.

Véase también *Órgano de control.*

Puerto Seguro: (safe harbor). En EEUU no hay ninguna legislación que garantice niveles de protección de datos similares a los exigidos por la Unión Europea, por lo tanto el Departamento de Comercio de los Estados Unidos en colaboración con la Comisión Europea ha puesto en marcha el programa puerto seguro, que permite a las empresas estadounidenses certificarse como organizaciones que cumplen con los altos requisitos de seguridad exigidos por las instituciones europeas. De esta manera empresas americanas como Google se pueden adherir al programa voluntariamente y ofrecer sus servicios en la Unión Europea. Este acuerdo está en vigor desde el año 2000. El Acuerdo de "Puerto Seguro" consta de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). La lista de entidades estadounidenses adheridas a los principios de Puerto Seguro está Disponible en http://www.export.gov/safeharbor.

Receptor de los datos personales: El receptor de los datos personales en el marco de una transferencia de datos, asumirá la calidad de responsable de las bases de datos que se le hubieren conferido, debiendo cumplir los preceptos de la Ley de protección de datos como hubiere establecido el responsable transferente.

Reclamos: El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos días hábiles e informará de la situación al interesado.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.


COL

Sinónimos: *Ejercicio de derechos ARCO.*

Recurso contra resolución administrativa de protección de datos: Contra las resoluciones que resuelven cuestiones relativas a las violaciones a los preceptos de las leyes de protección de datos o a los procedimientos de acceso, rectificación, cancelación y oposición, emitidas por los órganos de control, se agota la vía administrativa, quedando abierta la vía recursiva judicial.


ARG COL CTR ESP MEX PER URU

Sinónimos: *Medios de impugnación de decisiones del órgano de control.*

Véase también *Juicio de nulidad, Órgano de control, Procedimiento de protección de derechos, Resolución del procedimiento de protección de derechos, Acción de protección de datos personales, Procedimiento administrativo de protección de datos, Acción de habeas data.*

Registración de Bases de Datos: Todo archivo, registro, base o banco de datos que contenga datos de carácter personal, debe inscribirse en el Registro que al efecto habilite el

organismo de control, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos.

Están obligados a notificar la creación, modificación o supresión de bases de datos al Registro que corresponda, aquellas personas físicas o jurídicas, de naturaleza pública o privada, titulares de bases de datos que contengan datos de carácter personal.

La inscripción de un fichero deberá mantenerse actualizada. Cualquier modificación que afecte al contenido de la inscripción deberá ser previamente notificada al Registro, a fin de proceder a su inscripción en el registro correspondiente. Asimismo, cuando el responsable de una base de datos decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el Registro.

La falta de declaración de las bases de datos personales al Registro correspondiente, puede dejar al responsable incurso en falta leve o grave a la Ley de Protección de Datos.

Los términos *"registración de bases de datos", "declaración de ficheros", "inscripción de bases de datos", "inscripción de ficheros"* son sinónimos.

Sinónimos: *Declaración de ficheros, Inscripción registral.*

Registro: En materia de protección de datos, existen dos acepciones.

(1) Registro, referido al conjunto ordenado de datos personales referentes a una persona identificada o identificable. Son sinónimos de registro los términos banco, archivo, o base de datos.

(2) Registro, referido al Organismo de Control encargado de velar por el cumplimiento del deber de inscribir y declarar bases de datos que contengan datos de carácter personal por parte de los titulares de las mismas, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos.

Registro de accesos: dentro de las medidas de seguridad de nivel alto, se establece que de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. El período mínimo de conservación de los datos registrados será de dos años. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

No será necesario este registro de accesos en caso de que concurran las siguientes circunstancias:

- Que el responsable del fichero o del tratamiento sea una persona física.

- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad. ESP

Registro de Bases de Datos Personales: Es el órgano de control a cargo de la Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay al que corresponde velar por el cumplimiento del deber de inscripción de bases de datos a cargo delas personas físicas o jurídicas, públicas o privadas, comprendidas en lo dispuesto en el artículo 22 de la Ley No. 18.331 de 11 de agosto de 2008, quienes deberán inscribirse en el Registro directamente o por intermedio de sus representantes, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos.

