El impacto de la Regulación General de Protección de Datos (GDPR) en Colombia

Junio 2018

KPMG.com/co

El impacto de la Regulación General de Protección de Datos (GDPR) en Colombia

La Regulación General de Protección de Datos (conocida en inglés como General Data Protection Regulation - GDPR) tiene como objetivos proteger la privacidad de los ciudadanos de la Unión Europea (UE), armonizar las leyes de privacidad de datos en los países miembros de esta región y replantear el enfoque de las organizaciones en el manejo los datos personales de su nómina, clientes y proveedores[1]. Este reglamento, que reemplazó la Directiva 95/46/CE de la UE, entró en vigor desde el 25 de Mayo de 2016, pero es de obligatorio cumplimiento para las organizaciones de la Unión Europea a partir del 25 de mayo de 2018 y ya no será necesario la implementación de legislaciones locales.

1. La Regulación General de Protección de Datos (GDPR) y las organizaciones colombianas

Dentro del contenido tratado en la regulación, uno de los aspectos más relevantes es la aplicación extraterritorial de la norma, la cual incluye a residentes en la Unión Europea (UE), organizaciones que operan dentro de esta región y empresas que a pesar de trabajar fuera de la UE tienen ciudadanos de esta zona dentro de su nómina.

Para el caso de las empresas colombianas, se deben adherir al GDPR aquellas que cumplan con alguna de las siguientes condiciones (independientemente de si existe un establecimiento dentro de la Unión Europea)[2] [3]:

- Ofrecer bienes y servicios en la UE (esta situación afecta especialmente a aquellas compañías que ofrezcan servicios vía web a ciudadanos europeos que deseen acceder a dichos servicios).
- Realizar actividades de tratamiento de datos personales, relacionadas con el control del comportamiento de ciudadanos de la Unión Europea.

Es importante hacer énfasis en que no importa la ubicación de la organización: ésta debe cumplir con lo pactado en la regulación si está realizando algún tratamiento de datos personales sobre ciudadanos que pertenezcan a la UE.

Otro tema que vale la pena mencionar es la forma en que se debe presentar el consentimiento a los titulares de la información para su aprobación: éste debe ser claro y distinguible de otros asuntos, debe ser inteligible, usar un lenguaje comprensible y de acceso tan sencillo para el titular que no debe costarle trabajo tanto el otorgar como el retirar este consentimiento[4].

Ahora, cuando el consentimiento incluye datos de menores de edad, éste debe ser concedido por los padres de familia. La regulación solicita esta condición para menores de 16 años e incluso, los países miembro de la UE pueden reducir el umbral de la edad por medio de una ley[5]. En Colombia, el consentimiento de todo dato (excepto público) será dado por el representante legal del menor mientras se respete el interés de éste y se asegure el respeto de sus derechos fundamentales[6].

2. Aspectos fundamentales de GDPR:

La regulación está compuesta por 99 artículos divididos en 11 capítulos[7]:

- Provisiones generales
- Principios

---

1. Visión general de GDPR. Fuente: https://www.eugdpr.org/
2. Ídem.
3. General Data Protection Regulation. Article 3: Territorial Scope
4. Cambios claves en el GDPR. Fuente: https://www.eugdpr.org/key-changes.html
5. Condiciones aplicables al consentimiento de menores de edad en relación a los servicios de información. Fuente: https://gdpr-info.eu/art-8-gdpr/
6. Artículo 2.2.2.25.2.9 de Decreto 1074 de 2015.
7. Artículos contenidos en GDPR. Fuente: https://www.eugdpr.org/article-summaries.html

- Derechos de los usuarios
- Controladores y procesadores
- Transferencia de datos personales a terceros de organizaciones internacionales
- Autoridades supervisoras independientes
- Cooperación y consistencia
- Remediaciones, responsabilidad y sanciones
- Situaciones de procesamiento de datos específicas
- Actos delegados y de implementación
- Provisiones finales

En el contenido de la regulación, en su artículo 27, se enfatiza en el aspecto de contar con un representante de protección de datos en la UE. Salvo algunas excepciones, las organizaciones que deban atender la regulación deberán tener esta figura designada por escrito cuando el responsable o encargado del tratamiento de datos no resida en esta región. Dicho representante será el encargado de atender las preguntas, quejas, solicitudes y demás consultas de parte de las autoridades de control (Data Protection Authority - DPA) y de los titulares[8].

