MEDINA CUADROS

Reglamento Europeo de Protección de Datos

NOVIEMBRE 2018

1. Análisis al nuevo Reglamento Europeo de Protección de Datos

El 25 de Mayo de 2018 entra en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que supone una de las mayores reformas normativas a nivel comunitario en esta materia.

- Vamos a analizar los cambios que trae consigo este Reglamento, que deroga la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, que era hasta ahora la norma comunitaria básica en cuestión de protección de datos.

- La primera nota a destacar de este nuevo Reglamento es que su contenido **es directamente aplicable en todos los Estados Miembros de la UE, sin necesidad de tener que llevar a cabo una transposición normativa al ordenamiento interno de cada Estado**. Por tanto, a partir del 25 de Mayo, el Reglamento resulta de plena aplicación en España.

- Y teniendo en cuenta esta circunstancia, lo deseable sería que para esa fecha ya se hubiera aprobado y publicado la Ley que reforme la actual LOPD 15/1999, de 13 de Diciembre, para evitar que puedan producirse distorsiones entre la nueva norma comunitaria y la Ley estatal vigente. Pero, hasta que ello ocurra, el Reglamento UE coexistirá con la Ley 15/1999; lo que, con toda seguridad, causará no pocos problemas de compatibilidad o contradicción entre ambas normas.

- Adentrándonos en las novedades que implica, podemos mencionar las siguientes:

1.1.- Ámbito de aplicación.

- Las disposiciones del Reglamento extienden su aplicación al tratamiento de datos personales derivado de actividades realizadas en la Unión Europea, con independencia de que el tratamiento tenga lugar en la Unión o no, o de que el responsable o encargado de tratamiento no establecido en la Unión, siempre que los interesados o titulares de esos datos sean residentes en la UE.

1.2.- Se suprime la obligación de registro de los ficheros de datos ante la Agencia de protección de Datos.

- Esta es quizá una de las novedades más destacadas de la nueva regulación porque acaba con una obligación muy consolidada.

- Sin embargo, sí se establece una obligación de registro interno de actividades de tratamiento de datos personales que se realicen en aquellas entidades que cuenten con más de 250 trabajadores o, si tuviera menos de 250 trabajadores, cuando el tratamiento afecte a datos considerados sensibles (de salud, religión o creencias, etnia, afiliación política o sindical, antecedentes penales…).

- Hay que mencionar que entre los datos especialmente protegidos se incluyen ahora los datos genéticos o biométricos.

1.3.- Creación de la figura del *"Delegado de Protección de Datos" (DPO)*.

- No se trata de una figura generalizada. Puede ser personal interno o externo de la empresa.

- Su labor es asesorar a la entidad en el cumplimiento de la normativa de protección de datos (identificando riesgos y proponiendo soluciones para solucionarlos), notificar a las autoridades competentes en la materia (en España la AEPD) las violaciones de seguridad y tramitar las autorizaciones que sean necesarias.

- Se le considera el enlace entre la entidad y la autoridad de control.

- Existe un procedimiento de certificación de la formación en protección datos del DPO que en España es gestionado por la ENAC.

- Resulta obligatorio en las AAPP y en empresas cuya actividad implique el tratamiento sistemático de datos a gran escala, de carácter especial o relativos a infracciones penales.

1.4.- Derechos de los ciudadanos.

- Los derechos de los interesados reconocidos hasta ahora son los denominados Derechos ARCO, que se refieren al derecho de acceso, al de rectificación, al de cancelación y al de oposición; aunque el nuevo Reglamento introduce modificaciones en el procedimiento para ejercitarlos, simplificándolo y contemplando la posibilidad de presentar las solicitudes de forma electrónica.

- El plazo para responder a las peticiones ARCO por el responsable de tratamiento es un mes, que puede ampliarse hasta dos meses.

- En el derecho de acceso se reconoce el derecho a obtener una copia de los datos; que antes solo se preveía en el caso de la historia clínica.

