Introducción a la Protección de Datos Personales

Módulo 4

URCDP

Versión: 1

Año: 2024

1. Actualizaciones en protección de datos personales

a. Breve reseña:

Como ya se ha mencionado, la Ley Nº 19.670, de 15 de octubre de 2018, en sus artículos 37 a 40, realiza actualizaciones a la normativa de protección de datos personales e incorpora nuevas tendencias internacionales en la materia. Su finalidad fue contemplar el avance de la tecnología y el nuevo contexto que esto apareja, y adoptar las mejores soluciones internacionales para dar respuesta adecuada a los titulares de los datos personales.

Es así entonces que se incorporan como elementos nuevos el concepto de extraterritorialidad, el de vulneraciones de seguridad, el de responsabilidad proactiva (que incluye la realización de evaluaciones de impacto, adopción de medidas de privacidad por diseño y por defecto), así como la creación de la figura del delegado de protección de datos para determinadas situaciones.

A dichos efectos, y para poder ampliar los conceptos que se incorporaron a la normativa de protección de datos, se reglamentaron los artículos indicados por decreto Nº 64/020, de 17 de febrero de 2020

Parte de las modificaciones introducidas se mencionaron en los apartados anteriores, sin perjuicio de lo cual, debido a su trascendencia, se ampliará su desarrollo en los capítulos que siguen.

b. La adopción de nuevas medidas en el marco de la responsabilidad proactiva

En términos generales, la nueva normativa modifica el principio de responsabilidad haciéndolo evolucionar hacia el concepto de responsabilidad proactiva. En este sentido, nos remitimos a lo explicado con carácter general cuando desarrollamos este principio en la presente guía.

c. Privacidad por diseño y Privacidad por defecto

La *privacidad por diseño* implica que desde el comienzo del tratamiento se adopten medidas que aseguren el cumplimiento de las normas de protección de datos personales.

El objetivo es que la protección de datos personales no sea una medida que se adopta con posterioridad, sino que se considera desde el inicio del tratamiento de datos personales.

En ese marco, responsables y encargados de tratamiento, en su caso, deberán incorporar en el diseño de las bases de datos, las operaciones de tratamiento, las aplicaciones y los sistemas informáticos, aquellas medidas dirigidas a dar cumplimiento a la normativa de protección de datos personales. A esos efectos, previo al tratamiento y durante todo su desarrollo, aplicarán medidas técnicas y organizativas apropiadas, tales como, por ejemplo:

a) Técnicas de disociación, seudonimización y minimización de datos.
b) Mecanismos para asegurar el ejercicio de los derechos de los titulares de los datos personales.
c) Documentación de los consentimientos o de otros fundamentos que legitimen el tratamiento.
d) Tiempo de conservación de los datos, considerando sus tipos y su tratamiento.
e) Adopción de planes de contingencia que incluyan medidas de seguridad de la información.
f) Análisis funcionales y modelos de arquitectura de los datos.
g) Otras medidas establecidas por la URCDP.

Asimismo, es importante tener en cuenta la *privacidad por defecto*. En este caso, responsables y encargados del tratamiento (cuando corresponda) aplicarán las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Es importante remarcar que esta obligación tiene relación directa con la cantidad de datos personales recogidos por el responsable, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación cuando así corresponda.

d. Las vulneraciones de seguridad.

Las nuevas disposiciones establecen que tanto el responsable y el encargado de tratamiento de datos deben adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar su seguridad.

A estos efectos, se considera importante valorar la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por Agesic[1].

Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables y encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados.

El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarlo a la Unidad Reguladora y de Control de Datos Personales en un plazo máximo de 72 horas de conocida la vulneración.

La comunicación a la Unidad Reguladora y de Control de Datos Personales deberá contener información relevante, tal como la fecha cierta o estimada de la ocurrencia de la vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

Se regula además que en caso que la vulneración hubiere sido conocida por el encargado del tratamiento, se la comunicará de inmediato al responsable del tratamiento. Por su parte, el responsable de tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarla en un lenguaje claro y sencillo a los titulares de los datos que hayan sufrido una afectación significativa en sus derechos.

[1] Se puede consultar el documento en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Solucionada la vulneración, el responsable deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la URCDP.

Todo lo anterior podrá ser evaluado por el Consejo de la Unidad y solicitar información en caso de que entienda que no se cumplió con los pasos mencionados.

