BOGOTÁ

ACTUALIDAD
DEL ENTORNO DE NEGOCIOS

Protección de datos y empresas en Colombia.

Número 12
2018

Invest in Bogotá!

ACTUALIDAD
DEL ENTORNO DE NEGOCIOS

Protección de datos y empresas en Colombia

Número 12
2018

JUAN GABRIEL PÉREZ
DIRECTOR EJECUTIVO

ADRIANA FORERO
GERENTE DE APOYO ESTRATÉGICO

MAURICIO ROMERO
JEFE DE INVESTIGACIONES
E INTELIGENCIA DE MERCADOS

JUAN DAVID MARTÍNEZ
OFICIAL DE CLIMA DE INVERSIÓN

1. EDITORIAL

La integración de la economía global, el desarrollo del sector servicios y las nuevas tecnologías de la información han impuesto retos importantes a los Estados para proteger la privacidad de los datos de las personas. Con base en experiencias internacionales y recomendaciones de organismos como Naciones Unidas y la Organización para la Cooperación y el Desarrollo Económico (OCDE), Colombia cuenta hoy con un Régimen de Protección de Datos Personales liderado por la Superintendencia de Industria y Comercio (SIC).

En la era de la economía digital, el crecimiento acelerado del comercio electrónico y los servicios que involucran múltiples usuarios han traído consigo nuevos riesgos asociados al uso de la información. De igual manera lo ha hecho la proliferación de labores intensivas en almacenamiento, tratamiento, análisis y gestión de datos. Como resultado de las tendencias del mercado y algunos acuerdos internacionales suscritos por Colombia, se ha ido desarrollando el Régimen Colombiano de Protección de Datos Personales ("RCPDP") tan importante para la llegada de empresas internacionales en segmentos como los contact centers y centros de servicios compartidos, por ejemplo.

En la economía bogotana el sector servicios representa más del 60% del PIB. Dentro del grupo de los sectores con mayor potencial de atracción de inversión extranjera directa en la ciudad se encuentran algunos que en el desarrollo de su actividad productiva manejan grandes volúmenes de datos e información: servicios de TI, tercerización de procesos de negocio (BPO por sus siglas en inglés) y servicios empresariales y de consultoría.

- Hemos destinado esta edición del Boletín de Entorno de Negocios a la presentación de los parámetros básicos de la protección de datos en Colombia, las implicaciones de la transferencia internacional de datos, los requisitos para el tratamiento de datos en las empresas y algunas conclusiones y recomendaciones.

Agradecemos de manera especial a los expertos en protección de datos del área de servicios legales de EY Colombia y la Superintendencia de Industria y Comercio por sus comentarios y aportes a este Boletín.

2. ABECÉ DE LA PROTECCIÓN DE DATOS EN COLOMBIA*

En Colombia se reconoce el derecho de todos los ciudadanos de conocer, actualizar, rectificar y eliminar la información que ellos han suministrado a terceros y que se ha incorporado en bases de datos públicas o privadas.

Cada vez que una empresa recibe datos de una persona residente en Colombia, a través del ingreso de dichos datos a la página de internet o al adquirir un servicio o producto que esa empresa vende, es común que se les solicite entregar información personal, como nombre, número de identificación, fecha de nacimiento, lugar de domicilio, dirección de correo electrónico, entre otros.

Esta información consiste en datos personales que deben sujetarse al Régimen de Protección de Datos Personales del Régimen General de Protección de Datos establecido en la *Ley 1266 de 2008*, *Ley 1581 de 2012*, el *Decreto 1074 de 2015*** y el Título V de la Circular única expedida por la Superintendencia de Industria y Comercio.

A continuación, encuentre la información básica para cumplir debidamente con un tratamiento de datos que no viole los derechos de sus clientes o usuarios.

¿En qué consiste el derecho de habeas data?

La Constitución Política de Colombia reconoce el derecho de Habeas Data como aquel que tiene toda persona de **conocer, actualizar, rectificar y eliminar** la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

La Corte Constitucional Colombiana*** lo definió como el derecho que otorga la facultad al titular de datos personales de exigir a las administradoras de esos datos el acceso, inclusión, exclusión,

* Esta guía tomó como base el trabajo previo adelantado por la Oficina de Protección de Datos de la Superintendencia de Industria y Comercio en los siguientes documentos/cartillas de orientación: **(i)** *Protección de Datos Personales: Aspectos Prácticos sobre el Derecho de Hábeas Data*; **(ii)** *Compendio Protección de Datos Personales*; **(iii)** *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability).*

** Capítulos 25, 26,27 y 28 el decreto 1074 de 2015.

*** Corte Constitucional, Sentencia de Constitucionalidad No. 748 de 2011.

corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información.

