GDPR

Cómo cumplir con la nueva Ley de Protección de Datos de la Unión Europea

pwc

Incidentes de seguridad y la conciencia de protección de datos

La reputación repercute en la confianza que tienen las personas sobre las organizaciones. Cada día, distintos eventos ponen a prueba el renombre de las empresas y su capacidad para manejar de forma adecuada uno de los activos más importantes para los consumidores: ***sus datos personales.***

Los incidentes de seguridad de la información, que en los últimos años han afectado incluso a grandes compañías multinacionales, han aumentado la preocupación entre los gobiernos y las sociedades sobre el uso y la protección de los datos personales. A raíz de esos acontecimientos, las personas toman más consciencia sobre la privacidad de sus datos, a quiénes se los proporcionan y con qué fines se usan.

A mediados de mayo del presente año, el Banco de México confirmó que el Sistema de Pagos Electrónicos Interbancarios (SPEI), desarrollado y operado por el banco central, fue objetivo de un supuesto ciberataque en el que se sustrajeron alrededor de 300 millones de pesos (mdp), afectando a diversas instituciones financieras, según reportes de medios.

El pintor inglés ***Benjamin Haydon*** *decía que la reputación contiene tres dificultades:*

la primera consiste en ganar un buen prestigio; la segunda, en conservarlo toda la vida; y la tercera, en preservarlo después de la muerte.

No obstante, la banca no es la única que ha sido víctima de ataques, ya que estas cuestiones tienen un impacto directo sobre las empresas de todos los sectores; un incidente de seguridad tiene repercusiones en el negocio, en investigaciones y en sanciones por parte de las autoridades, así como un impacto negativo en la reputación corporativa.

De acuerdo con la ***Global State of Information Security Survey (GSISS) 2018, de PwC, 72.2% de las empresas a nivel global declaró haber detectado al menos un incidente de seguridad en los últimos 12 meses. En México, la tasa de estos incidentes es mayor que el promedio global (78.6%).***

En abril de 2016, el Parlamento Europeo aprobó la Regulación General de Protección de Datos (GDPR, por sus siglas en inglés); la nueva ordenación es la más importante que se ha hecho en los últimos 20 años en Europa, debido a su alcance global y por la relevancia de las multas y sanciones.

Esta regulación sustituye la Directiva de Protección de Datos de 95/46 de 1995 que, aunque pretendía reunir todas las leyes de los estados miembros en materia de protección de datos, aún dejaba un margen de interpretación de las legislaciones locales. Este hecho y los constantes cambios tecnológicos aumentaron la necesidad de desarrollar GDPR.

La importancia de conocer y cumplir con GDPR

El 25 de mayo de 2018 entró en vigor GDPR en la Unión Europea.

Aunque la Unión Europea (UE) dió un plazo de casi 2 años para prepararse para cumplir con esta regulación, algunas empresas aún enfrentan el reto de saber si están obligadas a alinearse a la nueva regulación, debido a que sus oficinas y centros de datos no se encuentran dentro de la UE. Para responder a lo anterior, es fundamental destacar que GDPR considera como sujetos de cumplimiento a todas las empresas multinacionales que tengan negocios en alguno o varios países de la Unión Europea y procesen y almacenen datos de personas físicas y morales, sin importar que la información esté alojada fuera de estos países.

Por ello, las compañías tienen que estar conscientes de que cumplir con las leyes de protección de datos locales no es suficiente.

De acuerdo con el ***GSISS 2018***, ***14.1%*** de las empresas a nivel global aún ***no han comenzado a prepararse para GDPR***, ***31% inició una evaluación de operaciones*** de acuerdo a los requerimientos de la regulación, mientras que ***24% dijo haberlo completado.***