Asimismo se encuentra disponible la Guía sobre Vulneraciones de Seguridad creada por la Unidad[2].

e. Las evaluaciones de impacto en la protección de datos

La evaluación de impacto en la protección de datos es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Ello considerando que el tratamiento de datos personales puede provocar impactos en los derechos de las personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente. [3]

El decreto N° 64/020 indica una serie de situaciones donde los responsables de tratamiento y eventualmente los encargados, deben realizarla en forma obligatoria:

- Utilizar datos sensibles como negocio principal
- Proyectarse un tratamiento permanente o estable de los datos especialmente protegidos
- Se realiza tratamiento con fines de perfilamiento

[2] GUIA PARA LA GESTIÓN, DOCUMENTACIÓN Y COMUNICACIÓN DE VULNERACIONES DE SEGURIDAD EN DATOS PERSONALES https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/GUIA%20PARA%20LA%20GESTI%C3%93N%2C%20DOCUMENTACI%C3%93N%20Y%20COMUNICACI%C3%93N%20DE%20VULNERACIONES%20DE%20SEGURIDAD%20EN%20DATOS%20PERSONALES.pdf

[3] Definición contenida en la Guía de Evaluación de Impacto de esta Unidad y la AAIP disponible en: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

- Tratamiento de datos de grupos de personas en situación de especial vulnerabilidad
- Tratamiento de grandes volúmenes de datos personales
- Transferencia de datos personales a países no adecuados
- Otros que determine la Unidad

El Consejo Ejecutivo de la Unidad, por Resolución N° 30/020, de 12 de mayo de 2020 estableció la obligación de realizar una evaluación de impacto en forma previa al tratamiento de datos biométricos. Posteriormente, la ley N° 19.924, de 18 de diciembre de 2020 incorporó a la ley N° 18.331 el literal Ñ al artículo 4° y el artículo 18 bis, en los que se definen los datos biométricos y se impone legalmente la misma obligación.

En general, a la hora de realizar una evaluación de impacto se recomienda determinar quiénes van a ser los participantes del proceso y la forma en que se va a documentar la evaluación. En segundo lugar, es necesario realizar un análisis del marco normativo aplicable. Ambas se consideran tareas previas e imprescindibles antes de la evaluación en sí misma. [4]

En cuanto a las etapas subsiguientes, es necesario realizar en forma sucesiva un análisis preliminar, un contexto de tratamiento, un análisis de gestión de riesgos y culminar con un plan de tratamiento de riesgos, etapas que detallan en la Guía indicada, a cuya lectura y aplicación nos remitimos.

f. Delegados de Protección de Datos Personales

Los Delegados de Protección de Datos Personales son un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrolla la autoridad de control.

Dentro de la actualización del marco normativo nacional en materia de protección de datos personales, se crea la figura del Delegado de Protección de Datos Personales. La Ley establece determinados casos en los cuales resulta necesaria su designación, a saber:

[4] A los efectos de conocer más detalladamente cómo se debe realizar una evaluación de impacto se sugiere consultar la guía disponible en https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

- ✓ Entidades públicas o privadas, estatales o no, las privadas y las parcialmente de propiedad estatal
- ✓ Entidades privadas que traten datos sensibles como negocio principal.
- ✓ Entidades privadas que traten grandes volúmenes de datos personales. De acuerdo con la reglamentación posterior se entiende que gran volumen de datos es aquel que implique un tratamiento de datos de más de 35.000 personas.

La referencia a Entidades puede alcanzar a personas físicas o jurídicas que realicen el tratamiento de datos personales o terceros, en calidad de responsable o encargado de tratamiento.

El decreto reglamentario expresamente indica que además la Unidad, de oficio o ante una gestión expresa, puede expedirse en el sentido de indicar la pertinencia o no de su designación.

Sus funciones principales son[5]:

- ✓ Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.
- ✓ Supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.
- ✓ Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en la materia.
- ✓ Actuar como nexo entre la entidad y la URCDP.

La norma además establece que debe poseer las condiciones necesarias para el correcto desempeño de sus funciones y actuar con autonomía técnica.

Además, existen otros aspectos que merecen ser analizados como por ejemplo la calidad y condiciones del delegado, su posición y su plazo de designación, cese o renuncia.

[5] Ver artículo 40 de la Ley N° 19.670

En ese marco, es importante indicar que el delegado puede desempeñar sus funciones a través de cualquier modalidad contractual sea en forma dependiente o no.

