



A partir del próximo 25 de mayo de 2018 comenzará a aplicarse el Reglamento Europeo de Protección de Datos Personales 2016/679, reglamento éste de aplicación directa en todos los estados miembro, sustituyendo y prevaleciendo sus disposiciones sobre cualquier otra norma nacional en la misma materia, y que introduce cambios radicales respecto de la normativa hasta ahora en vigor. Conviene pues, a este respecto, dedicar unas pocas líneas.

Parece que con este Reglamento las instituciones comunitarias se han tomado muy en serio la privacidad de las personas. El Reglamento incrementa exponencialmente las sanciones por inadecuación al procedimiento previsto para tratamiento de los datos por parte de las empresas, llegando las sanciones a alcanzar la cifra de los 20 millones de euros o al 4% de su facturación anual global (la que fuera más alta de las dos).

El Reglamento presenta un enfoque más garantista de los derechos y libertades y pone en el punto de mira la responsabilidad de las empresas en la privacidad de los datos personales a lo largo de una serie de cuestiones clave.

La nueva regulación traslada el control sobre los datos personales desde las organizaciones hacia los verdaderos titulares de los mismos, los usuarios o, lo que es lo mismo, los ciudadanos. Esto queda claramente establecido en cuestiones tales como la importancia del consentimiento en la nueva norma. El consentimiento para el tratamiento de los datos deberá ser libre, específico, informado e inequívoco y el responsable del tratamiento debe poder probar que el titular consintió el tratamiento de sus datos. Desaparecen interminables condiciones de uso que nadie lee y serán sustituidas por iconos y textos más simples. Muchos consentimientos genéricos y tácitos del pasado dejarán de ser válidos, cambiando además las actuales opciones de privacidad que por defecto hacen públicos nuestros datos.

Poder exigir el borrado automático de nuestros datos personales (el conocido como "derecho al olvido" o derecho de supresión) y la portabilidad de nuestros datos a otro servicio son derechos ahora consagrados que castigarán a las empresas que maltraten a los usuarios. Por cuanto respecta a las brechas de seguridad o ataques informáticos, la nueva normativa establece la obligación tanto de comunicarlo a la autoridad en 72 horas como de comunicarlo a los propios usuarios afectados, lo que abre la puerta a que puedan presentarse demandas colectivas que hoy son muy complicadas.

El nuevo Reglamento ofrece además desarrollos y novedades significativas en materia de responsabilidad activa que obligan a las empresas a tomar medidas técnicas y organizativas cuya profundidad se pondera en cada caso y exige una previa valoración por el responsable o el encargado del tratamiento. En este sentido una interesante novedad es la figura de la Evaluación de Impacto, que debe realizarse a criterio del responsable cuando la naturaleza de los datos o el alcance del tratamiento entrañen un alto riesgo para los derechos y libertades del titular y, a partir de dicha valoración, poder adoptar las medidas que procedan. Si la evaluación arroja un alto riesgo, el responsable deberá obtener autorización estatal antes de iniciar la recogida de información. El reglamento anima además en este sentido a adoptar códigos de conducta por parte de las empresas que operan bases de datos y abre la posibilidad a que asociaciones sectoriales adopten códigos modelo susceptibles de ser preaprobados por la autoridad. Asimismo se incentiva el nacimiento de organismos privados de certificación que, previa acreditación estatal, certifiquen la adecuación de responsables y encargados a la nueva normativa.

Además de las figuras del responsable y el encargado del tratamiento, emerge en el nuevo Reglamento la figura del Delegado de Protección de Datos, que será obligatorio para autoridades y organismos públicos y responsables y encargados que tengan entre sus actividades operaciones de tratamiento que requieran observación sistemática o el tratamiento a gran escala de datos sensibles

Los empresarios tendrán que relacionarse con un único supervisor en Europa, lo que supondrá un importante ahorro. La autoridad de control principal competente será la autoridad de control del Estado miembro en el que el responsable del tratamiento tenga su establecimiento principal, aunque la autoridad de control del encargado del tratamiento deba considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el Reglamento. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

Se instaura el “mecanismo de ventanilla única”. Este sistema supondrá que el interesado va a poder presentar las reclamaciones en su país de origen, que la autoridad competente lo admitirá o no, y si lo considera, le dará debido trámite para que sea la autoridad de control del país dónde el responsable tenga su establecimiento principal, la que adopte la decisión final que corresponda.

Por último destacar que este Reglamento aplicará a todas las empresas europeas pero también a todas aquellas que estando fuera de la UE realicen actividades dentro que impliquen el tratamiento de datos personales, incluso si no tienen ningún tipo de presencia física dentro del territorio de la Unión.

Siendo pues muchas las medidas y novedades que introduce el nuevo Reglamento, queremos recordar que desde la Agencia Española de Protección de Datos se está ofreciendo detallada información así como herramientas muy útiles para las empresas como son la Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento (http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf) o la herramienta de ayuda FACILITA, diseñada como un recurso útil para cualquier empresa o profesional, ya que con tan solo tres pantallas de preguntas muy concretas permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si puede considerar que sus datos personales de escaso riesgo para los derechos y libertades de las personas o si debe realizar un análisis de riesgos (<http://www.servicios.agpd.es/Facilita>).

En definitiva, pronto veremos un amplio conjunto de novedades en vigor. Todo ello por la actual tramitación parlamentaria del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que deroga la LOPD de 1999 y que dará cumplimiento al mandato del Reglamento Europeo aprovechando los espacios de adecuación el ámbito nacional que permite el propio Reglamento de completar, definir, detallar o matizar determinadas cuestiones relativas al tratamiento de datos personales, pero no olvidemos que irremediamente el 25 de mayo de 2018 porque el nuevo Reglamento por su propio rango normativo es, como decíamos al principio, de aplicación directa y obligatoria en los estados y no precisa de disposición alguna nacional para ser transpuesto a derecho interno.

Responsabilidad de las empresas en la privacidad de los datos personales