Ojo al dato

Implicaciones del nuevo Reglamento Europeo de Protección de Datos (REPD)

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (REPD) ENTRÓ EN VIGOR EL 25 DE MAYO DE 2016, PERO SU APLICACIÓN TENDRÁ LUGAR **DOS AÑOS DESPUÉS**, EL PRÓXIMO 25 DE MAYO DE 2018. CREA UNA **NUEVA CULTURA DE PROTECCIÓN DE DATOS**, QUE EXIGIRÁ CAMBIOS EN LAS ORGANIZACIONES Y EN EL DISEÑO DE RECOGIDA DE DATOS, ASÍ COMO EN LA TECNOLOGÍA Y EN SU TRATAMIENTO.

El objetivo de la moratoria de dos años de espera es ofrecer tiempo a los Estados de la Unión Europea, a las Instituciones Europeas y a organizaciones y empresas que tratan datos, para que vayan preparándose y adaptándose a los nuevos requerimientos.

El porqué de esta nueva regulación se establece en los *Considerandos* de la propia norma: conseguir un espacio mayor de libertad, seguridad, justicia y unión económica, asegurando el bienestar de las personas físicas. La rápida evolución tecnológica y la globalización han provocado un aumento sustancial, y sin precedentes, de intercambio de datos personales; es imprescindible generar la confianza necesaria para el desarrollo de la economía digital.

Las novedades pasan por el nombramiento del Delegado de Protección de Datos, la privacidad desde el diseño de la comunicación y por defecto, la realización de evaluaciones de impacto en privacidad, análisis de riesgos o la gestión de brechas de seguridad. Todo el tejido empresarial español, así como el sector público, tendrán que concienciarse y comprometerse con este derecho fundamental.

Aplicación

El Reglamento se aplicará, como hasta ahora, a responsables del tratamiento de datos presentes en la Unión Europea. Y, como novedad, se amplía a encargados no establecidos en la UE, siempre que ofrezcan bienes o servicios a ciudadanos de la Unión, o como consecuencia de una monitorización y seguimiento de su comportamiento, tales como servicios de localización de vehículos, personas etc. Esta novedad supone una garantía adicional para los ciudadanos europeos. Hasta ahora había empresas que podían tratar sus datos y, sin embargo, se regían por normativas de otros países, que no siempre ofrecen el mismo nivel de protección que la normativa europea. Como en la actualidad no es necesario mantener una presencia física sobre un territorio para comerciar (y tratar datos), el Reglamento General de Protección de Datos (REPD) ha querido adaptar los criterios de cumplimiento de las empresas a internet.

Novedades

Incluye nuevas herramientas, como el derecho al olvido y el derecho a la portabilidad, para que los ciudadanos

tengan mayor capacidad de decisión y control sobre sus datos personales confiados a terceros.

El **derecho al olvido** es una consecuencia del derecho que los ciudadanos tienen a solicitar, y obtener, que sus datos personales sean suprimidos. Puede suceder cuando, por ejemplo, los datos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando los ciudadanos hayan retirado el consentimiento o, incluso, si los datos fueron recogidos de forma ilícita.

Este derecho –recogido ahora en el Reglamento Europeo– se reconoció por primera vez en la sentencia del Tribunal de Justicia de la Unión Europea el 13 de mayo de 2014. El interesado puede solicitar que se bloqueen en los resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten obsoletas, incompletas, falsas o irrelevantes, o que no sean de interés público, entre otros motivos.

El **derecho a la portabilidad**, por su parte, permite que quien ha proporcionado sus datos, de modo automatizado, los pueda recuperar en un formato que facilite su traslado a otro responsable designado por el interesado. Por ejemplo, en el sector de la telefonía el cambio de compañía conservando el mismo número. El artículo 20 del nuevo Reglamento recoge que el interesado podrá recibir sus datos personales, que ha proporcionado a un responsable, *en formato estructurado, de uso común y lectura mecánica*.

Otra novedad es la edad necesaria para prestar consentimiento válido. El Reglamento establece los 16 años como aquélla en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en esta sociedad de la información (por ejemplo, redes sociales). Sin embargo, permite rebajar esa edad y que cada Estado miembro establezca la suya propia, con un límite: 13 años. En España, ese límite es de 14 años. Por debajo de esa edad, se precisa el consentimiento de sus padres o tutores.

Para las empresas que recopilan datos personales el consentimiento tiene que ser verificable, y el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender.

La desaparición del consentimiento tácito supone, por tanto, la revisión de las políticas de privacidad y tratamiento de datos personales, así como de los textos informativos.