Conforme el decreto N° 64/020, los delegados deben contar con conocimiento en derecho, especializados en protección de datos personales debiendo acreditarse dicha calidad al momento de su comunicación a la URCDP. La Unidad ha clarificado el alcance de esta disposición a través de la resolución N° 32/020 del 19 de mayo de 2020, por la que se establece que se deberá tener en cuenta especialmente su calidad de profesional del área jurídica o poseer conocimientos en derecho, con énfasis en derechos humanos. Además, deberá contar con conocimientos sobre regulación en materia de protección de datos personales, lo que podrá acreditarse mediante cursos o actividades brindadas por la URCDP u otras entidades nacionales e internacionales. Se valorará especialmente la realización de cursos vinculados a responsabilidad proactiva y tratamiento de categorías especiales de datos. Se tendrá en cuenta, además, la experiencia previa en el ámbito de la protección de datos. [6]

La evaluación de sus conocimientos corresponde a responsables y encargados en función de los citados criterios, aclarándose por Resolución N° 44/020 de 21 de julio de 2020 de la URCDP que el énfasis en derechos humanos es el necesario para contextualizar el derecho a la protección de datos en sus relaciones con otros derechos.[7]

El Delegado de Protección de Datos puede ser una persona jurídica. En estos casos, se debe informar a la URCDP quienes son sus integrantes y cuál es su órgano de administración, sin perjuicio de lo cual, es necesario identificar a sus representantes y a una persona física que se constituya en el nexo con la Unidad, de conformidad con la precitada resolución idéntica obligación existe para equipos de delegados, de conformidad con lo indicado por resolución de la URCDP N° 44/020.

[6] Puede consultarse la Resolución en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-32020

[7] Puede consultarse la Resolución en

A los efectos de desarrollar en tiempo y forma sus tareas, el delegado tiene que poder participar en forma adecuada en todas las cuestiones relativas a la protección de datos. Para ello debe poder tener acceso a las bases de datos y a las operaciones de tratamiento.

La persona designada como delegado debe guardar absoluta confidencialidad de las informaciones que tiene acceso por su calidad y no debe tener conflicto de intereses.

El delegado debe actuar con plena autonomía técnica y no debe recibir instrucciones en el desempeño de sus funciones.

Cabe indicar que cuando corresponde la designación de un delegado se cuenta con un plazo de 90 días a contar desde el inicio del tratamiento para comunicarlo a la Unidad. También se preveía un plazo para su designación para aquellas entidades que debían contar con esta figura desde la entrada en vigor del Decreto. La comunicación del delegado se realiza a través del Sistema de Gestión disponible a través de la web de la URCDP.

Por otra parte, el decreto establece que un conjunto de entidades con cometidos o actividades afines pueden nombrar un único delegado de protección de datos, al igual que varias entidades públicas, siempre que pueda cumplir las funciones legalmente establecidas en relación a todas y cada una de ellas.

5. Inteligencia Artificial y protección de datos

En relación con la incorporación del concepto de Inteligencia Artificial en la normativa de protección de datos personales, se debe comenzar por considerar que el art. 16 de la Ley N° 18.331 establece el derecho a la impugnación de valoraciones personales. Es así, que 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.

La mención a tratamiento automatizado comprende al tratamiento que se realiza mediante el uso de algoritmos que dan base a la Inteligencia Artificial.

En tal sentido, es que se entendió necesario ampliar el art. 13 de la Ley N° 18.331, en relación con el derecho de información. Es así que se agregó un literal g) que expresa que en el caso de tratamientos automatizados de datos regulados por el artículo 16 de la ley, se debe informar los criterios de valoración, los procesos aplicados y la solución tecnológica o el programa utilizado.

Además, esta misma norma agregó una nueva competencia relacionada con Inteligencia Artificial en cuanto permite a la URCDP establecer los criterios y procedimientos que deban observar los responsables y encargados, en el tratamiento automatizado de datos personales indicados en el artículo 16 de la ley.

Por otra parte, el artículo 74 de la Ley N° 20.212, 17 de noviembre de 2023, atribuyó a la AGESIC el cometido de diseñar y desarrollar una estrategia nacional de datos e inteligencia artificial basada en estándares internacionales, en los ámbitos público y privado. En todo lo que respecta al tratamiento de datos personales, la norma indica que será preceptiva la actuación conjunta con la Unidad Reguladora y de Control de Datos Personales.