Boletín Sector Público
002- junio 2015

Guía para la implementación del principio de responsabilidad demostrada en el tratamiento de datos personales

La nueva reglamentación de la SIC

Con ocasión a las funciones que le asisten a la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, el 28 de mayo de 2015 se publicó la "Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)", en línea con el artículo 26 y 27 del Decreto 1377 de 2013. Directriz que acoge los planteamientos formulados por la Organización para la Cooperación y el Desarrollo Económico (OCDE), específicamente en lo relativo al Programa Integral de Gestión de Datos Personales.

El principio de responsabilidad demostrada exige que los obligados del régimen de protección de datos adopten medidas apropiadas y efectivas para el cabal cumplimiento de las exigencias de la Ley 1581 de 2012 y decretos reglamentarios. Mecanismos que deben ser acordes con el tamaño y estructura de la organización, que serán sujetos de verificación por la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio en cualquier momento.

En línea con lo anterior, la guía para la implementación del principio de responsabilidad responde a un llamado de la industria que ha solicitado mayor orientación en la creación de un Programa Integral de Gestión de Datos Personales. Por tanto, la misma gira entorno a tres (3) ejes temáticos: (i) el gobierno corporativo; (ii) los controles del sistema de gestión integral de datos

personas y; (iii) la sostenibilidad del programa integral para la gestión de datos personales. Temas que desarrollaremos a continuación:

Gobierno Corporativo

Hace alusión a la formulación de políticas y procedimientos para el tratamiento, que reflejen una cultura de respeto a la protección de los datos personales. Exigiéndose la articulación de los siguientes actores: (i) la alta gerencia, (ii) el oficial de protección de datos personales y (iii) demás empleados de la organización.

El éxito de la implementación de datos personales, tal y como se deja plasmado en la guía para la implementación del principio de responsabilidad demostrada, depende del compromiso de la alta gerencia con el régimen de protección de datos personales. Puesto que la implementación de las obligaciones que lo integran, demandan recursos económicos y de personal que no pueden ser subestimados.

En particular, la guía para la implementación de datos personales considera un nuevo rol dentro de las organizaciones. El Oficial de Protección de Datos Personales, como ha decidido llamársele, será el funcionario responsable dentro de toda compañía de coordinar y conocer todo lo relativo al tratamiento de datos personales. Entre las funciones principales que se le encargan, resaltan las siguientes:

- Impulsar la cultura de protección de datos de dentro de la organización.

- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales, así como las acciones tendientes para su sostenibilidad.

- Inscribir las bases de datos de la organización en el Registro Nación de Bases de Datos y, actualizar la información según las instrucciones que en el futuro imparta la Superintendencia de Industria y Comercio.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que la realice la Superintendencia de Industria y Comercio.

En conclusión, el Oficial de Protección de Datos Personales tendrá el control y la responsabilidad de la implementación transversal del Sistema Integral de Gestión de Datos Personales.

Sistema Integral de Gestión de Datos Personales

Es un programa corporativo basado en controles, que responde al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos. Entendiéndose por “controles” una etapa dentro del sistema de gestión en el que se verifica si los resultados de la implementación se ajustan a las obligaciones del régimen de protección de datos personales y políticas para el tratamiento de la información personal.

En tanto la organización cumpla con todos los controles, se acercará a cumplir con el principio de responsabilidad demostrada. De lo contrario, tendrá que tomar las medidas necesarias que la conduzcan a satisfacer este principio.

En línea con lo expuesto, a continuación describimos de forma general los controles que deberá verificar el Oficial de Protección de Datos Personales para asegurar que las políticas adoptadas por la organización se implementen al interior de la compañía:

- **Procedimientos operacionales:** Consisten en la elaboración de procedimientos que hagan alusión a la recolección y utilización de los datos personales al interior de la compañía. Por tanto, exige la definición de funcionarios, roles y actividades que deberán observarse para cumplir con las actividades propuestas.

- **Inventario de bases de datos con información personal:** La compañía debe establecer un procedimiento que le permita de manera efectiva, identificar la totalidad de los presentes y futuros encargados del tratamiento de la información personal, con el propósito de: (i) diseñar disposiciones contractuales que giren en torno a la confidencialidad y manejo de la información personal; (ii) la forma en la que se realizará el tratamiento de datos personales por el encargado y; (iii) la facultad de verificar en todo momento por el responsable del tratamiento, que el encargado está cumplimiento con las exigencias del régimen de protección de

datos personales y demás obligaciones que se le hubieren señalado contractualmente.

- **Procedimientos asociados a la protección de datos personales:** La organización deberá elaborar procedimientos que tengan relación con: el (i) almacenamiento, uso y circulación de información personal; (ii) supresión y/o disposición de datos personales; (iii) acceso de la información personales; (iv) actualización de la información y/o su corrección y; (v) atención de consultas y reclamos de los titulares de la información.