Véase también *Unidad Reguladora y de Control de Datos Personales, Registro.* URU

Registro de Incidencias: Dentro de las medidas de seguridad de nivel básico, se establece que deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecerse un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Si las medidas a implementar corresponden a datos de nivel medio, en el registro deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos. ESP

Registro de solicitudes ARCO: El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción. El plazo señalado se interrumpirá en caso de que el responsable requiera información al titular.

Véase también *Solicitud de derechos ARCO, Plazo para responder solicitud de derecho ARCO.*

Registro General de Protección de Datos: Es el órgano de la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 14 a 17 de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ante éste Registro los responsables de ficheros deben notificar el tratamiento de datos personales, mediante el sistema NOTA. ESP

Véase también *AEPD, Agencia Española de Protección de Datos, Registro.*

Registro Nacional de Bases de Datos: Es el Organismo de Control encargado de velar por el cumplimiento del deber de inscribir y declarar bases de datos que contengan datos de carácter personal de la República Argentina, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos, conforme lo dispuesto en los artículos 3 y 21 de la Ley 25.326. El Registro Nacional de Bases de Datos funciona en el ámbito de la Dirección Nacional de Protección de Datos Personales. ARG

El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. Es administrado por la Superintendencia de Industria y Comercio y es de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. COL

Véase también *DNPD, Dirección Nacional de Datos Personales, Registro.*

Registro Nacional de Protección de Datos Personales: Registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales. El ejercicio de esta función no posibilita el conocimiento del contenido de los bancos de datos personales por parte de la Autoridad Nacional de Protección de Datos Personales, salvo procedimiento administrativo en curso. Asimismo, registrará las autorizaciones, sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales, los códigos de conducta, y otros actos materia de inscripción conforme al reglamento de protección de datos personales. PER

Reglamento: Normativa de desarrollo de la Ley de Protección de datos personales. Tiene por objeto reglamentar las disposiciones de la Ley de Protección de Datos Personales en Posesión de los Particulares.

Relación entre el responsable y el encargado: La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.

Sinónimo: *Contrato de transmisión de datos.*

Remisión: La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano. Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento.

El encargado, será considerado responsable con las obligaciones propias de éste, cuando:

- Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o
- Efectúe una transferencia, incumpliendo las instrucciones del responsable.

El encargado no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable conforme a lo previsto en la normativa. MEX

Véase también *Encargado del tratamiento, acceso a datos por cuenta de terceros.*

Requisitos de solicitud para el ejercicio de derechos ARCO: La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:

- El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
- Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales.

Véase también *Ejercicio de derechos ARCO, Medios para el ejercicio de derechos ARCO.*

Requisitos del consentimiento: La obtención del consentimiento deberá ser:

- Libre: no debe mediar error, mala fe, violencia física o psicológica o dolo, que puedan afectar la manifestación de voluntad del titular;
- Específico: referido a una o varias finalidades determinadas y definidas que justifiquen el tratamiento;
- Informado: que el titular tenga conocimiento previo al tratamiento, a qué serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento. Asimismo, de saber quién es el responsable que interviene en el tratamiento de sus datos personales, y su lugar o medio de contacto;
- Expreso: debe ser escrito e inequívoco, de forma tal que pueda demostrarse de manera indubitable su otorgamiento.
- Individualizado: debe existir mínimo un otorgamiento del consentimiento por parte de cada titular de los datos personales. CTR

Sinónimos: *Características del consentimiento.*

Resolución de Inscripción: La inscripción del registro de una base de datos o fichero ante el órgano de control, no exime al responsable al cumplimiento y seguimiento del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

Sinónimos: *Inscripción registral.*

Resolución del procedimiento administrativo de protección de derechos: Las resoluciones podrán sobreseer o desechar la solicitud de protección de datos por improcedente, o, confirmar, revocar o modificar la respuesta del responsable, e imponer sanciones.

