El Reglamento de protección de datos en 12 preguntas

Publicado por la AEPD

El Reglamento General de Protección de Datos ha entrado en vigor el 25 de mayo de 2016. La AEPD ha elaborado este documento simplificado, que sigue el formato pregunta-respuesta, para facilitar la comprensión del nuevo marco normativo a los ciudadanos y ayudar a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.

1. La entrada en vigor del Reglamento, ¿supone que ya no se aplica la Ley Orgánica de Protección de Datos española?

No. El Reglamento ha entrado en vigor el 25 de mayo de 2016 pero **no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018**. Hasta entonces, tanto la Directiva 95/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

2. ¿Cuál es, entonces, el significado de que el Reglamento haya entrado en vigor?

El periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

En esos dos años, por ejemplo, los Estados miembros pueden adoptar o iniciar la elaboración de determinadas normas que sean necesarias para permitir o facilitar la aplicación del Reglamento. Esas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita.

3. ¿A qué empresas u organizaciones se aplica?

El Reglamento se aplicará como hasta ahora a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, y se amplía a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

Para que esta ampliación del ámbito de aplicación pueda hacerse efectiva, esas organizaciones deberán nombrar un representante en la Unión Europea, que actuará como

punto de contacto de las Autoridades de supervisión y de los ciudadanos y que, en caso necesario, podrá ser destinatario de las acciones de supervisión que desarrollen esas autoridades. Los datos de contacto de ese representante en la Unión deberán proporcionarse a los interesados entre la información relativa a los tratamientos de sus datos personales.

4. ¿Qué implica para los ciudadanos que el Reglamento amplíe el ámbito de aplicación territorial?

Esta novedad supone una garantía adicional a los ciudadanos europeos. En la actualidad, para tratar datos no es necesario mantener una presencia física sobre un territorio, por lo que el Reglamento pretende adaptar los criterios que determinan qué empresas deben cumplirlo a la realidad del mundo de internet.

Ello permite que el Reglamento sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión y, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea.

5. ¿Qué nuevas herramientas de control de sus datos poseen los ciudadanos?

El Reglamento introduce nuevos elementos, como el derecho al olvido y el derecho a la portabilidad, que mejoran la capacidad de decisión y control de los ciudadanos sobre los datos personales que confían a terceros.

El derecho al olvido se presenta como la consecuencia del derecho que tienen los ciudadanos a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita. Asimismo, según la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que reconoció por primera vez el derecho al olvido recogido ahora en el Reglamento europeo, supone que el interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público, entre otros motivos.

Por su parte, el derecho a la portabilidad implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado.

6. ¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?

El Reglamento establece que la edad en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales) es de 16 años. Sin embargo, permite rebajar esa edad y que cada Estado miembro establezca la suya propia, estableciendo un límite inferior de 13 años. En el caso de España, ese límite continúa en 14 años. Por debajo de esa edad, es necesario el consentimiento de padres o tutores.

En el caso de las empresas que recopilen datos personales, es importante recordar que el consentimiento tiene que ser verificable y que el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender.

7. ¿Qué implica la responsabilidad activa recogida en el Reglamento?

Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar. Para ello, el Reglamento prevé una batería completa de medidas:

- 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
- Promoción de códigos de conducta y esquemas de certificación.

8. Entonces, ¿supone una mayor carga de obligaciones para las empresas?

El Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Pero ello no implica necesariamente ni en todos los casos una mayor carga. En muchos casos será sólo una forma de gestionar la protección de datos distinta de la que se viene empleando ahora.

En primer lugar, algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya existentes, como es el caso de las medidas de seguridad o de la

obligación de documentación y, hasta cierto punto, la evaluación de impacto y la consulta a Autoridades de supervisión.

Otras constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que, en todo caso, formarían parte de una correcta puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto, la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos.

En todos los casos, el Reglamento prevé que la obligación de estas medidas, o el modo en que se apliquen, dependerá de factores tales como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos.

Por ello, es necesario que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo. Estos análisis pueden ser operaciones muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen, por ejemplo, datos sensibles, u operaciones más complejas en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que por sus características requieren de una valoración cuidadosa de sus riesgos.

Las Autoridades de protección de datos europeas de forma colectiva, y la Agencia Española individualmente, estamos ya trabajando en el desarrollo de herramientas que faciliten la identificación y valoración de riesgos y en recomendaciones sobre la aplicación de medidas, especialmente en relación con pymes que realizan los tratamientos de datos más habituales en la gestión empresarial.

9. ¿Cambia la forma en la que hay que obtener el consentimiento?

