

ABC

PARA PROTEGER LOS DATOS PERSONALES

LEY 1581 DE 2012

DECRETO 1377 DE 2013

Bogotá, 2013

ABC PARA PROTEGER LOS DATOS PERSONALES

Certicámara S.A., entidad de certificación digital experta en seguridad de la información y en promover la protección de los datos personales, presenta este documento que contribuirá a entender los aspectos más relevantes de la Ley 1581 de 2012 y del Decreto 1377 de 2013.

Los antecedentes normativos

La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C – 748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada.

Como Ley Estatutaria (ley de especial jerarquía), tiene como fin esencial salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección. La Jurisprudencia Constitucional trató desde el inicio el derecho al hábeas data como una garantía del derecho a la intimidad, de allí que se hablaba de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. Actualmente el hábeas data es un derecho autónomo, compuesto por la autodeterminación informática y la libertad (incluida la libertad económica). Este derecho como fundamental autónomo, requiere para su efectiva protección mecanismos que lo garanticen, los cuales no sólo han de depender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tengan la capacidad de fijar políticas públicas en la materia, sin injerencias de carácter político para el cumplimiento de esas decisiones.



Dentro de los contenidos mínimos que se desprenden del derecho de hábeas data se encuentra que las personas tienen la facultad de conocer – acceso – la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las mismas donde se encuentra dicha información; tienen además, el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; derecho a que la información contenida en bases de datos sea rectificadas o corregidas, de tal manera que concuerde con la realidad; derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular – salvo las excepciones previstas en la normativa –.

La Ley obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas, como entidad responsable del tratamiento (persona natural o

jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos) deben definir los fines y medios esenciales para el tratamiento de los datos de los usuarios y/o titulares, incluidos quienes fungen como fuente y usuario, y los deberes que se le adscriben responden a los principios de la administración de datos y a los derechos –intimidad y hábeas data – del titular del dato personal.

Luego de presentar los antecedentes jurídicos, es clave entender que la información hoy en día es el activo más importante que se utiliza en todas las actividades cotidianas, como podemos evidenciar, el flujo de información se ha multiplicado en los últimos años llevando a un crecimiento acelerado del mismo, lo que implica que a mayor información circulando por el mundo globalizado en que nos encontramos se deben proteger velozmente los datos personales.

Obligaciones particulares a partir del Decreto 1377 del 27 de junio de 2013:

El Decreto tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros:

- 1). El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).
- 2). Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.
- 3). Determinación de canal electrónico y físico para recibir las autorizaciones.
- 4). Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).
- 5). Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión.

Para datos recolectados a partir de la expedición del Decreto 1377 se necesita:

- 1). Aviso de Privacidad (que se puede hacer estratégicamente en el mismo formato de autorización de la captura).
- 2). Definir o crear un área o sujeto responsable de la protección de la información personal, según el tamaño empresarial del cliente (es decir aquí opera el criterio de responsabilidad demostrada consagrado en los arts. 26 y 27 del Decreto 1377).
- 3). Establecer cláusulas para transmisiones y transferencias de datos (si estas aplican).
- 4). Definir o conocer cuáles son los grupos de interés del cliente.
- 5). Definir las finalidades y los tratamientos genéricos en cada grupo de interés, pues esto se debe indicar en la política de tratamiento y en el formato de autorización.

En este documento a continuación se explicarán algunos aspectos relacionados con la protección de datos, y sobre cómo tener buenas prácticas en torno al manejo de la información para evitar sanciones a

los encargados y responsables del tratamiento de las bases de datos. Lo anterior es posible de lograr teniendo claras las siguientes definiciones:

¿Qué son los datos personales?

Es cualquier información concerniente a personas físicas, que tenga carácter de privado, que esté ligada a su intimidad y que toque temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros.

¿Cuál es la importancia de los datos personales?

Su importancia radica en que la información personal puede ser utilizada para varios fines, como la comercialización, la vida laboral, e incluso para cometer delitos, ya que su identidad puede ser suplantada si es que se tiene acceso a la información adecuada.



¿En qué consiste la protección de datos?

Son todas las medidas que se toman, tanto a nivel técnico como jurídico, para garantizar que la información de los usuarios de una compañía, entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas.

¿Qué medidas se deben tomar para una efectiva protección de datos?

Las medidas que se deben adoptar frente a la protección de datos dependen de la posición que se ocupe frente a la información, ya que puede estar a cargo de una persona física titular de la información; por otro lado, puede ser una persona natural o jurídica como encargada del tratamiento de datos y/o responsable del mismo.

¿Quién es el titular de la información?

Es la persona física cuyos datos son objeto de tratamiento.

Si usted es titular de la información debe:

- ✓ Tener claridad de dónde se encuentran sus datos personales actualmente
- ✓ Saber quién custodia sus datos personales
- ✓ Conocer qué personas tienen acceso a su información personal
- ✓ Conocer los mecanismos legales con que puede defender sus derechos de información ante las entidades ya sean públicas o privadas
- ✓ Identificar sus bases de datos
- ✓ Entender que su información constituye un derecho y sobre ella usted tiene el poder de decidir, quién la tiene, en qué condiciones la tiene y hasta cuándo la tiene.

¿Quién es el responsable del tratamiento?

Es la persona natural o jurídica que decide sobre la base de datos o el tratamiento de datos, ya sea por sí sola o en sociedad con otros.

Importante: si su empresa, realiza actividades como responsable del tratamiento de datos personales debe acondicionar e implementar los siguientes mecanismos:

- ✓ El aviso de privacidad.



- ✓ El procedimiento para obtener la autorización del titular previo al inicio del tratamiento.
- ✓ Herramientas que garanticen condiciones de seguridad adecuadas para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información.
- ✓ Medidas tecnológicas para proteger los datos personales y sensibles.
- ✓ Manual interno de políticas y procedimientos para cumplir con la Ley sobre protección de datos.
- ✓ Elaborar las políticas del tratamiento de la información y suministrarlas al registro nacional de bases de datos, el cual está a cargo de la Superintendencia de Industria y Comercio.

¿En qué consisten las sanciones? Las sanciones para los encargados y los responsables del tratamiento de datos personales que pueden ser la misma persona natural o jurídica de naturaleza privada, están en cabeza de la Superintendencia de Industria y Comercio, y van desde:

- ✓ Multas de carácter personal o institucional hasta por 2.000 Salarios Mínimos Mensuales Legales Vigentes.
- ✓ Suspensión de las actividades relacionadas con el tratamiento hasta por seis meses.
- ✓ Cierre temporal de las operaciones relacionadas con el tratamiento.
- ✓ Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos.

Para tener en cuenta: la Ley 1581 del 17 de Octubre de 2012, en su artículo 28 estableció un plazo de 6 meses para la implementación y adaptación de políticas por parte de las empresas que hagan las veces de encargados y/o responsables del tratamiento de datos.

Es el momento de comenzar con la cultura de protección de datos personales, pues la información es un derecho que debe ser protegido.

CERTICÁMARA tiene la posibilidad de ofrecer una consultoría integral para dar cumplimiento a la Ley 1581 de 2012 y al Decreto 1377 de 2013. **Cada sector empresarial tiene unas características especiales en el momento de implementar la Ley.**

CONTÁCTENOS:

Bogotá: Dirección: Carrera 7 No. 26-20 Piso 18. Edificio Seguros Tequendama /
Teléfono: (1) 3790300 / Fax: 7442727 Opción 8. Línea Soporte Bogotá: 7442727.

Línea Gratuita Nacional: 018000181531.

Email: comercial@certicamara.com. Web: www.certicamara.com



consultoría