Es importante resaltar que la Corte Constitucional ha definido como presupuesto esencial para la legitimidad del proceso de administración de datos personales, el consentimiento previo, expreso e informado del ciudadano al permitir recolectar y tratar sus datos privados por un tercero.

¿Qué es un dato personal?

El dato personal en el Régimen General de Protección de Datos (RGDP) se refiere a cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural. En Colombia, los datos personales pueden ser clasificados en públicos semiprivados o privados, así:

- **Datos Públicos**

Son los datos que le interesan al público en general. Por ejemplo: documentos públicos, sentencias judiciales, estado civil de las personas, número de cédula.

- **Datos semiprivados.**

Aunque tienen un carácter privado, sólo le interesan al titular y a un grupo determinado de personas, y sólo pueden ser tratados mediante una autorización. El ejemplo típico son las historias crediticias que administran las centrales de riesgo.

- Datos privados:

Su característica principal es que pertenecen e interesan única y exclusivamente a la persona titular de la información; consisten, por ejemplo, en información relacionada con intereses personales, fotografías, datos de salud, mensajes de voz, entre otros. Estos datos sólo pueden ser tratados con consentimiento previo, expreso e informado del titular.

¿Cuál es el ámbito de aplicación de la ley frente a los datos personales?

A todo tratamiento de datos personales se le aplica la ley de habeas data. Para poder realizar un tratamiento de datos es obligatorio contar con el consentimiento previo del titular de los datos y expresar claramente el uso y la finalidad de ese dato. Los únicos datos que pueden ser tratados sin consentimiento previo son los datos públicos. En principio toda información personal puede ser recolectada por terceros siempre y cuando el titular de los datos haya autorizado expresamente su entrega y tratamiento.

Sujetos que intervienen en el tratamiento de la información*

Titular de la información. Persona natural a quien hacer referencia la información que reposa en una base de datos. Ejemplo: Un usuario que celebró el contrato de prestación de servicio de comunicaciones.

Responsable de la información. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el tratamiento de los datos.

Encargado del tratamiento. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza tratamiento de datos personales por cuenta del responsable del tratamiento.

* Artículo 3 Ley 1581 de 2012.

¿Cuáles son las sanciones sujetas al incumplimiento del Régimen General de Protección de Datos?*

De acuerdo con la ley colombiana, la Superintendencia de Industria y Comercio podrá imponer a los responsables del tratamiento y encargados del tratamiento las siguientes sanciones:

a. Multas de carácter personal e institucional hasta por el equivalente de dos mil (2000) salarios mínimos mensuales legales vigentes (COP 1.562.484.000,00, para 2018) al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b. Suspensión de las actividades relacionadas con el tratamiento de datos hasta por un término de seis (6) meses.

c. Cierre temporal de las operaciones relacionadas con el tratamiento de datos.

d. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

* Artículo 23 Ley 1581 de 2012.

3. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Para la ley colombiana, la circulación internacional de información personal, su recopilación y tratamiento, son necesarios para el funcionamiento de las sociedades modernas y la construcción de relaciones comerciales y personales. Lo anterior se cumple, siempre y cuando esas transferencias de datos protejan los derechos fundamentales de los titulares de los datos. Es por ello que, en Colombia, la transferencia internacional de datos personales de cualquier tipo a países que no garanticen un nivel adecuado de protección de los mismos es prohibida, salvo excepciones expresas que se encuentran en la Ley 1581 de 2012.