Asimismo, la regulación establece nuevos derechos para los titulares de los datos tales como[9]:

- Derecho al olvido: El responsable del tratamiento debe borrar los datos personales del titular, dejar de difundir los datos y hacer que terceros dejen de procesarlos.
- Derecho al acceso: Es el derecho que tienen los titulares a obtener confirmación de saber por parte del responsable la forma en que se están tratando los datos personales, a dónde van y con qué propósito. Además, el titular puede recibir una copia de sus datos personales en formato electrónico sin recargos.
- Portabilidad de datos: Es el derecho que un titular posee de recibir los datos personales que le concierne en formato legible y tiene el derecho de transmitirlos a otro responsable.

Otros elementos clave que establece la regulación incluyen:

- Análisis de impacto de privacidad, el cual toma gran importancia con el fin de garantizar los conceptos de Privacidad por diseño y Privacidad por omisión.
- Las brechas o violaciones a la privacidad de los datos deben reportarse a la autoridad de supervisión dentro de las setenta y dos (72) horas posteriores al descubrimiento de la brecha. Se espera que la organización cuente con la estructura necesaria para responder en los tiempos estipulados. Si la notificación no se realiza dentro del tiempo requerido, debe presentarse una justificación razonada a la autoridad supervisora[10].

3. Consecuencias sobre las organizaciones que no cumplan con la regulación GDPR

El incumplimiento de la regulación por parte de una organización puede llegar a sanciones de hasta veinte (20) millones de euros o el cuatro por ciento (4%) de la facturación anual global del año fiscal anterior. La dimensión de la sanción dependerá, entre otros, de las circunstancias, naturaleza y gravedad de la falla, el número de titulares de los datos que se ven afectados, la medida en que los mismos se ven

8. Representantes de responsables o encargados de tratamiento de datos no establecidos en la UE. Fuente: https://gdpr-info.eu/art-27-gdpr/
9. Cambios claves en el GDPR. Fuente: https://www.eugdpr.org/key-changes.html
10. Notificación de una violación de datos a la entidad supervisora. Fuente: https://gdpr-info.eu/art-33-gdpr/

afectados, las acciones tomadas por el responsable de los datos para mitigar el daño y el nivel de responsabilidad del responsable o el encargado de los datos en la falla, teniendo en cuenta las medidas técnicas y organizacionales implementadas[11].

4. ¿Qué hacer para estar preparado ante los requisitos de la GDPR?

1. Definir la estrategia para privacidad y protección de datos personales.

Esto incluye considerar elementos como:

- ¿Cuál es el apetito de riesgo de la organización?
- ¿Cuáles aspectos de la regulación son los más críticos para la organización y sus clientes?
- ¿Cuáles son los requerimientos regulatorios comunes entre la legislación local y la GDPR?

2. Realizar un diagnóstico: ¿Dónde se encuentra la organización ahora?

Con el fin de establecer el tamaño de la tarea que se avecina y qué áreas específicas deben abordarse, es clave comprender la madurez del programa de privacidad actual de la organización. Esto requiere un proceso pragmático y enfocado para realmente entender la exposición al riesgo de privacidad que existe en su organización.

3. Tomar acciones, con un enfoque pragmático

KPMG recomienda construir un plan realista que lo ayude a gestionar el riesgo a un nivel consistente con su estrategia de negocios. Esto no significa necesariamente tomar una posición de liderazgo en todos los aspectos, sino una visión clara de los elementos clave.

¿Por dónde comenzar? Esto dependerá del apetito de riesgo, pero a continuación sugerimos algunas áreas en las que puede enfocarse:

- Estructura de gobierno.
- Inventario de bases de datos de información personales de los cuales se es responsable y encargado. Más allá del requerimiento en Colombia de llevar a cabo la inscripción de bases de datos personales en el Registro Nacional de Bases de Datos, el tener claridad de la información que se maneja, su finalidad y el rol de la organización en la misma, le permitirá priorizar y tomar decisiones enfocadas.
- Gestión de riesgo.
- Derechos de los titulares.
- Terceras partes y contratos.
- Gestión de incidentes.
- Entrenamiento y sensibilización.

4. Definir e incorporar en el "día a día" de la organización

En línea con el requerimiento de Responsabilidad Demostrada estipulado en el Decreto 1377 de 2013 en Colombia, cumplir con GDPR se trata de definir, implementar y mantener procesos sostenibles. Esto afecta todas las actividades relacionadas con la información personal de la organización y puede conllevar, por lo tanto, una transformación importante al interior de la misma.

Esto requerirá coordinación en todo el negocio. Es clave entonces obtener la combinación correcta de insumos por parte de legal, tecnologías de información, recursos humanos y mercadeo. No subestime el nivel de esfuerzo: la información personal está en todas partes en su organización.

colombia@kpmg.com.co
www.kpmg.com/co
T:+57 618 8000


KPMG en Colombia


KPMG en Colombia


KPMG_CO


KPMG en Colombia


@KPMGenColombia