

Decreto N° 64/020

REGLAMENTACION DE LOS ARTS. 37 A 40 DE LA LEY 19.670 Y ART. 12 DE LA LEY 18.331, REFERENTE A PROTECCION DE DATOS PERSONALES

Documento Actualizado

Promulgación: 17/02/2020

Publicación: 21/02/2020

Sección: Último Momento

El Registro Nacional de Leyes y Decretos del presente semestre aún no fue editado.

Reglamentario/a de:

Ley N° 19.670 de 15/10/2018 artículos 37, 38 y 40,  
Ley N° 18.331 de 11/08/2008 artículo 12.

VISTO: los artículos 37 a 40 de la Ley N° 19.670 de 15 de octubre de 2018;

RESULTANDO: que contienen nuevas disposiciones en materia de protección de datos personales que impactan en el sistema nacional y procuran brindar a las personas un nivel de protección acorde a los nuevos desarrollos tecnológicos y a la evolución en las formas de tratamiento de los datos personales;

CONSIDERANDO: I) que el derecho a la protección de datos personales es un derecho inherente a la persona humana comprendido en el artículo 72 de la Constitución de la República, como lo reconoce el artículo 1° de la Ley N° 18.331 de 11 de agosto de 2008;

II) que a efectos del dictado de esta reglamentación se han tenido en cuenta las disposiciones y doctrinas más recientes, tales como el Reglamento Europeo N° 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N° 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, suscrito por la República Oriental del Uruguay el 10 de octubre de 2018;

III) que la ubicuidad de las personas en el mundo digital y la protección de sus derechos requiere atender debidamente el alcance de la protección de su información personal, lo que corresponde complementar con los mecanismos de control de cumplimiento en el ámbito internacional y las necesarias obligaciones de responsables y encargados, que no obstante situarse en el exterior del país, realizan tratamientos de datos de personas que se ubican en éste;

IV) que por otra parte, por la trascendencia y el volumen de la información tratada por múltiples organizaciones respecto de las personas y las eventuales vulneraciones de seguridad, resulta imprescindible establecer un régimen claro en lo que atañe al procedimiento que se debe realizar en esas situaciones;

V) que el estado actual de la protección de datos personales ha llevado a fortalecer el principio de responsabilidad, en su evolución hacia un principio de responsabilidad demostrada, que impone al responsable y encargado en su caso, la obligación de demostrar que las actividades de tratamiento cumplen con la legislación aplicable. En ese sentido se ha incorporado un mínimo de medidas -entre las que se encuentran la protección de datos desde el diseño y por defecto y las evaluaciones de impacto previas-, máxime en los casos en que existe un mayor riesgo para las personas;

VI) que, asimismo, la Ley que se reglamenta ha incorporado la figura del delegado de protección de datos, el que debe contar con las competencias necesarias e independencia técnica para cumplir sus funciones en forma apropiada. Su designación resulta pertinente en los casos de entidades públicas, entidades que traten datos sensibles o que realicen tratamiento de grandes volúmenes de datos personales;

VII) que acorde con lo previsto en el artículo 32 de la Ley N° 18.331 de 11 de agosto de 2008, se consultó al Consejo Consultivo de la Unidad Reguladora y de Control de Datos Personales y se contemplaron, en lo pertinente, sus planteos, elevándose proyecto de reglamentación por parte del Consejo Ejecutivo de dicha Unidad.

ATENCIÓN: a lo expuesto y a lo previsto por el artículo 168 ordinal 4° de la Constitución de la República;

EL PRESIDENTE DE LA REPÚBLICA  
- actuando en Consejo de Ministros -

DECRETA:

CAPÍTULO I - ÁMBITO TERRITORIAL

Artículo 1

Ámbito territorial. A los efectos de lo dispuesto por el artículo 37 de la Ley N° 19.670 de 15 de octubre de 2018, se entenderá que el responsable o encargado de tratamiento se encuentra establecido en territorio uruguayo cuando realice en éste una actividad estable, sin importar la forma jurídica adoptada para ello.

