

Boletín Informativo Telecomunicaciones & Tecnología Regional

Mayo 2018

ENTRADA EN VIGENCIA DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES (GDPR)

El GDPR, que entra en vigencia el 25 de Mayo del 2018, regula una nueva forma de proceder en el uso de los datos personales, unifica la regulación a todos los países de la Unión Europea y define mecanismos para que esta reglamentación tenga efectos fuera de la UE.

ALCANCE EXTRATERRITORIAL, ¿A QUIENES APLICA?

1. Será aplicable a todos los responsables y encargados del tratamiento de datos personales, establecidos/domiciliados en la UE, sin perjuicio del país en el que efectivamente se lleve a cabo el tratamiento, es decir, donde sean recopilados, almacenados, analizados, transferidos o usados los datos personales.
2. Se aplicará al tratamiento de los datos personales de interesados que residan en la UE, a las empresas que les ofrece bienes o servicios, independientemente de que dicha empresa se encuentre en el territorio de la UE o fuera de éste. Debe existir evidencia del ofrecimiento de los bienes o servicios por lo que el sólo acceso a un sitio web no basta para determinar dicha intención. Sin embargo, hay ciertos aspectos que serán considerados como una forma proactiva de comercialización de bienes o servicios, que hará aplicable la norma.
3. También aplica al tratamiento los datos personales de interesados que residan en la UE, cuando empresas ubicadas fuera de la UE, realicen seguimiento u observación del comportamiento de dichos interesados, es decir, aplicará a aquellas empresas que realicen seguimiento en línea de conductas o ubicación, para ser usadas posteriormente, mediante técnicas de tratamiento de datos personales, en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.
4. Por último, el GDPR aplicará cuando sea de aplicación el Derecho de los Estados miembros de la UE, en virtud del Derecho Internacional Público.

CONCEPTOS PRINCIPALES:

- Registro de procesamiento de datos
- Análisis de riesgo y evaluación de impacto relativa a la protección de datos. (Data Protection Impact Assessment)
- Privacidad y políticas de protección, desde el diseño y por defecto.
- Violación de seguridad de los datos (security breach). Obligación de comunicarla a la autoridad dentro de las 72 horas siguientes, si vulnera derechos o libertades personales, deberá ser en el menor tiempo posible.
- Derechos del titular del dato
- Información y consentimiento

CAMBIOS PRINCIPALES:

- Restricciones en el procesamiento (Derechos de rectificación, acceso, oposición, decisiones individuales automatizadas, portabilidad, supresión de datos.)
- Delegado de protección de datos (evaluación y cumplimiento de políticas.)
- Transferencias internacionales
- Sanciones
- Responsabilidades en el tratamiento
- Extraterritorialidad de la norma

SANCIONES

Debemos estar atentos al comportamiento que tendrán las autoridades de protección de Datos de la UE, en cuanto a los métodos para hacer cumplir las disposiciones, especialmente aquellas que se aplican extraterritorialmente. Sin embargo, mientras eso ocurre, las empresas que luego de este análisis estén bajo la regulación del GDPR, deben reforzar sus políticas de privacidad y sus procedimientos de mitigación de riesgos, entre otros, según sea aplicable.

CONTÁCTENOS:

- Chile: Barros & Errázuriz www.bye.cl
- Colombia: Gómez-Pinzón Abogados www.gomezpinzon.com
- México: Mijares, Angoitia, Cortés y Fuentes. www.macf.com.mx
- Perú: Miranda & Amado www.mafirma.pe