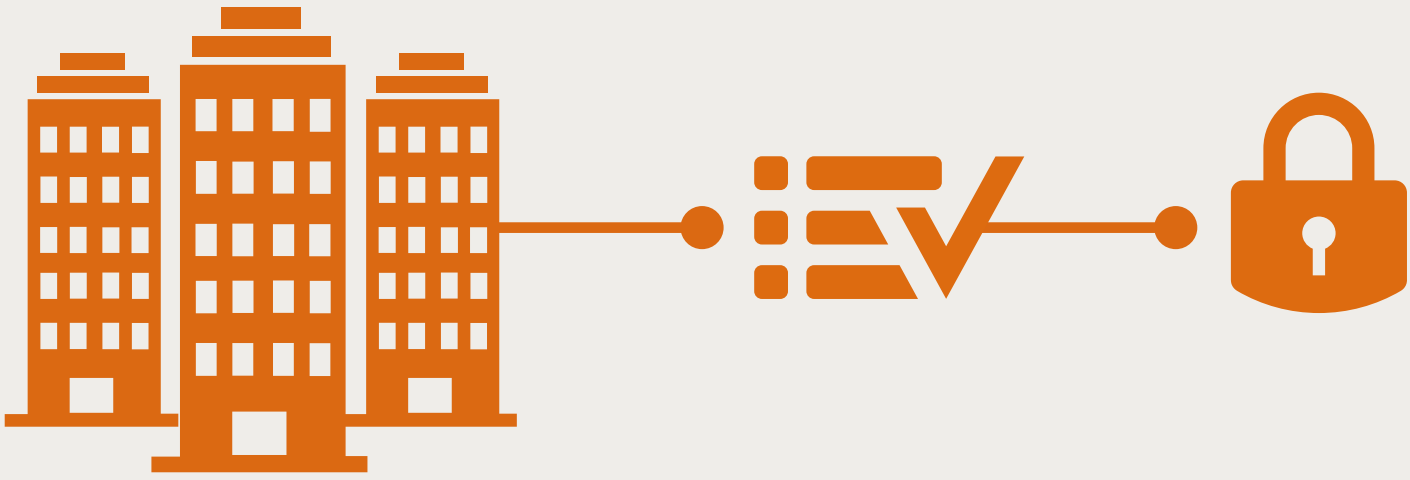
En el caso de ***México***, ***12.4%*** de las empresas entrevistadas aún ***no comenzaban a prepararse para GDPR***, ***41.1% inició una evaluación*** y ***28.5%*** dijo haberla ***terminado***.

Cabe recordar que la Ley Federal de Protección de Datos Personales en Protección de los Particulares (LFPDPPP) entró en vigor desde 2010. Aunque muchas de sus disposiciones vayan en el mismo sentido de lo que establece la GDPR, esta ley no exime a las compañías mexicanas de cumplir con la legislación europea so pena de recibir importantes sanciones.

Sanciones y multas

Las multas y sanciones que contempla GDPR presentan dos características: tienen que ser efectivas, proporcionadas y disuasorias; y tendrán en cuenta la naturaleza, gravedad, duración, intencionalidad o negligencia en la infracción. Las sanciones más importantes que establece la GDPR para las empresas son:

- Multa de 20 millones de euros o el 4% de sus ingresos globales anuales (el monto que sea más alto) por incumplimiento flagrante en los principios básicos de GDPR, relativos al procesamiento, consentimiento, transferencia de datos y violaciones a los derechos de los titulares de los mismos.
- Multa de 10 millones de euros o el 2% de sus ingresos globales anuales (el monto que sea más alto) por infracciones en los controles, procesos, certificación y monitoreo de datos.
- Prohibición temporal o definitiva a una empresa por el procesamiento de datos y el envío de los mismos a un país fuera de la UE, si se concluye que la compañía incumple reglas.
- Acuerdos ilimitados y pagos por daños y perjuicios impuestos por el tribunal a las fallas de control que afectan a los denunciantes



Derechos y libertades en el procesamiento de datos

La regulación europea indica que las actividades de procesamiento de datos personales que hacen las empresas pueden suponer un "alto riesgo" para los derechos y libertades de los residentes de la UE. No solamente se refiere a la privacidad de datos, sino a la libertad de expresión, pensamiento y movimiento; los derechos a la libertad, la conciencia y religión; y la prohibición de la discriminación.

El reporte titulado: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation*, de la UE, enlista 10 escenarios o casos de uso que la comunidad europea considera que tienen factores que contribuyen al procesamiento de datos de "alto riesgo":

1. ***Evaluación de individuos que experimentarían un impacto importante***
2. ***Toma de decisiones automatizada que tendría un efecto legal en los individuos***
3. ***Monitoreo sistemático de individuos***
4. ***Procesamiento de las categorías especiales de usos datos personales de la UE***
5. ***Procesamiento de datos a gran escala***
6. ***Combinación de datos de diferentes fuentes***
7. ***Procesamiento de datos de individuos vulnerables***
8. ***Tecnologías innovadoras como el Internet of Things (IoT)***
9. ***Transferencia de datos personales fuera de Europa***
10. ***Procesamiento de datos que impide que los individuos accedan a servicios o ejerzan un derecho***

Dos de los requisitos de GDPR tienen que ver con que las empresas informen a las Autoridades de Protección de Datos (DPA) de un procesamiento de alto riesgo; y evaluaciones de las notificaciones de violación de datos e impacto de la protección de datos (DPIA).

En lo que respecta a la notificación de violación de datos, las empresas que sufren un ataque a los datos personales de la UE deben notificar a las DPA correspondientes en un periodo de 72 horas después de identificar la infracción. En el caso de las violaciones que representan un "alto riesgo" para los derechos y libertades de los individuos, las empresas deben notificar también a los afectados "sin demora indebida".

En lo referente a las DPIA, las empresas están obligadas a llenar un formato de todo el procesamiento de datos de alto riesgo y notificar a las DPA de los nuevos procesamientos de datos en los que no se pudieron mitigar dichos riesgos.

Las empresas deben hacer una evaluación de su procesamiento de datos para determinar si algún aspecto afecta los derechos y libertades de los usuarios.

