RCD ALERT

Diciembre 2017

PROTECCIÓN DE DATOS Y PRIVACIDAD

CUENTA ATRÁS PARA LA APLICACIÓN DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

RESUMEN

El 25 de mayo de 2018 será de plena aplicación el Reglamento Europeo de Protección de Datos (GDPR). El GDPR amplía las obligaciones y responsabilidad de las empresas y demás entidades que tratan datos personales, en consonancia con la ampliación de los derechos de privacidad de los ciudadanos. Aplica también a empresas de fuera de la Unión Europea que traten datos personales de ciudadanos de la UE, y prevé importantes sanciones para el caso de incumplimiento de los principios básicos de protección de datos (se establecen multas de hasta 10 o 20 millones de euros, o de hasta el 2% o el 4% del volumen de negocio total anual global), subrayando obligaciones de las empresas y entidades como la de prevención y la de responsabilidad proactiva. No debe ser visto como una amenaza, sino como una oportunidad, pero es necesario que todos los operadores se asesoren adecuadamente a fin de implementar las medidas necesarias, en sus respectivas organizaciones, para garantizar que, a 25 de mayo de 2018, estén en condiciones de cumplir con el GDPR y disposición de demostrarlo.

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), Reglamento UE 2016/679, de 27 de abril de 2016, será de aplicación a partir del 25 de mayo de 2018, fecha a partir de la cual será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

El GDPR se aplicará a cualquier empresa establecida en la UE, y también a empresas no establecidas en la UE pero que traten datos personales de ciudadanos de la UE, ya sea para ofrecer bienes y servicios, o controlar su comportamiento dentro de la propia UE (art. 3 GDPR), en cuyo caso tales empresas extracomunitarias deberán designar un representante en la UE que atienda las consultas de las autoridades e interesados (art. 27 GDPR).

El GDPR se basa en la prevención y el 'principio de responsabilidad proactiva' de las empresas y demás operadores, lo que implica que cada empresa es responsable de cumplir el GDPR y debe estar en disposición de acreditarlo (arts. 5.2 y 24.1 GDPR).

Por ello, es necesario que cada empresa se asesore convenientemente y analice sus actuales procesos de tratamiento de datos personales, a fin de decidir las medidas necesarias, en función de su propio modelo de negocio, costes de implantación y riesgos existentes para los interesados, en aras de garantizar el cumplimiento del GDPR.

El GDPR establece nuevos derechos para los ciudadanos, adicionales a los ya conocidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), como el derecho de supresión o derecho al olvido (art. 17 GDPR), el derecho de limitación (suspensión y/o conservación) del tratamiento (art. 18 GDPR), el derecho a la portabilidad de los datos incluyendo su transmisión entre empresas (art. 20 GDPR) o el derecho a no ser objeto de decisiones en base a procesos puramente automatizados, como la elaboración de perfiles (art. 22 GDPR).

La referida ampliación de los derechos de los interesados conlleva, a su vez, un amplio abanico de obligaciones complementarias para las empresas y demás operadores tales como:

- Las empresas con más de 250 trabajadores o que traten datos sensibles (como por ejemplo los relativos a la salud o que revelen origen étnico o racial, convicciones religiosas o ideas políticas) deberán llevar un registro de actividades de tratamiento de datos (art. 30 GDPR), que en España sustituirá a la clásica obligación de declarar los ficheros en la Agencia Española de Protección de Datos;

- la protección de datos desde el diseño (por ejemplo, cuando una nueva aplicación para móviles esté en fase de desarrollo) y por defecto, garantizando que los datos no sean accesibles a un número indeterminado de personas sin la intervención del interesado (art. 25 GDPR);

- notificar a las autoridades y los interesados en caso de violaciones de seguridad (piratería informática, virus, etc.) de los datos que constituyan un riesgo (arts. 33 y 34 GDPR);

- valorar la adecuación de las medidas de seguridad necesarias según el riesgo, como puede ser el cifrado de datos o la seudonimización (art. 32.1 GDPR) e implementarlas;

- en determinados supuestos, designar un Delegado de Protección de Datos que supervise el cumplimiento del GDPR y actúe como punto de contacto de las autoridades competentes (arts. 37-39 GDPR); o

- también en determinados supuestos, evaluar los riesgos sobre la privacidad antes de efectuar determinados tratamientos, en particular mediante el uso de nuevas tecnologías (art. 35 GDPR).

Por otro lado, es aconsejable, como sello distintivo en la gestión de la protección de datos, que las empresas y entidades valoren la adhesión a códigos de conducta (art. 40 GDPR) en los que se detallen las prácticas concretas de un sector, incluyendo lo relativo a la protección de datos, por ejemplo en relación con temas tales como la seudonimización o la información proporcionada a los niños y su protección, puesto que ello puede ser tenido en cuenta positivamente en la valoración de posibles sanciones.

Y no podemos dejar de hacer una referencia, precisamente, al sistema de sanciones (art. 83 GDPR) previsto por el GDPR, que establece básicamente dos listados de obligaciones cuyo incumplimiento se sancionaría con multas de hasta 10 o 20 millones de euros, o de hasta el 2% o el 4% del volumen de negocio total anual global de una empresa (optándose por la cifra de mayor cuantía), respectivamente, estando el incumplimiento de los principios básicos de protección de datos o de las obligaciones que afectan a los derechos de los interesados entre las causas de aplicación de las sanciones más elevadas.

En definitiva, el GDPR pretende generar un espacio europeo de confianza que precisamente fomente el desarrollo de la economía en la era digital, dominada por la actividad online y los flujos transfronterizos de datos, a cada segundo, en una escala sin precedentes hasta ahora, y en todos los sectores de actividad.

Por ello, el GDPR no debe ser considerado por las empresas como una amenaza, un lastre o una carga burocrática y limitativa de la posibilidad de hacer negocios (como indica el GDPR (Considerando #4), “el derecho a la protección de datos personales no es un derecho absoluto”), sino como un argumento de posicionamiento y como una oportunidad de negocio, perfectamente compatible con el necesario y legítimo desarrollo de la economía.

La prioridad que cada empresa o institución conceda a esta cuestión y la transparencia con que la aborde serán factores competitivos y diferenciadores de cada entidad, lo que explica que el propio GDPR obligue a que en los Estados Miembros se promueva la creación de mecanismos de certificación, sellos y marcas de protección de datos para que las entidades que lo deseen puedan demostrar ante sus interlocutores el cumplimiento de la norma (art. 42.1 GDPR).

¿TIENE ALGUNA CONSULTA?

Desde el Área de Protección de datos y Privacidad trabajamos para poder resolver las dudas que pueda plantear este nuevo reglamento y su afectación a la actividad de las distintas empresas y organizaciones. Si tiene alguna consulta, no dude en ponerse en contacto con nosotros.

CONTACTO:

Área de Protección de datos y Privacidad de RCD
rcd@rcd.legal
www.rcd.legal