En caso que el responsable o encargado no se encuentre establecido en territorio uruguayo, la Ley N° 18.331 de 11 de agosto de 2008 y esta reglamentación igualmente regirán si:

a) Las actividades de tratamiento de datos están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República lo cual se apreciará a través de elementos tales como el uso del idioma, la referencia al pago en moneda nacional o la provisión de servicios conexos -no necesariamente prestados por el responsable o encargado- en territorio uruguayo.

b) Las actividades de tratamiento de datos están relacionadas con el análisis del comportamiento de los habitantes de la República, incluyendo las destinadas a la elaboración de perfiles, siendo aplicable al efecto en especial lo dispuesto en el artículo 16 de la ley N° 18.331 de 11 de agosto de 2008.

c) Lo disponen normas de derecho internacional público o un contrato. En ningún caso los contratantes podrán excluir la aplicación de la ley nacional, cuando ésta corresponda.

d) En el tratamiento se utilizan medios situados en el país, tales como redes de información y de comunicación, centros de datos e infraestructura informática en general.

(\*)Notas:

Ver en esta norma, artículo: 2.

Artículo 2

Alcance de las obligaciones. En las situaciones previstas en el inciso segundo del artículo anterior, los responsables y encargados de tratamiento, en su caso, deberán dar cumplimiento a las obligaciones previstas en la Ley N° 18.331 de 11 de agosto de 2008, y modificativas, incluyendo el registro de sus bases de datos y brindar la información de contacto correspondiente ante la Unidad Reguladora y de Control de Datos Personales.

Se exceptúa de la obligación de registro de las bases de datos, las situaciones referidas en el literal d) del inciso segundo del artículo 1° siempre que los medios se utilicen exclusivamente con fines de tránsito y el responsable del tratamiento designe un representante domiciliado en territorio nacional ante la Unidad Reguladora y de Control de Datos Personales.

CAPÍTULO II - VULNERACIONES DE SEGURIDAD

Artículo 3

Medidas de Seguridad. El responsable y el encargado de tratamiento, en su caso deberán 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. A estos efectos valorarán la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

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.

Artículo 4

Comunicación de vulneraciones de seguridad. El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarla 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.

En caso que la vulneración hubiere sido conocida por el encargado del tratamiento, éste la comunicará de inmediato al responsable del tratamiento.

Este último, 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.

Solucionada la vulneración, el responsable del tratamiento deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la Unidad Reguladora y de Control de Datos Personales.

CAPÍTULO III - MEDIDAS DE RESPONSABILIDAD PROACTIVA

Artículo 5

Responsabilidad proactiva. Los responsables y encargados de tratamiento de datos personales en su caso, deberán adoptar, en atención a la naturaleza de los datos, los tratamientos que efectúen y los riesgos que impliquen, las medidas indicadas en el presente Capítulo y toda aquella que corresponda según lo dispuesto en el artículo 12 de la Ley N° 18.331 de 11 de agosto de 2008, en la redacción dada por el artículo 39 de la Ley N° 19.670 de 15 de octubre de 2018.

Para adoptar estas medidas se deberá tener en cuenta el estado de la técnica, el costo de su aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que aquel entrañe para los derechos de las personas.

Las medidas adoptadas deberán ser documentadas, revisadas periódicamente y evaluadas en su efectividad.

La documentación de las medidas deberá contener, como mínimo, la forma, medios y finalidad del tratamiento, los procedimientos orientados a dar cumplimiento a las normas de protección de datos, la planificación de mecanismos para responder a vulneraciones de seguridad, y el rol del delegado de protección de datos cuando corresponda.

Esta documentación deberá estar disponible ante la solicitud efectuada por la Unidad Reguladora y de Control de Datos Personales.