Véase también *Sanciones, Procedimiento administrativo de protección de datos, Procedimiento de tutela de derechos, Procedimiento trilateral de protección de datos.*

Resolución del procedimiento de verificación: Concluirá con la resolución que emita el órgano de control, en la cual, en su caso, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma establezca. La resolución podrá instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para su inicio. Esta resolución será notificada al verificado y al denunciante. CTR MEX

Responsable: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, titular de bases de datos, que decide sobre el tratamiento de datos personales.

Sinónimos: *Responsable de archivo, fichero, registro, base o banco de datos, Responsable del fichero o del tratamiento*

Véase también *Responsable de Seguridad.*

Responsable de archivo, fichero, 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.

Sinónimos: *Responsable; Responsable del fichero o del tratamiento.*

Responsable de seguridad: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponda al responsable del fichero o al encargado del tratamiento.

Véase también *Obligaciones del responsable, Medidas de seguridad de nivel medio, Seguridad de los datos.*

Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Sinónimos: *Responsable de archivo, fichero, registro, base o banco de datos; Responsable.*

Respuesta del Responsable: En todos los casos, el responsable deberá dar respuesta a las solicitudes que reciba del titular, con independencia de que figuren o no datos personales de éste en sus bases de datos.

La respuesta del responsable al titular, deberá referirse sobre la totalidad del registro perteneciente al titular, aún cuando el requerimiento solo comprenda un aspecto de los datos personales, y deberá presentarse en un formato legible, comprensible y de fácil acceso. En caso de uso de códigos, siglas o claves se deberán proporcionar los significados correspondientes.

Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aún cuando se vinculen con el titular solicitante. CTR

Sinónimos: *Medios para el cumplimiento de derechos ARCO, Obligación de acceso a la información.*

Véase también *Declaración de ficheros.*

Revocación del consentimiento: En cualquier momento, el titular podrá revocar su consentimiento para el tratamiento de sus datos personales, para lo cual el responsable deberá establecer mecanismos sencillos y gratuitos, que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.

En caso de que los datos personales hubiesen sido remitidos con anterioridad a la fecha de revocación del consentimiento y sigan siendo tratados por encargados, el responsable deberá hacer de su conocimiento dicha revocación, para que procedan a efectuar lo conducente.

Sinónimos: *Revocatoria de la autorización*

Revocatoria de la autorización: El responsable de la base de datos, ante la presentación de la solicitud de revocación del consentimiento, contará con un plazo de cinco días hábiles a partir del recibido de la misma, para proceder conforme a la revocación. Asimismo, dentro del mismo plazo de cinco días hábiles, deberá informarles de dicha revocación a aquellas personas físicas o jurídicas a quienes haya transferido los datos, mismas que deberán proceder en un plazo de cinco días hábiles a partir de la notificación a ejecutar la revocación del consentimiento.

La revocación del consentimiento no tendrá efecto retroactivo.  CTR

El responsable de la base de datos, ante la presentación de la solicitud de revocación del consentimiento, contará con un plazo de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.  COL

Sinónimos: *Revocación del consentimiento.*

Sanciones: La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

La Ley 25.326 de Habeas Data de Argentina, divide entre sanciones administrativas y penales, sin perjuicio de la responsabilidad por daños y perjuicios derivados que le cupieran al responsable y encargados ante la inobservancia de la Ley.

Sanciones administrativas: La DNPD podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos argentinos a cien mil pesos argentinos, clausura o cancelación del archivo, registro o banco de datos.

Sanciones penales: (Art. 117 bis del Código Penal) 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. 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. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 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.

(Art. 157 bis del Código Penal) 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 otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.3. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

Se considerará reincidente a quien habiendo sido sancionado por una infracción a la Ley Nº 25.326 o sus reglamentaciones incurriera en otra de similar naturaleza dentro del término de tres años, a contar desde la aplicación de la sanción.


ARG

La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- Multas de carácter personal e institucional hasta por el equivalente de dos mil salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
- Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;


COL

Constituyen infracciones a Ley de Protección de Datos Personales de México, las siguientes conductas llevadas a cabo por el responsable:

- No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;
- Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;
- Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;
- Dar tratamiento a los datos personales en contravención a los principios establecidos en la Ley;
- Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la Ley;
- Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;
- No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;
- Incumplir el deber de confidencialidad;
- Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;
- Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;
- Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
- Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
- Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;
- Obstruir los actos de verificación de la autoridad;
- Recabar datos en forma engañosa y fraudulenta;
- Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;
- Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;
- Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y
- Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Las infracciones a la presente Ley serán sancionadas por el Instituto con:

- Apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular.
- Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal;
- Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y
- En caso de que de manera reiterada persistan las infracciones, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. Tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.
- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
- Tratándose de datos personales sensibles, las penas de prisión citadas se duplicarán.