Una de las bases fundamentales para tratar datos personales es el consentimiento. El Reglamento pide que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es ?inequívoco?, el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

Las empresas deberían revisar la forma en la que obtienen y registran el consentimiento. Prácticas que se encuadran en el llamado consentimiento tácito y que son aceptadas bajo la actual normativa dejarán de serlo cuando el Reglamento sea de aplicación.

Además, el Reglamento prevé que el consentimiento haya de ser ?explícito? en algunos casos, como puede ser para autorizar el tratamiento de datos sensibles. Se trata de un

requisito más estricto, ya que el consentimiento no podrá entenderse como concedido implícitamente mediante algún tipo de acción positiva. Así, será preciso que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que 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 del consentimiento para que sea posible verificarlo ante una auditoría.

10. ¿Deben las empresas revisar sus avisos de privacidad?

Con carácter general, sí. El Reglamento prevé que se incluyan en la información que se proporciona a los interesados una serie de cuestiones que con la Directiva y muchas leyes nacionales de trasposición no eran necesariamente obligatorias. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados puede dirigir sus reclamaciones a las Autoridades de protección de datos. Si creen que hay un problema con la forma en que están manejando sus datos. Es importante recordar que el Reglamento exige de forma expresa que la información que se proporcione sea fácil de entender y presentarse en un lenguaje claro y conciso.

11. En qué consiste el sistema de 'ventanilla única'?

Este sistema está pensado para que los responsables establecidos en varios Estados miembros o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE tengan una única Autoridad de protección de datos como interlocutora. También implica que cada Autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, a partir de la aplicación del Reglamento valorará si el supuesto tiene carácter transfronterizo, en cuyo caso habrá que abrir un procedimiento de cooperación entre todas las Autoridades afectadas buscando una solución aceptable para todas ellas. Si hay discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos, un organismo de la Unión integrado por los directores de todas las Autoridades de protección de datos de la Unión. Ese Comité resolverá la controversia mediante decisiones vinculantes para las Autoridades implicadas.

Este nuevo sistema no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades distintas de la del Estado donde residan. Siempre pueden plantear sus reclamaciones o denuncias ante su propia Autoridad nacional (en el caso español, la Agencia Española de Protección de Datos). La gestión será realizada por esa Autoridad, que será también responsable de informar al interesado del resultado final de su reclamación o denuncia.

La ventanilla única, en todo caso, no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado.

12. ¿Tienen las empresas que empezar a aplicar ya las medidas contempladas en el Reglamento?

No. El Reglamento está en vigor, pero no será aplicable hasta 2018.

Sin embargo, puede ser útil para las organizaciones que tratan datos empezar ya a valorar la implantación de algunas de las medidas previstas, siempre que esas medidas no sean contradictorias con las disposiciones de la LOPD, que sigue siendo la norma por la que han de regirse los tratamientos de datos en España.

Por ejemplo, las organizaciones deben tener en cuenta que a partir de mayo de 2018 deberán realizar análisis de riesgo de sus tratamientos y que puede ser útil para ellas empezar desde ahora a identificar el tipo de tratamientos que realizan, el grado de complejidad del análisis que deberán llevar a cabo, etc. En esta tarea podrían utilizar las herramientas y recursos que paulatinamente vayan desarrollando las Autoridades de protección de datos.

Igualmente, nada impide que las organizaciones comiencen a planificar o a establecer el registro de tratamientos de datos o a implantar las evaluaciones de impacto o cualquiera otra de las medidas previstas.

Del mismo modo, las organizaciones podrían comenzar a diseñar e implantar los procedimientos para notificar adecuadamente a las Autoridades de protección de datos o a los interesados las quiebras de seguridad que pudieran producirse.

En general, las organizaciones que tratan datos personales deberían comenzar a preparar la aplicación de estas medidas, así como de otras modificaciones prácticas derivadas del Reglamento. Por ejemplo, el Reglamento exige que los responsables de tratamiento faciliten a los interesados el ejercicio de sus derechos. Aunque la interpretación de ?facilitar? pueda variar dependiendo de los casos, incluye en todos ellos algún tipo de actuación positiva por parte de los responsables para hacer más accesibles y sencillas las vías para el ejercicio de derechos.

La ventaja de una pronta aplicación es que permitirá detectar dificultades, insuficiencias o errores en una etapa en que estas medidas no son obligatorias y, en consecuencia, su corrección o eficacia no estarían sometidas a supervisión. Ello permitiría corregir errores para el momento en que el Reglamento sea de aplicación.

Fuentes: Editado por la Agencia Española de Protección de datos.