Artículo 6

Evaluación de impacto en la protección de datos personales. En forma previa al inicio del tratamiento, el responsable y el encargado del tratamiento en su caso, deberán realizar una evaluación de impacto en la protección de datos personales, cuando en las operaciones de tratamiento pueda:

a) Utilizarse datos sensibles como negocio principal.

b) Projectarse un tratamiento permanente o estable de los datos especialmente protegidos a que refiere el Capítulo IV de la Ley N° 18.331 de 11 de agosto de 2008, o de los datos vinculados a la comisión de infracciones penales, civiles o administrativas.

c) Implicar una evaluación de aspectos personales de los titulares con el fin de crear o utilizar perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad de comportamiento y solvencia financiera y localización.

d) Llevarse a cabo el tratamiento de datos de grupos de personas en situación de especial vulnerabilidad y, en particular, de menores de edad o personas con discapacidad.

e) Producirse un tratamiento de grandes volúmenes de datos personales.

f) Transferirse datos personales a otros Estados u organizaciones internacionales respecto de los que no exista nivel adecuado de protección.

g) Otros que determine la Unidad Reguladora y de Control de Datos Personales.

(\*)Notas:

Ver en esta norma, artículo: 7.

Artículo 7

Contenido de la evaluación de impacto en la protección de datos personales - La evaluación prevista en el artículo precedente deberá contener, como mínimo:

a) Una descripción sistemática del tratamiento a realizar y su finalidad.

b) Una evaluación del tratamiento con relación al cumplimiento de la normativa de protección de datos personales.

c) Una evaluación de los riesgos para los derechos de los titulares de los datos.

d) Un detalle de las medidas de seguridad y de los mecanismos para demostrar el cumplimiento de la normativa de protección de datos personales.

En relación a los tratamientos ya iniciados y que se encuentren incluidos en los supuestos del artículo 6°, el responsable y el encargado de tratamiento en su caso, deberán realizar esta evaluación en un plazo de 1 año a contar de la publicación de este decreto en el Diario Oficial.

Si del resultado de la correspondiente evaluación surge un riesgo potencial y significativo para los derechos de los titulares de los datos, el responsable y el encargado del tratamiento en su caso, deberán ponerlo en conocimiento de la Unidad Reguladora y de Control de Datos Personales, con información pormenorizada de las medidas que adoptaron o adoptarán, y en este último caso el respectivo plazo.

A los efectos de la realización de la evaluación de impacto, según el tipo o volumen de datos y de su tratamiento, la Unidad antes citada fijará criterios que contribuyan al cumplimiento de la obligación prevista en el presente artículo.

Artículo 8

Privacidad por diseño. El responsable y el encargado 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, 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:

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 Unidad Reguladora y de Control de Datos Personales.

Artículo 9

Privacidad por defecto. El responsable y el encargado del tratamiento, en su caso, 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.

Esta obligación refiere a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación.

CAPÍTULO IV - DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

Artículo 10

Alcance. De acuerdo con lo dispuesto en el artículo 40 de la Ley N° 19670 de 15 de octubre de 2018, deberán designar un delegado de protección de datos personales:

a) Entidades públicas, estatales o no estatales y las privadas total o parcialmente de propiedad estatal.

b) Entidades privadas que traten datos sensibles como negocio principal. De conformidad con lo establecido por el artículo 4° literal b) de la Ley N° 18.331 de 11 de agosto de 2008, son datos sensibles aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

c) Entidades privadas que realicen tratamiento de grandes volúmenes de datos.

Se considera tratamiento de grandes volúmenes de datos cualquier actividad en la que se realice un tratamiento de datos personales de más de 35.000 personas.

La Unidad Reguladora y de Control de Datos Personales, de oficio o ante gestión realizada ante la misma, podrá expedirse sobre la pertinencia de que una entidad privada cuente con un delegado de protección de datos.

Artículo 11

Funciones de los delegados de protección de datos. Las funciones principales de los delegados de protección de datos serán:

a) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

b) Supervisar el cumplimiento de la normativa sobre dicha protección en la entidad o entidades para las que preste servicios.

c) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

d) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

Artículo 12

Calidad y condiciones del delegado. El delegado de protección de datos podrá desempeñar sus funciones a través de cualquier modalidad contractual, sea que implique dependencia o no. Deberá contar con conocimientos en Derecho, especializados en materia de protección de datos personales, los que deberán acreditarse.