MEX

Constituyen infracciones a Ley de Protección de Datos Personales de Uruguay, aplicables a responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, la violación a cualquiera de las normas establecidas en la Ley 18.331, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida:

- Observación.
- Apercibimiento.
- Multa de hasta 500.000 UI (quinientas mil unidades indexadas).
- Suspensión de la base de datos respectiva por el plazo de cinco días.
- Clausura de la base de datos respectiva.

URU

Las infracciones a la Ley Orgánica de Protección de Datos 15/1999 (LOPD) se gradúan en sanciones leves, graves y muy graves. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

- El carácter continuado de la infracción.
- El volumen de los tratamientos efectuados.
- La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
- El volumen de negocio o actividad del infractor.
- Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- El grado de intencionalidad.
- La reincidencia por comisión de infracciones de la misma naturaleza.
- La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
- La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Las infracciones leves serán de apercibimiento o multa. Para infracciones leves, se aplicara multa entre 601,01 a 40.000 euros. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

ESP

En caso de violación de las normas de la Ley de Protección de Datos 29.733 o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:

- Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).

- Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
- Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

En ningún caso, la multa impuesta puede exceder del diez por ciento de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior. La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.

La imposición de la multa se efectúa sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar.

La Autoridad Nacional de Protección de Datos Personales puede imponer multas coercitivas por un monto que no supere las diez unidades impositivas tributarias (UIT), frente al incumplimiento de las obligaciones accesorias a la sanción, impuestas en el procedimiento sancionador. Las multas coercitivas se imponen una vez vencido el plazo de cumplimiento. La imposición de las multas coercitivas no impide el ejercicio de otro medio de ejecución forzosa, conforme a lo dispuesto en el artículo 196 de la Ley 27444, Ley del Procedimiento Administrativo General.

Si se ha incurrido en alguna de las faltas tipificadas en la Ley Nº 8968, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:

- Para las faltas leves, una multa hasta de cinco salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.
- Para las faltas graves, una multa de cinco a veinte salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.
- Para las faltas gravísimas, una multa de quince a treinta salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República, y la suspensión para el funcionamiento del fichero de uno a seis meses.

Sin perjuicio de las responsabilidades administrativas de los responsables o usuarios de los ficheros de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente Ley, y de las sanciones penales, a la Dirección de Protección de Datos Personales corresponde aplicar las sanciones administrativas de:

a. Apercibimiento;
b. Suspensión de operaciones relacionadas con el tratamiento de los datos personales; y
c. Clausura o cancelación de los ficheros de datos personales de manera temporal o definitiva.

En el caso de infracciones leves a la Ley 787, se aplicará al infractor, dependiendo de las circunstancias del caso, del daño causado y de las condiciones del propio infractor, la sanción que corresponda conforme a los literales a) y b). En el caso de infracciones graves,

se impondrá al infractor dependiendo de las circunstancias del caso, del daño causado y de las condiciones del propio infractor, la sanción que corresponda conforme al literal c).

Véase también *Atenuación de sanciones*

Secreto profesional: Los responsables del tratamiento de datos personales, así como las personas que, en el ejercicio de sus funciones, tengan conocimiento de los datos personales tratados, están obligados al secreto profesional, incluso después de la terminación de sus funciones.

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

Véase también *Principio de seguridad de los datos, Responsable de seguridad, Obligaciones del responsable, Medidas de seguridad de nivel medio.*

Sentencia habeas data: Vencido el plazo para la contestación del informe o contestado el mismo, o luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.

En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.

La sentencia que haga lugar al habeas data deberá contener:

- 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.
- 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.
- 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.