- Se contempla la posibilidad de formular denuncias a través de asociaciones de usuarios, así como la posibilidad de que el responsable de tratamiento establezca un canon para sufragar los costes que el derecho de acceso implique.

- La nueva regulación amplía estos derechos reconociendo el tan mencionado ***"Derecho al olvido"***, el Derecho a la limitación de tratamiento y el Derecho a la portabilidad de los datos.

- El "*Derecho al olvido*", denominado en el Reglamento como Derecho de supresión reconoce al interesado la facultad de obtener, sin dilación indebida por parte del responsable del tratamiento, la supresión de los datos personales que le conciernan. **Se conoce también como Derecho al borrado.**

- El responsable del tratamiento está obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a)los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b)el interesado retire el consentimiento en que se basa el tratamiento, porque ya no obedece a los fines específicos para el que se otorgó dicho consentimiento (Artículo 6, apartado 1, letra a), o Artículo 9, apartado 2, letra a);

c)el interesado se oponga al tratamiento (Artículo 21, apartado 1, o Artículo 21, apartado 2);

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1; y que se refieren a los menores.

Este "*Derecho al olvido*" incluye la supresión de los datos personales también cuando se hayan hecho públicos y, por tanto, también la supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos, en internet y en las redes sociales.

- El **Derecho a la limitación de tratamiento** permite al interesado impedir el tratamiento temporal de sus datos cuando se cumpla alguna de las condiciones siguientes:

a)el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b)el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c)el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d)el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

- Todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

- Finalmente, el Derecho a la portabilidad de los datos reconoce al interesado el derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado; e incluso a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

1.5.- Desaparece el consentimiento tácito del interesado.

- La nueva regulación elimina el "*consentimiento tácito*" del afectado para llevar a cabo el tratamiento de sus datos personales, y lo sustituye por un consentimiento libre, expreso e inequívoco, acompañado de derecho revocación en cualquier momento.

- Las entidades deben revisar la forma en que recaban y conservan el consentimiento del interesado, porque éste debe ser siempre verificable.

- Debe ser manifiesto para el tratamiento de datos sensibles.

1.6.- Se incrementan las obligaciones de información.

- Las entidades que realicen el tratamiento de datos personales están obligadas por la nueva norma a facilitar al interesado una mayor información, más completa, más comprensible y más sencilla; especialmente cuando el interesado sea menor de edad.

- Cabe facilitar la información en dos fases, en el momento de recabar el consentimiento se facilitará la información más básica, y con posterioridad se ampliará esta información con aspectos tales como la identidad del delegado de protección de datos, la información sobre cesiones o transferencias internacionales de datos

- Cabe la utilización de iconos normalizados para informar del tratamiento de los datos.

1.7.- Incremento sustancial en las sanciones.

- En el Reglamento se fijan sanciones que pueden alcanzar hasta los 20 millones de euros. No se establece una cuantía mínima de sanción y se fija como criterio para cuantificarlas un porcentaje de hasta el 4% del volumen global negocio anual de la entidad infractora.

- El Reglamento no excluye de las sanciones a las AAPP, aunque la transposición normativa estatal puede acordarlo así

1.8.- Responsabilidad proactiva y análisis de riesgos.

- La citada responsabilidad implica poder acreditar que el tratamiento de datos es conforme al Reglamento, especialmente en el tratamiento de datos sensibles.

- El análisis de riesgos supone establecer mecanismos para analizar los posibles riesgos para los datos personales que supone el tratamiento y establecer las medidas de protección adecuadas a su nivel y a la finalidad del tratamiento.

- Finalmente, se establece la realización de evaluaciones de impacto en la protección de datos que puede tener un determinado sistema de tratamiento, producto o servicio, antes de su implantación.

1.9.- Reporte de los problemas o brechas de seguridad.