De acuerdo con la SIC, los siguientes países garantizan un nivel adecuado de protección de datos:

- Alemania
- Chipre
- Eslovaquia
- Estados Unidos de América
- Hungría
- Letonia
- México
- Polonia
- República Corea
- Austria
- Costa Rica
- Eslovenia
- Finlandia
- Irlanda
- Lituania
- Noruega
- Portugal
- Rumania
- Bélgica
- Croacia
- Estonia
- Francia
- Islandia
- Luxemburgo
- Países Bajos
- Reino Unido
- Serbia
- Bulgaria
- Dinamarca
- España
- Grecia
- Italia
- Malta
- Perú
- República Checa
- Suecia

* Países que han sido declarados con nivel adecuado de protección por la Comisión Europea

Para poder transferir datos personales a los países con niveles no adecuados de protección de datos, la legislación establece los siguientes casos como excepciones:

a. Transferencia de información, con autorización expresa e inequívoca por parte del titular para la transferencia.

b. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular, por razones de salud o higiene pública.

4. ¿CÓMO TRATAR LA INFORMACIÓN RECOLECTADA EN SU EMPRESA?

El Régimen Colombiano de Protección de Datos Personales ("RCPDP") regula el tratamiento de la información personal durante el ciclo de vida de los datos y, por lo tanto, es aplicable a la recolección, uso, almacenamiento, circulación y/o supresión de los datos personales por parte del responsable.

Este tratamiento debe obedecer a una finalidad específica dada a conocer de manera clara al titular de los datos, a través de la política de tratamiento de datos personales, o mediante la implementación de avisos de privacidad. Así mismo, los usos dados a la información personal deberán ceñirse, en todo momento, a lo que se encuentre delimitado en estos instrumentos.

De acuerdo al área de servicios legales de EY Colombia, desde el punto de vista legal, las obligaciones del RCPDP que resultan aplicables a cada una de las etapas del tratamiento de la información personal, son:

Recolección

Cualquier recolección de datos personales que no cuente con la autorización previa, expresa e informada de sus titulares es ilegítima, y dará lugar a la imposición de sanciones por parte de la Superintendencia de Industria y Comercio ("SIC"). La autorización adquiere una relevancia especial cuando se trata de datos personales susceptibles de ser clasificados como datos sensibles por estar ligados con la intimidad de las personas, caso en el cual se deberá advertir al titular que los datos son sensibles y, por lo tanto, no están en la obligación de autorizar su tratamiento.

La autorización puede ser obtenida por cualquier medio, a más tardar al momento de la recolección de los datos personales objeto de tratamiento y, de acuerdo con lo dispuesto por la Ley 1581 de 2012, debe incluir una mención detallada de cada una de las finalidades para las cuales se está obteniendo la información; de tal forma que no haya lugar a dudas acerca de la voluntad del titular para que sus datos fueran recolectados.

c. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

d. Transferencias acordadas en el marco de tratados internacionales en los que la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

e. Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular.

f. Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, la Ley facultó a la Superintendencia de Industria y Comercio para pronunciarse sobre las trasferencias internacionales de datos mediante una Declaración de Conformidad (Art. 26 Ley 1581 de 2012).

Declaración de Conformidad

- Documento que certifica que la finalidad de la exportación de la base de datos que contiene información personal cumple con una política conforme a la ley de protección de datos colombiana. Así mismo, entre otros requerimientos, la declaración de conformidad certifica que el usuario en el extranjero receptor de los datos cumple con los estándares mínimos sobre el tratamiento de datos, en especial sobre la seguridad de la información y confidencialidad requerida por la Superintendencia de Industria y Comercio.

Para solicitar la Declaración de Conformidad sobre las transferencias internacionales de información personal, el interesado deberá radicar una petición ante la Superintendencia de Industria y Comercio.

Haga clic aquí **para mayor información.**

La Ley 1581 de 2012 consagra algunas excepciones en las cuales es viable la recolección y el tratamiento de datos personales sin que medie la autorización del titular. Así, si los datos son requeridos en virtud de un procedimiento judicial o administrativo, son datos de naturaleza pública o son necesarios para atender una emergencia sanitaria o médica, entre otras, el responsable del tratamiento podrá omitir el procedimiento de verificación de la autorización por parte del titular para acceder y tratar sus datos.

Uso, circulación y almacenamiento

Una vez los datos personales han sido recolectados, los responsables del tratamiento deben garantizar a los titulares el pleno, oportuno y efectivo ejercicio de sus derechos en relación con su información personal. Para ello deben tener implementada una Política para el Tratamiento de la Información que contenga, como mínimo, la siguiente información:

I. Los datos de identificación del responsable del tratamiento (nombre o razón social, domicilio, dirección, correo electrónico y teléfono).

