



CIRCULAR INFORMATIVA

29 de septiembre de 2016

PROTECCIÓN DE DATOS

NUEVO REGLAMENTO COMUNITARIO DE PROTECCIÓN DE DATOS

La publicación del nuevo reglamento de protección de datos aplicable a nivel europeo prefigura la que sin duda será la norma de mayor relevancia adoptada en los últimos años en este ámbito tan sensible. Además de consensuar a nivel comunitario las garantías de protección sobre los datos de carácter personal tratados por las empresas, su objetivo principal es reforzar el control de los usuarios sobre su información privada.

Algunas de las principales novedades que impondrá la nueva regulación son las que siguen:

- Responsabilidad activa. Las empresas deberán adoptar medidas que aseguren razonablemente que cumplen con los principios, derechos y garantías que el reglamento establece. Se prevén requerimientos relacionados con: protección de datos desde el diseño; protección de datos por defecto; medidas de seguridad; mantenimiento de un registro de tratamientos; realización de evaluaciones de impacto sobre la protección de datos; nombramiento de un delegado de protección de datos; notificación de violaciones de la seguridad de los datos; y promoción de códigos de conducta y esquemas de certificación.
- Ampliación de los derechos de los interesados. A los derechos de acceso, rectificación y cancelación, se añaden como novedad el derecho al olvido y el derecho de portabilidad. El derecho al olvido se presenta como la consecuencia del derecho de los ciudadanos a solicitar que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos. El derecho de portabilidad implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado pueda solicitar recuperarlos en un formato que le permita su traslado a otro responsable.
- Transferencias internacionales de datos. Tras un largo debate sobre la mejor solución para la transferencia de datos a nivel internacional, el reglamento establece que la autorización de la Agencia Española de Protección de Datos dejará de ser necesaria para transferir datos a terceros países cuando se usen las "cláusulas contractuales

tipo” adoptadas por la Comisión Europea o una autoridad de control, o normas corporativas vinculantes.

- Nuevas obligaciones para los responsables de ficheros. Las entidades que traten datos personales deberán cumplir con nuevos deberes organizativos: designación de un Data Protection Officer (nueva figura dentro de la empresa que centralizará la gestión de la protección de datos y podrá formar parte de la plantilla o desempeñar sus funciones en el marco de un contrato de servicios); registro de las actividades de tratamiento de datos (sistematizará las actividades vinculadas al tratamiento de datos y estará a disposición de las autoridades competentes en caso de que lo soliciten); y notificación de una violación de seguridad en 72 horas al órgano de control, o si es de alto riesgo, al interesado.
- Nuevo sistema de recogida de datos. Los textos legales aplicados por la empresa deberán adaptarse a nuevas obligaciones informativas. En ciertos casos se deberá incluir un consentimiento inequívoco y/o explícito, así como los datos de contacto del delegado de protección de datos, el plazo de conservación de los datos y el derecho a presentar reclamación ante la autoridad de control competente.
- Nuevo régimen sancionador. Se endurecen las sanciones en caso de incumplimiento (se podrán imponer multas de hasta 20 millones de euros o de hasta el 4% del volumen de negocios a nivel mundial del infractor).
- Autoridades competentes. La autoridad de control principal que resultará competente será la del lugar donde el responsable cuente con su establecimiento principal. En grupos de empresa multinacionales radicadas en la Unión Europea, será la que se corresponda con su sede central de operaciones.
- Ventanilla única. Opción mediante la que los responsables establecidos en varios Estados miembros o que estando en un solo Estado miembro y hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE, tengan una única autoridad de protección de datos como interlocutora.
- Evaluación de impacto. Las empresas deberán asumir la responsabilidad de evaluar el grado de riesgo que representa para las personas que sean objeto de tratamiento, debiendo realizar una evaluación de impacto cuando se prevea un alto riesgo para los derechos, libertades e intereses legítimos de las mismas.
- Encargos de tratamiento. Los responsables y encargados del tratamiento estarán obligados a llevar un registro de actividades cuando empleen a un mínimo de 250 personas, o el tratamiento pueda suponer un riesgo para los derechos y libertades del interesado, o se traten categorías especiales de datos o datos relativos a condenas y delitos penales. Los encargados de tratamiento deberán suscribir un contrato de prestación de servicios por cuenta del responsable siguiendo sus instrucciones - deberán ser documentadas- y estarán sujetos a las mismas sanciones que los responsables. Y se introduce la figura de corresponsable del tratamiento cuando existan varios responsables o encargados que determinen los fines y los medios del tratamiento.
- Seudonimización. El nuevo marco normativo introduce el concepto de datos codificados para cuando los datos no puedan atribuirse a un interesado sin recurrir a información adicional, separada y sujeta a medidas de seguridad que garanticen el anonimato del mismo.

Por último, y a modo de conclusión, señalar que la vacatio legis de la nueva norma es de dos años, por lo que no será obligatoria hasta el año 2018. Ello permitirá a las empresas prepararse y adaptarse al cambio de tercio que traerá consigo este nuevo reglamento.

Atentamente,

Rosa Maria Abadie

Directora del DEPARTAMENTO de IP & IT

Para más información puede contactar con el departamento de IP & IT de BELLAVISTA telefónicamente o mediante correo electrónico ip@bellavistalegal.eu