



La figura del Oficial de Protección de Datos Personales en el contexto colombiano

Heidy Balanta

Escuela de Privacidad

Gerente Escuela de Privacidad

hb@escueladeprivacidad.com

La legislación colombiana en protección de datos personales no menciona expresamente la figura del Oficial de Protección de datos personales, sin embargo, tácitamente se ha entendido así, debido a las características que la misma ley ha asignado y por el derecho comparado que así cataloga a dicho rol, responsable de hacer cumplir con el programa de protección de datos personales al interior de la Organización.

NORMATIVA

Existen dos artículos del Decreto 1377 de 2013, donde mencionan las características del Oficial de Protección de Datos Personales.

Artículo 23, Decreto 1377 de 2013. "Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto"

Artículo 27, Decreto 1377 de 2013. Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:

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 este decreto.

Conforme a lo anterior, el Decreto establece que puede ser una "persona" o "área" quien puede cumplir o hacer las veces de oficial de protección de datos personales.

También, dicho decreto menciona la necesidad de la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción de las políticas sobre el tratamiento de datos personales, se debe advertir acá, que lo pretendido por el legislador es adecuar la ley a un componente presupuestal y administrativo de la organización, esto significa que, probablemente una organización con un tamaño pequeño no tendrá presupuesto para contratar a una persona encargada de ser oficial de protección de datos personales, pero si puede asignar a una de sus áreas o de los roles que tiene, funciones relativas al rol de Oficial de Protección de Datos Personales. Sin embargo, una organización grande, o que maneje información altamente sensible, o un número ingente de datos personales, aunado con el daño que podría ocasionar la exposición de dichos a sus titulares, irremediablemente se debe sugerir un área o una persona dedicada exclusivamente a cumplir con las funciones de Oficial de Protección de Datos Personales.

DOCTRINA

Ahora, la Superintendencia de Industria y Comercio, si ha reconocida de forma doctrinaria la figura del Oficial de Protección de Datos Personales, en concepto con Radicado: 17-145072-2, manifiesta:

"Por lo anterior, la función del oficial de protección de datos o del área encargada de protección de datos en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta, para cumplir la norma de protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro de la empresa. El oficial de protección de datos personales tendrá la labor de: (i) estructurar, diseñar y administrar el programa que permita a la organización cumplir con las normas sobre protección de datos, (ii) establecer los controles de ese programa, su evaluación y revisión permanente"

La conceptualización anterior, se encuentra también en la Guía de Responsabilidad Demostrada de la SIC, donde a su vez dicho concepto y Guía coinciden en otras obligaciones:

"Ahora bien, las organizaciones para el desarrollo, implementación y seguimiento de un Programa Integral de Gestión de Datos Personales deben garantizar su

eficacia permanente, el cumplimiento y la adherencia a estándares de responsabilidad demostrada. Los responsables deben supervisar, evaluar y revisar su programa para asegurar que siga siendo pertinente y eficaz, para ello el Oficial de Protección de Datos debe desarrollar un plan de supervisión y revisión anual"

Guía de Responsabilidad Demostrada

Otras de las obligaciones que establece la Guía para el Oficial de Protección de Datos Personales, son las siguientes:

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos dentro de la organización
- Mantener un inventario de las bases de datos personales en poder de la Organización y clasificarlas según su tipo
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
- Analizar las responsabilidades de cada cargo de la organizacional, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización
- Integrar las políticas de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc)

- Medir la participación, y calificar el desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.
- Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.
- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la SIC
- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

LA FIGURA DEL OFICIAL DE PROTECCIÓN DE DATOS EN EUROPA

Guidelines on Data Protection Officers ('DPOs') Puede acceder al documento de las recomendaciones en el siguiente enlace: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

A continuación, se relacionan algunas recomendaciones dadas por el Grupo del Artículo 29 sobre las características que debe tener el oficial de Protección de Datos Personales, articuladas con el nuevo reglamento europeo para la protección de datos personales.

Competencias y experiencias

- Debe ser designado sobre la base de cualidades profesionales y, con el conocimiento de la legislación y las prácticas en materia de protección de datos
- Tener todo el conocimiento, relacionado con las operaciones de tratamiento de datos efectuadas
- El nivel requerido de experiencia no está estrictamente definido, pero debe ser proporcional a la sensibilidad, complejidad y cantidad de datos que procesa la organización.

Cualidades profesionales

- Conocer las buenas prácticas en protección de datos personales y tener un conocimiento profundo en materia de legislación de datos personales.

