Introducción a la Protección de Datos Personales

Módulo 2

URCDP

Versión: 1

Año: 2024

1. ¿Cuáles son los principios de la protección de datos personales?

El régimen normativo uruguayo se sustenta en un conjunto de principios, que determinan la forma, contenido y condiciones para el tratamiento de los datos, pero además operan como mandatos para responsables, encargados y titulares en la forma de cumplir las obligaciones impuestas, facilitar el ejercicio o ejercer efectivamente los derechos; y también como criterio orientador para la URCDP, con respecto a la forma de valorar los comportamientos en el cumplimiento de las disposiciones legales y reglamentarias.

Estos principios se encuentran detallados en el artículo 5°, y se especifican en los artículos 6° a 12 de la Ley:

a. Legalidad

De acuerdo con el principio de legalidad la formación de base de datos será lícita cuando se encuentra debidamente inscrita ante el órgano de control.[1]

Todo el proceso de inscripción de las bases de datos se realiza mediante el Sistema de Gestión de la URCDP

A esos efectos, la Unidad tiene disponible en su sitio web el Sistema de Registro que permita la solicitud de inscripción de registros de bases de datos en línea. Asimismo, se publican mensualmente los datos de los responsables que se encuentran inscriptos ante la Unidad. [2]

Además, conforme con este principio, no se pueden formar base de datos que tengan finalidades violatorias de derechos humanos o que sean contrarias a la ley o a la moral pública.

b. Veracidad

De acuerdo con el principio de veracidad, los datos personales que se recaben para ser objeto de tratamiento deben ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la que se obtuvieron. A estas

[1] El proceso de inscripción y las condiciones para ello se encuentran determinados en el decreto N° 664/008, de 22 de diciembre de 2008.
[2] https://www.gub.uy/unidad-reguladora-control-datos-personales/registro-bases-datos

características se agrega que los datos deben ser exactos y actualizarse cuando ello fuere necesario.

Este mismo principio agrega que los datos personales no pueden ser obtenidos por medios fraudulentos, desleales, abusivos, extorsivos o en forma contraria a las disposiciones de la normativa de protección de datos personales.

La norma agrega que cuando se constate la inexactitud de o falsedad de los datos, el responsable debe suprimirlos, sustituirlos o completarlos de acuerdo con cada situación.

Por ejemplo, si una persona cambia de estado civil y quiere actualizarlo en una base privada, debe acreditar el cambio en forma fehaciente y el responsable debe actualizar la información.

Por último, se indica que deben ser eliminados aquellos datos que hayan caducado de acuerdo a las previsiones de la normativa de protección de datos personales.

c. Finalidad

Respecto a este principio es importante resaltar que los datos personales objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

La norma aclara que los datos deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados.

Por ejemplo, los datos personales recabados para un sorteo deben eliminarse una vez que se realiza éste.

Este mismo principio establece que se regularán los casos en los que, basados en valores históricos, estadísticos o científicos, conforme con la legislación específica, se pueden conservar datos personales aun cuando no exista tal necesidad o pertinencia.

El artículo 37 del decreto N° 414/009 regula el procedimiento para la autorización de conservación de datos en base a las finalidades indicadas, siempre a petición del responsable que pretenda obtener la declaración.

Es interesante destacar que, en la solicitud, el responsable deberá identificar el tratamiento de datos al que pretende aplicar a la excepción, establecer las causas que justificarían la declaración, presentar las medidas que se propone implantar para garantizar los derechos de los titulares de los datos y acompañar los documentos necesarios para justificar la solicitud.

Sobre este trámite se aclara que la Unidad puede previamente a adoptar una resolución, solicitar la opinión de instituciones u organismos, públicos o privados, que tengan competencia o mérito para ser consultados en relación al caso.

d. Previo consentimiento informado

Otro principio de especial trascendencia para la protección de datos personales es el consentimiento. El responsable debe recabar en forma libre, previa e informada el consentimiento de los titulares de datos.

El consentimiento se puede recabar de distintas formas (dependiendo del tipo de dato): por grabaciones, formularios, aceptación en sitios web, entre otros.

Este principio indica los casos en los cuales no se considera necesario el previo consentimiento, y si bien el artículo los considera excepciones a éste, en los hechos funcionan como otras bases legitimantes del tratamiento, es así cuando:

- ✓ Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. En este punto cabe señalar que la Ley define en forma taxativa las fuentes públicas de información en el artículo 9° bis.
- ✓ 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.

La información del Diario Oficial, los registros públicos, las publicaciones en medios de comunicación, entre otras, son fuentes públicas, pero internet no lo es.

En cuanto al consentimiento, se deben tener presente los artículos 5° y 6° del decreto 414/009, que establecen algunos requisitos especiales para su recolección. Es así que el primero de estos artículos indica que se debe informar a los titulares de los datos personales de la finalidad a la que se destinarán los datos y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario se considera que el consentimiento es nulo.