- Se establece la obligación del responsable de tratamiento de notificar los fallos de seguridad a la AEPD en un plazo máximo de 72 horas y también a los afectados, si se ponen en riesgo sus derechos.

1. 10.- Regulación más estricta de de las transferencias internacionales de datos fuera de la UE.

Adaptación de las pymes y profesionales

- Las pymes y los autónomos y profesionales son los responsables de tratamiento de los datos personales que utilizan en el desarrollo de sus actividades y ello les obliga a adaptarse a las previsiones del nuevo Reglamento Europeo.

- Para llevar a cabo esta adaptación deben tener en cuenta:

1.- Si están obligadas o no a disponer de Delegado de Protección de Datos.

2.- Que ha desparecido la obligación de registrar los ficheros de datos y se ha sustituido por el registro interno de actividades de tratamiento. Deberán valorar si están obligadas o no a llevar este registro, conforme a los requisitos señalados anteriormente.

3.- Revisar las razones a las que obedece el tratamiento de datos y si se posee o no el consentimiento expreso del afectado.

4.- Revisar si la información que se ofrece a los interesados en la recogida de datos cumple con los requisitos de trasparecía que establece el Reglamento.

5.- Revisar si los procedimientos de ejercicio de los derechos de los interesados (ARCO, derecho al olvido y portabilidad de los datos) se ajustan a las exigencias del Reglamento, tanto en su sencillez y accesibilidad como en la posibilidad de cumplir los plazos de respuesta establecidos en la norma.

6.- Revisar las medidas de seguridad realizando el análisis de riesgos y determinar la necesidad de realizar, de forma previa, evaluaciones de impacto respecto a nuevos tratamientos de datos.

- Para ello, la AEPD ha desarrollado una herramienta de ayuda denominada **Facilita RGPD**., que tiene la finalidad de facilitar la adecuación al RGPD a las empresas y profesionales (responsables o encargados de tratamientos) que traten datos personales de escaso riesgo para los derechos y libertades de las personas.

- **Facilita RGPD** es una herramienta fácil y gratuita, que permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si se adapta a los requisitos exigidos para utilizar **Facilita RGPD** o si debe realizar un análisis de riesgos.

- La herramienta genera diversos documentos adaptados a la empresa concreta, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargado de tratamiento, el registro de actividades de tratamiento, y un anexo con medidas de seguridad orientativas consideradas mínimas.

- **Facilita RGPD** está orientada a empresas que tratan datos personales de escaso riesgo, como por ejemplo, datos personales de clientes, proveedores o recursos humanos.

2. Ejes relevantes

- La diligencia como nuevo paradigma
- Peculiaridades de las AAPP
- Peculiaridades de las pymes
- La aplicación extraeuropea del Reglamento
- Tratamiento basado en consentimiento
- El derecho al olvido
- Libertad de expresión e información

3. Análisis del articulado

- Disposiciones generales
- Principios
- Derechos del interesado
- Responsable y encargado del tratamiento
- Transferencia de datos a terceros países
- Autoridades de control independientes
- Cooperación y coherencia
- Recursos, responsabilidad y sanciones
- Situaciones específicas de tratamiento
- Actos delegados y actos de ejecución

4. Principales novedades y periodo transitorio

- Decálogo de medidas que se deben adoptar
- Deber de información
- Derechos
- Delegado de Protección de Datos
- Revisión del consentimiento
- Revisión de la base del tratamiento de derechos
- Responsabilidad proactiva
- Certificaciones
- Medidas y violaciones de seguridad
- Contratos y funciones de encargado de tratamiento
- Transferencias de datos transfronterizos
- Recomendaciones de la Agencia

5. Consideraciones finales

- Homogeneidad a nivel europeo
- Disminución de la burocracia
- Seguridad jurídica
- Vías de reacción frente a infracciones
- Elementos para avanzar y construir

Key Solution

GRACIAS POR SU ATENCIÓN

NOVIEMBRE 2018