- Tener conocimiento sobre el funcionamiento del sector y de la organización
- Conocer el funcionamiento de los sistemas de información y seguridad de los datos y las necesidades de protección de datos
- Conocer las normas y procedimientos administrativos de la organización.

Aspectos a tener en cuenta para determinar el perfil

- Debido al rol que desempeña, debe fomentar la cultura de protección de datos, debe tener contacto con personal de la organización para implementar los elementos esenciales de un programa de protección de datos personales
- Debe estar involucrado, de manera adecuada y oportuna, en todas las cuestiones relacionadas con la protección de datos
- Es crucial que participe desde el primer momento posible en todas las cuestiones relacionadas con los datos
- Debe Ser considerado como un socio de discusión dentro de la organización
- Revisión de no caer en un conflicto de intereses o de obligaciones

En cuanto a su contratación

- Revisar que no tenga conflicto de intereses con respecto a su función, teniendo como relación si se contrata con exclusividad para la organización o si es un externo con un contrato de prestación de servicios
- Entre más estable es el contrato, existe mayores garantías de la efectividad del puesto.
- No ocupar otro puesto dentro de la organización, diferente al de Oficial de Protección de Datos Personales, debido a la estructura organizativa, esta debe obedecer a que cada cargo deba desempeñar su función específica.

Recomendaciones a tener en cuenta para una adecuada función de Oficial de Protección de Datos Personales

Las siguientes recomendaciones pueden que no apliquen a todas las organizaciones, como se anotó anteriormente influye mucho su estructura administrativa y tamaño, por lo anterior, tenga en cuenta solo las que considere puede ser de su utilidad.

- Debe establecer en la política o en el manual el área o persona que hará las veces de oficial de protección de datos personales. Esta política y manual debe estar aprobado por el órgano directivo o representante legal de la

- organización. También puede ser a través de cualquier documento que sea vinculante, no solo para el área o la persona, sino para toda la organización.
- Ajuste el manual de funciones con un nuevo rol de Oficial de protección de datos personales, estableciendo las obligaciones que tendrá a su cargo.
 - Algunas organizaciones, dada su estructura y tamaño tienen dos tipos de cargos, Jefe Oficial de Protección de Datos Personales, que normalmente es un directivo que tiene una alta posición dentro de la organización y puede dar órdenes y tomar decisiones, pero a la par, puede establecerse un nuevo cargo, como operativo, que sea el que este en el día a día de la implementación del programa y le rinda cuentas a al Oficial Jefe
 - Algunas organizaciones crean un comité, en el cual se distribuyen las funciones de oficial de protección de datos personales, y se establece una secretaría técnica permanente que a veces puede ser el área jurídica o la que la organización considere más pertinente. Estos comités a veces no funcionan por las múltiples ocupaciones que tienen los encargados por áreas, y si su organización es una de aquellas que tiende a incumplir la participación en este tipo de comités, lo mejor es que lo obvie y busque otras alternativas
 - Si bien, no es del resorte de este artículo, los propietarios de la información de la organización (aquellos que tengan que responder por cada base de datos) también deben ajustarse sus contratos, con responsabilidades puntuales en la protección adecuada de la información personal que custodian.
 - La organización puede contratar a una empresa externa para que haga las veces de oficial de protección de datos personales, lo importante es que quede formalizado, haya evidencia y sea vinculante para toda la organización, pues en ocasiones es un dolor de cabeza las instrucciones que imparte el Oficial, debido a que no son tenidas en cuenta por algunas áreas o empleados dentro de la organización.
 - El Oficial debe conocer al derecho y al revés la organización, sus sistemas de información, sistemas de gestión, bases de datos, funciones de los cargos, formas de tratamiento, por lo tanto, debe tener en cuenta la vinculación de una persona nueva, debido a que iniciaría con dicha desventaja, por lo que se le debe dar un tiempo prudencial mientras conoce toda la organización

Por último, el perfil más adecuado es complejo de definirlo, puede ser un híbrido de todo, y tampoco está a la vuelta de la esquina, pero se recomienda que sea, un



ingeniero, abogado, administrador de empresas, o carreras afines, que tenga amplio conocimiento en sistemas de gestión de seguridad de la información, en protección de datos personales, en gestión del riesgo, y en especial, en legislación en protección de datos personales. Es importante que cuente con una alta fibra humana y empatía, pues una de sus actividades, es el permanente contacto con los empleados de la organización lo que requiere una adecuada transmisión de directrices y recomendaciones.