Véase también *Acción de habeas data.*

Servicios de atención al público: Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no

contravengan los establecidos en el artículo 32 de la Ley. En tal caso, la identidad del titular se considerará acreditada por los medios establecidos por el responsable para la identificación de los titulares en la prestación de sus servicios o contratación de sus productos, siempre que a través de dichos medios se garantice la identidad del titular.

Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Sobreseimiento: La solicitud de protección de datos será sobreseída cuando: el titular fallezca; el titular se desista de manera expresa; admitida la solicitud de protección de datos, sobrevenga una causal de improcedencia; y por cualquier motivo quede sin materia la misma.

Solicitud de derechos ARCO: La solicitud de derechos ARCO no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Se puede efectuar de manera directa, presentándose el interesado ante el responsable o de manera indirecta, a través de la intimación fehaciente por medio escrito que deje constancia de recepción. También pueden ser utilizados otros servicios de acceso directo o semidirecto como los medios electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin. En cada supuesto, se podrán ofrecer preferencias de medios para conocer la respuesta requerida.

En el caso de datos de personas fallecidas, deberá acreditarse el vínculo mediante la declaratoria de herederos correspondiente, o por documento fehaciente que verifique el carácter de sucesor universal del interesado.

Vencido el plazo para contestar, el interesado podrá denunciar el hecho ante el órgano de control.

La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:

- El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
- Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales.

Véase también *Ejercicio de derechos ARCO, Medios para el ejercicio de derechos ARCO, Requisitos de solicitud de acceso.*

Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Soporte electrónico: Medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales.

Soporte físico: Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales.

Subcontratación de servicios: Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.

Véase también *Subcontratista, Encargado, Encargado del tratamiento.*

Subcontratista: Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.


POR

Sinónimos: Encargado de tratamiento, Encargado.

Súper usuario: Perfil de ingreso que cuenta con acceso para consultar la base de datos, de forma inmediata, actualizada y sin restricción alguna.

Supresión: Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable.

Suspensión de transferencias internacionales: En el supuesto de transferencia de datos a terceros países con nivel no adecuado, el Director de la AEPD podrá denegar o suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

- Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
- Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
- Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
- Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
- Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

En tales supuestos, el Director podrá dictar acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundado. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos. El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador. El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.  ESP

Tercero: La persona física o moral, nacional o extranjera, distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Tercero de Confianza (TTP, Trusted Third Parties): Entidad pública o privada encargada de la emisión de certificados digitales que atestigüen la autenticidad de la identidad de los propietarios de los mismos.

Tercero interesado: En caso de que no se haya señalado tercero interesado, éste podrá apersonarse en el procedimiento mediante escrito en el que acredite interés jurídico para intervenir en el asunto, hasta antes del cierre de instrucción. Deberá adjuntar a su escrito el documento en el que se acredite su personalidad cuando no actúe en nombre propio y las pruebas documentales que ofrezca.

Titular de los datos: La persona a quien corresponden los datos personales.

Sinónimos: *Afectado, Interesado.*

Transferencia de datos: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento. El transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Transferencias dentro del mismo grupo del responsable: En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en toda la normativa aplicable en materia de protección de datos.

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.

Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio.

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

La prohibición no regirá en los siguientes supuestos:

- Cuando sea para solicitar o proveer auxilio o colaboración judicial internacional;
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

- Cuando se refiera a transferencias dinerarias, bancarias o bursátiles, conforme a su regulación específica;
- Cuando la transferencia se hubiera acordado en el marco de tratados internacionales o convenios en los cuales el país de origen de los datos 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.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Será posible realizar transferencias internacionales de datos de carácter personal a Estados que no ofrezcan el nivel de protección adecuado, cuando el cedente garantice que el destinatario ofrecerá dicho nivel de protección; dicha garantía podrá derivarse, por ejemplo, de cláusulas contractuales apropiadas. En particular, cuando la transferencia se lleve a cabo en el seno de organizaciones o de grupos multinacionales, dicha garantía podrán consistir en la existencia de normas internas de privacidad cuya observancia resulte vinculante.