¿Qué debe incluir el DPIA?

a) una descripción sistemática de las operaciones de procesamiento previstas, así como del objetivo de las mismas y, cuando proceda, del interés legítimo que persigue la empresa que procesa estos datos;

b) una evaluación de la necesidad y proporcionalidad de las operaciones de procesamiento, en relación con los propósitos;

c) una evaluación de los riesgos a los derechos y libertades de los interesados mencionados en el párrafo 1; y

d) las medidas previstas para abordar los riesgos, incluidas las salvaguardas, las medidas de seguridad y los mecanismos para garantizar la protección de los datos personales y para demostrar su cumplimiento.

El papel del DPO

En el caso de las empresas que manejan grandes cantidades de datos, GDPR pide el nombramiento de un Oficial de Protección de Datos (DPO, por sus siglas en inglés) en las empresas que almacenen grandes cantidades de datos personales, ya sean de empleados o de gente externa a la compañía.

De acuerdo con el Artículo 39 de GDPR, entre las responsabilidades de un DPO están:

- Educar a la empresa y a los empleados sobre los requisitos de cumplimiento
- Capacitar al personal involucrado en el procesamiento de datos
- Realizar auditorías para garantizar el cumplimiento y abordar posibles problemas de forma proactiva
- Servir como punto de contacto entre la empresa y las autoridades supervisoras de GDPR
- Supervisar el rendimiento y proporcionar asesoramiento sobre el impacto de los esfuerzos de protección de datos
- Mantener registros completos de todas las actividades de procesamiento de datos realizadas por la empresa

De acuerdo con la regulación, los DPO reportarán directamente al nivel directivo más alto en la organización y operarán con independencia. Esto puede crear tensión y conflictos de interés en organizaciones multinacionales que ya tienen la figura de Chief Privacy Officer (CPO), quien se encarga de la protección de la información, pero con un enfoque orientado hacia la estrategia del negocio. Por otro lado, el DPO tiene que estar involucrado en todos los asuntos referentes a la protección de datos, desde el diseño de los sistemas de protección de información, participar en las juntas directivas y en el entrenamiento y capacitación del personal.

Conclusión

GDPR puede tener un impacto significativo entre las grandes compañías multinacionales y en cómo cumplirán con la regulación de privacidad de la UE, sin importar el sector en el que se encuentren.

De acuerdo con el GSISS 2018, las empresas multinacionales están tomando varias acciones para aminorar su exposición. ***El 30.6% dijo que están reubicando sus centros de datos dentro de Europa, 28.5% está anonimizando los datos europeos y 26.8% está reduciendo su presencia en la Unión Europea.***

Ahora que la regulación ha entrado en vigor, aumentan las posibilidades de que las autoridades de protección locales (DPA) europeas investiguen las prácticas de privacidad de las compañías.

Derivado de esta relación entre las compañías y las DPA, las multinacionales pueden estar expuestas a los siguientes riesgos:

- Mayor capacidad del regulador para imponer sanciones
- Falta de guías que señalen las prioridades sobre las que las DPAs actuarán y la expectativa de que las empresas ya tengan las capacidades para cumplir con las mismas en mayo
- Recursos restringidos para las DPA, aumentando el riesgo de no tener las suficientes capacidades de atender constantes notificaciones de violaciones de datos y hacer las investigaciones debidas.

Con el fin de administrar mejor dichos riesgos es recomendable:

- Evaluar la relación actual entre la compañía y las DPA de la UE
- Definir y registrar actividades de procesamiento de alto riesgo
- Crear capacidades para detectar y notificar oportunamente violaciones de datos

Es importante que, como primer paso, las empresas confirmen si tienen que cumplir con GDPR. Después, obtener la asesoría adecuada para conducir una evaluación de las actividades que pueden ser de alto riesgo en el procesamiento de datos personales e implementar la estrategia correcta para alinearse con los nuevos requerimientos.

Confiar en que no es necesario cumplir con estas disposiciones de alcance internacional tiene fuertes consecuencias a nivel económico, pero, sobre todo, en la reputación corporativa. Los consumidores están dispuestos a premiar o castigar a las empresas que no tomen las precauciones debidas. Si construir la reputación lleva toda una vida, vale la pena hacer lo necesario para preservarla.

Contactos

Fernando Román
Socio Líder
Cybersecurity & Privacy México
fernando.roman@pwc.com
(55) 5263 5898

Yonathan Parada
Socio
Cybersecurity & Privacy
yonathan.parada@pwc.com
(81) 8881 4106

www.pwc.com/mx

@PwC_Mexico *PwC México* *PwCMx* *pwc.mx* *PwC México* *pwc.mx/click2grow*

En PwC México somos líderes responsables, comprometidos con la comunidad, el cuidado del medio ambiente y nuestra gente, quien vive la diversidad e inclusión como parte de la cultura de PwC.

Elaborado por MPC: 20180521-eh-GDPR-Datos