Responsabilidad activa

Uno de los aspectos esenciales de esta nueva legislación es la prevención que se supone a empresas y organizaciones que tratan datos. Actuar sólo cuando ya se ha producido la infracción es insuficiente. Esa infracción ha podido dañar a personas de un modo muy difícil de compensar...

Esta **responsabilidad activa** implica que las empresas deben incluir medidas que aseguren que pueden cumplir con los principios, derechos y garantías del REPD.

> Hasta ahora, había empresas que trataban datos y que se regían por normativas de otros países...

Para ello, el Reglamento prevé medidas como: protección de datos desde el diseño y por defecto, mantenimiento de un registro de tratamientos, evaluaciones de impacto sobre la protección de estos datos, nombramiento de un delegado (externo o interno) que los proteja, notificación de violaciones de la seguridad de los datos, códigos de conducta, esquemas de certificación, etc.

Exige un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos, habilitando nuevas formas de gestionarla distintas de las que se empleaba hasta ahora y una nueva elaboración de procesos y procedimientos para su implantación.

Los menores de edad han de estar más protegidos

Algunas de las medidas que introduce el Reglamento mantiene las anteriores y otras reemplazan a las ya existentes –por ejemplo, las medidas de seguridad o de la obligación de documentación.

Las organizaciones que tratan datos deben realizar un análisis de riesgo de sus tratamientos para determinar qué medidas han de aplicar y cómo. Pueden ser entidades que sólo realizan un tratamiento sencillo, que no implica, por ejemplo, ningún dato sensible, hasta aquellas que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que requieren una valoración cuidadosa de sus riesgos.

Las autoridades europeas de protección de datos, de forma colectiva, y la Agencia Española, individualmente, han trabajado en el desarrollo de herramientas tales como aplicaciones, documentación, guías, etc. para facilitar la identificación y valoración de riesgos y recomendaciones sobre la aplicación de medidas. Tienen especial singularidad las pymes que realizan los tratamientos de datos más habituales en la gestión empresarial.

Consentimiento

Una de las bases fundamentales dentro de las organizaciones y empresas para tratar datos personales es el **consentimiento.** El Reglamento pide que el consentimiento, con carácter general, sea **libre, informado, específico e inequívoco**. Para ello, requiere una declaración de los interesados o una acción positiva que indique su conformidad. Es decir, no puede deducirse el consentimiento del silencio o inacción de los ciudadanos (consentimiento tácito). Así, las empresas están obligadas a revisar la forma en la que obtienen y registran el consentimiento. Éste ha de ser consentimiento explícito (autorizar el tratamiento de datos sensibles, por ejemplo). La declaración u acción se debe referir, explícitamente, al tratamiento en cuestión.

El consentimiento tiene que ser **verificable**. Quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento. Por ello, es importante revisar los sistemas de registro de la aprobación del usuario para su verificación ante una auditoría o requerimiento.

El REPD también prevé la obligación de explicar la base legal para el tratamiento

La experiencia nos llevará a analizar el coche conectado y los datos que genera

de los datos, sus períodos de retención y que los interesados puedan dirigir sus reclamaciones a las Autoridades de protección de datos si creen que hay un problema. La legislación exige, de forma expresa, que la información que se proporcione sea fácil de entender y se presente en un lenguaje claro y conciso. Las empresas y organizaciones que tratan datos pueden realizar esta sencilla lista de comprobación o *checklist*:

1. ¿Cuál es el nivel de datos tratados: básico, medio o alto? ¿Cómo recabo esos datos? ¿Tengo el consentimiento expreso?
2. ¿Se han comunicado los ficheros AGPD o sus modificaciones?
3. ¿Los empleados han firmado el compromiso expreso de confidencialidad?
4. ¿Quién tiene acceso a esos datos? ¿Existen cesión de datos y están debidamente documentadas?
5. ¿Existe documento de seguridad?
6. ¿Existen medidas de acceso a los programas informáticos? ¿está debidamente guardada la documentación en papel?
7. ¿Se ha realizan copias de seguridad?
8. ¿Es obligatorio realizar auditoria externa? ¿Es obligatorio tener Delegado de Protección de datos?

Estos dos años, en definitiva, han servido para que empresas y organizaciones que tratan datos personales preparen la aplicación de estas medidas, y otras modificaciones prácticas derivadas del Reglamento. En este periodo han podido detectar dificultades, insuficiencias o errores para que el 25 de mayo de 2018 cumplan el Reglamento con plena aplicación ■

PARA SABER MÁS

Reglamento Europeo de Protección de Datos (REPD 2016/679).

Agencia Española de Protección de Datos
www.agpd.es

www.revistacesvimap.com

@revistacesvimap