Véase también *Nivel adecuado, Países con nivel adecuado de protección de datos.*

Transferencia lógica o electrónica de los datos personales: El intercambio de datos personales desde los ambientes de procesamiento o almacenamiento hacia cualquier destino fuera de las instalaciones físicas de la entidad, solo procederá con la autorización del titular del banco de datos personales y se hará utilizando los medios de transporte autorizados por el mismo, tomando las medidas necesarias, entre las que se encuentran cifrado de datos, firmas digitales, información, checksum de verificación, entre otros, destinados a evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino. PER

Transferencia nacional de datos: Las transferencias nacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

- Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales. MEX

Transmisión: Toda comunicación o entrega parcial o total de datos personales realizada por los sujetos obligados a una persona distinta del titular.

Traslado de la documentación: Dentro de las medidas de seguridad de nivel alto, siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado. ESP

Tratamiento: Cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.

Sinónimos: *Tratamiento de datos.*

Tratamiento automatizado: Se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, recolección, grabación, conservación, elaboración, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, y, en general el procesamiento de datos personales que abarque cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Sinónimos: *Tratamiento.*

Tratamiento de datos con fines de publicidad y prospección comercial: En la recopilación de domicilios o direcciones, reparto de documentos, publicidad, prospección comercial, venta directa o a distancia, 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.

Cuando los datos sean facilitados por los propios interesados u obtenidos con su consentimiento, debe previamente informárselas finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

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. 

Véase también *Datos relativos a bases de datos con fines de publicidad.*

Tratamiento de datos en decisiones sin intervención humana valorativa: Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.

Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada.

Sinónimos: *Derecho a la impugnación de valoraciones personales*, *Impugnación de valoraciones personales, Derecho al tratamiento objetivo de datos personales, Decisión individual automatizada.*

Tratamiento de datos en la nube: Por cómputo en la nube se entiende el modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece las leyes y sus normativas reglamentarias.
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio,
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y

e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales. MEX

Tutela de derechos: La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.

Unidad Reguladora y de Control de Datos Personales: Es la Autoridad de Aplicación en materia de protección de datos del Uruguay, conforme lo dispuesto en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data. Tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad uruguaya, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.

Sinónimos: *URCDP*

Véase también *Registro*.

URCDP: Es la Unidad Reguladora y de Control de Datos Personales de Uruguay, creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios.

Sinónimos: *Registro*.

Véase también *URCDP.*

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.

Verificación: El IFAI, con el objeto de comprobar el cumplimiento de la normativa en protección de datos personales, puede iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas. El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del IFAI. Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el IFAI determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente. MEX

Sinónimos: *Procedimiento de verificación, Procedimiento de fiscalización, Inspección.*

Véase también *IFAI, Instituto, Procedimiento de verificación, Visitas de verificación.*

Visitas de fiscalización: Para mejor resolver, se podrá ordenar a la Dirección de Supervisión y Control la realización de una visita de fiscalización, que se efectuará dentro de los cinco días siguientes de recibida la orden. PER

Sinónimos: *Visitas de verificación, Inspección.*

Visitas de verificación: El personal del IFAI que lleve a cabo las visitas de verificación deberá estar provisto de orden escrita fundada y motivada con firma autógrafa de la autoridad competente del Instituto, en la que deberá precisarse el lugar en donde se encuentra el establecimiento del responsable, o bien en donde se encuentren las bases de datos objeto de la verificación, el objeto de la visita, el alcance que deba tener la misma y las disposiciones legales que lo fundamenten. El Instituto podrá realizar diversas visitas de verificaciones para allegarse de los elementos de convicción necesarios, las cuales se desarrollarán en un plazo máximo de diez días cada una. Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante. MEX

Sinónimos: *Visitas de fiscalización.*

Véase también *IFAI, Instituto, Procedimiento de verificación.*

Vulneración de seguridad: Se entiende por incidencia o vulneración de seguridad cualquier anomalía que afecte o pueda afectar a la seguridad e integridad de los datos de carácter personal (estén automatizados o no). Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada.

El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

El responsable deberá informar al titular al menos lo siguiente:

- La naturaleza del incidente;
- Los datos personales comprometidos;

- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata, y
- Los medios donde puede obtener más información al respecto.

En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

Sinónimos: *Incidencia de seguridad.*