II. El tratamiento al cual serán sometidos los datos y la finalidad del mismo, la cual debe coincidir, con las finalidades detalladas en la autorización otorgada por el titular de los datos.

III. La enunciación taxativa de los derechos que le asisten al Titular, tales como el derecho a actualizar y rectificar sus datos; el derecho a solicitar prueba de la autorización otorgada y la facultad del titular de presentar quejas ante la Superintendencia de Industria y Comercio por el tratamiento inadecuado de sus datos personales.

IV. La identificación de la 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, o revocar la autorización.

V. El procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

VI. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Asímismo, los responsables del tratamiento deben garantizar a los titulares lo siguiente:

I. Que los datos personales objeto de tratamiento son veraces, completos, exactos, comprobables, comprensibles y están actualizados. La actualizacion de los datos personales puede ser realizada por solicitud de los titulares del dato personal, por lo cual es importante que se les permita a los titulares conocer la información que sobre ellos reposa en las bases de datos y el tratamiento que se le está dando a ésta.

II. Que el tratamiento de datos personales es realizado por personas autorizadas por el titular del dato personal. Esta garantía se vuelve particularmente importante cuando el responsable del tratamiento realiza transmisión o transferencia de datos personales a terceros.

III. Que los datos personales no se encuentran disponibles en internet u otros medios de divulgación o comunicación masiva, y son conservados bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

IV. Que, en caso de que existan reclamos por parte de los titulares, se proceda con el registro en las bases de datos de la leyenda "reclamo en trámite". Así mismo, en caso en que exista algún proceso judicial sobre algún dato personal notificado a la empresa, esta debará proceder a insertar en las bases de datos que contengan el dato, la leyenda "**información en discusión judicial**".

V. Que se abstiene de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la SIC.

ELIMINACIÓN

Finalmente, una vez el dato personal ha cumplido la finalidad para la cual fue recolectado, los responsables de la información deben, en aplicación del principio de finalidad, eliminarlo.

No obstante, entendiendo la necesidad de algunos responsables de conservar alguna información de terceros para llevar a cabo, entre otros, análisis estadísticos, operativos, comerciales y/o estratégicos, es completamente válido optar por la despersonalización de los datos, desvinculándolos de cualquier persona determinada, de tal forma que puedan seguir siendo usados por parte del responsable.

5. CONCLUSIONES Y RECOMENDACIONES

Para aprovechar el potencial de la economía digital en el actual contexto de globalización, cobra alta relevancia contar con reglas del juego claras para la protección del derecho a la privacidad de los datos de las personas para mantener la confianza entre el consumidor y el sector productivo.

Con la introducción del RCPDP, el tratamiento de datos personales se convirtió en un tema regulado y cualquier anomalía en el cumplimiento de las normas vigentes, deriva en fuertes sanciones económicas e, incluso, puede implicar la suspensión o el cierre de las operaciones comerciales del responsable del tratamiento que incumpla los deberes del RPDP. Desde la entrada en vigencia de la ley 1581 de 2012 y hasta mayo de 2017, la SIC ha impuesto sanciones por más de COP 4200 millones y el valor promedio de una multa ronda los COP 128 millones.

Para el cumplimiento de las obligaciones del Régimen de Protección de Datos Personales, el área de servicios legales de EY recomienda a las organizaciones, como mínimo, lo siguiente:

- Diseñar e implementar procedimientos de gobierno corporativo que den cumplimiento a los requisitos mínimos del RPDP.

- Definir y aplicar mecanismos que les permitan obtener, conservar y, sobretodo, probar que han obtenido los datos personales de manera idónea y que los han tratado conforme a las autorizaciones obtenidas.

- Robustecer sus procesos internos para evitar el uso inadecuado de los datos personales de todos sus grupos de interés (i.e.: empleados, clientes, proveedores, etc.).

- Adoptar medidas que les permitan argumentar un nivel de diligencia aceptable frente al estándar introducido por el denominado "principio de responsabilidad demostrada" aplicado por la SIC. En virtud de este principio se le da libertad a los responsables del tratamiento para regular sus propios procedimientos, siempre y cuando tengan la intención de obrar diligentemente en el tratamiento y la protección de los datos personales.

- Implementar procedimientos para eliminar los datos personales almacenados una vez estos hayan sido utilizados para la finalidad para la cual fueron recolectados.

