MAR ESPAÑA
Directora de la Agencia Española de Protección de Datos

Novedades del Reglamento de protección de datos para entidades

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos, el nuevo marco legal que comenzará a aplicarse el 25 de mayo de 2018 y que sustituirá la vigente normativa. La vacatio legis elegida fue de dos años, un plazo que inicialmente podía parecer largo. Sea como fuere, nos encontramos prácticamente en su ecuador y quizás, a medida que transcurre el tiempo, ya no se antoja tan abultado el lapso de tiempo previsto por el legislador para que las organizaciones se adapten a las obligaciones que impone el nuevo Reglamento europeo.

En la Agencia Española de Protección de Datos somos conscientes de que estas nuevas reglas de juego pueden plantear incógnitas, incertidumbre y, probablemente, un cierto temor entre los responsables del tratamiento de datos personales. Por ello, desde el primer momento la Agencia ha tratado de responder a las necesidades que marca el nuevo Reglamento y ha desarrollado materiales y recursos para facilitar el cumplimiento de la normativa entre los sujetos obligados.

Al día siguiente de la entrada en vigor el Reglamento, la Agencia publicó un documento en el que resumía, en 12 preguntas, las principales dudas que podía despertar la llegada del nuevo marco europeo de protección de datos. Poco después, abordó en un segundo documento las implicaciones prácticas de la nueva normativa para entidades, a través del cual emitió una serie de recomendaciones dirigidas a las organizaciones para que estas fueran adaptando sus procesos, por cuanto la nueva normativa implica una gestión distinta a la que se viene empleando hasta ahora.

Posteriormente, la Agencia publicó en su página web las directrices sobre la aplicación del Reglamento

aprobadas por el Grupo de Autoridades europeas de protección de datos, del que la AEPD forma parte, y que iban dirigidas a responsables y encargados de tratamiento. El siguiente paso ha sido la creación de nuevos materiales que incluyen una 'Guía del Reglamento para responsables', 'Directrices para elaborar contratos entre responsables y encargados', y una 'Guía para el cumplimiento del deber de informar'. Todos ellos están disponibles en una nueva sección web específica, que se actualizará de forma progresiva, con información útil para la paulatina adaptación al Reglamento.

A estos materiales se unirá una herramienta de autoevaluación online en la que actualmente trabaja la Agencia, diseñada con el objetivo de favorecer que las pymes puedan valorar de forma rápida y sencilla si únicamente llevan a cabo tratamientos de datos que, en principio, suponen un bajo o muy bajo riesgo para los derechos de los interesados. Asimismo, esta herramienta da acceso a las medidas que estas tendrían que tomar para cumplir con el Reglamento europeo.

En definitiva, la AEPD sigue esforzándose por dar cumplimiento a uno de los ejes de actuación sobre los que se sustenta el Plan Estratégico de la Agencia 2015-2019: el de lograr una Agencia cercana a los responsables y a los profesionales de la privacidad.

Novedades del Reglamento

El Reglamento introduce un buen número de novedades que en algunos casos modifican o dejan sin efecto mecanismos hasta ahora aceptados en la aún vigente normativa de protección de datos. Uno de ellos tiene que ver con la figura del consentimiento. Si bien tanto en la Directiva 95/46/CE como en el Reglamento se indica que el consentimiento debe ser inequívoco, en la nueva regulación se explica qué se entiende por tal y se subraya que este debe implicar una declaración de voluntad o una clara actuación o acción afirmativa.

Esa es una importante novedad que marca el fin del camino para el consentimiento tácito, una peculiaridad del modelo español, articulada en el pasado como solución ante la imposibilidad de hacer tratamientos sobre la base del interés legítimo del responsable.

Ahora el consentimiento tácito no solamente es contrario al Reglamento, sino que ya no cumple con el propósito que originariamente cumplía, dado que a raíz de una Sentencia del Tribunal de Justicia de la Unión Europea el interés legítimo es una base legal para el tratamiento válida en España como consecuencia de la aplicación directa de las correspondientes disposiciones de la Directiva. De hecho, muchos tratamientos que se estaban haciendo sobre la base del consentimiento tácito se pueden hacer sobre otra base legal, en especial,

el interés legítimo. También es importante resaltar que, de una manera clara y taxativa, ya no se permite que una inacción se asuma como consentimiento.

Otro aspecto novedoso e importante es que el Reglamento hace obligatorio proporcionar a los interesados una cantidad de información bastante más amplia de la que exige explícitamente la Directiva. Ésta no especifica el tipo de información necesaria para un tratamiento equitativo pero el Reglamento sí lo hace. Y esta novedad hay que situarla en concordancia con otro mandato que establece el Reglamento: que la información que se ofrezca a los usuarios se tiene que dar de forma clara, inteligible y en un lenguaje sencillo.

