PROTECDATA
COLOMBIA

POLÌTICAS INTERNAS EN MATERIA DE PROTECCIÒN DE DATOS PERSONALES

En Colombia, el marco legal en Protección de Datos Personales se desarrolló jurisprudencialmente partir de la Constitución del año 1991, con observancia en los principios de legalidad, libertad, finalidad, necesidad, veracidad, utilidad, circulación restringida, incorporación, caducidad, individualidad, confidencialidad y seguridad propios de la información que se almacenaba en bases de datos públicas o privadas. Todos ellos, enfocados en la adecuada recolección, almacenamiento y uso de datos personales que realizaran los responsables del tratamiento o los encargados del mismo. Lo cual, constituye un valioso aporte de la Corte Constitucional que derivo en el proyecto de ley que finalmente surtió el respectivo trámite legislativo dando origen al marco legal en Protección de Datos personales.

El fundamento legal para el tratamiento de datos personales se encuentra entonces en el Artículo 15 Constitución Política de 1991, en el que se reconoció por primera vez el derecho de *habeas data*. Precepto constitucional que fue desarrollado en principio en la Ley Estatutaria 1266 de 2008, ley de carácter sectorial que regula el sector financiero. Posteriormente, se expidió la Ley 1581 de 2012, mediante la cual se regula el derecho fundamental de *habeas data* con la finalidad de proteger los datos personales registrados en cualquier base de datos donde se realicen operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y/o privada. Ley que fue parcialmente reglamentada parcialmente mediante Decreto 1377 de 2013 y Decreto 886 de 2014.

En el año 2012, en virtud de la expedición de la Ley 1581, Colombia es considerada dentro del grupo de países que cumple con estándares internacionales en materia de protección de datos personales. Hecho que sin lugar a dudas implica unas obligaciones y/o deberes que asisten a los Responsables del Tratamiento, dentro de los cuales se resalta la adopción del manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos, tal como lo establece el Literal k) del artículo 17 de la Ley 1581 de 2012, que regula los deberes de los Responsables del Tratamiento.

En este sentido, el artículo 13 del Decreto 1377 de 2013, señala el deber legal de los Responsables del Tratamiento de desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas, siguiendo los siguientes parámetros:

> *"Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:*
>
> *1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.*
>
> *2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.*

3. Derechos que le asisten como Titular.

4. 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 y revocar la autorización.

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

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

Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 5° del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas."

Nótese que las citadas normas expresamente indican unos requisitos mínimos que deben contener las políticas internas de cada organización con la obligación de darlas a conocer a todos sus empleados. Estas políticas deben constar por escrito e incluir los principios que rigen la protección de datos de acuerdo con el artículo 4 Ley 1581 de 2012 y normas que lo desarrollen. Asimismo, deben documentar los procedimientos para el tratamiento, conservación y supresión de los datos personales según el artículo 11 del Decreto 1377 de 2013. No obstante, es importante precisar que éstos requisitos fueron desarrollados en los decretos reglamentarios de la Ley 1581 de 2012 y a través de la GUIA DE RESPONSABILIDAD DEMOSTRADA expedida por la SIC.

En concordancia con lo anterior el artículo 26 del Decreto 1377 de 2013, los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio -SIC-, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y decretos reglamentarios, de acuerdo con los siguientes criterios:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

Se trata de una carga probatoria en cabeza del Responsable del Tratamiento en cumplimiento del principio de responsabilidad demostrada que deberá ajustarse a lo establecido en la guía expedida por la SIC, para el efecto.

Adicionalmente, los Responsables deben estar en capacidad de suministrar una descripción de los procedimientos implementados para la recolección de los datos personales, la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. Así como, aportar evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas, esto es, de acuerdo con el artículo 27 de la misma norma, relacionado con las *Políticas internas efectivas*, que se hayan implementado las medidas acordes con las instrucciones impartidas por la SIC, aplicando los siguientes criterios:

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y decreto 1377 de 2013.

2. La adopción de mecanismos internos para poner en práctica las políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

Es importante tener en cuenta que la aplicación de los anteriores criterios en las medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta por la SIC, al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley.

No se trata entonces, de reproducir las normas en un documento si no de desarrollarlas de acuerdo con los criterios antes mencionados y los que trae la GUIA DE RESPONSABILIDAD DEMOSTRADA, donde se establece la obligación de incorporar políticas de tratamiento de la información de imperativo cumplimiento que establezcan reglas sobre los siguientes puntos:

- ✓ La recolección, uso y divulgación de información personal, incluyendo los requisitos para obtener la autorización de los Titulares.
- ✓ El acceso y corrección de datos personales.
- ✓ La conservación y eliminación de información personal.
- ✓ El uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos.
- ✓ Inclusión en todos los medios contractuales de la empresa de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce a suficiencia la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma responsable.
- ✓ Presentación de quejas, denuncias y reclamos.

Adicional a ello, los sujetos obligados deben igualmente incluir en otras políticas de la organización (vgr. Talento humano, contratos, transparencia, etc.) elementos que permitan cumplir las normas sobre protección de datos personales.

Finalmente, como ya se analizó es de imperativo cumplimiento desarrollar en las políticas internas de cada organización, entre otros aspectos los siguientes: los principios y definiciones; medidas de seguridad y controles administrativos, tecnológicos y físicos; indicar los requisitos para obtener el consentimiento de los titulares; establecer las funciones y obligaciones de las diferentes áreas y del personal con acceso a las bases de datos; mencionar las bases de datos y finalidades, así, como los sistemas de información; indicar el procedimiento de notificación, gestión y respuesta ante incidencias; establecer las medidas de conservación y eliminación de los datos personales almacenados, esto es, medidas para el transporte, destrucción y reutilización de documentos y soportes.