- **Identificación y administración de riesgos asociados al tratamiento de datos personales:** De conformidad con la estructura organizacional y procedimientos internos para el tratamiento de datos personales, deberá identificarse los riesgos asociados al tratamiento de datos personales con el propósito de evaluar y/o anticipar el incumplimiento de las normas de protección de datos personales.

- **Programas continuos de formación y educación:** En consideración a que el régimen de protección de datos personales es un asunto que exige el conocimiento de todos los niveles de la organización, deberán diseñarse programas de capacitación que tengan por objeto, dar a conocer las obligaciones propias del régimen de protección de datos personales así como las medidas implementadas por la organización en el marco del cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios. Junto con la capacitación de carácter general que la guía para la implementación del principio de responsabilidad demostrada propone, deberá diseñarse capacitaciones complementarias que se encuentren adaptadas a la funciones de cada área o funcionario que realiza el tratamiento de información personal.

- **Protocolos de respuesta en el manejo de violaciones e incidentes:** En materia de seguridad de la información, se estipula la elaboración de protocolos de respuesta que se anticipen a riesgos y/o acciones que conlleven una vulnerabilidad de seguridad. Previéndose junto con lo anterior, mecanismos para rendir informes internos y reportar incidentes de seguridad a titulares de la información, la Superintendencia de Industria y Comercio y la Alta Dirección.

Utilizando los controles expuestos, la organización podrá asegurar que cumple con el principio de responsabilidad demostrada y por tanto, con las obligaciones de la Ley 1581 de 2012 y decretos reglamentarios.

Sostenibilidad del Sistema Integral de Gestión de Datos Personales

El Sistema Integral de Gestión de Datos Personales exige una evaluación y revisión continúa de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión. En consecuencia, el Oficial de Protección de Datos Personales será la persona encargada al interior de la organización de desarrollar un plan de supervisión y revisión anual que tome en cuenta las siguientes etapas:

- **Fase de diagnóstico:** En ella deberá evaluarse en qué estado de cumplimiento se encuentra la organización, acudiéndose, entre otras, a: (i) elaboración de auditorías internas; (ii) debilidades identificadas en la atención de consultas y reclamos y; (iii) Revisión de las tendencias y obligaciones legales que surjan con ocasión a la protección de datos personales.

- **Fase de adecuación:** Consiste en determinar las acciones a implementar por la organización, en aras de hacer más efectivo el Sistema Integral de Gestión de Datos Personales.

- **Fase de implementación:** Previa aprobación de la alta dirección de la organización, efectuar los cambios que resulten pertinentes en los componentes del Sistema Integral de Gestión de Datos Personales. Junto con acciones de capacitación al personal.

- **Fase de revisión:** La guía para la implementación del principio de responsabilidad demostrada exige que la revisión del Sistema Integral de Gestión de Datos Personales sea anual, sin embargo nada impide que en razón a la debida diligencia, la compañía efectué revisiones periódicas de las acciones implementadas.

El Sistema Integral de Gestión de Datos personales demanda labores continuas de supervisión y evaluación, de las cuales dependerá el éxito del mismo al interior de la organización.

Conclusiones

Cuando una organización apuesta por implementar estándares elevados que den muestra de su compromiso por la protección de datos personales, el artículo 27 del Decreto 1377 de 2013 prevé a su favor, que la *"verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un responsable, será tenida en cuenta al momento de evaluar la imposición de sanciones por violaciones a los deberes y obligaciones establecidos en la ley*".

Por tanto, el desarrollo de un Programa Integral para la Gestión de Datos Personales es una herramienta fundamental que da cuenta del compromiso del responsable del tratamiento, al tiempo que es una medida eficaz para evitar cualquier infracción al régimen de datos personales, diferente a una eventual falla que en nada corresponde con debilidades de gestión de los datos personales.

Nuestros servicios

Entendiendo la complejidad que conlleva la elaboración de un Programa Integral para la Gestión de Datos Personales, hemos diseñado una propuesta para nuestros clientes que incluye la elaboración del programa en mención, a partir de un enfoque multidisciplinario. Por tanto ponemos a disposición de nuestros clientes, la experiencia metodológica en el asunto de la referencia. Consistente en el levantamiento detallado de información con el propósito de producción de entregables tales como: (i) manual de políticas y procedimientos de datos personales; (ii) modelos de aviso de privacidad y/o solicitudes de autorización; (iii) modelos de cláusulas contractuales; (iv) lineamientos jurídicos para la elaboración de procedimientos asociados al tratamiento de datos personales e; (v) elaboración de la relación de las bases de datos personales en línea con las exigencias futuras para la inscripción de los repositorios de información en el Registro Nacional de Bases de Datos Personales y demás requerimientos asociados.

Para mayor información no dude en contactarnos:

Mario Andrade Perilla
Socio Tax & Legal
maandrade@deloitte.com
Tel: 5461810 Ext 2022

Daniel E. Ramírez
Senior Manager – Servicios legales
deramireze@deloitte.com
Tel: 5461810 Ext 2028, 2088