Las organizaciones que tratan datos también pueden albergar dudas sobre otra novedad que contempla el Reglamento: el registro de tratamientos. En la Agencia somos conscientes del cambio de paradigma que supone, ya que antes la terminología giraba en torno a la noción de fichero y ahora en el Reglamento todo se refiere a tratamientos, lo que supone un cambio de mentalidad y de enfoque. Sabemos que puede no ser fácil debido a que la noción de tratamiento puede ser muy amplia e incluir muchas operaciones de tratamiento.

No se trata de hacer una anotación por cada actividad de tratamiento, ese no es el objetivo del Reglamento. El objetivo de este registro es que la organización sepa qué datos trata y para qué. En la Agencia pensamos que una posible forma de organizar este registro –y quizá la más asequible para las organizaciones- puede ser enumerar con qué fines se tratan los ficheros de datos que ahora pueden estar incluidos en el Registro General de Protección de Datos. Es decir, partiendo de la noción de fichero proponemos pasar a la de tratamiento, vinculando esos conjuntos estructurados de datos a los fines a los que se usan. No sería necesario especificar si se almacenan o se ceden datos, sino que se tienen esos conjuntos de datos y para qué se utilizan.

La Agencia propone esta vía en la 'Guía del Reglamento General de Protección de Datos para responsables de tratamiento' como una forma de partir de lo que tienes para tratar de identificar para qué se usan esos datos. Al final, no se tiene que ver como una carga sino como una herramienta para que la organización se conciencie de qué está haciendo con los datos y sepa lo que hace.

En lo que respecta a las medidas de cumplimiento también podemos encontrar cambios en el nuevo Reglamento, que implanta un modelo de responsabilidad activa de la organización. Quizá uno de los más significativos es que concede libertad a las organizaciones para decidir cómo aplican las medidas de seguridad. Vamos a pasar de una situación en la que en nuestro reglamento de la LOPD señalaba una lista cerrada de medidas que se tenían que cumplir en función de los datos tratados, a un escenario distinto en el que el Reglamento traslada al responsable la responsabilidad de valorar los riesgos que implican sus tratamientos y decidir qué medidas aplica.

En el mismo sentido, el Reglamento establece la obligación de notificar las quiebras de seguridad a las autoridades de supervisión y a los titulares de los datos afectados. Esta obligación no es universal. En el caso de las autoridades sólo habrá de cumplirse cuando la quiebra suponga un riesgo para los derechos y libertades de los afectados, mientras que los interesados solo habrán de ser informados cuando ese riesgo sea alto.

Por otra parte, es importante señalar que las relaciones entre el responsable y el encargado del tratamiento varían bastante en el Reglamento con respecto a la Directiva del año 95, principalmente porque esta no indicaba nada sobre el contenido de estas relaciones, no así el Reglamento, que incluye numerosos aspectos que deben ser incluidos en esos contratos. Se establece, además, una obligación de diligencia debida por la cual el responsable tiene que contratar a un encargado que ofrezca garantías de que también cumple con el Reglamento. En nuestra legislación, sobre todo en el reglamento de la LOPD ya se incluían muchos de estos aspectos, por lo que, en ese sentido, creo que en España va a ser más fácil adaptar los contratos a lo que pide el Reglamento.

No quiero finalizar sin hacer mención a otra novedad fundamental: el delegado de protección de datos y las situaciones en las que las entidades pueden tener que contar con esta figura. El Reglamento considera su designación obligatoria cuando responsables o encargados traten, a gran escala, datos especialmente protegidos o que sean el resultado de un seguimiento regular y sistemático de los usuarios. Pero, además, prevé que deba ser nombrado en todas las autoridades públicas, atendiendo, sin duda, a las características peculiares que tienen los tratamientos de datos en este ámbito. Hay que decir que el Reglamento ofrece mucha flexibilidad en cuanto al delegado de protección de datos, ofreciendo la posibilidad de contratarlo a tiempo partido o externalizando el servicio.

Es cierto que la adaptación a la nueva normativa puede suponer un notable esfuerzo para las organizaciones que tratan datos, pero al hacerlo cumplirán un doble objetivo: lograr los objetivos que exige el Reglamento y, por extensión, mejorar la protección de los ciudadanos. Y en la consecución de estos objetivos, las organizaciones nos encontrarán siempre a su lado. ✱