Por su parte, el artículo 6° indica las formas existentes para recabarlo. Este deber se entiende cumplido cuando se permita al titular la elección entre dos opciones claramente identificadas que no encuentren pre marcadas a favor o en contra.

También es necesario indicar que el responsable de la base de datos debe recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, a través de cualquier medio conforme a derecho, lo cual puede ser requerido por la URCDP en cualquier momento.

e. Seguridad de los datos

De acuerdo con el principio de seguridad de los datos, el responsable o el usuario dela base de datos debe adoptar las medidas que resulten 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 y detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

La norma establece que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Por último, se indica que queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

El artículo 38 de la Ley N° 19.670, incorpora el régimen de comunicación de vulneraciones de seguridad, y establece que cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, debe informar inmediata y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la URCDP, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy).

Se pueden establecer medidas físicas, como, por ejemplo, utilizar llaves de seguridad, alarmas, control de ingreso, y también medidas lógicas, como por ejemplo contraseñas, claves de seguridad.

El decreto N° 64/020, en sus artículos 3 y 4, reglamenta la comunicación mencionada, y establece que tanto el responsable como el encargado de tratamiento en su caso, deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales. Además, especifica las circunstancias, contenido y plazo para las comunicaciones a los titulares de los datos afectados y a la URCDP.

f. Reserva

Según este principio aquellas personas físicas o jurídicas que obtengan legítimamente información proveniente de una base de datos que les brinde tratamiento están obligadas a utilizarlas en forma reservada y exclusivamente para el tratamiento habitual de su actividad. La norma indica que está prohibida toda difusión a terceros.

Además, esta norma establece que la infracción a este artículo hace incurrir en el delito de secreto profesional previsto en el artículo 302 del Código Penal.

Los funcionarios públicos tienen implícita la reserva en su relación funcional así como los dependientes en su relación laboral.

g. Responsabilidad proactiva

El artículo 12 de la Ley N° 18.331 -modificado por el artículo 39 de la Ley N° 19.670- regula el principio de responsabilidad, modificando la redacción original de esta norma y estableciendo un nuevo parámetro en la materia.

El artículo en su versión original indicaba que el responsable era "responsable" de las infracciones a la normativa de protección de datos personales que pudieran suceder, con carácter general. En este caso la Unidad perseguía el cumplimiento de la normativa y exhortaba de diversas formas a responsables a los efectos de su cumplimiento.

Este principio fue objeto de la modificación señalada evolucionando el concepto hacia el de una responsabilidad *"proactiva"*. Así, existe una nueva orientación en la materia que lleva a responsables y encargados de tratamiento a ir más allá del sólo cumplimiento de la Ley, y adoptar medidas en forma autónoma que demuestren dicho cumplimiento.

Sobre este punto cabe mencionar que en la nota de interés publicada en la revista de la Unidad sobre la modificación de este principio se expresó que: *"Esta formulación se visualizó como insuficiente, como ya se mencionó, a la luz de la evolución en las estrategias y medios para el tratamiento de los datos. Resultaba necesario virar hacia un régimen que impusiera un conjunto mayor de obligaciones en cabeza no sólo de responsables sino además de encargados, de modo de asegurar que todo tratamiento de datos incluyera, desde su concepción, los principios y normas en la materia".*

Se agrega que *"Se hace una explícita referencia a la responsabilidad proactiva, dentro de la que se incluyen la privacidad por diseño, privacidad por defecto, evaluación de impacto, entre otras, con el objetivo de garantizar un tratamiento adecuado de los datos personales, y demostrar su efectiva implementación. Estas medidas deberán documentarse a efectos de demostrar, cuando sea requerido por la URCDP, el cumplimiento efectivo de las normas en la*

materia. Obligación que no corresponde sólo a los responsables, sino además, en determinados casos, a los encargados". [3]

La fuente de inspiración es la normatividad europea, donde también se la conoce como *"accountability",* e incluye entre otras medidas la implementación del principio de transparencia del responsable hacia el sujeto de los datos en relación al conjunto de tratamientos realizados, contar con un delegado de protección de datos personales, listar las actividades de tratamiento, realizar una evaluación de impacto a la privacidad y notificar las brechas de seguridad.

Los responsables y encargados deben adoptar medidas que aseguren y demuestren el cumplimiento de la normativa de protección de datos personales

En Uruguay el decreto N° 64/020 avanza en el tema y regula, entre otros, los casos en los cuales se debe realizar una evaluación de impacto en forma obligatoria (art. 6°), el concepto de privacidad por diseño (artículo 8°) y por defecto (artículo 9°). La Unidad podrá complementar estos aspectos, como en los hechos realizó a través de la inclusión de los datos biométricos en el elenco de tratamientos que requerían una evaluación de impacto previa (Resolución N° 30/020, de 12 de mayo de 2020). Todo ello se desarrollará más adelante en la presente guía.