En el caso de que el delegado sea persona jurídica, deberá comunicarse a la Unidad Reguladora y de Control de Datos Personales como está integrado su órgano de administración, así como los datos de sus integrantes y de la persona o personas físicas que se designen para realizar la tarea.

Artículo 13

Posición del delegado de protección de datos. El delegado de protección de datos deberá participar de forma adecuada en todas las cuestiones relativas a la protección de datos personales.

Para desarrollar sus tareas en el desempeño de sus funciones, se le brindará pleno acceso a las bases de datos personales y a las operaciones de tratamiento. Actuará con autonomía técnica y no recibirá instrucciones en el desempeño de sus funciones específicas como delegado de protección de datos.

El delegado de protección de datos deberá guardar absoluta confidencialidad de las informaciones a las que tenga acceso por su calidad, siendo de aplicación lo establecido en el artículo 11 de la Ley N° 18.331 de 11 de agosto de 2008.

Este delegado podrá desempeñar otras funciones en cuanto no generen conflicto de intereses.

Artículo 14

Plazo de designación, cese o renuncia del delegado. Cuando corresponda la designación de un delegado de protección de datos personales, ésta deberá ser comunicada a la Unidad Reguladora y de Control de Datos Personales en un plazo de 90 días a contar del inicio del tratamiento.

Toda entidad que al momento de la entrada en vigencia del presente decreto se encuentre en la situación prevista en el artículo 40 de la Ley N° 19.670 de 15 de octubre de 2018, deberá designar al delegado de protección de datos en el plazo previsto en el inciso anterior, a contar de la publicación del presente decreto en el Diario Oficial.

Todo cese o renuncia de un delegado de protección de datos deberá ser comunicado a la Unidad Reguladora y de Control de Datos Personales en el plazo previsto en el inciso anterior, debiendo designarse un nuevo delegado.

El delegado de protección de datos podrá comunicar directamente a la Unidad Reguladora y de Control Datos Personales su cese o renuncia.

Artículo 15

Posibilidad de designar un único delegado. Un conjunto de entidades con cometidos o actividades afines, podrán nombrar un único delegado de protección de datos siempre que éste pueda cumplir cabalmente con las funciones legalmente establecidas en relación a todas y cada una de ellas.

También podrán designar un único delegado de protección de datos en los términos señalados en el presente artículo, varias entidades públicas que formen parte de la misma estructura administrativa, lo que se efectuará por resolución fundada, en especial en cuanto a la viabilidad del cabal cumplimiento antes referido.

La Unidad Reguladora y de Control de Datos Personales podrá requerir la designación de delegados de protección de datos adicionales a fin de proteger los derechos de los titulares de los datos en los casos previstos en la presente disposición.

CAPÍTULO V - NORMAS FINALES

Artículo 16

Criterios y sanciones. La Unidad Reguladora y de Control de Datos Personales fijará criterios en el cumplimiento, auditoría y evaluación de las medidas establecidas en la Ley N° 18.331 de 11 de agosto de 2008 y en el presente decreto. El Consejo Ejecutivo de esa Unidad impondrá las sanciones correspondientes a los incumplimientos a las disposiciones del presente decreto de conformidad con lo dispuesto por el artículo 35 de la Ley N° 18.331 de 11 de agosto de 2008, en la redacción dada por el artículo 152 de la Ley N° 18.719 de 27 de diciembre de 2010 y el artículo 83 de la Ley N° 19.355 de 19 de diciembre de 2015.

Artículo 17

Deróganse los artículos 7° y 8° del Decreto N° 414/009 de 31 de agosto de 2009.

Artículo 18

Comuníquese, publíquese.

TABARÉ VÁZQUEZ - JORGE VÁZQUEZ - RODOLFO NIN NOVOA - DANILO ASTORI - JOSÉ BAYARDI - EDITH MORAES - VÍCTOR ROSSI - GUILLERMO MONCECCHI - ERNESTO MURRO - JORGE BASSO - ENZO BENECH - BENJAMÍN LIBEROFF - ENEIDA DE LEÓN - MARINA ARISMENDI