- Realizar campañas y capacitaciones internas para promover el tratamiento adecuado, durante todo el ciclo de vida del dato, de los datos personales tratados por la organización.

- Designar y entrenar a una persona o área encargada de la atención de reclamaciones en materia de protección de datos personales, así como establecer canales de atención para atender a los titulares de los datos personales.

- Cuando se detecten riesgos en la administración y gestión de los datos personales, informar oportunamente a la SIC acerca de los incidentes que involucren una violación a los códigos de seguridad de la organización.

- Implementar las medidas de seguridad necesarias para salvaguardar la información de los menores de edad, observando los más altos estándares de seguridad.

- Documentar contractualmente, de la forma más adecuada para cada caso y respecto de cada grupo de interés, los términos y condiciones que regirán el tratamiento de los datos personales involucrados en cada relación comercial para (i) ajustarlos a los lineamientos adoptados por la organización y (ii) cumplir con los estándares establecidos por el RCPDP.

- Revisar los procesos de recolección de datos e implementar los avisos de privacidad necesarios para cada uno, de tal forma que siempre medie una autorización clara, expresa e informada del titular frente al tratamiento de sus datos personales, especialmente cuando se trate de datos sensibles como la información biométrica de las personas que se obtiene en las zonas de video-vigilancia ubicadas en las instalaciones de las organizaciones.

- Dar cumplimiento al Decreto 090 del 18 de enero 2018 donde se obliga a todas las empresas y sociedades sin ánimo de lucro que tengan activos totales superiores a $3.315.600.000 COP a registrar sus bases de datos en el Registro Nacional de Bases de Datos.

Los plazos para el registro son los siguientes:

- Las sociedades y entidades sin ánimo de lucro cuyos activos totales sean superiores a $20.225.160.000 COP a más tardar el 30 de septiembre de 2018.
- Las sociedades y entidades sin ánimo de lucro cuyos activos totales sean superiores $3.315.600.000 COP hasta $20.225.160.000 COP a más tardar el 30 de noviembre de 2018.

Las instrucciones para el registro de su base de datos en el Registro Nacional de Base de Datos se encuentran en la Circular Externa No. 001 del 2016.

El manual de ayuda para realizar esa operación lo puede encontrar *haciendo clic acá.*

Finalmente, es recomendable que las organizaciones vayan más allá de la simple adopción de una política de tratamiento de datos personales e implementen esquemas de reporte periódico de información relevante a sus organismos de gobierno corporativo, realicen procesos internos de auditoría para identificar potenciales fallas, diseñen planes de acción encaminados a optimizar su cumplimiento del RPDP e, incluso, busquen una articulación funcional entre sus procedimientos de tratamiento y aquellos que han sido adoptados por sus proveedores, revisando los términos y condiciones que rigen sus relaciones contractuales, para incluir obligaciones adecuadas para el tratamiento de datos personales.

Cualquier duda o pregunta sobre protección de datos personales o cualquier otro tema no dude contactar a Invest in Bogota, su aliado para hacer negocios en Bogotá.

Referencias

- Corredor Castellanos, G.R. (Diciembre 2015). Consolidación de la economía digital y desafíos en materia de protección de la privacidad. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 14. Universidad de los Andes (Colombia)
- *Compendio Protección de Datos Personales* – Dirección de Protección de Datos, Superintendencia de Industria y Comercio.
- *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)* - Dirección de Protección de Datos, Superintendencia de Industria y Comercio.
- *Protección de Datos Personales: Aspectos Prácticos sobre el Derecho de Hábeas Data* - Dirección de Protección de Datos, Superintendencia de Industria y Comercio.
- *Manual de usuario del Registro Nacional de Bases de Datos* – RNBD - Dirección de Protección de Datos, Superintendencia de Industria y Comercio.

Normatividad

- *Ley 1266 de 2008*
- *Ley 1581 de 2012*
- *Decreto 1377 de 2013*
- *Decreto 1074 de 2015*
- *Decreto 090 de 2018*
- *Sentencia C-748 de 2011*
- *Circular No. 001 de 2016 de Superintendencia de Industria y Comercio.*

ACTUALIDAD
DEL ENTORNO DE NEGOCIOS

Protección de datos y empresas en Colombia

Número 12
2018

www.investinbogota.org

Invest in Bogotá