Como se verá, en materia de evaluaciones de impacto, la Unidad en conjunto con su homónimo de Argentina publicaron una guía que tiene como objetivo explicar cuáles son los pasos y contenidos que hay que tener en cuenta para su realización.

2. ¿Cuáles son los derechos de la protección de datos personales?

Como se indicó, la protección de datos personales supone además de un tratamiento en base a principios y el cumplimiento de obligaciones por responsables y encargados, el efectivo ejercicio de derechos por parte los titulares de los datos. Estos derechos se encuentran explicitados en los artículos 13 a 17 de la Ley.

[3] Se puede consultar la 4° Edición de la Revista de Protección de Datos Personales en file:///C:/Users/flavia.baladan/Downloads/Revista%20PDP%202019.pdf

- ✓ El **derecho de información** es aquel por el cual se debe informar previamente a los titulares en forma expresa, precisa e inequívoca sobre la finalidad de los datos y sus destinatarios, la existencia de bases de datos y los datos de contacto de su responsable, el carácter obligatorio o no de los cuestionarios que se propongan, las consecuencias de proporcionar o no la información, la posibilidad de ejercer los derechos y la existencia o no de transferencias internacionales.

  El artículo 62 de la Ley N° 20.075, de 20 de octubre de 2002, agregó que en los casos de tratamientos automatizados de datos regulados por el artículo 16 de la ley, se debe informar a los titulares de datos los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado. Además, que cuando los datos personales no sean recolectados directamente de sus titulares, la información deberá ser proporcionada a estos en un plazo de cinco días hábiles de recibida la solicitud por parte de los responsables. El incumplimiento habilitará al titular a realizar las acciones que correspondan. Asimismo, se indica que el órgano de control podrá establecer condiciones específicas para la publicidad permanente de la información indicada, cuando las condiciones técnicas y el tipo de tratamiento realizado así lo permitan.
- ✓ El **derecho de acceso** es el que tiene toda persona que, previamente, acredite su identidad, de acceder a toda la información sobre sí mismo con la que cuente el responsable de tratamiento.
- ✓ El derecho de **actualización** es el que tiene el titular a que se modifiquen los datos que resulten inexactos a la fecha de ejercicio del derecho.
- ✓ El derecho **de rectificación** es el que tiene el titular a que se modifiquen los datos que resulten ser inexactos o incompletos.
- ✓ El derecho de **inclusión** es el que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando acredite un interés fundado.

  El titular del dato personal puede solicitar ser incluido en una base de datos si por ejemplo le trae aparejado un beneficio.
- ✓ El derecho de **supresión** es el que tiene el titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados

o excesivos. La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas y de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular, que justificaren el tratamiento de los datos. El responsable deberá documentar ante el titular haber cumplido con lo solicitado indicando las cesiones o transferencias de los datos suprimidos e identificando al cesionario.

El titular del dato personal puede solicitar en cualquier momento que le supriman sus datos de una base de datos cuando ya no sea necesario su tratamiento, o si fue cargado por error, o sin su consentimiento.

- ✓ El derecho a la **impugnación de las valoraciones personales** implica que las personas tienen derecho a no verse sometidas a una decisión basada en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros, con efectos jurídicos que les afecte de manera significativa. La persona afectada 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, la persona 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.

  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, como por ejemplo en el caso de un concurso de méritos.

- ✓ Estos derechos se pueden ejercer de forma gratuita (cada 6 meses) y ante el responsable, quien tendrá un plazo de respuesta de 5 días hábiles a contar de la solicitud, por los medios que se hayan indicado. En caso de falta de respuesta se habilita la acción de Habeas Data.

3. La comunicación de datos

En nuestro país, se permite la comunicación de datos personales. El literal B del art. 4 de la Ley la define como toda revelación de datos realizada a una persona distinta del titular. Por su parte, el art. 17 de la misma norma, regula los requisitos necesarios para realizar la comunicación de datos, los cuales son:

I. la existencia de interés legítimo del emisor y destinatario, y
II. el previo consentimiento informado del titular o en el marco de las excepciones.

A saber:

A. así lo disponga una ley de interés general.
B. en los supuestos del artículo 9° de la Ley.
C. se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de titulares de datos mediante mecanismos de disociación adecuados cuando ello sea pertinente.
D. se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de datos no sean identificables.

Es importante remarcar que el destinatario y el emisor son responsables solidaria y conjuntamente por el cumplimiento de la normativa de protección de datos.

Son ejemplos de comunicación de datos la publicación de todo tipo de listados y los intercambios de información entre organismos públicos basados en normas que así lo indiquen, entre otros. En estos casos es necesario analizar el cumplimiento de los requisitos y su adecuación a los requisitos legales. Asimismo, al momento de inscribir las bases de datos, se hace un control de la existencia de la comunicación de datos[4].

[4] Se puede consultar los dictámenes y resoluciones sobre este tema en el sitio web de la Unidad: www.gub.uy/urcdp