Política de Privacidad

Régimen normativo en materia de protección de datos personales

El régimen jurídico relativo a la protección de datos personales, se encuentra previsto en la Ley Número 18.331 (“Ley de Protección de Datos Personales”) y su Decreto Reglamentario Número 414/009, así como en los artículos 37 a 40 de la Ley Número 19.670 “Aprobación de Rendición de Cuentas y Balance de Ejecución Presupuestal - Ejercicio 2017”, y su Decreto Reglamentario Número 064/020.

Principios aplicables a la protección de datos personales

El ordenamiento jurídico de la República Oriental del Uruguay, prevé un conglomerado de principios, que determinan la forma, el contenido y las condiciones para el tratamiento de los datos, siendo además guías esenciales para la garantía de los derechos relativos a datos personales.

Puntualmente, los principios aplicables en la materia se encuentran previstos en el artículo 5 de la Ley Número 18.331, y desarrollados en las subsiguientes disposiciones, artículos 6 a 12.

Legalidad

De acuerdo con el principio de legalidad, la formación de base de datos será lícita cuando se encuentre debidamente inscripta ante el órgano de control.
Todo el proceso de inscripción de las bases de datos es mediante el sistema de registro en línea, y su formación no podrá implicar finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

Veracidad

Según 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 ello, 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.
Cuando se constate la inexactitud de o falsedad de los datos, el responsable debe suprimirlos, sustituirlos o completarlos de acuerdo con cada situación. Finalmente, deberán eliminarse aquellos datos que hayan caducado de acuerdo a las previsiones de la normativa de protección de datos personales.

Finalidad

Los datos personales objeto de tratamiento, no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. En efecto, los datos deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados.
A texto expreso, la normativa dispone que tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular.

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, expresa e informada, el consentimiento de los titulares de datos. Dicho consentimiento puede ser recabado de distintas maneras, a saber: por grabaciones, formularios, aceptación en sitios web, entre otros, y siempre atendiendo a la clase de dato que se trate.
A modo de excepciones, 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, a 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.

Tanto la información del Diario Oficial, los registros públicos, las publicaciones en medios de comunicación, entre otras, son fuentes públicas, no encontrándose allí incluida la internet.

En cuanto al consentimiento, debe además tenerse presentes los artículos 5 y 6 del Decreto Reglamentario Número 414/009, que establecen algunos requisitos especiales para su recolección.

Así, la solicitud del consentimiento del titular para la recolección y tratamiento de sus datos, deberá ser informada de forma que conozca inequívocamente 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, el consentimiento será 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.

Seguridad de los datos

De acuerdo con el principio de seguridad de los datos, el responsable o el usuario de la 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, así como 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, asimismo, 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. En este aspecto, los artículos 3 y 4 del Decreto Número 64/020 establecen 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.

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, se establece que 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 (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público.

Responsabilidad proactiva

Los responsables y encargados deben adoptar medidas que aseguren y demuestren el cumplimiento de la normativa de protección de datos personales. De manera vinculada, el Decreto Número 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, así como indica el concepto de privacidad por diseño y por defecto.

Getnet

Derechos vinculados a datos personales

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.

Tales derechos se encuentran explicitados en los artículos 13 a 16 de la Ley Número 18.331.

Derecho de información

Ante la recolección de datos, 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.

Derecho de Acceso

Éste es el derecho 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.

Derecho de Actualización

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.

Derecho de Rectificación

Esta potestad, es la que tiene el titular a que se modifiquen los datos que resulten ser inexactos o incompletos.

Derecho de Inclusión

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.

Derecho de Supresión

En cuanto al 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.

Cabe destacar, que 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.

Derecho a la impugnación de las valoraciones personales

Implica 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.

Tipología de Datos Personales

Datos sensibles

Son todos aquellos datos personales que revelen el origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o la vida sexual de las personas.

Datos de salud

Se consideran datos de salud, las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Estos datos pueden recabarse por parte de los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud, respetando los principios del secreto profesional, la normativa específica y lo establecido en la Ley Número 18.331.

Datos relacionados con el ámbito laboral

En el ámbito laboral, el uso y tratamiento de los datos personales está limitado al contrato de trabajo y en mérito a éste es que se debe recabar la información necesaria para cumplir la función.

Datos de la actividad comercial o crediticia

El tratamiento de datos destinado a informar sobre la solvencia patrimonial o crediticia está autorizado, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia, que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos.

Los datos deben ser obtenidos de fuentes de acceso público, o procedentes de informaciones facilitadas por el acreedor o en los casos previstos en la normativa.

Datos biométricos

Se trata de datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona tales como datos dactiloscópicos, reconocimiento de imagen o voz.

Datos de telecomunicaciones

Las telecomunicaciones en todas sus variedades, son merecedoras de especial atención, a los efectos de la protección de los datos personales. Por ello, la normativa prevé la adopción de medidas particulares para presentar la seguridad en la explotación de su red o en la prestación de su servicio, e incluso se

determina la obligación de informar a los abonados la existencia de riesgos de violaciones de seguridad a la red pública de comunicaciones electrónicas y las medidas a adoptarse.

Datos de Publicidad

En el ámbito de la publicidad, en la recopilación de domicilios, reparto de documentos, publicidad, prospección comercial, venta 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 titulares u obtenidos con su consentimiento.