Ya está aquí el reglamento general de protección de datos (RGPD), de la unión europea.

La cifra de infiltración de datos personales es creciente. En México se estima que 87% de las empresas han tenido algún incidente de seguridad de la información y que desde el 2014 los costos anuales generados por ciberdelitos ascendieron a 18 mil millones de dólares, según estimaciones realizadas por diversas firmas de consultoría.

Este contexto ha preocupado a los gobiernos de todo el mundo. Un caso a destacar es el de la Unión Europea, que en abril de 2016 anunció la aprobación del Reglamento General de Protección de Datos de la Unión Europea (GDPR), el cual entrará en vigor en mayo de 2018 Con el objetivo de brindar a las personas un mayor control sobre cómo se utilizan sus datos personales, al mismo tiempo que brindan a las empresas un entorno jurídico simple y sencillo para operar en cuanto a la protección de datos.

¿Por qué es importante para México?

Porque con este reglamento se refuerzan y unifican la protección de datos para todos los individuos dentro de la Unión Europea (UE), además de ocuparse de la exportación de datos personales fuera de esta región. Esta normativa obliga a todas las organizaciones a tomar nuevas medidas en la protección de los datos personales de los consumidores, incluso las empresas mexicanas que se encuentran en negocios con la UE.

En cuanto a las medidas de seguridad que se deben de llevar a cabo para la protección de datos, tanto en México como en la Unión Europea detallan que el controlador de datos debe asumir la responsabilidad de los mismos y adoptar e implementar medidas que garanticen su seguridad y buen resguardo.

Una de las mayores diferencias entre la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el GDPR es la manera en que abordan la cuestión del interés legítimo (concepto indeterminado que responde a las razones que tiene un responsable del tratamiento, para

recoger, almacenar o ceder a terceros los datos de alguien).

Un tema que preocupa a todos aquellos que tienen que lidiar con la privacidad de los datos son las evaluaciones de impacto de protección de datos (DPIAs por sus siglas en inglés). Estas evaluaciones, requeridas por el Reglamento General de Protección de Datos (GDPR), pueden lograrse exitosamente si seguimos estas lecciones:

Saber cuándo realizar un DPIA

Este reglamento requiere de estas evaluaciones en al menos tres escenarios:

Una evaluación sistemática y exhaustiva de los aspectos personales relacionados con las personas físicas

Tramitación a gran escala de las categorías especiales de datos o de los datos personales relacionados con condenas penales e infracciones

Un monitoreo sistemático del área de acceso público a gran escala

Estos no son los únicos casos en los que se requiere una DPIA. Es necesario que cada empresa que implemente un programa GDPR revise sus operaciones de procesamiento de datos en busca de otras amenazas potenciales a los derechos y libertades de las personas de acuerdo al marco legal de derechos humanos de la Convención Europea de Derechos Humanos, la Carta de la Unión Europea y las leyes estatales que cubren los derechos anteriores, los derechos relacionados, el derecho público y las leyes de protección del consumidor.

Menos es más

Muchas de las compañías de la Unión Europea implementan cuestionarios muy largos en sus evaluaciones de impacto de protección de datos, lo cual ha resultado contraproducente, ya que las personas no las terminan. Es importante tener en cuenta que las DPIA deben ser cortas, extendiéndose en líneas adicionales de interrogatorio solo cuando sea necesario, y deben escribirse en un lenguaje cotidiano y no legal.

Comprobar la efectividad y mejorar

Las compañías deben probar los casos prácticos de las evaluaciones de impacto de protección de datos en diferentes niveles (alto, medio y bajo) para así poder gestionar de la mejor manera las cargas de trabajo. Por ejemplo, en los casos de uso de alto impacto requieren un proyecto formal y un análisis multi-semanal, los de impacto medio requieren la revisión de un especialista en privacidad sin necesidad de un proyecto formal,

mientras que aquellos con impacto bajo son, por lo general, candidatos para preguntas frecuentes internas.

El Reglamento General de Protección de Datos requiere que se realicen este tipo de evaluaciones (DPIA) para todo el procesamiento de datos de alto riesgo y, de ser necesario, enviarla a alguna autoridad de protección de datos.

Implementar las DPIA en la primera línea de defensa

Es mejor que el control de las evaluaciones de impacto de protección de datos se libere de la segunda línea de defensa (las varias funciones de supervisión de riesgos, controles y cumplimiento establecidas por la administración) y se integre directamente en el negocio donde se produce el procesamiento de datos para así ser más efectivo.

Sin embargo, las personas de la segunda y tercera línea de defensa en auditoría interna también deben estar capacitados y equipados para servir de respaldo a la primera línea.

Plan para trabajar con software

Las empresas de Estados Unidos que han trabajado con las evaluaciones de impacto de protección de datos sugieren que aquellas organizaciones con operaciones europeas empiecen el primer año a trabajar con hojas de cálculo en su primer año y comenzar a planificar el despliegue de software. Esta implementación en dos fases responde al hecho de poder proteger de forma más exhaustiva a sus empresas contra las quejas de los sujetos de los datos, los litigios y las investigaciones de los reguladores.

Es importante destacar que las leyes y regulaciones pertenecientes a la protección de datos y la privacidad no solo afectan los departamentos de informática, sino que permean la vida diaria de prácticamente de todos los individuos, por lo que es importante protegerlos.

Solicita información de un especialista